

A PAC-Bayesian Framework for Optimal Control with Stability Guarantees

Mahrokh Ghoddousi Boroujeni,¹ Clara Lucía Galimberti,¹ Andreas Krause,² and Giancarlo Ferrari-Trecate¹

Abstract—Stochastic Nonlinear Optimal Control (SNOC) involves minimizing a cost function that averages out the random uncertainties affecting the dynamics of nonlinear systems. For tractability reasons, this problem is typically addressed by minimizing an empirical cost, which represents the average cost across a finite dataset of sampled disturbances. However, this approach raises the challenge of quantifying the control performance against out-of-sample uncertainties. Particularly, in scenarios where the training dataset is small, SNOC policies are prone to overfitting, resulting in significant discrepancies between the empirical cost and the true cost, i.e., the average SNOC cost incurred during control deployment. Therefore, establishing generalization bounds on the true cost is crucial for ensuring reliability in real-world applications. In this paper, we introduce a novel approach that leverages PAC-Bayes theory to provide rigorous generalization bounds for SNOC. Based on these bounds, we propose a new method for designing optimal controllers, offering a principled way to incorporate prior knowledge into the synthesis process, which aids in improving the control policy and mitigating overfitting. Furthermore, by leveraging recent parametrizations of stabilizing controllers for nonlinear systems, our framework inherently ensures closed-loop stability. The effectiveness of our proposed method in incorporating prior knowledge and combating overfitting is shown by designing neural network controllers for tasks in cooperative robotics.

I. INTRODUCTION

Stochastic Nonlinear Optimal Control (SNOC) involves minimizing a cost function that averages out stochastic uncertainties affecting the nonlinear system dynamics, such as process noise and disturbances. Beyond the Linear Quadratic Gaussian scenario, this problem is often intractable and is typically replaced by minimizing the average cost across a dataset of sampled uncertainties, namely, the empirical cost. However, this approximation method leads to the challenge of determining generalization bounds, i.e., to upper-bound the true (uncomputable) cost using its (computable) empirical version. A remarkably similar problem has been thoroughly explored in Machine Learning within the scope of Probably Approximately Correct (PAC)-Bayesian learning [1]. Here, the generalization error of predictors drawn from an arbitrary posterior distribution is upper-bounded with a high probability, either in expectation or for a single draw. This upper bound comprises the empirical cost and a discrepancy measure between the posterior and a prior distribution.

However, PAC-Bayesian bounds have never been exploited for the analysis of SNOC problems, with the exception of [2], where it was employed in a different context, focusing on zero-shot generalization to new environments. Related contributions utilize PAC-Bayes for learning control policies in Markov Decision Processes [3], [4]. However, these approaches assume finite action or state spaces, which might not be well-suited for SNOC. One reason for the limited application of classic PAC-Bayesian bounds in control is that they require the use of aggregated predictors, resulting from weighted averaging of all predictors according to the posterior distribution. In the SNOC context, such aggregation would require integrating actions from all possible controllers according to the posterior, a computationally challenging and impractical approach. Instead, we adopt a less commonly employed variant of PAC-Bayes bounds that apply to randomized predictors [1], which are single predictors drawn from the posterior. This allows us to establish a generalization bound when deploying a *single controller* sampled from the posterior, which is more practical. The proposed PAC-Bayesian bound provides an alternative to existing methods for validating certificates of learned controllers, such as those based on mixed-integer programs or satisfiability-modulo-theory certificates [5], [6].

PAC-Bayesian bounds apply to control policies that are derived from the posterior distribution, either through integration or sampling. Ensuring stability when deploying the resulting controller is crucial in control systems. This requires that the posterior distribution assigns a non-zero weight only to controllers that stabilize the closed-loop system.

Recently, there has been a significant advancement on using neural networks in control loops [7]–[12] or for providing stability certificates [13], [14]. In particular, [7]–[9] allow using broad families of nonlinear controllers (e.g., based on neural networks) for guaranteeing closed-loop stability while enabling the optimization of very general cost functions. The flexibility in selecting the cost function allows for promoting a broad spectrum of closed-loop specifications, ranging from safety to minimizing the L_2 -gain, among others. In this work, we exploit [7], which proposes an unconstrained parametrization of all and only stabilizing controllers for a given system. The controller implementation leverages Deep Neural Networks (DNNs) from [15] which are flexible architectures capable of achieving complex tasks. Since [7] guarantees closed-loop stability for any parameter choice, every posterior distribution over the induced space of parameters will exclusively assign non-zero probability to stabilizing controllers.

¹ Institute of Mechanical Engineering, EPFL, Switzerland. {mahrokh.ghoddousiboroujeni, clara.galimberti, giancarlo.ferraritrecate}@epfl.ch.

² Department of Computer Science, ETH Zürich, Switzerland. krausea@ethz.ch.

Research supported by the Swiss National Science Foundation under the NCCR Automation (grant agreement 51NF40.80545).

A. Contributions

We develop a novel framework for establishing a generalization bound for SNOC cost based on randomized bounds in PAC-Bayes theory, a class of bounds not previously exploited in control design. Based on the derived bound, we provide a new control policy design algorithm, which involves sampling the controller from an inferred posterior distribution. We leverage [7] to define this posterior distribution only over stabilizing controllers for a given system, enabling the deployment of our probabilistic algorithm while ensuring stability by design. To our knowledge, this is the first PAC-Bayesian control design algorithm with stability guarantees. Finally, we employ Stein Variational Gradient Descent (SVGD) [16] to make sampling the controller from the posterior numerically tractable. We demonstrate the feasibility of our method through two examples. First, we showcase how our approach can incorporate prior coarse knowledge into control design using a toy example. Then, we demonstrate the potential of our approach in a cooperative robotic task.

B. Notation

\mathbb{N}_0 denotes $\mathbb{N} \cup \{0\}$. \mathbb{R}^+ (\mathbb{R}_0^+) stands for positive (non-negative) real numbers. We denote the truncated sequence (x_0, x_1, \dots, x_t) as $x_{t:0}$, where $x_\tau \in \mathbb{R}^n$ for all $\tau = 0, \dots, t$. In the limit, as $t \rightarrow \infty$, this sequence is denoted as $x_{\infty:0} := (x_0, x_1, \dots)$. The set of all sequences $x_{\infty:0}$ is denoted as ℓ^n . Moreover, $x_{\infty:0}$ belongs to $\ell_p^n \subset \ell^n$ for $p \in \mathbb{N} \cup \{+\infty\}$, if $\|x_{\infty:0}\|_p = (\sum_{\tau=0}^{\infty} |x_\tau|^p)^{1/p} < +\infty$ for $p \in \mathbb{N}$, and $\sup_\tau |x_\tau| < +\infty$, for $p = \infty$, where $|\cdot|$ denotes the Euclidean norm. We represent causal operators over sequences with $A_{\infty:0} : \ell^n \rightarrow \ell^{n'}$, defined as $A_{\infty:0}(x_{\infty:0}) = (A_0(x_0), A_1(x_{1:0}), \dots, A_t(x_{t:0}), \dots)$. Every instance $A_t(x_{t:0})$, for a fixed $t \in \mathbb{N}_0$, is a function in $\mathbb{R}^{n \times (t+1)} \rightarrow \mathbb{R}^{n'}$. The operator $A_{\infty:0}$ is said to be ℓ_p -stable if $A_{\infty:0}(x_{\infty:0}) \in \ell_p^{n'}$ for all $x_{\infty:0} \in \ell_p^n$. Similar to sequences, we define truncated operators as $A_{t:0}(x_{t:0}) = (A_0(x_0), A_1(x_{1:0}), \dots, A_t(x_{t:0}))$. Finally, the zero vector in \mathbb{R}^n is denoted as 0_n .

II. STOCHASTIC NONLINEAR OPTIMAL CONTROL

We consider nonlinear discrete-time time-varying systems described by the equation:

$$x_0 = \bar{x} + w_0, \quad (1a)$$

$$x_t = f_t(x_{t-1:0}, u_{t-1:0}) + w_t, \quad t = 1, 2, \dots, \quad (1b)$$

where $\bar{x} \in \mathbb{X} \subset \mathbb{R}^n$ denotes the nominal initial state, $x_t \in \mathbb{X} \subset \mathbb{R}^n$ represents the state vector, $u_t \in \mathbb{U} \subset \mathbb{R}^m$ denotes the control input, and $w_t \in \mathbb{W} \subset \mathbb{R}^n$ stands for unknown process noise. The uncertainty on x_0 is modeled through w_0 . The noise follows a potentially unknown distribution, $w_t \sim \mathcal{D}_t$. We assume the nominal initial state, \bar{x} , and the system dynamics, f_t , are known. To control the system (1), we employ a time-varying dynamical feedback controller parameterized by $\theta \in \Theta \subset \mathbb{R}^d$, given by:

$$u_t = -K_t^\theta(x_{t:0}), \quad t = 0, 1, \dots \quad (2)$$

Given a system, a controller parameterized by θ , and a sequence of noise samples, $w_{t:0}$, the closed-loop system (1)-(2) yields unique state and input trajectories, $(x_{t:0}, u_{t:0}) = r_{t:0}^\theta(w_{t:0})$. The deterministic mapping $r_{t:0}^\theta : \mathbb{W}^{t+1} \rightarrow (\mathbb{X} \times \mathbb{U})^{t+1}$, is referred as the *rollout map*, where its components are $r_t^\theta : w_{t:0} \mapsto (x_t, u_t)$. For notation simplicity, we omit the dependence of $r_{t:0}^\theta$ on the nominal initial state, \bar{x} , and the system dynamics, f_t . Moreover, when clear from the context, we will drop the subscript and write r^θ . In this work, we assume that system (1) is ℓ_p -stable or has been already prestabilized, i.e., the map $(w_{\infty:0}, u_{\infty:0}) \rightarrow x_{\infty:0}$ is ℓ_p -stable. As in [7], the closed-loop system (1)-(2) is called ℓ_p -stable if the rollout map, $r_{\infty:0}^\theta$, is ℓ_p -stable.

We consider the following SNOC problem over a finite horizon of $T \in \mathbb{N}$:

$$\text{SNOC : } \min_{\theta \in \Theta} \mathcal{L}(\theta, \mathcal{D}_{T:0}), \quad (3a)$$

$$\text{s.t. } (x_t, u_t) = r_t^\theta(w_{t:0}), \quad t = 0, \dots, T, \quad (3b)$$

$$r_{\infty:0}^\theta \text{ is } \ell_p\text{-stable}, \quad (3c)$$

where,

$$\mathcal{L}(\theta, \mathcal{D}_{T:0}) := \mathbb{E}_{w_{T:0} \sim \mathcal{D}_{T:0}} L(\theta, w_{T:0}), \quad (4)$$

$$L(\theta, w_{T:0}) := \frac{1}{T} \sum_{t=0}^T l(x_t, u_t). \quad (5)$$

The objective is to synthesize a controller parameterized by θ that minimizes the cost \mathcal{L} while adhering to the closed-loop dynamics and stability constraints imposed by (3b) and (3c), respectively. In (5), $l : \mathbb{X} \times \mathbb{U} \rightarrow \mathbb{R}_0^+$ denotes a stage cost function, which we assume to be piecewise differentiable and nonnegative for all $(x, u) \in \mathbb{X} \times \mathbb{U}$. Given θ and $w_{T:0}$, L defined in (5) averages the stage cost over the horizon T , referred to as the *finite-horizon (FH) cost*. The cost \mathcal{L} in (4), dubbed the *true cost*, represents the expectation of the FH cost for any realization of noise sampled from $\mathcal{D}_{T:0} := (\mathcal{D}_0, \dots, \mathcal{D}_T)$. By averaging out the random noise affecting the dynamics, the true cost, \mathcal{L} , provides a suitable criterion for optimizing the controller parameters, as in (3).

Computing the true cost is often prohibitive due to involving an expectation calculation or is infeasible due to unknown noise distributions, $\mathcal{D}_{T:0}$. Instead, SNOC methods typically resort to optimizing the *empirical cost* based on observed data, $\mathbb{S} := \{w_{T:0}^i\}_{i=1}^s$, consisting of $s \in \mathbb{N}$ noise sequences of length $T+1$ drawn from $\mathcal{D}_{T:0}$, indicated as $\mathbb{S} \sim \mathcal{D}_{T:0}^s$. The empirical cost is defined as:

$$\hat{\mathcal{L}}(\theta, \mathbb{S}) := \frac{1}{s} \sum_{i=1}^s L(\theta, w_{T:0}^i), \quad (6)$$

averaging the FH cost of noise sequences in \mathbb{S} . Unlike $\mathcal{L}(\theta, \mathcal{D}_{T:0})$, the empirical cost can be computed and optimized to obtain the controller parameters. The resulting controller is referred to as the *empirical controller*. However, the empirical controller may exhibit significantly worse performance when confronted with out-of-sample noise sequences than those in the training set \mathbb{S} , a phenomenon corresponding

to overfitting in supervised learning. To rigorously certify the performance of \mathcal{L} , we aim to upper-bound it using its empirical estimate, $\hat{\mathcal{L}}$, employing the PAC-Bayes framework, briefly introduced in the next section. In Section IV, we delve into considerations about closed-loop stability.

III. GENERALIZATION BOUNDS

In this section, we establish a generalization bound on the true cost and use it for proposing a control design algorithm.

A. PAC-Bayes generalization bound

We leverage the PAC-Bayes framework that applies to learning algorithms that incorporate a prior distribution \mathcal{P} with the observed data \mathbb{S} to derive a posterior distribution \mathcal{Q} . Importantly, \mathcal{P} and \mathcal{Q} are not necessarily linked through Bayes' law. In the context of learning controllers, both \mathcal{P} and \mathcal{Q} are defined over the controller parameters, θ . In this study, we utilize PAC-Bayes bounds that necessitate the prior distribution to be chosen independently from the data and yield bounds for individual samples from the posterior.

We make the following assumption which facilitates deriving PAC-Bayesian bounds.

Assumption 1: The FH cost is upper-bounded by $C \in \mathbb{R}^+$, i.e., $L(\theta, w_{T:0}) \in [0, C)$, for all $\theta \in \Theta$ and $w_{T:0} \in \mathbb{W}^{T+1}$.

Assumption 1 may not apply to a wide range of SNOC problems. For instance, even a simple quadratic stage cost can lead to an unbounded L if the closed-loop system is unstable. Therefore, we propose to map any unbounded cost function to $[0, C)$ by applying the following transformation:

$$\tilde{L}(x_{T:0}, u_{T:0}) := C \tanh(L(x_{T:0}, u_{T:0})/\gamma), \quad (7)$$

where \tanh represents the hyperbolic tangent function and $\gamma \in \mathbb{R}^+$ is a suitable constant. The transformed cost grows almost linearly with the original cost between 0 and γ , and then smoothly saturates at the maximum value of C . In general, we expect that the stage cost, l , decreases over time. Therefore, the cost at the initial nominal state, $l(\bar{x}, 0_m)$, is a reasonable selection for γ . This choice retains the transformed cost predominantly within the linear region rather than in the saturation region. In the sequel, we apply (7) to any unbounded FH cost (5) used in the SNOC problem (3), whenever necessary.

Next, we present our PAC-Bayes bound on the true cost, \mathcal{L} .

Theorem 1 (Adapted from Theorem 2.7 in [1]):

Consider the noise distribution $\mathcal{D}_{T:0}$, a dataset $\mathbb{S} \sim \mathcal{D}_{T:0}^s$, a prior distribution \mathcal{P} independent of \mathbb{S} , and the FH cost L . Under Assumption 1, for every $\lambda > 0$, confidence level $\delta \in (0, 1)$, posterior distribution \mathcal{Q} , and controller parameters $\theta \sim \mathcal{Q}$, the inequality,

$$\mathcal{L}(\theta, \mathcal{D}_{T:0}) \leq \hat{\mathcal{L}}(\theta, \mathbb{S}) + \frac{1}{\lambda} \left(\ln \frac{d\mathcal{Q}}{d\mathcal{P}}(\theta) + \ln \frac{1}{\delta} \right) + \frac{\lambda C^2}{8s}, \quad (8)$$

holds with probability at least $1 - \delta$ over simultaneously sampling $\mathbb{S} \sim \mathcal{D}_{T:0}^s$ and $\theta \sim \mathcal{Q}$. The true and empirical costs, \mathcal{L} and $\hat{\mathcal{L}}$, are defined in (4) and (6) respectively.

Theorem 1 provides an upper bound on the true cost of any θ sampled from \mathcal{Q} based on its empirical cost, a discrepancy

TABLE I
CORRESPONDENCE BETWEEN SUPERVISED LEARNING AND SNOC

Supervised Learning		SNOC	
Sample	$(x, y) \in \mathbb{X} \times \mathbb{Y}$	Noise sequence	$w_{T:0} \in \mathbb{W}^{T+1}$
Predictor	$h^\theta : \mathbb{X} \rightarrow \mathbb{Y}$	Rollout	$r^\theta : \mathbb{W}^{T+1} \rightarrow (\mathbb{X} \times \mathbb{U})^{T+1}$
Loss	$l(\theta, x, y)$	FH cost	$L(\theta, w_{T:0})$

measure between the posterior and prior at θ , and a term that is constant with respect to θ . Theorem 1 and its proof are derived by adapting Theorem 2.7 from [1], originally formulated for supervised learning, to the SNOC framework. This adaptation involves establishing a correspondence between elements in supervised learning and elements in our problem, as summarized in Table I. While supervised learning deals with data samples comprising features and labels, in our context, we work with noise sequences. In supervised learning, a predictor, h^θ , maps features to a label, whereas in SNOC, the rollout map, r^θ , generates closed-loop state and input sequences. Moreover, in supervised learning, a loss function evaluates a predictor at a given sample point, while in SNOC, we use the FH cost to evaluate trajectories generated by the rollout map. By recognizing and aligning these correspondences, we can effectively apply PAC-Bayes bounds from supervised learning to the SNOC domain.

The majority of PAC-Bayes bounds in supervised learning focus on *aggregated predictors*, which combine the output of all possible predictors according to the posterior distribution, $\mathbb{E}_{\theta \sim \mathcal{Q}} h^\theta(\cdot)$ [1]. Consequently, these bounds involve the average of true and empirical losses with respect to sampling predictors from the posterior, denoted as $\mathbb{E}_{\theta \sim \mathcal{Q}} \mathcal{L}(\theta, \cdot)$ and $\mathbb{E}_{\theta \sim \mathcal{Q}} \hat{\mathcal{L}}(\theta, \cdot)$, respectively (see, for instance, [17]). Adapting PAC-Bayes bounds for aggregated predictors to SNOC leads to obtaining bounds in which the control action is obtained by combining actions from all possible controllers sampled from the posterior, i.e., $u_t = -\mathbb{E}_{\theta \sim \mathcal{Q}} K_t^\theta(x_{t:0})$. However, such averaging is generally impractical in control systems, where using a unique controller to obtain u_t is preferred. Moreover, computing the expectation can be computationally prohibitive. Therefore, Theorem 1 is derived by adapting a less commonly used family of PAC-Bayes bounds in supervised learning that considers randomized predictors, which obtain the output using a single predictor drawn from the posterior distribution. Consequently, Theorem 1 aligns well with the standard setup in control systems as it holds for a fixed sample of the controller parameters from the posterior, $\theta \sim \mathcal{Q}$.

B. Optimal posterior

While the prior and posterior terms in Theorem 1 resemble Bayesian terminology, the posterior distribution, \mathcal{Q} , is not necessarily obtained through Bayes' theorem. The flexibility in choosing \mathcal{Q} can be exploited to achieve desired characteristics. In particular, for a given θ sampled from \mathcal{Q} , it is desirable that \mathcal{Q} is selected to minimize the upper bound on \mathcal{L} , which is the right-hand side of (8). However, this choice

is hampered by a circular dependency since \mathcal{Q} must be fixed before sampling θ . To overcome this issue, we propose to select \mathcal{Q} by minimizing the expected value of the upper bound over the draw of the controller parameters:

$$\begin{aligned} \mathcal{Q}^* &:= \arg \min_{\mathcal{Q}} \mathbb{E}_{\theta \sim \mathcal{Q}} \left[\hat{\mathcal{L}}(\theta, \mathbb{S}) + \frac{1}{\lambda} \left(\ln \frac{d\mathcal{Q}}{d\mathcal{P}}(\theta) + \ln \frac{1}{\delta} \right) + \frac{\lambda C^2}{8s} \right] \\ &= \arg \min_{\mathcal{Q}} \mathbb{E}_{\theta \sim \mathcal{Q}} \left[\hat{\mathcal{L}}(\theta, \mathbb{S}) + \frac{1}{\lambda} \ln \frac{d\mathcal{Q}}{d\mathcal{P}}(\theta) \right] \\ &= \arg \min_{\mathcal{Q}} \mathbb{E}_{\theta \sim \mathcal{Q}} [\hat{\mathcal{L}}(\theta, \mathbb{S})] + \frac{1}{\lambda} \text{KL}(\mathcal{Q} \parallel \mathcal{P}), \end{aligned} \quad (9)$$

where KL stands for the Kullback–Leibler divergence. This expression involves a trade-off, modulated by λ , between minimizing the expected empirical cost and enhancing the similarity of the posterior to the prior. This similarity is captured through the KL divergence term. The prior can be selected such that the similarity term promotes the integration of existing knowledge into the learning procedure or regulates the posterior complexity to avoid overfitting. Examples of such priors are provided in Section VI. In extreme cases, \mathcal{Q}^* becomes a degenerate distribution at the minimizer(s) of $\hat{\mathcal{L}}$ as $\lambda \rightarrow \infty$, and $\mathcal{Q}^* \rightarrow \mathcal{P}$ as $\lambda \rightarrow 0$. Below, we present first the closed-form solution for \mathcal{Q}^* and then an approach to select λ .

Corollary 1 (Lemma 1.1.3 in [17]): The minimizer of (9) is the *Gibbs* distribution, characterized by:

$$\mathcal{Q}^*(\theta) = \mathcal{P}(\theta) e^{-\lambda \hat{\mathcal{L}}(\theta, \mathbb{S})} / Z_\lambda(\mathcal{P}, \mathbb{S}), \quad (10)$$

$$Z_\lambda(\mathcal{P}, \mathbb{S}) := \mathbb{E}_{\theta \sim \mathcal{P}} e^{-\lambda \hat{\mathcal{L}}(\theta, \mathbb{S})}, \quad (11)$$

where $Z_\lambda(\mathcal{P}, \mathbb{S})$ normalizes the distribution \mathcal{Q}^* .

We refer to \mathcal{Q}^* as the *optimal posterior* distribution. By substituting (10) into (8), one obtains:

$$\mathcal{L}(\theta, \mathcal{D}_{T:0}) \leq \frac{1}{\lambda} \left(\ln \frac{1}{\delta} - \ln Z_\lambda(\mathcal{P}, \mathbb{S}) \right) + \frac{\lambda C^2}{8s}, \quad (12)$$

holding with probability at least $1 - \delta$ over simultaneously sampling $\mathbb{S} \sim \mathcal{D}_{T:0}^s$ and $\theta \sim \mathcal{Q}$. The term $-1/\lambda \ln Z_\lambda(\mathcal{P}, \mathbb{S})$ always falls within the range $[0, C]$ and decreases when the prior \mathcal{P} assigns higher probability to controller parameters with lower empirical costs for \mathbb{S} , as evident from (11). Therefore, the bound tightens when the prior \mathcal{P} is “more aligned” with \mathbb{S} . Recall, however, that the prior \mathcal{P} is chosen independently from \mathbb{S} . The simplified bound (12) applies when using the optimal posterior distribution, \mathcal{Q}^* , hence eliminating the explicit dependence on \mathcal{Q} , and is tighter than the generic bound in (8).

The bound (12) is more valuable when its right-hand side is smaller. This can be achieved by tuning $\lambda > 0$, which according to Theorem 1, can be freely selected. However, computing the term $-1/\lambda \ln Z_\lambda(\mathcal{P}, \mathbb{S})$ in (12) can be challenging due to its complexity. Under Assumption 1, this term is in $[0, C]$. Therefore, we replace $-1/\lambda \ln Z_\lambda(\mathcal{P}, \mathbb{S})$ with C to obtain an upper bound on (12). Below, we propose selecting λ based on this looser upper bound.

Proposition 1: The optimal $\lambda > 0$ that minimizes the upper bound on the right-hand side of (12) obtained by

replacing $-1/\lambda \ln Z_\lambda(\mathcal{P}, \mathbb{S})$ with C , is given by:

$$\lambda^* = \sqrt{8s \ln(1/\delta)} / C. \quad (13)$$

Given a prior \mathcal{P} and a dataset \mathbb{S} , (10) and (13) completely specify a posterior distribution, requiring no additional free parameters. The resulting distribution achieves a balance between fitting the data and incorporating prior knowledge.

IV. LEARNING STABILIZING CONTROLLERS

In order to guarantee closed-loop stability, we leverage the control design approach in [7]. In general, stability can be imposed in an SNOC problem (3) in two ways. The first one is to resort to constrained optimization approaches that ensure global or local stability by enforcing appropriate Lyapunov-like inequalities during optimization [10], [11], [14]. However, enforcing such constraints often becomes a computational bottleneck in complex applications. This issue has been highlighted in [5], discussing that popular stability verification methods are feasible for controllers with an order of 10^2 parameters. The second possibility is to use unconstrained optimization approaches searching within classes of control policies with built-in stability guarantees [7]–[9]. These methods allow learning controllers through optimization algorithms based on gradient descent, without imposing further constraints to ensure stability. Additionally, unconstrained approaches usually have a much lower computational burden than constrained ones. In Section V-B, we show that unconstrained approaches also enable the use of algorithms for sampling the posterior, such as SVGD. Moreover, in Section VI-B, we demonstrate the scalability of these approaches by training a stabilizing controller with more than 10^4 parameters.

In this work, we follow [7], which proposes an *unconstrained parametrization* of all and only stabilizing nonlinear control policies for a nonlinear time-varying system, as per (1), exploiting the internal model control framework [18]. This method is based on choosing a unique free operator, denoted as $\mathcal{M}_{\infty:0}$. The main result is that, assuming ℓ_p -stability of system (1), the closed-loop map is ℓ_p -stable if and only if the operator $\mathcal{M}_{\infty:0}$ is also ℓ_p -stable.¹ The control action u_t , for any $t \in \mathbb{N}_0$, can be obtained as:

$$\hat{w}_t = x_t - f_t(x_{t-1:0}, u_{t-1:0}), \quad (14a)$$

$$u_t = \mathcal{M}_t(\hat{w}_{t:0}). \quad (14b)$$

The noise is reconstructed in (14a) using the knowledge of the system dynamics, and then, u_t is calculated through (14b). Note that (14) is a dynamical feedback controller, as in (2), with input $x_{t:0}$, output u_t , and internal states $\hat{w}_{t:0}$ and $u_{t:0}$.

Implementing (14) requires parameterizing $\mathcal{M}_{\infty:0}$. This is addressed in [7] by adopting the Recurrent Equilibrium Networks (RENs) of [15], which allows representing a broad set of ℓ_2 -stable operators. Below, we briefly summarize this approach and refer the reader to [15] for a more comprehensive explanation. The resulting parametrized operator,

¹For ease of reading, we neglect the base controller in [7]; assuming that, if needed, it is already included in the system dynamics f_t .

$\mathcal{M}_{\infty;0}^\theta$, is a dynamical system, given by:

$$\begin{bmatrix} \xi_{t+1} \\ \zeta_t \\ u_t \end{bmatrix} = \Omega(\theta) \begin{bmatrix} \xi_t \\ \sigma(\zeta_t) \\ \hat{w}_t \end{bmatrix}, \quad \xi_0 = 0_{n_\xi}, \quad (15)$$

where $\xi_t \in \mathbb{R}^{n_\xi}$ is the internal state and $\zeta_t \in \mathbb{R}^{n_\zeta}$ is an internal variable. Recall that θ , \hat{w}_t , and u_t are the parameters, inputs, and outputs, respectively. The activation function $\sigma : \mathbb{R} \rightarrow \mathbb{R}$ is applied element-wise and it must be piece-wise differentiable with first derivatives restricted to the interval $[0, 1]$. The mapping $\Omega : \mathbb{R}^d \rightarrow \mathbb{R}^{(n_\xi+n_\zeta+m) \times (n_\xi+n_\zeta+n)}$ ensures that ζ_t has a unique value for every $t \in \mathbb{N}_0$, and that (15) is an ℓ_2 -stable operator for every $\theta \in \mathbb{R}^d$, i.e., one has $\Theta = \mathbb{R}^d$. We also highlight that RENs can embed arbitrarily deep NNs by suitably selecting the structure of the matrix $\Omega(\theta)$ [15]. Overall, (14a)-(15) specify a DNN-based controller which ensures closed-loop stability for any choice of parameters $\theta \in \mathbb{R}^d$.

V. PRACTICAL IMPLEMENTATION

A. Estimating the upper bound

In (12), we have derived an upper bound on the true cost when employing the optimal posterior. However, explicitly computing this upper bound is generally challenging due to the involvement of the Z_λ term, as given by (11), which requires integrating over the controller parameters sampled from the prior. Consequently, we resort to bounding this term by its empirical counterpart.

Proposition 2: Consider the setup of Theorem 1 when using the optimal posterior, Q^* , given by (10). Let $\theta_1, \dots, \theta_{n_p}$ be n_p independent samples from the prior, \mathcal{P} . For every confidence level $\hat{\delta} \in (0, 1)$ and any $n_p \geq (e^{\lambda C} - 1)^2 \ln(1/\hat{\delta})/2$, the inequality,

$$\begin{aligned} \mathcal{L}(\theta, \mathcal{D}_{T;0}) &\leq \frac{1}{\lambda} \ln \frac{1}{\delta} + \frac{\lambda C^2}{8s} \\ &\quad - \frac{1}{\lambda} \ln \left(\frac{1}{n_p} \sum_{i=0}^{n_p} e^{-\lambda \hat{\mathcal{L}}(\theta_i, \mathbb{S})} - (1 - e^{-\lambda C}) \sqrt{\frac{\ln(1/\hat{\delta})}{2n_p}} \right), \end{aligned}$$

holds with probability at least $(1 - \delta)(1 - \hat{\delta})$ over simultaneously sampling $\mathbb{S} \sim \mathcal{D}_{T;0}^s$, $\theta \sim Q$, and $\theta_1, \dots, \theta_{n_p} \sim \mathcal{P}^{n_p}$.

Proof: Under Assumption 1, $e^{-\lambda \hat{\mathcal{L}}(\theta, \mathbb{S})} \in [e^{-\lambda C}, 1]$ for any θ . This allows applying Hoeffding's inequality [19] to lower-bound Z_λ :

$$Z_\lambda(\mathcal{P}, \mathbb{S}) \geq \frac{1}{n_p} \sum_{i=0}^{n_p} e^{-\lambda \hat{\mathcal{L}}(\theta_i, \mathbb{S})} - (1 - e^{-\lambda C}) \sqrt{\frac{\ln(1/\hat{\delta})}{2n_p}}, \quad (16)$$

holding with probability at least $(1 - \hat{\delta})$ over simultaneously sampling $\theta_1, \dots, \theta_{n_p} \sim \mathcal{P}^{n_p}$. Since $n_p \geq (e^{\lambda C} - 1)^2 \ln(1/\hat{\delta})/2$, the right-hand side of (16) is positive, enabling us to substitute (16) into (12). Since θ , \mathbb{S} , and $\theta_1, \dots, \theta_{n_p}$ are independent random variables, the probability that both inequalities (12) and (16) hold simultaneously is the multiplication of the probability that each inequality holds individually, i.e., $(1 - \delta)(1 - \hat{\delta})$. ■

Proposition 2 leverages sampled controllers from the prior. For common prior distributions with known cumulative density functions, sampling from the prior is straightforward. Hence, the estimated bound can be easily computed. Although the resulting bound is less tight than the original one in (12), the additional conservatism diminishes as n_p grows.

B. Sampling from the posterior

The optimal posterior distribution, Q^* , can be computed according to (10) up to the normalization constant $Z_\lambda(\mathcal{P}, \mathbb{S})$, as discussed in Section V-A. Direct sampling from such distributions that do not integrate to unity, called improper distributions, is challenging in general. Although one could use Markov chain Monte Carlo methods for sampling from an improper distribution, this approach tends to be computationally slow, especially for large datasets [20]. Instead, we employ a Variational Bayes method, as proposed in [21], which allows approximating Q^* by a tractable distribution and then sampling from this approximated distribution. Specifically, we use Stein Variational Gradient Descent (SVGD) [16] which approximates Q^* using a set of $k \in \mathbb{N}$ particles, denoted as $\{\phi_1, \dots, \phi_k\}$. In our context, each particle ϕ_κ for $\kappa = 1, \dots, k$ corresponds to the parameters of a controller, i.e., $\phi_\kappa \in \Theta$. SVGD initializes these particles by sampling them from the prior and then iteratively updates them aiming that their density in the parameter space Θ matches the probability mass of Q^* . SVGD relies on gradient descent for updating the particles, rendering it well-suited for integration with the unconstrained parametrization outlined in Section IV. After training, Q^* is approximated as a uniform distribution over the trained particles. Hence, sampling from the approximated distribution corresponds to randomly selecting one of the particles with equal probability. The application of SVGD to approximate Gibbs distributions arising in PAC-Bayesian methods has been found useful in previous work, such as [22], [23]. For more details and the precise implementation of SVGD, we refer to [16].

VI. EXPERIMENTS

We conduct experiments using two systems: *i*) a simple Linear Time-Invariant (LTI) system, and *ii*) a system of two planar robots navigating to prespecified locations while avoiding collisions. To train our algorithm and compute the upper bound, we utilize Q^* and λ^* as per (10), and (13) and apply the transformation (7) with $C = 1$. We compare our algorithm against the empirical controller. To maintain the standard setting, the empirical controller is trained without applying the transformation (7). The code to reproduce our experiments can be found at <https://www.github.com/DecodEPFL/PAC-SNOC>.

A. LTI system

Setup: We use a scalar stable LTI system, given by:

$$\begin{aligned} x_0 &= \bar{x} + w_0, \\ x_t &= ax_{t-1} + bu_{t-1} + w_t, \quad t = 1, 2, \dots, \end{aligned}$$

with $a = 0.8$, $b = 0.1$, and $\bar{x} = 2$. This simple setup will allow us to thoroughly illustrate our control design method and the derived PAC bounds. At each time step, the noise w_t is drawn from a Gaussian distribution with mean $\mu_w = 0.3$ and variance $\sigma_w^2 = 0.09$, i.e., $w_t \sim \mathcal{N}(0.3, 0.09)$. We assume the noise distribution is unknown. Instead, we possess a dataset of s noise sequences over a horizon of $T = 10$, and we vary s to analyze its impact.

The stage cost function is quadratic and defined as $l_{LQ}(x_t, u_t) = 5x_t^2 + 0.003u_t^2$. We utilize the affine state feedback controller $u_t = -(kx_t + \beta)$, where k and β represent the controller gain and bias. We set $\theta = [k, \beta]^\top$. Ensuring closed-loop stability for this system corresponds to imposing $k \in (-2, 18)$. This constraint can be readily enforced during optimization by projecting the gain, k , into this set during training, obviating the need for complex techniques to guarantee stability, such as (14).

Baselines: Our methodology is compared against two alternative approaches. First, an *empirical* controller obtained by minimizing $\hat{\mathcal{L}}(\theta, \mathbb{S})$ defined in (6). Second, a *benchmark* (ideal) controller that assumes precise knowledge of the noise mean value, which allows setting $\beta = \mu_w/b$. The benchmark controller's gain, k , is optimized by minimizing the empirical cost over a large dataset comprising 1024 noise sequences. While the benchmark controller demonstrates strong performance, its practicality is limited by its dependence on a substantial amount of data and accurate knowledge of μ_w . Nevertheless, it is involved in this experiment as the best-performing competitor.

Prior distribution: The prior distribution for $\theta = [k, \beta]^\top$ must be chosen independently from the data, \mathbb{S} . We opt for a prior that is independent for k and β . Specifically, the prior for k is a Gaussian distribution centered at the infinite horizon LQR (IH-LQR) gain—which can be obtained using the stage cost l_{LQ} —and with a variance of 1.0. Although the IH-LQR may not be optimal for our scenario with a finite horizon of $T = 10$, it is a reasonable data-independent choice. The choice of the prior distribution for β can incorporate known information about the expected value of the noise, μ_w . We explore two scenarios: In the first case, we assume to only know that μ_w lies in the interval $[-0.5, 0.5]$ and we set the prior for β as the uniform distribution over $[-0.5/b, 0.5/b]$, i.e., $\mathcal{U}(-5, 5)$. In the second case, μ_w is known with some uncertainty, and we set the prior distribution for β as a Gaussian distribution with a mean of $\mu_w/b = 3$ and a variance of 1.5^2 . These prior distributions are called \mathcal{P}_U and \mathcal{P}_N , respectively.

Optimal posterior distribution: As both \mathcal{P} and \mathcal{Q}^* are bivariate distributions, we approximate their Probability Density Function (PDF) by discretizing a region encompassing over 95% of the probability mass. In Figure 1, we depict the discretized \mathcal{P} (left column) and \mathcal{Q}^* when using $s = 8$ (middle column) and $s = 512$ (right column), and setting $\delta = 0.2$. The top and bottom rows correspond to \mathcal{P}_U and \mathcal{P}_N , respectively, and the color represents the approximated PDF. Additionally, the empirical and benchmark controllers are marked on the plots.

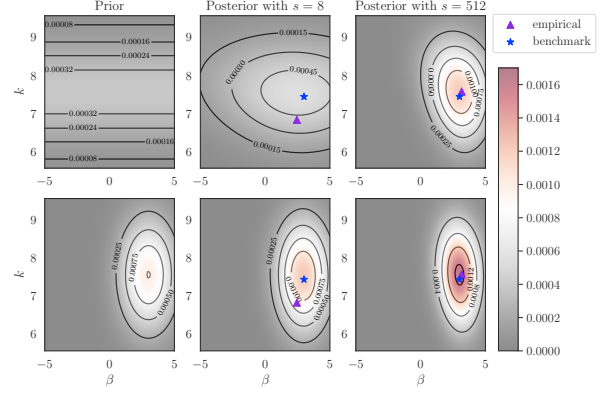


Fig. 1. Discretized PDF for the prior distributions (left) and the optimal posterior distributions with $s = 8$ (middle) and $s = 512$ (right). The top and bottom rows correspond to \mathcal{P}_U and \mathcal{P}_N , respectively. Horizontal and vertical axes in each plot represent β and k , while color indicates the PDF. The empirical and benchmark controllers are marked.

For $s = 8$, both posterior distributions associated with \mathcal{P}_U and \mathcal{P}_N are concentrated near the benchmark controller, whereas the empirical controller is positioned further away. This observation suggests that controllers sampled from the posterior are likely to more closely resemble the benchmark controller, potentially resulting in better out-of-sample performance than the empirical controller. As the number of data sequences increases to $s = 512$, both posterior distributions become more tightly concentrated around the benchmark controller. As expected, the empirical distribution also improves, getting closer to the benchmark. Comparing the rows of Figure 1 reveals that the more informative prior \mathcal{P}_N (second row), which reflects additional knowledge about μ_w , yields a sharper posterior distribution. This observation suggests that our algorithm effectively integrates existing knowledge into the control design algorithm.

Validity and tightness of the bound for \mathcal{Q}^* and λ^* : A desirable upper bound ensures that the true cost of sampled controllers is below the upper bound in at least $1 - \delta$ cases while avoiding being overly loose. Below, we assess the quality of our bound (12). We calculate the term Z_λ on the right-hand side using the discretized prior distributions illustrated in Figure 1. For the left-hand side, that is the true cost of a sampled θ , direct computation is intractable. Hence, we approximate it for each sampled θ by evaluating the empirical cost using a large dataset of 1024 noise sequences, each of length $T+1=11$, sampled independently from $\mathcal{N}(\mu_w, \sigma_w^2)$ ¹¹. This approximation's accuracy is justified by the law of large numbers. We investigate the influence of the training dataset size (s), the prior distribution (\mathcal{P}), and the confidence level (δ) on both the upper bound and the true cost. We recalculate \mathcal{Q}^* and λ^* and sample θ from the resulting posterior distribution for each scenario.

Figure 2 illustrates the true cost, \mathcal{L} , and the upper bound as per (12) on the vertical axis for various configurations. The colors correspond to different choices for δ and the prior distribution, while the size of the training set, s , is

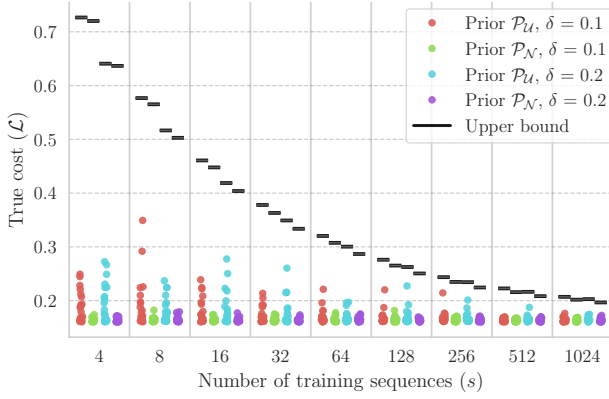


Fig. 2. Comparison of the true cost, \mathcal{L} , and the upper bound (12) for various configurations as a function of s . Colors denote δ and prior distribution choices. The true cost in each setup is approximated for 10 vectors θ sampled from \mathcal{Q}^* , shown as vertically aligned circles.

indicated on the x -axis. For each configuration, the true cost is estimated for 10 different θ vectors sampled from \mathcal{Q}^* through exhaustive test data sampling. The true costs of these sampled points are represented by circles aligned on the same vertical line. Note that the upper bound and the true cost in this figure are calculated after the transformation (7) has been applied to the FH cost to upper-bound it to $C = 1$. Therefore, all values on the vertical axis are less than 1.

In Figure 2, we observe that the true cost consistently remains below the calculated upper bounds, indicating that they are all valid. When δ and s are fixed, the upper bound corresponding to \mathcal{P}_N is tighter than that for \mathcal{P}_U . This observation aligns with our discussion in Section III-B that a more informative prior tightens the upper bound. Conversely, with a fixed prior and a fixed s , increasing δ leads to a tighter upper bound, as it allows a higher probability of violating the bound. Moreover, as s increases, the upper bound uniformly tightens. A theoretical analysis of the impact of s on the upper bound will be developed in future research.

B. Navigating planar robots

Setup: We consider two point-mass robots moving in the Cartesian plane whose goal is to coordinately pass through a narrow valley and reach a target position while avoiding obstacles and collisions between them—see Figure 3. Each robot is modeled as a double integrator subject to nonlinear drag forces. The overall system state is denoted with $x \in \mathbb{R}^8$ and consists of the positions and velocities of the robots in the Cartesian coordinates. The inputs are the forces over the robots in each direction, represented by $u \in \mathbb{R}^4$. Each robot is prestabilized by a simple proportional controller that takes it to the desired end position, possibly resulting in collisions and poor performance. The system dynamics is subject to noise w_t as in (1). We consider that the noise only affects the initial condition, i.e., $w_t = 0$ for $t > 0$. Additionally, w_0 is drawn from a zero-mean Gaussian distribution with variance $\sigma_w^2 = 0.2^2$, which we assume to be unknown. The dataset consists of $s = 30$ noise sequences

over a horizon of $T = 100$, where only the first elements are nonzero.

The stage cost is the sum of a quadratic function plus collision and obstacle avoidance regularizations, defined as:

$$l(x_t, u_t) = (\Delta x_t)^\top Q(\Delta x_t) + u_t^\top R u_t + l_{ca}(d_t) + l_{oa}(x_t),$$

where $\Delta x_t = x_t - x_{\text{target}}$, x_{target} is the desired state with the target positions and zero velocities, and $d_t \in \mathbb{R}_0^+$ is the distance between the robots at time t . The collision avoidance term is zero if the robots are further than a safe distance $D > 0$. If $d_t < D$, one has $l_{ca}(d_t) = (d_t + \nu)^{-2}$, where $\nu > 0$ is a small positive constant. The obstacle avoidance term, l_{oa} , is a function of the distance between the robots and each obstacle. This experiment is taken from [7], where the model and the stage cost function are further detailed.

Controller design: The controller is given by (14) and (15), ensuring that the closed-loop system remains stable as discussed in Section IV. We set $n_\xi = 8$ and $n_\zeta = 8$, which leads to $d = 864$ parameters in total. This controller architecture is trained once using the empirical approach which minimizes $\hat{\mathcal{L}}(\theta, \mathbb{S})$, and once using our approach. In our method, we set $\delta = 0.1$ to ensure the bound (12) holds with a probability of at least 0.9. Additionally, we utilize a zero-mean spherical Gaussian prior with variance 7^2 , which imposes an L_2 -regularization on the parameters θ of the REN (15). This choice is motivated by the fact that L_2 -regularization of DNN weights helps mitigate overfitting in supervised learning. The variance of the prior is fine-tuned through cross-validation.

Results: Similar to the previous example, we approximate the controllers' true cost using a large test dataset of 500 new noise trajectories. To have a fair comparison, the test cost is calculated without transformation (7). Table II compares the cost and percentage of trajectories in which the robots collide, for the training and test datasets. The empirical controller results in a marginally lower cost within the training dataset, whereas our approach exhibits superior performance in the test dataset. Both controllers avoid collisions in the training data but result in some collisions in the test data. This is because collision avoidance is only promoted through the stage cost function but not formally ensured. Nevertheless, our method results in fewer collisions in the test data. These observations highlight that the empirical controller tends to overfit the training samples, while our controller generalizes better to out-of-sample data. Training the empirical controller and our controller took 212 and 129 minutes, respectively, using an AMD Ryzen Threadripper 3990X 64-Core Processor.

In Figure 3, each plot illustrates three trajectories starting from three initial conditions outside the training dataset in three cases: (a) for the prestabilized system without an external controller, (b)-(c) using the empirical controller, and (d)-(f) employing the controller obtained by our approach. The utilized controllers for generating these plots are the same as those evaluated in Table II. All trajectories are computed until $t = 400$ to illustrate that stability is preserved. As observed in the plot (a), the prestabilizing controller

TABLE II

COMPARISON BETWEEN THE TRAINED EMPIRICAL CONTROLLER AND A SAMPLED CONTROLLER USING OUR TRAINING APPROACH.

Controller	Cost		Collisions	
	Train	Test	Train	Test
Empirical	21.79	23.14	0.0%	5.8%
Ours	21.86	22.29	0.0%	5.0%

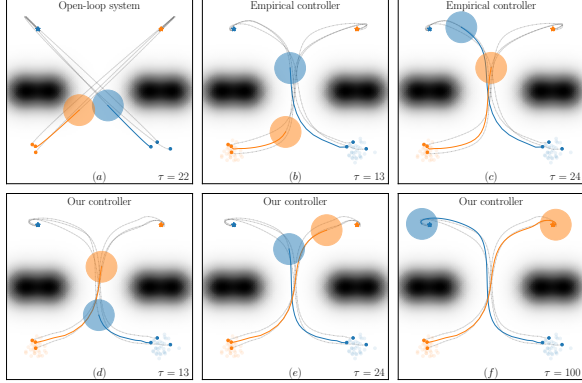


Fig. 3. Closed-loop test trajectories in the interval $[0, 400]$ of (a) the pre-stabilized system before training; (b)-(c) the trained empirical controller; and (d)-(f) one sampled controller from \mathcal{Q}^* using SVGD. Training initial conditions are marked with \circ . Snapshots are taken at instants τ indicated in each plot. Colored balls represent the agents, with their radius indicating their size for collision avoidance.

leads to collisions between robots and oscillations around the target position, indicating poor performance. Conversely, both of the employed controllers avoid collisions and achieve optimized trajectories in the plots (b)-(f). Animations are available in our Github repository.

Scalability: Using our approach, we train a controller with $n_\xi = 32$, $n_\zeta = 32$, leading to a total of $d = 11040$ parameters. The resulting test cost is 21.25 and the collision ratio is 1.0%, improving the results in Table II. This experiment showcases the capability of our method in effectively training large controllers.

VII. CONCLUSIONS AND FUTURE WORK

This paper presents a novel generalization bound for the SNOG cost, drawing upon randomized bounds within the PAC-Bayes theory. By combining the derived bound with the unconstrained parametrization of stabilizing controllers proposed in [7], we propose an innovative control policy design algorithm suitable for addressing SNOG problems.

Possible directions for future work are: exploring model selection techniques among a set of sampled controllers to enhance performance while maintaining valid generalization bounds, and utilizing the knowledge obtained from existing controllers for a given system to set the prior distribution.

REFERENCES

- [1] P. Alquier, "User-friendly introduction to PAC-Bayes bounds," *Foundations and Trends® in Machine Learning*, vol. 17, no. 2, pp. 174–303, 2024.
- [2] A. Majumdar, A. Farid, and A. Sonar, "PAC-Bayes control: learning policies that provably generalize to novel environments," *The International Journal of Robotics Research*, vol. 40, no. 2-3, pp. 574–593, 2021.
- [3] M. Fard and J. Pineau, "PAC-Bayesian model selection for reinforcement learning," in *Advances in Neural Information Processing Systems*, vol. 23, 2010.
- [4] M. Fard, J. Pineau, and C. Szepesvári, "PAC-Bayesian policy evaluation for reinforcement learning," *Proceedings of the 27th Conference on Uncertainty in Artificial Intelligence, UAI 2011*, p. 195–202, 2011.
- [5] C. Dawson, S. Gao, and C. Fan, "Safe control with learned certificates: A survey of neural Lyapunov, barrier, and contraction methods for robotics and control," *IEEE Transactions on Robotics*, vol. 39, no. 3, pp. 1749–1767, 2023.
- [6] R. Schwan, C. N. Jones, and D. Kuhn, "Stability verification of neural network controllers using mixed-integer programming," *IEEE Transactions on Automatic Control*, 2023.
- [7] L. Furieri, C. L. Galimberti, and G. Ferrari-Trecate, "Neural system level synthesis: Learning over all stabilizing policies for nonlinear systems," in *61st Conference on Decision and Control (CDC)*, 2022, pp. 2765–2770.
- [8] R. Wang, N. H. Barbara, M. Revay, and I. Manchester, "Learning over all stabilizing nonlinear controllers for a partially-observed linear system," *IEEE Control Systems Letters*, vol. 7, pp. 91–96, 2022.
- [9] L. Furieri, C. L. Galimberti, M. Zakwan, and G. Ferrari-Trecate, "Distributed neural network control with dependability guarantees: a compositional port-Hamiltonian approach," in *Learning for Dynamics and Control Conference*. PMLR, 2022, pp. 571–583.
- [10] F. Gu, H. Yin, L. El Ghaoui, M. Arcaç, P. Seiler, and M. Jin, "Recurrent neural network controllers synthesis with stability guarantees for partially observed systems," in *AAAI*, 2022, pp. 5385–5394.
- [11] P. Pauli, J. Köhler, J. Berberich, A. Koch, and F. Allgöwer, "Offset-free setpoint tracking using neural network controllers," in *Learning for Dynamics and Control*. PMLR, 2021, pp. 992–1003.
- [12] F. Bonassi, M. Farina, J. Xie, and R. Scatolini, "On recurrent neural networks for learning-based control: recent results and ideas for future developments," *Journal of Process Control*, vol. 114, pp. 92–104, 2022.
- [13] A. Abate, D. Ahmed, M. Giacobbe, and A. Peruffo, "Formal synthesis of Lyapunov neural networks," *IEEE Control Systems Letters*, vol. 5, no. 3, pp. 773–778, 2020.
- [14] F. Berkenkamp, M. Turchetta, A. P. Schoellig, and A. Krause, "Safe model-based reinforcement learning with stability guarantees," *Advances in Neural Information Processing Systems*, pp. 909–919, 2018.
- [15] M. Revay, R. Wang, and I. R. Manchester, "Recurrent equilibrium networks: Flexible dynamic models with guaranteed stability and robustness," *IEEE Transactions on Automatic Control*, 2023.
- [16] Q. Liu and D. Wang, "Stein variational gradient descent: A general purpose Bayesian inference algorithm," in *Advances in Neural Information Processing Systems*, vol. 29, 2016.
- [17] O. Catoni, "PAC-Bayesian supervised classification: The thermodynamics of statistical learning," *IMS Lecture Notes Monograph Series*, vol. 56, pp. 1–163, 2007.
- [18] C. G. Economou, M. Morari, and B. O. Palsson, "Internal model control: extension to nonlinear system," *Industrial & Engineering Chemistry Process Design and Development*, vol. 25, no. 2, pp. 403–411, 1986.
- [19] S. Boucheron, G. Lugosi, and P. Massart, *Concentration Inequalities: A Nonasymptotic Theory of Independence*. Oxford University Press, 2013.
- [20] P. J. Green, K. Łatuszyński, M. Pereyra, and C. P. Robert, "Bayesian computation: a perspective on the current state, and sampling backward and forwards," *Stat. Comput.*, vol. 25, no. 4, pp. 835–862, 2015.
- [21] P. Alquier, J. Ridgway, and N. Chopin, "On the properties of variational approximations of Gibbs posteriors," *Journal of Machine Learning Research*, vol. 17, no. 236, pp. 1–41, 2016.
- [22] J. Rothfuss, V. Fortuin, M. Josifoski, and A. Krause, "PACOH: Bayes-optimal meta-learning with PAC-guarantees," in *International Conference on Machine Learning*. PMLR, 2021, pp. 9116–9126.
- [23] M. G. Boroujeni, A. Krause, and G. Ferrari-Trecate, "Personalized federated learning of probabilistic models: A PAC-Bayesian approach," *arXiv preprint arXiv:2401.08351*, 2024.