ROSCOM: Robust Safe Reinforcement Learning on Stochastic Constraint Manifolds

Shangding Gu, Puze Liu, Alap Kshirsagar, Guang Chen, Jan Peters *Fellow, IEEE*, Alois Knoll *Fellow, IEEE*

***Abstract*—Reinforcement Learning (RL) has demonstrated remarkable success across various domains. Nonetheless, a significant challenge in RL is to ensure safety, particularly when deploying it in safety-critical applications such as robotics and autonomous driving. In this work, we develop a robust and safe RL methodology grounded in manifold space. Initially, we construct a constrained manifold space, taking safety constraints into consideration. We then propose a robust safe RL approach, supported by theoretical analysis, based on the value at risk and conditional value at risk, in order to enhance the robustness of safety. Our methodology is designed to ensure safety within stochastic constraint environments. Following the theoretical analysis, we develop a practical, safe algorithm to search for a robust safe policy on stochastic constraint manifolds (ROSCOM). We evaluate the effectiveness of our approach through circular motion and air-hockey tasks. Our experiments demonstrate that ROSCOM outperforms existing baselines in terms of both reward and safety.**

***Note to Practitioners*—Real-world applications often involve inherent uncertainties, noise, and high-dimensional spaces. This complexity accentuates the urgency and challenge of ensuring safety in robot learning, especially when implementing RL in practical environments. To address this critical issue, we build a stochastic constraint manifold to delineate the safety space, thus establishing a rigorous framework for robot learning at each iteration. Compared with state-of-the-art baselines, our method can provide remarkable performance regarding safety and reward performance. For example, in an air hockey robot learning task, our method has demonstrated a remarkable 50% enhancement in safety performance compared to the ATACOM framework [1], while concurrently exhibiting superior reward performance. Moreover, in contrast to traditional algorithms, including CPO [2], PCPO [3], our method has achieved a 99% improvement in safety performance, coupled with significantly superior reward performance. These empirical insights render our approach not only theoretically sound but also practically efficacious, indicating its potential as a useful tool in real robot learning and beyond.**

***Index Terms*—Safe Reinforcement Learning, Constrained Manifolds, Robust Reinforcement Learning, Robotics.**

Manuscript received October 26, 2023; revised February 14, 2024; accepted July 6, 2024. This work is supported by the National Natural Science Foundation of China (No. 62372329), in part by Shanghai Scientific Innovation Foundation (No.23DZ1203400), in part by Xiaomi Young Talents Program, and in part by "The Adaptive Mind", funded by the Excellence Program of the Hessian Ministry of Higher Education, Science, Research and Art. (*Corresponding authors: Guang Chen.*)

Shangding Gu and Alois Knoll are with the Department of Informatics, Technical University of Munich, Munich 85748, Germany (e-mail: shangding.gu@tum.de; knoll@mytum.de).

Puze Liu, Alap Kshirsagar and Jan Peters are with the Department of Informatics, Technical University of Darmstadt, Darmstad 64289, Germany (e-mail: puze.liu@ias.tu-darmstadt.de; alap.kshirsagar@tu-darmstadt.de; jan.peters@tu-darmstadt.de).

Guang Chen is with the Department of Computer Science and Technology, Tongji University, Shanghai 201804, China (e-mail: guangchen@tongji.edu.cn).

I. Introduction

REINFORCEMENT Learning (RL) has garnered substantial attention in recent years due to its capability to address complex problems and exhibit impressive performance in various tasks [4], [5], such as AlphaGo [6], finance [7], multi-robot control [8], [9], and autonomous driving [10]. However, the deployment of RL in real-world applications, particularly in safety-critical systems, presents challenges as an RL agent may execute unsafe actions that could harm humans or damage the agent's environment [4]. Safe RL methods tackle this issue by incorporating safety requirements during the learning process and ensuring that the decisions made by the RL agent do not lead to hazardous outcomes.

Numerous state-of-the-art (SOTA) methods have been proposed to ensure RL safety, including CPO [2], PCPO [3], RCPO [11], MACPO [8], and MAPPO-Lagrangian [8]. However, these approaches are not applicable to situations where the robot constraints are stochastic. Such scenarios are frequently encountered in real-world applications with high-dimensional space, like robotics and autonomous driving. The robot's observations may exhibit uncertainty due to noisy sensors, while the robot's constraints may be stochastical owing to the presence of other agents, such as humans. Thus, to ensure the safety of a robot and its environment, it is essential to consider stochastic constraints during robot learning in high-dimensional space.

In this work, we aim to address the critical question: *How can we guarantee RL safety with stochastic constraints in high-dimensional space?* To ensure safety in stochastic environments with high-dimensional space, we need to calculate safety bounds and construct constraint manifolds that incorporate these bounds. Manifolds are highly effective for managing high-dimensional data, a fact that is well-supported by numerous studies [12]–[14]. With the constraint manifolds, we can search for a safe policy for robot learning, where the constraint manifold is well-suited for representing high-dimensional constraints. The contributions of this work are as follows:

- We introduce a problem formulation that considers stochastic constraints on manifolds. Specifically, the stochastic constraints are incorporated into the state space based on manifolds.
- We offer theoretical safety bounds on the stochastic constraint manifold by leveraging Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR) methods [15], [16].

- We propose an algorithm for searching a robust safe policy on a stochastic constraint manifold (ROSCOM) and demonstrate its effectiveness compared to several SOTA safe RL algorithms.

II. Related Work

Deploying RL in real-world applications necessitates the assurance of safety for both the agent and the environment, in addition to robustness in the face of uncertainties. Researchers have proposed a variety of safe and robust RL methods to apply RL in safety-critical environments, such as autonomous driving and robotics [4], [10], [17], [18]. Despite these efforts, there remains a need for further development of RL methods that can address safety and robustness challenges concurrently. This section provides a brief analysis of the current state of research in the domain of safe and robust RL.

A. Safe Reinforcement Learning.

In recent years, research on safe RL has gained significant attention due to its importance in addressing the safety concerns in various applications [4]. Safe RL can be formulated as a constrained optimization problem with methods falling into three main categories: constrained state space, constrained action space, and constrained cumulative cost.

The first category comprises methods that leverage constrained state space as a safe state space [19]–[22]. These methods often incorporate Gaussian Process models to estimate safe state space during exploration [19]–[22]. Another notable approach is ATACOM [1], which projects exploration states onto a constrained manifold. Our method also belongs to this category.

The second category includes methods that employ a constrained action space as a safe action space [23]–[28]. For instance, some methods use temporal logic verification to ensure the safety of actions during exploration [26], while others rely on Lyapunov functions to constrain the action space with energy functions [23]–[25].

The third category focuses on optimizing safe policies based on cumulative safety cost [2], [3], [8], [11]. Examples include CPO [2] for single-agent settings and MACPO [8] and MAPPO-Lagrangian [8] for multi-agent settings. These methods demonstrate the versatility of Safe RL approaches in addressing safety concerns across various domains and settings.

B. Robust Reinforcement Learning.

Existing robust RL methods tackle three types of uncertainties: reward uncertainty [29], [30], transition uncertainty [31]–[38], and observation uncertainty [39]–[43].

To address reward uncertainty, Liang *et al.* [29] proposed a human-preferences-based learning method, while Li *et al.* [30] developed a meta-learning approach that learns uncertain rewards using normalized maximum likelihood.

For transition uncertainty, Chua *et al.* [31] introduced a probabilistic dynamics model to balance the trade-off between model-based and model-free RL methods. Zhang *et al.* [32] employed a natural player to disrupt the multi-agent system's transitions, similar to an adversarial agent, enabling the ego player to enhance its performance in adversarial environments.

Regarding observation uncertainty, Lutjens *et al.* [39] presented a certified adversarial robustness method for handling uncertainties during exploration. Zhang *et al.* [41] proposed a robust policy regularizer for uncertain observations in both discrete and continuous environments. These methods demonstrate the breadth of approaches in robust RL for addressing various uncertainties, thus facilitating the development of more reliable and resilient agents in diverse application scenarios.

The existing methods primarily focus on addressing either the safety or robustness aspect of RL, but not both simultaneously. The challenge of robust and safe RL lies in ensuring safety in uncertain environments, such as those with uncertain observations and constraints. The work of Liu *et al.* [18] is the closest to addressing this challenge, as they proposed a robust and safe RL method in an adversarial setting where two attackers disturb agent behaviors. However, the adversarial setting may limit the practicality of their method in real-world applications.

In contrast to Liu *et al.* [18], our approach ensures RL safety under stochastic constraints by employing a constraint manifold, which is capable of handling high-dimensional data in real-world environments. The stochastic constraints are generated by a stochastic function rather than an adversarial agent. Unlike Liu *et al.* [18], who employ neural networks to model the adversarial agent's behaviors. Lastly, our work provides theoretical safety bounds based on the constraint manifold, ensuring safety in stochastic constraints.

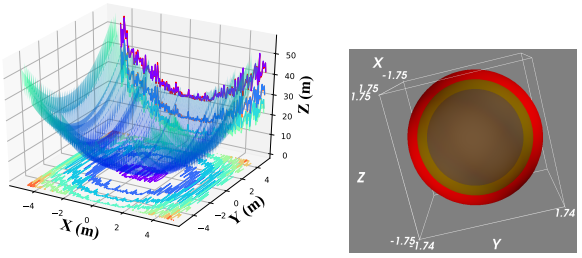
Our method focuses on the observation uncertainty, where the state space is disturbed by some noise, and we need to ensure safety via safety bounds. By addressing both safety and robustness in RL simultaneously, our method paves the way for more reliable and resilient agents that can operate effectively in safety-critical applications and stochastic constrained environments.

III. Problem Formulation

A robust safe RL problem [4] can be seen as a standard MDP with a constraint set under stochastic constraints, to illustrate this problem, we consider a tuple $(\mathcal{S}, \mathcal{A}, P, r, \rho_0, \gamma, c_i, \epsilon_i)$, where $\mathcal{S}$ is a state space, $\mathcal{A}$ is an action space, $P : \mathcal{S}\times\mathcal{A}\times\mathcal{S} \to [0, 1]$ is a transition function, r denotes the reward, ρ_0 is the initial state distribution, γ is a discount factor, $c_i : \mathcal{S} \to \mathbb{R}$ denotes a deterministic state-constraint function of constraint i, $\forall\ i = 1, \ldots, N$, $\epsilon_i : \mathcal{S} \to \mathbb{R}$ denotes a stochastic state-constraint function of constraint i.

In robust safe RL, the goal of an optimal policy π is to maximize the reward while ensuring safety by selecting an action a under stochastic constraints. $\tau \sim \pi$ is a trajectory, $\tau = (s_0, a_0, s_1, \ldots)$, which depends on π, $s_0 \sim \rho_0$, $a_t \sim \pi(\cdot|s_t)$, $s_{t+1} \sim P$, where the state $s_t \in \mathcal{S}$ at time step t, the action $a_t \in \mathcal{A}$ at time step t, $t \in \{0, 1, \cdots, T\}$, T is the episode length.

We formulate the robust safe RL problem as an MDP problem as shown in Equation (1), in which the stochastic



(a) (b)

Fig. 1: Schematic diagram of stochastic constraints and safety bound. (a). 3D stochastic constraints, Gaussian noise in the x, y, and z directions; (b). 3D safety bound, the areas of dark brown and red denote the new safe space, and the area of light brown denotes the uncertain space.

constraints are taken into account. Figure 1 shows an example of the stochastic constraints. In this Equation, we need to search for a policy to maximize the discounted cumulative reward value while ensuring learning safety. Specifically, the safety constraints consist of deterministic constraints $c_i(s_t)$ and stochastic constraints $\epsilon_i(s_t)$ at time step t, the stochastic constraints $\epsilon_i(s_t)$ are from some uncertain noises due to imperfect observation. The aggregate of these constraints, $c_i(s_t)$ plus $\epsilon_i(s_t)$, need to remain below a predefined threshold δ with a probability of η. Particularly, for all states s_t, if the constraints $c_i(s_t)$ and $\epsilon_i(s_t)$ are equal to zero, then states s_t are the safe set (safe set indicates that we can ensure robot learning safety within these states), that is the safe set $= \{s_t | c_i(s_t) = 0,\ \epsilon_i(s_t) = 0\}$. Conversely, for all states within the unsafe set, $c_i(s_t)$ and $\epsilon_i(s_t)$ are positive real values, expressed as $\mathbb{R}^+$. That is the unsafe set $= \{s_t | c_i(s_t) \in \mathbb{R}^+,\ \epsilon_i(s_t) \in \mathbb{R}^+\}$. For each type of constraint i, there corresponds a safety bound δ_i and a safety probability η_i. For simplicity, we denote these as δ and η, respectively.

$$\begin{aligned} \max_{\pi} \ & \mathbb{E}_{\tau\sim\pi}\left[\sum_{t}^{T}\gamma^t r\left(s_t, a_t\right)\right], \\ \text{s.t.} \ & Pr(|c_i(s_t) + \epsilon_i(s_t)| \leq \delta) > \eta. \end{aligned} \tag{1}$$

IV. Method

We first present the definitions of state constraint manifolds. Subsequently, we provide the theoretical safety bounds based on VaR and CVaR to search for safe policies. Sections IV-A is to build a stochastic constrained manifold, and Section IV-B aims to provide safety bounds on a stochastic constrained Manifold. Lastly, Section IV-C presents a practical algorithm for searching robust safe policies within a stochastic constraint manifold.

A. State Constraints on a Manifold

Similiar to ATACOM [1], in the high-dimensional state space $\mathcal{S}$ (the state variable $\boldsymbol{s} \in \mathcal{S}$) is consisted of two sets, a controllable set $\boldsymbol{q} \in \mathcal{Q} \in \mathbb{R}^Q$ and an uncontrollable set $\boldsymbol{x} \in \mathcal{X}$, $\boldsymbol{s} = [\boldsymbol{q}, \boldsymbol{x}]^\top$. In this study, constraints are defined on the controllable set, $Pr(|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})| < \boldsymbol{\delta}) > \boldsymbol{\eta}$, where $\boldsymbol{c}_i = [\boldsymbol{f}_i, \boldsymbol{g}_i] \in \mathbb{R}^{F+G}$ denotes constraints, equality constraints $\boldsymbol{f}_i = \boldsymbol{0}$, $\boldsymbol{f}_i \in \mathbb{R}^F$ and inequality constraints $\boldsymbol{g}_i < \boldsymbol{0}$, $\boldsymbol{g}_i \in \mathbb{R}^G$, $\boldsymbol{\epsilon}_i \in \mathbb{R}^{F+G}$ denotes stochastic constraints, $\boldsymbol{\delta} \in \mathbb{R}^{F+G}$ denotes a set of safety bounds, for simplicity, we use $\boldsymbol{\eta} \in \mathbb{R}^{F+G}$ to denote a set of safety probability $\eta^{o, o\in\{1,2,\ldots,F+G\}}$, $\boldsymbol{f}_i$ to denotes a set of equality constraints $f_i^{o_1, o_1\in\{1,2,\ldots,F\}}$, $\boldsymbol{g}_i$ to denotes a set of equality constraints $g_i^{o_2, o_2\in\{1,2,\ldots,G\}}$. Note, when comparing values of a high-dimensional data set, we assess each individual element within the data set.

Definition 1. *If the constraints are differentiable, we can have the following constraint manifolds. $\mathcal{M}_1$ is the equality constraints manifold with stochastic constraints, $\mathcal{M}_2$ is the inequality constraints manifold with stochastic constraints, as shown in Equation (2):*

$$\begin{bmatrix} \mathcal{M}_1 = \{|\boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_{\boldsymbol{f}_i}(\boldsymbol{q})| - \boldsymbol{\delta} = \boldsymbol{0}\} \\ \mathcal{M}_2 = \left\{|\boldsymbol{g}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_{\boldsymbol{g}_i}(\boldsymbol{q})| - \boldsymbol{\delta} + \frac{1}{2}\boldsymbol{\mu}_s^2 = \boldsymbol{0}\right\} \end{bmatrix} \Longrightarrow$$

$$\begin{bmatrix} \mathcal{M}_{1V} = \{\boldsymbol{f}_{iV}(\boldsymbol{q}) = \boldsymbol{0}\} \\ \mathcal{M}_{2V} = \left\{\boldsymbol{g}_{iV}(\boldsymbol{q}) + \frac{1}{2}\boldsymbol{\mu}^2 = \boldsymbol{0}\right\} \end{bmatrix} \tag{2}$$

In Equation (2), $\mathcal{M}_{1V}$ and $\mathcal{M}_{2V}$ represent the manifolds of equality and inequality constraints with VaR (Value at Risk) bounds, respectively. In the following section, we will describe how to compute these manifolds to ensure safety. $\boldsymbol{\epsilon}_{f_i} \in \mathbb{R}^F$ denotes the stochastic constraints on the equality constraint manifold, $\boldsymbol{\epsilon}_{g_i} \in \mathbb{R}^G$ denotes the stochastic constraints on the inequality constraint manifold, $\boldsymbol{f}_{iV}(\boldsymbol{q})$ and $\boldsymbol{g}_{iV}(\boldsymbol{q})$ denotes equality constraints and inequality constraints with VaR safety bounds considering stochastic constraints. To construct the safety manifold under inequality constraints, the slack variables $\boldsymbol{\mu}_s \in \mathbb{R}^G$ and $\boldsymbol{\mu} \in \mathbb{R}^G$ are leveraged, which are introduced into the constraints [1].

Therefore, we have the new constraint set $\boldsymbol{c}(\boldsymbol{q}, \boldsymbol{\mu}_s) \in \mathbb{R}^{F+G}$, as shown in Equation (3), $\boldsymbol{J}_{fiV}(\boldsymbol{q}) \in \mathbb{R}^{F\times Q}$ is the Jacobian matrice of $\boldsymbol{f}_{iV}(\boldsymbol{q}) \in \mathbb{R}^F$. We have two equality constraint sides when inequality constraints are converted to equality constraints with safety bounds. Thus, we consider two safety sides of the equality constraints, $\boldsymbol{J}_{fiV}^+(\boldsymbol{q}) \in \mathbb{R}^{F\times Q}$ and $\boldsymbol{J}_{fiV}^-(\boldsymbol{q}) \in \mathbb{R}^{F\times Q}$. $\boldsymbol{J}_{fiV}^+(\boldsymbol{q}) \in \mathbb{R}^{F\times Q}$ and $\boldsymbol{J}_{fiV}^-(\boldsymbol{q}) \in \mathbb{R}^{F\times Q}$ are the Jacobian matrices of the safety bounds for the function $\boldsymbol{g}_{iV}(\boldsymbol{q}) \in \mathbb{R}^G$.

$$\boldsymbol{c}(\boldsymbol{q}, \boldsymbol{\mu}, \dot{\boldsymbol{q}}, \dot{\boldsymbol{\mu}}) = \begin{bmatrix} \boldsymbol{J}_{fiV}(\boldsymbol{q})^+ & \boldsymbol{0} \\ \boldsymbol{J}_{fiV}(\boldsymbol{q})^- & \boldsymbol{0} \\ \boldsymbol{J}_{giV}(\boldsymbol{q}) & diag(\boldsymbol{\mu}_s) \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{q}} \\ \dot{\boldsymbol{\mu}}_s \end{bmatrix} \tag{3}$$

$$= \boldsymbol{J}_{\boldsymbol{c}}(\boldsymbol{q}, \boldsymbol{\mu}_s) \begin{bmatrix} \dot{\boldsymbol{q}} \\ \dot{\boldsymbol{\mu}}_s \end{bmatrix}, \tag{4}$$

where $\boldsymbol{J}_c(\boldsymbol{q}, \boldsymbol{\mu}_s) \in \mathbb{R}^{(2F+G)\times(Q+G)}$ is the Jacobian Matrix, by leveraging SVD [44] and QR [45], we can have $\boldsymbol{J}_c(\boldsymbol{q}, \boldsymbol{\mu}_s)\boldsymbol{N}_c(\boldsymbol{q}, \boldsymbol{\mu}_s) = \boldsymbol{0}$, $\boldsymbol{N}_c(\boldsymbol{q}, \boldsymbol{\mu}_s) \in \mathbb{R}^{(Q+G)\times(Q-2F)}$ is the null space, which can be seen as the tangent space bases of a constraint manifold.

Remark 1. *Inspired by ATACOM [1], the nullspace of the Jacobian matrix $\boldsymbol{J}_c(\boldsymbol{q}, \boldsymbol{\mu}_s) \in \mathbb{R}^{(2F+G)\times(Q+G)}$ for the tangent-space bases of the constraint manifold is $\boldsymbol{N}_c(\boldsymbol{q}, \boldsymbol{\mu}_s) \in \mathbb{R}^{(Q+G)\times(Q-2F)}$, we can search a safe policy at each time step t on the constraint manifold $\boldsymbol{c}(\boldsymbol{q}, \boldsymbol{\mu}_s)$.*

In the subsequent section, we will delve into the methodologies and strategies to guarantee safety on a stochastic manifold. The complexities inherent to these manifolds necessitate rigorous approaches to maintain safety, and our discussion will shed light on these critical procedures.

B. Ensuring Safety with VaR and CVaR on a Stochastic Constraint Manifold

This section presents a theoretical analysis of the safety bounds based on stochastic constraints. First, we give the definition of the safety bounds and the risk measurements. Then, we derive safety bounds for stochastic constraints by leveraging VaR and CVaR [15], [16].

Definition 2. *VaR and CVaR. For safety constraints $|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|$, the value-at-risk (VaR) of $|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|$ with confidence level $\boldsymbol{\eta} \in (\mathbf{0}, \mathbf{1})$ is defined as:*

$$\mathrm{VaR}_\eta(|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|) = \min\{\boldsymbol{\delta} \mid F(\boldsymbol{\delta}) \geq \boldsymbol{\eta}\},$$

where $F(\boldsymbol{\delta}) = P(|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})| \leq \boldsymbol{\delta})$ is the cumulative distribution function (CDF), $\boldsymbol{\epsilon}_i(\boldsymbol{q})$ denotes the stochastic costs. The conditional value-at-risk (CVaR) of $|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|$ with confidence level $\boldsymbol{\eta}$ is defined as the expectation of the $\boldsymbol{\eta}$-tail distribution of $|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|$ as

$$\mathrm{CVaR}_\eta(\boldsymbol{\epsilon}_i(\boldsymbol{q})) = \mathbb{E}\left\{\boldsymbol{\delta} \mid \boldsymbol{\delta} \geq \mathrm{VaR}_\eta(|\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|)\right\}.$$

Here, we assume stochastic constraints $\boldsymbol{\epsilon}_i(\boldsymbol{q})$ subject to a Gaussian distribution N, $Z = \boldsymbol{\epsilon}_i(\boldsymbol{q}) \sim N(\boldsymbol{\mu}, \boldsymbol{\sigma}^2)$.

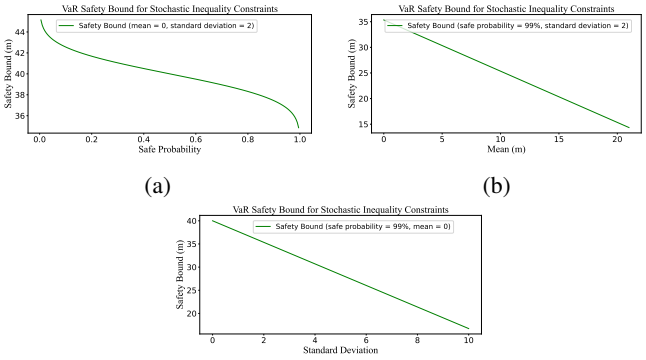
1) Safety Bound for Inequality Constraints with Stochastic Noises on a Manifold:

We rewrite VaR for inequality constraints as following equations, where $\boldsymbol{g}_i(\boldsymbol{q})^a$ denotes the old deterministic inequality constraints, $\boldsymbol{g}_i(\boldsymbol{q})$ denotes the new deterministic inequality constraints, $\boldsymbol{\delta}_g$ denotes the safety bound for inequality constraints, $\boldsymbol{\mu}$ denotes the mean of stochastic constraints $\boldsymbol{\epsilon}_i(\boldsymbol{q})$, $\boldsymbol{\sigma}$ denotes the standard deviation of stochastic constraints $\boldsymbol{\epsilon}_i(\boldsymbol{q})$, $\boldsymbol{\eta}$ is the safety probability for robot learning.

$$F(\boldsymbol{\delta}_g) = P(\boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \leq \boldsymbol{\delta}_g), \tag{5}$$

$$\begin{aligned}
&\mathrm{VaR}_\eta(\boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon}_i(\boldsymbol{q})) = \min\{\boldsymbol{\delta}_g \mid F(\boldsymbol{\delta}_g) \geq \boldsymbol{\eta}\} \\
&= \min\{\boldsymbol{\delta}_g \mid P(\boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon_i}(\boldsymbol{q}) \leq \boldsymbol{\delta}_g) \geq \boldsymbol{\eta}\} \\
&= \min\{\boldsymbol{\delta}_g \mid P\left(\frac{\boldsymbol{\epsilon_i}(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}} \leq \frac{\boldsymbol{\delta}_g - \boldsymbol{g}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) \geq \boldsymbol{\eta}\} \\
&= \min\{\boldsymbol{\delta}_g \mid \Phi\left(\frac{\boldsymbol{\delta}_g - \boldsymbol{g}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) \geq \boldsymbol{\eta}\}.
\end{aligned} \tag{6}$$

(1) Computing safety bounds for inequality stochastic constraints with VaR on a manifold:



(a) (b)

(c)

Fig. 2: VaR safety bounds on a manifold for inequality constraints in terms of (a) safe probability, (b) constraints' mean, and (c) constraints' standard deviation.

Lemma 1. *The safety bound BV_{g1} on a stochastic inequality constraint manifold via VaR is given by,*

$$\boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{g}_i(\boldsymbol{q}) \leq \underbrace{-\Phi^{-1}(\boldsymbol{\eta})\boldsymbol{\sigma} - \boldsymbol{\mu} + \boldsymbol{g}_i(\boldsymbol{q})}_{\textit{safety bound } BV_{g1}}.$$

Proof. With Equation (6), we can have the following safety safety bound,

$$\begin{aligned}
&\Phi\left(\frac{\boldsymbol{\delta}_g - \boldsymbol{g}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) \geq \boldsymbol{\eta} \\
&\implies \frac{\boldsymbol{\delta}_g - \boldsymbol{g}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}} \geq \Phi^{-1}(\boldsymbol{\eta}) \\
&\implies \boldsymbol{\delta}_g \geq \Phi^{-1}(\boldsymbol{\eta})\boldsymbol{\sigma} + \boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\mu}.
\end{aligned} \tag{7}$$

We can observe the following equation if we want to ensure total safety with probability $\boldsymbol{\eta}$,

$$\begin{aligned}
&\mathbf{0} = \boldsymbol{\delta}_g \geq \Phi^{-1}(\boldsymbol{\eta})\boldsymbol{\sigma} + \boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\mu} \\
&\implies \boldsymbol{g}_i(\boldsymbol{q})^a \leq -\Phi^{-1}(\boldsymbol{\eta})\boldsymbol{\sigma} - \boldsymbol{\mu}.
\end{aligned} \tag{8}$$

Therefore, the safety bound BV_{g1} via VaR that considered uncertain areas is given as follows:

$$\boldsymbol{g_i}(\boldsymbol{q})^a + \boldsymbol{g}_i(\boldsymbol{q}) \leq \underbrace{-\Phi^{-1}(\boldsymbol{\eta})\boldsymbol{\sigma} - \boldsymbol{\mu} + \boldsymbol{g}_i(\boldsymbol{q})}_{\text{safety bound } BV_{g1}}. \tag{9}$$

□

Based on Lemma 1, we can have VaR safety bound for inequality constraints in terms of (a) safety probability, (b) constraints' mean and (c) constraints' standard deviation, as shown in Figure 2. It demonstrates the robustness of our safety bound under varying conditions of safety probability (a), mean of constraints (b), and standard deviation of constraints (c). Once we have the safety bounds, we can search for the policy on the tangent space of safety bounds, which helps ensure performance stability. We also provide CVaR safety bound for inequality constraints, for details, see the following Lemma 2.

(2) Computing safety bounds for inequality stochastic constraints with CVaR on a manifold:

Inspired by the reference [46], since the stochastic constraints subjects to a Gaussian distribution, we can have

$$\phi = \frac{\mathbf{1}}{\boldsymbol{\sigma}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\boldsymbol{x}-\boldsymbol{g}_i(\boldsymbol{q})^a-\boldsymbol{u}}{\boldsymbol{\sigma}}\right)^2}, \tag{10}$$

$$\begin{aligned}\mathrm{CVaR}_{\boldsymbol{\eta}} &= \mathrm{E}[X \mid X \geq \boldsymbol{\delta}_g] = \boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{\mu} + \boldsymbol{\sigma}\frac{\phi\left(\Phi^{-1}(\boldsymbol{\eta})\right)}{\mathbf{1}-\boldsymbol{\eta}} \leq \mathbf{0} \\ \Longrightarrow \boldsymbol{g}_i(\boldsymbol{q})^a &\leq -\boldsymbol{\mu} - \boldsymbol{\sigma}\frac{\phi\left(\Phi^{-1}(\boldsymbol{\eta})\right)}{\mathbf{1}-\boldsymbol{\eta}},\end{aligned} \tag{11}$$

Lemma 2. *The safety bound BC_{g1} on an inequality stochastic constraint manifold via CVaR that considered uncertain areas is given as follows:*

$$\boldsymbol{g}_i(\boldsymbol{q})^a + \boldsymbol{g}_i(\boldsymbol{q}) \leq \underbrace{-\boldsymbol{\mu} - \boldsymbol{\sigma}\frac{\phi\left(\Phi^{-1}(\boldsymbol{\eta})\right)}{\mathbf{1}-\boldsymbol{\eta}} + \boldsymbol{g}_i(\boldsymbol{q})}_{\textit{safety bound } BC_{g1}}, \tag{12}$$

Proof. We have a random vector $\boldsymbol{X} \in \mathbb{R}^{F+G}$, and $\mathrm{CVaR}_{\delta_g}(\boldsymbol{X}) = \mathrm{E}\left(\boldsymbol{X} \mid \boldsymbol{X} > \boldsymbol{\delta}_g\right) = \int_{\boldsymbol{\delta}_g}^{\infty} \boldsymbol{x} f(\boldsymbol{x}) d\boldsymbol{x} / (1 - F\left(\boldsymbol{\delta}_g\right))$, where $F\left(\boldsymbol{\delta}_g\right)$ is a CDF, $f(\boldsymbol{x})$ is a Probability Density Function (PDF), and $\boldsymbol{\delta}_g = \mathrm{VaR}_{\boldsymbol{\delta_g}}$, and $P\left(\boldsymbol{X} > \boldsymbol{\delta}_g\right) = 1 - \boldsymbol{\eta}$, $\boldsymbol{x} \in \mathbb{R}^{F+G}$.

As shown in the first part, $\Phi\left[\left(\boldsymbol{\delta}_g - \boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right] = \boldsymbol{\eta}$, we have

$$\begin{aligned}&\int_{\boldsymbol{\delta}_g}^{\infty} \boldsymbol{x} f(\boldsymbol{x}) d\boldsymbol{x} = \int_{-\infty}^{\infty} \boldsymbol{x} f(\boldsymbol{x}) d\boldsymbol{x} - \int_{-\infty}^{\boldsymbol{\delta}_g} \boldsymbol{x} f(\boldsymbol{x}) d\boldsymbol{x} \\ &= \boldsymbol{\mu} - \int_{-\infty}^{\boldsymbol{\delta}_g} \boldsymbol{x} f(\boldsymbol{x}) d\boldsymbol{x} \\ &= \boldsymbol{\mu} - \boldsymbol{\mu}\Phi\left[\left(\boldsymbol{\delta}_g - \boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right] - \boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_g - \boldsymbol{\mu})/\boldsymbol{\sigma}} \boldsymbol{z}\phi(\boldsymbol{z}) d\boldsymbol{z} \\ &= \boldsymbol{\mu} - \boldsymbol{\mu}\boldsymbol{\eta} + \boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_g - \boldsymbol{\mu})/\boldsymbol{\sigma}} \phi'(\boldsymbol{z}) d\boldsymbol{z} \\ &= \boldsymbol{\mu}(1-\boldsymbol{\eta}) + \boldsymbol{\sigma}\phi\left[\left(\boldsymbol{\delta_g} - \boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right] \\ &= \boldsymbol{\mu}(1-\boldsymbol{\eta}) + \boldsymbol{\sigma}\phi\left[\Phi^{-1}(\boldsymbol{\eta})\right].\end{aligned}$$

Thus, we have the safety bound,

$$\begin{aligned}\mathrm{CVaR}_{\boldsymbol{\delta}_g}(X) &= \frac{\boldsymbol{\mu}(\mathbf{1}-\boldsymbol{\eta}) + \boldsymbol{\sigma}\phi\left[\Phi^{-1}(\boldsymbol{\eta})\right]}{\mathbf{1} - F\left(\boldsymbol{\delta}_g\right)} \\ &= \frac{\boldsymbol{\mu}(\mathbf{1}-\boldsymbol{\eta}) + \boldsymbol{\sigma}\phi\left[\Phi^{-1}(\boldsymbol{\eta})\right]}{\mathbf{1}-\boldsymbol{\eta}} \\ &= \boldsymbol{\mu} + \frac{\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\boldsymbol{\eta})\right]}{\mathbf{1}-\boldsymbol{\eta}}.\end{aligned} \tag{13}$$

□

In accordance with Lemma 2, it becomes apparent that we are able to establish a safety bound predicated on CVaR for inequality constraints, and this relationship is explicated with respect to three fundamental components: (a) the safe probability, (b) the mean of the constraints, and (c) the standard deviation of the constraints. The representation of these relationships is provided in Figure 3.

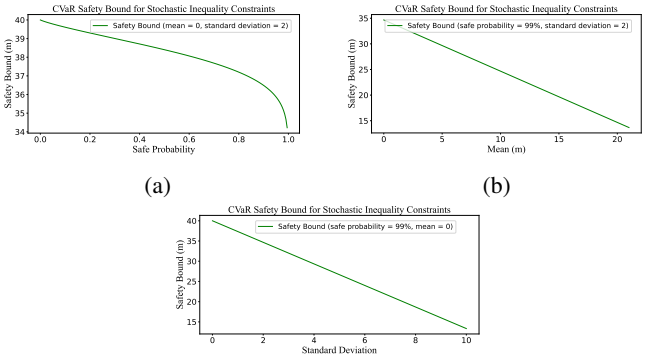


Fig. 3: CVaR safety bounds on a manifold for inequality constraints in terms of safe probability (a), constraints' mean (b), and constraints' standard deviation (c).

2) Safety Bounds for Equality Constraints with Stochastic Noises on a Manifold:

Stochastic equality constraints present a distinct challenge compared to stochastic inequality constraints due to their inherent two-sided constraint structure on a manifold, resulting in the existence of two separate safety bounds. The computation of probabilities for both sides of these equality constraints is a non-trivial task. To address this, we propose a transformation that allows us to reframe the problem of computing two equality safety bounds into two distinct problems centered around the computation of inequality safety bounds. Specifically, we aim for VaR and CVaR safety bounds based on the two inequality safety bounds obtained through this transformation.

Here, we rewrite VaR for equality constraints, $\boldsymbol{f_i}(\boldsymbol{q})$ denotes equality constraints, as shown in Equations (14) and (15).

$$\begin{aligned}F(\boldsymbol{\delta}_f) &= P(|\boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})| \leq \boldsymbol{\delta}_f) \\ &= P(-\boldsymbol{\delta}_f \leq \boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \leq \boldsymbol{\delta}_f) \\ &= P(\boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \leq \boldsymbol{\delta}_f) - P(\boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \leq -\boldsymbol{\delta}_f) \\ &= \Phi\left(\frac{\boldsymbol{\delta}_f - \boldsymbol{f}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) - \Phi\left(\frac{-\boldsymbol{\delta}_f - \boldsymbol{f}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right).\end{aligned} \tag{14}$$

$$\begin{aligned}&\mathrm{VaR}_{\eta}(|\boldsymbol{f}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q})|) = \min\left\{\boldsymbol{\delta}_f \mid F(\boldsymbol{\delta}_f) \geq \boldsymbol{\eta}\right\} \\ &= \min\left\{\boldsymbol{\delta}_f \mid \Phi\left(\frac{\boldsymbol{\delta}_f - \boldsymbol{f}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) - \right. \\ &\left.\Phi\left(\frac{-\boldsymbol{\delta}_f - \boldsymbol{f}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) \geq \boldsymbol{\eta}\right\}.\end{aligned} \tag{15}$$

For one side safety bound via VaR, $F(\boldsymbol{\delta}_f^a) = P(\boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon}_i(\boldsymbol{q}) > \boldsymbol{\delta}_f^a) < \frac{\mathbf{1}-\boldsymbol{\eta}}{2}$. For the other side safety bound via VaR, $F(\boldsymbol{\delta}_f^b) = P\left(\boldsymbol{f}_i(\boldsymbol{q})^b + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \leq -\boldsymbol{\delta}_f^b\right) < \frac{\mathbf{1}-\boldsymbol{\eta}}{2}$, $\boldsymbol{\delta}_f^b$ is the other side's constrained limit set.

(1) Computing Safety Bounds for Equality Constraints with VaR on a Manifold:

Theorem 1. *The first-side safety bound BV_{f1} on the equality stochastic constraint manifold via VaR that considers uncertain areas is given by,*

$$\boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{f}_i(\boldsymbol{q}) < \underbrace{-\Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} - \boldsymbol{\mu} + \boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BV_{f1}}.$$

The second-side safety bound BV_{f2} on the equality stochastic constraint manifold via VaR that considers uncertain areas is given by,

$$\underbrace{-\boldsymbol{\mu} - \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} + \boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BV_{f2}} < \boldsymbol{f}_i(\boldsymbol{q})^b + \boldsymbol{f}_i(\boldsymbol{q}).$$

Proof. Based on Equations (14) and (15), we can prove the first side of safety bounds.

(A). The first side safety bound via VaR:

With the VaR definition on constraint manifolds (as shown in Definition 2) and Equation (5), we can have

$$\begin{aligned}
F(\boldsymbol{\delta}_f^a) = P(\boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon}_i(\boldsymbol{q}) > \boldsymbol{\delta}_f^a) &< \frac{\mathbf{1}-\boldsymbol{\eta}}{2} \\
\implies \mathbf{1} - P(\boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \le \boldsymbol{\delta}_f^a) &< \frac{\mathbf{1}-\boldsymbol{\eta}}{2} \\
\implies \frac{\mathbf{1}+\boldsymbol{\eta}}{2} < P\left(\frac{\boldsymbol{\epsilon}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}} \le \frac{\boldsymbol{\delta}_f^a - \boldsymbol{f}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) & \\
\implies \frac{\mathbf{1}+\boldsymbol{\eta}}{2} < \Phi\left(\frac{\boldsymbol{\delta}_f^a - \boldsymbol{f}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) & \\
\implies \Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right) < \frac{\boldsymbol{\delta}_f^a - \boldsymbol{f}_i(\boldsymbol{q})^a - \boldsymbol{\mu}}{\boldsymbol{\sigma}} & \\
\implies \Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} + \boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{\mu} < \boldsymbol{\delta}_f^a. & \qquad (16)
\end{aligned}$$

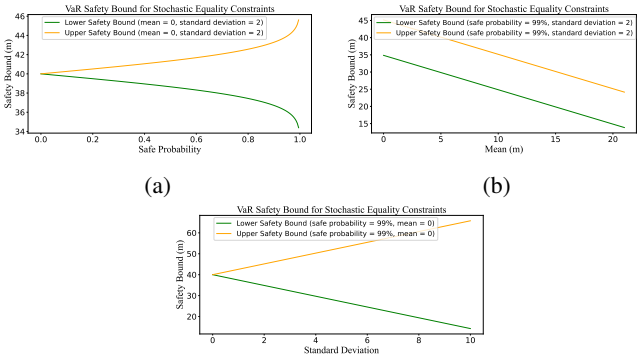
Since it's a equality constraint equation, we can have $\boldsymbol{\delta}_f^a = 0$, thus, the condition of uncertain areas of $\boldsymbol{f}_i(\boldsymbol{q})^a$ is as follows,

$$\begin{aligned}
\Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} + \boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{\mu} < \boldsymbol{\delta}_f^a = \mathbf{0} & \qquad (17) \\
\implies \boldsymbol{f}_i(\boldsymbol{q})^a < -\Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} - \boldsymbol{\mu}. & \qquad (18)
\end{aligned}$$

Therefore, the safety bound BV_{f1} via VaR that considered uncertain areas is given as follows:

$$\boldsymbol{f}_i(\boldsymbol{q})^a + \boldsymbol{f}_i(\boldsymbol{q}) < \underbrace{-\Phi^{-1}\left(\frac{\mathbf{1}+\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} - \boldsymbol{\mu} + \boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BV_{f1}}. \qquad (19)$$

(B). The second side safety bound via VaR:



(a) (b)

(c)

Fig. 4: VaR safety bounds on a manifold for Equality Constraints in terms of safe probability (a), constraints' mean (b), and constraints' standard deviation (c).

Similar to the proof of the first side safety bound, we can have

$$\begin{aligned}
F(\boldsymbol{\delta}_f^b) = P\left(\boldsymbol{f}_i(\boldsymbol{q})^b + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \le -\boldsymbol{\delta}_f^b\right) &< \frac{\mathbf{1}-\boldsymbol{\eta}}{2} \\
\implies P\left(\frac{\boldsymbol{\epsilon}_i(\boldsymbol{q}) - \boldsymbol{\mu}}{\boldsymbol{\sigma}} \le \frac{-\boldsymbol{\delta}_f^b - \boldsymbol{f}_i(\boldsymbol{q})^b - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) &< \frac{\mathbf{1}-\boldsymbol{\eta}}{2} \\
\implies \Phi\left(\frac{-\boldsymbol{\delta}_f^b - \boldsymbol{f}_i(\boldsymbol{q})^b - \boldsymbol{\mu}}{\boldsymbol{\sigma}}\right) &< \frac{\mathbf{1}-\boldsymbol{\eta}}{2} \\
\implies -\boldsymbol{\delta}_f^b - \boldsymbol{f}_i(\boldsymbol{q})^b - \boldsymbol{\mu} < \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} & \\
\implies -\boldsymbol{f}_i(\boldsymbol{q})^b - \boldsymbol{\mu} - \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} < \boldsymbol{\delta}_f^b. & \qquad (20)
\end{aligned}$$

The condition of uncertain areas of $\boldsymbol{f}_i(\boldsymbol{q})^b$ is as follows,

$$\begin{aligned}
-\boldsymbol{f}_i(\boldsymbol{q})^b - \boldsymbol{\mu} - \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} < \boldsymbol{\delta}_f^b = \mathbf{0} & \\
\implies -\boldsymbol{\mu} - \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} < \boldsymbol{f}_i(\boldsymbol{q})^b. & \qquad (21)
\end{aligned}$$

Thus, the safety bound BV_{f2} via VaR that considered uncertain areas is given as follows:

$$\underbrace{-\boldsymbol{\mu} - \Phi^{-1}\left(\frac{\mathbf{1}-\boldsymbol{\eta}}{2}\right)\boldsymbol{\sigma} + \boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BV_{f2}} < \boldsymbol{f}_i(\boldsymbol{q})^b + \boldsymbol{f}_i(\boldsymbol{q}). \qquad (22)$$

□

Leveraging the aforementioned Theorem, we are able to establish VaR safety bounds specific to equality constraints. These bounds are characterized by three crucial parameters: the safe probability, the constraints' mean, and the constraints' standard deviation. A detailed representation of this relationship is depicted in Figure 4. Furthermore, we present the CVaR safety bounds pertinent to equality constraints. A detailed elaboration of these bounds is introduced in Theorem 2, providing a comprehensive analysis of safety bounds.

(2) Computing Safety Bounds for Equality Constraints with CVaR on a Manifold:

Theorem 2. *For the first side, safety bound via CVaR:*

$$\begin{aligned}&\mathrm{CVaR}_{\eta}=\mathrm{E}[\boldsymbol{X}\mid \boldsymbol{X}\geq \boldsymbol{\delta}_f]=\boldsymbol{f}_i(\boldsymbol{q})^a+\boldsymbol{\mu}+\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}+\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}\\&\Longrightarrow \boldsymbol{f}_i(\boldsymbol{q})^a+\boldsymbol{\mu}+\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}+\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}\leq \boldsymbol{X}=\mathbf{0}\\&\Longrightarrow \boldsymbol{f}_i(\boldsymbol{q})^a\leq -\boldsymbol{\mu}-\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}+\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}.\end{aligned}\tag{23}$$

The first side-safety bound BC_{f1} on equality stochastic constraint Manifolds via CVaR that considered uncertain areas is given as follows:

$$\boldsymbol{f}_i(\boldsymbol{q})^a+\boldsymbol{f}_i(\boldsymbol{q})\leq \underbrace{-\boldsymbol{\mu}-\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}+\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}+\boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BC_{f1}}.\tag{24}$$

For the second side safety bound via CVaR:

$$\begin{aligned}&\mathrm{CVaR}_{\boldsymbol{\eta}}=\mathrm{E}[\boldsymbol{X}\mid \boldsymbol{X}\leq -\boldsymbol{\delta}_f]\\&=\boldsymbol{f}_i(\boldsymbol{q})^b+\boldsymbol{\mu}-\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}-\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}\\&\Longrightarrow \boldsymbol{f}_i(\boldsymbol{q})^b+\boldsymbol{\mu}-\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}-\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}\leq \boldsymbol{X}=\mathbf{0}\\&\Longrightarrow \boldsymbol{f}_i(\boldsymbol{q})^b\leq -\boldsymbol{\mu}+\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}-\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}.\end{aligned}\tag{25}$$

The second side-safety bound BC_{f2} on equality stochastic constraint manifolds via CVaR that considered uncertain areas is given as follows:

$$\boldsymbol{f}_i(\boldsymbol{q})^b+\boldsymbol{f}_i(\boldsymbol{q})\leq \underbrace{-\boldsymbol{\mu}+\boldsymbol{\sigma}\frac{\phi\left[\Phi^{-1}(\frac{\mathbf{1}-\boldsymbol{\eta}}{2})\right]}{\frac{\mathbf{1}-\boldsymbol{\eta}}{2}}+\boldsymbol{f}_i(\boldsymbol{q})}_{\text{safety bound } BC_{f2}}.\tag{26}$$

Proof. On the basis of Lemma 2 and Theorem 1, for a random vector $\boldsymbol{X}$ within equality constraints on a manifold, CVaR is denoted as $\mathrm{CVaR}_{\boldsymbol{\delta}_f}(\boldsymbol{X})=\mathrm{E}\left(\boldsymbol{X}\mid \boldsymbol{X}>\boldsymbol{\delta}_f\right)=\int_{\boldsymbol{\delta}_f}^{\infty}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}/(1-F\left(\boldsymbol{\delta}_f\right))$, and $\boldsymbol{\delta}_f=\mathrm{VaR}_{\boldsymbol{\delta_f}}$, and $P\left(\boldsymbol{X}>\boldsymbol{\delta}_f\right)=(1-\boldsymbol{\eta})/2$ [46].

Since $\boldsymbol{X}\sim N(\boldsymbol{\mu},\boldsymbol{\sigma}^2)$, $\boldsymbol{Z}=(\boldsymbol{X}-\boldsymbol{\mu})/\boldsymbol{\sigma}\sim N(\mathbf{0},\mathbf{1})$, the standard normal distribution function Φ specifies $\Phi(\boldsymbol{z})=P(\boldsymbol{Z}\leqslant \boldsymbol{z})$ and $\mathbf{1}-\Phi(\boldsymbol{z})=P(\boldsymbol{Z}>\boldsymbol{z})$.

(A). The first side safety bound via CVaR:

$$\begin{aligned}\int_{\boldsymbol{\delta}_f^a}^{\infty}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}&=\int_{-\infty}^{\infty}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}-\int_{-\infty}^{\boldsymbol{\delta}_f^a}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}\\&=\boldsymbol{\mu}-\int_{-\infty}^{\boldsymbol{\delta}_f^a}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}.\end{aligned}$$

Changing variables with $\boldsymbol{x}=\boldsymbol{\mu}+\boldsymbol{\sigma}\boldsymbol{z}$ and $d\boldsymbol{x}=\boldsymbol{\sigma}d\boldsymbol{z}$. Based on the change of variables, noting that $\phi(\boldsymbol{z})=\boldsymbol{\sigma}f(\boldsymbol{\mu}+\boldsymbol{\sigma}\boldsymbol{z})$, is a PDF which subjects to a Gaussian distribution, we have

$$\begin{aligned}\int_{-\infty}^{\boldsymbol{\delta}_f^a}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}&=\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}(\boldsymbol{\mu}+\boldsymbol{\sigma}\boldsymbol{z})\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}\phi(\boldsymbol{z})d\boldsymbol{z}+\boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}\boldsymbol{z}\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}\Phi\left[\left(\boldsymbol{\delta}_f^a-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]+\boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}\boldsymbol{z}\phi(\boldsymbol{z})d\boldsymbol{z}.\end{aligned}$$

As shown in the above Equations, $\Phi\left[\left(\boldsymbol{\delta}_f^a-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]=\boldsymbol{\eta}+(1-\boldsymbol{\eta})/2=(1+\boldsymbol{\eta})/2$, and the key here is the observation that the standard normal density function satisfies $\boldsymbol{z}\phi(\boldsymbol{z})=-\phi'(\boldsymbol{z})$.

$$\begin{aligned}&\int_{\boldsymbol{\delta}_f^a}^{\infty}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}\\&=\boldsymbol{\mu}-\boldsymbol{\mu}\Phi\left[\left(\boldsymbol{\delta}_f^a-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]-\boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}\boldsymbol{z}\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}-\boldsymbol{\mu}\frac{1+\boldsymbol{\eta}}{2}+\boldsymbol{\sigma}\int_{-\infty}^{(\boldsymbol{\delta}_f^a-\boldsymbol{\mu})/\boldsymbol{\sigma}}\phi'(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})+\boldsymbol{\sigma}\phi\left[\left(\boldsymbol{\delta}_f^a-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]\\&=\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})+\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1+\boldsymbol{\eta}}{2})\right].\end{aligned}$$

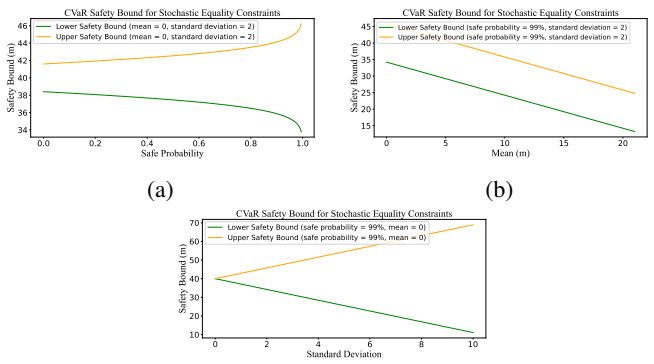
With the above Equations the definition of CVaR (as shown in Definition 2), we can have the following safety bounds,

$$\begin{aligned}\mathrm{CVaR}_{\boldsymbol{\delta}_f^a}(\boldsymbol{X})&=\frac{\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})+\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1+\boldsymbol{\eta}}{2})\right]}{1-F\left(\boldsymbol{\delta}_{\boldsymbol{f}}^{\boldsymbol{a}}\right)}\\&=\frac{\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})+\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1+\boldsymbol{\eta}}{2})\right]}{\frac{1-\boldsymbol{\eta}}{2}}\\&=\boldsymbol{\mu}+\frac{\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1+\boldsymbol{\eta}}{2})\right]}{\frac{1-\boldsymbol{\eta}}{2}}.\end{aligned}$$

(B). The second side safety bound via CVaR:

With proof of the first side CVaR safety bound, we can easily have the second side CVaR safety bound, which is shown as follows:

$$\begin{aligned}&\int_{-\infty}^{-\boldsymbol{\delta}_f^b}\boldsymbol{x}f(\boldsymbol{x})d\boldsymbol{x}=E[\boldsymbol{z}<(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu})/\boldsymbol{\sigma}]\\&=\int_{-\infty}^{(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu})/\boldsymbol{\sigma}}(\boldsymbol{\mu}+\boldsymbol{\sigma}\boldsymbol{z})\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\int_{-\infty}^{(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu})/\boldsymbol{\sigma}}\boldsymbol{\mu}\phi(\boldsymbol{z})d\boldsymbol{z}+\int_{-\infty}^{(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu})/\boldsymbol{\sigma}}(\boldsymbol{\sigma}\boldsymbol{z})\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}\Phi\left[\left(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]+\boldsymbol{\sigma}\int_{-\infty}^{(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu})/\boldsymbol{\sigma}}\boldsymbol{z}\phi(\boldsymbol{z})d\boldsymbol{z}\\&=\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})-\boldsymbol{\sigma}\phi\left[\left(-\boldsymbol{\delta}_f^b-\boldsymbol{\mu}\right)/\boldsymbol{\sigma}\right]\\&=\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2})-\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1-\boldsymbol{\eta}}{2})\right],\end{aligned}$$



(a) (b)

(c)

Fig. 5: CVaR safety bounds on a manifold for equality constraints in terms of safe probability (a), constraints' mean (b), and constraints' standard deviation (c).

$$\begin{aligned}\mathrm{CVaR}_{-\boldsymbol{\delta}_f^b}(\boldsymbol{X}) &= \frac{\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2}) - \boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1-\boldsymbol{\eta}}{2})\right]}{F\left(-\boldsymbol{\delta}_f^b\right)} \\ &= \frac{\boldsymbol{\mu}(\frac{1-\boldsymbol{\eta}}{2}) - \boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1-\boldsymbol{\eta}}{2})\right]}{\frac{1-\boldsymbol{\eta}}{2}} \\ &= \boldsymbol{\mu} - \frac{\boldsymbol{\sigma}\phi\left[\Phi^{-1}(\frac{1-\boldsymbol{\eta}}{2})\right]}{\frac{1-\boldsymbol{\eta}}{2}}.\end{aligned}$$

□

Thus, we can have CVaR safety bound for equality constraints in terms of safe probability, constraints' mean and constraints' standard deviation, as shown in Figure 5.

In the following section, we will introduce a practical algorithm aimed at effectively addressing and managing these stochastic constraints.

C. Practical Algorithm

Building upon the theoretical foundations outlined earlier, we have devised a practical algorithm, as detailed in Algorithm 1, designed to ensure safety in complex environments characterized by stochastic constraints. The algorithm unfolds in three key steps. Initially, stochastic constraints are formulated within the framework of a manifold. Subsequently, safety bounds are computed through the utilization of VaR and CVaR metrics. Finally, the algorithm projects the safe operational space onto the manifold and orchestrates the search for a secure policy that adheres to the stochastic constraint manifold.

Notably, to simplify computation, we leverage Gaussian noises to represent stochastic constraints $\boldsymbol{\epsilon}_i(\boldsymbol{q})$, which can be easily learned via Gaussian processes [47]. As shown in Equation (27), f represents the stochastic constraints that equal stochastic constraints $\boldsymbol{\epsilon}_i(\boldsymbol{q})$ plus deterministic constraints $\boldsymbol{c}_i(\boldsymbol{q})$, and we need to compute f's safety bounds given $\boldsymbol{c}_i(\boldsymbol{q})$ and $\boldsymbol{\epsilon}_i(\boldsymbol{q})$.

$$f = \boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i(\boldsymbol{q}) \quad \boldsymbol{\epsilon}_i(\boldsymbol{q}) \sim \mathcal{N}\left(0, \sigma_n^2\right). \tag{27}$$

The stochastic constraints are assumed as independent, and the constraints are subject to independent distributions.

Algorithm 1 Searching a **RO**bust **S**afe Policy on a Stochastic **CO**nstraint **M**anifold (ROSCOM)

1: Input stochastic constraints $\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i$.
2: Initialise a policy.
3: **for** $k = 0, 1, \ldots, T$ **do**
4: Compute the stochastic constraints $\boldsymbol{c}_i(\boldsymbol{q}) + \boldsymbol{\epsilon}_i$ at each step.
5: Compute the VaR and CVaR bounds for high dimensional inequality and equality constraints.
6: Project the safety bounds into the manifold space $\boldsymbol{c}(\boldsymbol{q}, \boldsymbol{\mu})$.
7: Compute the Jacobian matrix $\boldsymbol{J}_i(\boldsymbol{q}, \boldsymbol{\mu}_s) = \left[\frac{\partial}{\partial \boldsymbol{q}}\overline{\boldsymbol{J}}_i(\boldsymbol{q}, \boldsymbol{\mu}_s)^\top, \frac{\partial}{\partial \boldsymbol{\mu}}\overline{\boldsymbol{J}}_i(\boldsymbol{q}, \boldsymbol{\mu}_s)^\top\right] \in \mathbb{R}^{(n+N)\times N}$.
8: Compute the null space $\boldsymbol{N}(\boldsymbol{q}, \boldsymbol{\mu}_s)$.
9: Sampling trajectories on a tangent space of a constrained manifold with RL algorithms.
10: Compute action $\boldsymbol{a}_k = \Lambda\left(\ddot{\boldsymbol{q}}_k\right)$ based on ATACOM.
11: Deploy action $\boldsymbol{a}_k$ in the environment and provide the reward and observation to the RL algorithm.
12: **end for**

V. Experiments

In this section, we conduct a series of experiments with the primary objective of evaluating the effectiveness of our proposed method. Furthermore, we undertake a comparative analysis to assess the performance of our approach in relation to existing SOTA safe RL baselines.

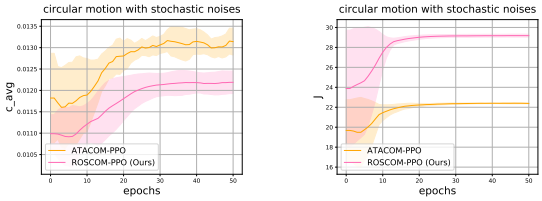
Specifically, we first compare our method with ATACOM [1] on circular motion tasks. Furthermore, to comprehensively evaluate the effectiveness of our methods, we compare our method with ATACOM and traditional CMDP algorithms on challenging air-hockey tasks. Generally, ATACOM requires constraint information, which is leveraged to guarantee safety most rigorously. For example, the constraint information is human posture in a human-robot interaction environment. However, traditional CMDP algorithms do not require constraint information, and they ensure safety by try-and-error learning, which could be helpful in uncritical safety environments. The representative SOTA algorithms of traditional CMDP settings are CPO [2], PCPO [3], and so on.

The environment settings are provided in Appendix VII-A and details of implementation are introduced in Appendix VII-B

A. Circular Motion Tasks

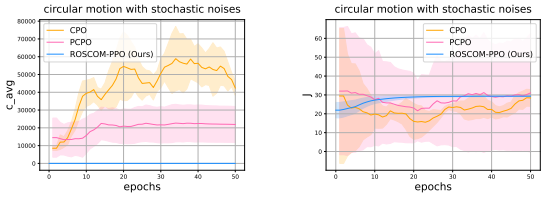
In the circular motion task, a robot must run on the blue circle as shown in Figure 6. If the robot runs away from the circle, it will incur a cost. However, the constraint is stochastic. The blue circle denotes the original constraint, the blue points denote the stochastic constraints, and the two green circles denote the safety bounds via VaR, the two red circles represent the safety bounds via CVaR for the new constraints.

1) Compare with ATACOM: The experimental results are presented in Figures 7 (a) and (b), where c_{avg} denotes the average cost of each trajectory, J denotes the reward performance, ROSCOM-PPO and ATACOM-PPO [1] denote



(a) Safety Performance (b) Reward Performance

Fig. 7: Compare our method with ATACOM [1] on a circular motion task regarding safety (lower values signify superior performance) and reward (higher values indicate better performance) performance.



(a) Safety Performance (b) Reward Performance

Fig. 8: Compare our method with traditional CMDP methods, CPO [2] and PCPO [3], on a circular motion task regarding safety and reward performance.

our ROSCOM with PPO methods [48], and ATACOM with PPO methods. Although the ATACOM method presents remarkable performance for ensuring robot learning safety, a comparative analysis of experimental outcomes suggests that our proposed methodology outperforms ATACOM. More precisely, the proposed method demonstrates superior reward and enhanced safety performance while taking into consideration the stochastic constraints.

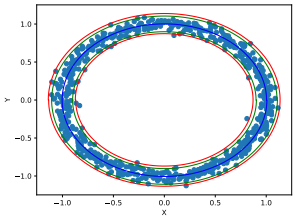


Fig. 6: Safety bounds on a stochastic constraint manifold. The green and red circles denote the safety bounds via VaR and CVaR. In stochastic constraints with Gaussian parameters, the mean is 0, the standard deviation is 0.05, and the safety probability is 99%.

2) Compare with Traditional CMDP Algorithms: In Figure 8, we present the results of comparison experiments focused on tasks involving circular motion. Specifically, as depicted in Figure 8(a), our proposed method not only maintains rigorous safety standards but also significantly outperforms traditional safe RL baselines, including representative baselines CPO [2] and PCPO [3]. These baselines fail to consistently ensure safety during the learning process. Further, Figure 8(b) illustrates that our method achieves performance comparable to that of the safe RL baselines. These experimental results demonstrate that our approach consistently surpasses traditional safe RL baselines in terms of the balance between safety and reward performance, indicating its efficacy and reliability in safe RL applications.

B. Air-Hockey Tasks

In the Air-Hockey task, as shown in Figure 9, the robot needs to learn to manipulate its hand and hit a lightweight plastic puck to score goals. However, due to noises, e.g., sensor measurement errors, the table height estimation by sensors can vary randomly. To prevent the robot from colliding with the table and causing damage to the robot and the table, we need to compute safety bounds for robot learning, so that the robot can complete the task safely, even with stochastic constraints.

1) Compare with ATACOM: As depicted in Figure 10, we compare our method with ATACOM, the experimental results demonstrate that our method is better than ATACOM in terms of safety and reward performance, e.g., the average cost value of trajectories is lower than ATACOM (Figure 10 (a)), and reward value is higher than ATACOM (Figure 10 (b)). The results indicate that our method can be more rigorous than ATACOM to ensure safety for critical applications.

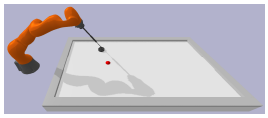


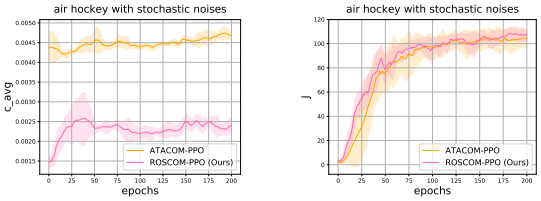
Fig. 9: An Air-Hockey task environment.

2) Compare with Traditional CMDP Algorithms: In order to provide a comprehensive evaluation of the efficacy of our proposed method, we extend our assessment by conducting comparative experiments. Specifically, we compare our method with SOTA representative safe RL baselines, including CPO [2] and PCPO [3].

The evaluation results, as depicted in Figure 11, reveal the remarkable superiority of our method in comparison to SOTA baselines regarding safety and reward performance. Firstly, our method exhibits significantly improved safety performance, as evidenced by the average cost values of each trajectory, as illustrated in Figure 11 (a). Secondly, in terms of reward performance, our approach outperforms the strong baselines, as demonstrated by Figures 11 (b) and (c), with Figure 11 (c) providing an enlarged view of Figure 11 (b) in terms of SOTA baselines' reward performance. Our methodology's capability to achieve superior outcomes is clearly demonstrated, showing its potential for robust and safe RL real-world applications.

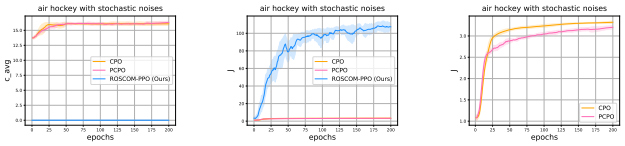
The distinct superiority of our method over traditional algorithms can be attributed to several key elements integrated within our approach. Firstly, the constrained space is leveraged to construct a constrained manifold, a feature that proves to be instrumental in facilitating efficient high-dimensional learning. Secondly, the tangent space of the constrained manifold is explicitly established for policy searching. It provides a rigorous safety assurance mechanism within the policy search process. By operating within the tangent space, the policy search is inherently aligned with safety protocols, ensuring that each iteration adheres to safety constraints.

These key points collectively contribute to the significant performance improvement of our method, positioning it as



(a) Safety Performance (b) Reward Performance

Fig. 10: Compare our method with ATACOM [1] on the Air-Hockey task.



(a) (b) (c)

Fig. 11: Compare our method with traditional CMDP methods, CPO [2] and PCPO [3], on the Air-Hockey task. Figure (a) shows the safety performance, Figures (b) and (c) show the reward performance.

a notably better solution than traditional algorithms, and promising enhanced safety and efficiency in complex, high-dimensional learning environments.

Influence of Safety Bounds on Reward Performance: (1) In our experiments, the safety bound significantly reduces learning oscillations during policy search, enhancing overall policy performance. For example, in the circular motion task, the state space's stochastic noise can lead to policy oscillations in the baseline algorithm such as ATACOM, subsequently degrading policy performance. Similar effects are observed in air hockey tasks. Unlike these methods, our approach establishes a stable safety bound that accommodates the uncertainty of the state space. This allows for more effective policy exploration than baseline methods, thereby improving safety and reward performance. (2) Compared to traditional safe RL methods, our approach is developed on constrained manifolds. This design facilitates safe exploration within the tangent space and guides the policy toward a higher-quality outcome. Consequently, our method achieves superior safety and reward performance relative to traditional approaches.

VI. Conclusion

In this paper, we investigated the problem of robust safe RL on stochastic constraint manifolds. Prior safe RL research has focused on deterministic constraints, whereas in this paper we considered stochastic constraints. First, we formulated the robust safe RL problem by considering the stochastic constraints. Second, we ensured safety by leveraging the risk measurement methods, e.g., VaR and CVaR. Safety bounds are computed on the stochastic constraint manifold to help search for a safe policy. Finally, we evaluated our method on the circular motion and Air-Hockey tasks. The experiment results demonstrate that our algorithm can achieve remarkable performance in terms of learning safety, and show better reward performance than the SOTA baselines. In the Future, we plan to investigate the model's efficiency and try to deploy our method in real-world robot control.

Acknowledgments

We thank Dr. Davide Tateo for his helpful discussions.

Appendix

VII. Details of Experiments

A. Environment Settings

Circle Motion Environments. In this task, the robot needs to run as fast as possible to reach the goal position while satisfying safety constraints. As shown in the following equations, $R(X_t, Y_t)$ denotes the reward value when the robot is at position (X_t, Y_t), X_t denotes the robot X-axis direction position and Y_t denotes its Y-axis direction position, similarly, (X_g, Y_g) denotes the goal position, ϵ denotes the stochastic constraints, and $C_{inequality}$ denotes the inequality constraints. other settings are similar to ATACOM [1].

$$R(X_t, Y_t) = \exp(-\sqrt{(X_t - X_g)^2 + (Y_t - Y_g)^2}) \tag{28}$$

$$C(X_t, Y_t) = |\sqrt{X_t^2 + Y_t^2} - (1 + \epsilon)| + C_{inequality} \tag{29}$$

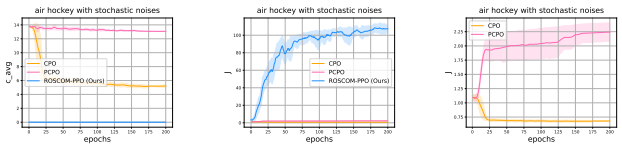
$$C_{inequality} = \begin{cases} |Y_t + 0.5 + \epsilon|, & Y_t < -(0.5 + \epsilon), \\ 0, & Others. \end{cases} \tag{30}$$

Air-Hockey Environments.

Other reward and constraint settings of the task are same to ATACOM [1], except for Equation (31), Z_{table} denotes the table height, Z_t denotes the robot Z-axis direction position, $puck$ height is 0.0149m. We provide more experiments to evaluate the effectiveness of our method regarding the different safety limits, as shown in Figure 12, the experiment results indicate that our method can perform remarkably better than SOTA safe RL baselines regarding reward and safety performance, and confirm the effectiveness of our method again. The implementation of CPO and PCPO from a repository of safe RL baselines [1] is used to carry out the comparison experiments.

Our method outperforms the SOTA safe RL baselines because the safety constraints are learned and projected on a Manifold space, which means our algorithm can receive the safety and task environment information in advance, which could help our method better search policy while satisfying safety constraints.

$$C_{inequality} = \begin{cases} |Z_t - (Z_{table} + \epsilon)|, & Z_t < (Z_{table} + \epsilon), \\ 0, & Others. \end{cases} \tag{31}$$



(a) (b) (c)

Fig. 12: Compare our method with traditional CMDP methods, CPO [2] and PCPO [3], on the Air-Hockey task with different safety bounds. Figure (a) shows the safety performance, Figures (b) and (c) show the reward performance.

Parameters	value	Parameters	value
actor lr	3e-4	critic lr	3e-4
batch size	64	gamma	0.99
horizon	500	epoch	50
eps ppo	0.1	noise ϵ mean	0
η	99%	noise ϵ std	0.5
network	MLP	regular	relu & linear
NN features	[32, 32]		

TABLE I: ROSCOM and ATACOM hyparameters used in Circle Motion experiments.

Parameters	value	Parameters	value
actor lr	3e-4	critic lr	3e-4
batch size	64	gamma	0.99
horizon	3000	epoch	200
eps ppo	0.1	noise ϵ mean	0
η	99%	noise ϵ std	0.5
network	MLP	regular	relu & linear
NN features	[64, 64]		

TABLE II: Algorithms' hyparameters of ROSCOM, ATACOM, CPO, PCPO, used in Air-Hockey experiments. Safety bound δ used for CPO and PCPO in Figures 8 and 11 is 25, and in Figure 12 is 5.

B. Details of Implementing Experiments

The parameters used in our experiments are provided in Tables I and II.

REFERENCES

[1] P. Liu, D. Tateo, H. B. Ammar, and J. Peters, "Robot reinforcement learning on the constraint manifold," in *Conference on Robot Learning*. PMLR, 2022, pp. 1357–1366.

[2] J. Achiam, D. Held, A. Tamar, and P. Abbeel, "Constrained policy optimization," in *International conference on machine learning*. PMLR, 2017, pp. 22–31.

[3] T.-Y. Yang, J. Rosca, K. Narasimhan, and P. J. Ramadge, "Projection-based constrained policy optimization," in *International Conference on Learning Representations*, 2020.

[4] S. Gu, L. Yang, Y. Du, G. Chen, F. Walter, J. Wang, Y. Yang, and A. Knoll, "A review of safe reinforcement learning: Methods, theory and applications," *arXiv preprint arXiv:2205.10330*, 2022.

[5] J. Yang, J. Ni, M. Xi, J. Wen, and Y. Li, "Intelligent path planning of underwater robot based on reinforcement learning," *IEEE Transactions on Automation Science and Engineering*, 2022.

[6] D. Silver, A. Huang, C. J. Maddison, A. Guez, L. Sifre, G. Van Den Driessche, J. Schrittwieser, I. Antonoglou, V. Panneershelvam, M. Lanctot *et al.*, "Mastering the game of go with deep neural networks and tree search," *nature*, vol. 529, no. 7587, pp. 484–489, 2016.

[1]https://github.com/PKU-Alignment/Safe-Policy-Optimization.git

[7] N. Abe, P. Melville, C. Pendus, C. K. Reddy, D. L. Jensen, V. P. Thomas, J. J. Bennett, G. F. Anderson, B. R. Cooley, M. Kowalczyk *et al.*, "Optimizing debt collections using constrained reinforcement learning," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2010, pp. 75–84.

[8] S. Gu, J. G. Kuba, Y. Chen, Y. Du, L. Yang, A. Knoll, and Y. Yang, "Safe multi-agent reinforcement learning for multi-robot control," *Artificial Intelligence*, vol. 319, p. 103905, 2023.

[9] S. Gu, D. Huang, M. Wen, G. Chen, and A. Knoll, "Safe multi-agent learning with soft constrained policy optimization in real robot control," *IEEE Transactions on Industrial Informatics*, 2024.

[10] S. Gu, G. Chen, L. Zhang, J. Hou, Y. Hu, and A. Knoll, "Constrained reinforcement learning for vehicle motion planning with topological reachability analysis," *Robotics*, vol. 11, no. 4, p. 81, 2022.

[11] C. Tessler, D. J. Mankowitz, and S. Mannor, "Reward constrained policy optimization," in *International Conference on Learning Representations*, 2018.

[12] J. B. Tenenbaum, V. d. Silva, and J. C. Langford, "A global geometric framework for nonlinear dimensionality reduction," *science*, vol. 290, no. 5500, pp. 2319–2323, 2000.

[13] E. S. Gastal and M. M. Oliveira, "Adaptive manifolds for real-time high-dimensional filtering," *ACM Transactions on Graphics (TOG)*, vol. 31, no. 4, pp. 1–13, 2012.

[14] A. J. Izenman, "Introduction to manifold learning," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 4, no. 5, pp. 439–446, 2012.

[15] Y. Chow, A. Tamar, S. Mannor, and M. Pavone, "Risk-sensitive and robust decision-making: a cvar optimization approach," *Advances in neural information processing systems*, vol. 28, 2015.

[16] C. Ying, X. Zhou, D. Yan, and J. Zhu, "Towards safe reinforcement learning via constraining conditional value at risk," in *ICML 2021 Workshop on Adversarial Machine Learning*, 2021.

[17] S. Gu, A. Kshirsagar, Y. Du, G. Chen, J. Peters, and A. Knoll, "A human-centered safe robot reinforcement learning framework with interactive behaviors," *Frontiers in Neurorobotics*, vol. 17, 2023.

[18] Z. Liu, Z. Guo, Z. Cen, H. Zhang, J. Tan, B. Li, and D. Zhao, "On the robustness of safe reinforcement learning under observational perturbations," *ICLR*, 2023.

[19] M. Turchetta, F. Berkenkamp, and A. Krause, "Safe exploration in finite markov decision processes with gaussian processes," *Advances in Neural Information Processing Systems*, vol. 29, 2016.

[20] F. Berkenkamp and A. P. Schoellig, "Safe and robust learning control with gaussian processes," in *2015 European Control Conference (ECC)*. IEEE, 2015, pp. 2496–2501.

[21] Y. Sui, A. Gotovos, J. Burdick, and A. Krause, "Safe exploration for optimization with gaussian processes," in *International conference on machine learning*. PMLR, 2015, pp. 997–1005.

[22] A. Wachi, Y. Sui, Y. Yue, and M. Ono, "Safe exploration and optimization of constrained mdps using gaussian processes," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, no. 1, 2018.

[23] Y. Chow, O. Nachum, E. Duenez-Guzman, and M. Ghavamzadeh, "A lyapunov-based approach to safe reinforcement learning," *Advances in neural information processing systems*, vol. 31, 2018.

[24] Y. Chow, O. Nachum, A. Faust, E. Duenez-Guzman, and M. Ghavamzadeh, "Lyapunov-based safe policy optimization for continuous control," *arXiv preprint arXiv:1901.10031*, 2019.

[25] T. Koller, F. Berkenkamp, M. Turchetta, and A. Krause, "Learning-based model predictive control for safe exploration," in *2018 IEEE conference on decision and control (CDC)*. IEEE, 2018, pp. 6059–6066.

[26] X. Li and C. Belta, "Temporal logic guided safe reinforcement learning using control barrier functions," *arXiv preprint arXiv:1903.09885*, 2019.

[27] Z. Marvi and B. Kiumarsi, "Safe reinforcement learning: A control barrier function optimization approach," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 6, pp. 1923–1940, 2021.

[28] N. Fulton and A. Platzer, "Safe reinforcement learning via formal methods: Toward safe control through proof and learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, no. 1, 2018.

[29] X. Liang, K. Shu, K. Lee, and P. Abbeel, "Reward uncertainty for exploration in preference-based reinforcement learning," in *International Conference on Learning Representations*.

[30] K. Li, A. Gupta, A. Reddy, V. H. Pong, A. Zhou, J. Yu, and S. Levine, "Mural: Meta-learning uncertainty-aware rewards for outcome-driven reinforcement learning," in *International conference on machine learning*. PMLR, 2021, pp. 6346–6356.

[31] K. Chua, R. Calandra, R. McAllister, and S. Levine, "Deep reinforcement learning in a handful of trials using probabilistic dynamics models," *Advances in neural information processing systems*, vol. 31, 2018.

[32] K. Zhang, T. Sun, Y. Tao, S. Genc, S. Mallya, and T. Basar, "Robust multi-agent reinforcement learning with model uncertainty," *Advances in neural information processing systems*, vol. 33, pp. 10 571–10 583, 2020.
[33] M. Rigter, B. Lacerda, and N. Hawes, "Rambo-rl: Robust adversarial model-based offline reinforcement learning," in *Advances in Neural Information Processing Systems*.
[34] C. Diehl, T. Sievernich, M. Krüger, F. Hoffmann, and T. Bertran, "Umbrella: Uncertainty-aware model-based offline reinforcement learning leveraging planning," *arXiv preprint arXiv:2111.11097*, 2021.
[35] A. Nilim and L. El Ghaoui, "Robust control of markov decision processes with uncertain transition matrices," *Operations Research*, vol. 53, no. 5, pp. 780–798, 2005.
[36] S. H. Lim, H. Xu, and S. Mannor, "Reinforcement learning in robust markov decision processes," *Advances in Neural Information Processing Systems*, vol. 26, 2013.
[37] Z.-k. Lou, F.-j. Hou, and X.-m. Lou, "Robust analysis of discounted markov decision processes with uncertain transition probabilities," *Applied Mathematics-A Journal of Chinese Universities*, vol. 35, no. 4, pp. 417–436, 2020.
[38] J.-T. Chien, W.-L. Liao, and I. El Naqa, "Exploring state transition uncertainty in variational reinforcement learning," in *2020 28th European Signal Processing Conference (EUSIPCO)*. IEEE, 2021, pp. 1527–1531.
[39] B. Lütjens, M. Everett, and J. P. How, "Certified adversarial robustness for deep reinforcement learning," in *Conference on Robot Learning*. PMLR, 2020, pp. 1328–1337.
[40] D. Wang, T. Fan, T. Han, and J. Pan, "A two-stage reinforcement learning approach for multi-uav collision avoidance under imperfect sensing," *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 3098–3105, 2020.
[41] H. Zhang, H. Chen, C. Xiao, B. Li, M. Liu, D. Boning, and C.-J. Hsieh, "Robust deep reinforcement learning against adversarial perturbations on state observations," *Advances in Neural Information Processing Systems*, vol. 33, pp. 21 024–21 037, 2020.
[42] A. Gleave, M. Dennis, N. Kant, C. Wild, S. Levine, and S. Russsell, "Adversarial policies: Attacking deep reinforcement learning," *In Proc. ICLR-20*, 2020.
[43] H. Zhang, H. Chen, D. Boning, and C.-J. Hsieh, "Robust reinforcement learning on state observations with learned optimal adversary," in *International Conference on Learning Representation (ICLR)*, 2021.
[44] R. Singh and P. Likins, "Singular value decomposition for constrained dynamical systems," *Journal of Applied Mechanics*, vol. 52, no. 4, p. 943, 1985.
[45] S. Kim and M. Vanderploeg, "Qr decomposition for state space representation of constrained mechanical dynamic systems1," *Journal of Mechanisms, Transmissions, and Automation in Design*, vol. 108, p. 183, 1986.
[46] M. Norton, V. Khokhlov, and S. Uryasev, "Calculating cvar and bpoe for common probability distributions with application to portfolio optimization and density estimation," *Annals of Operations Research*, vol. 299, no. 1, pp. 1281–1315, 2021.
[47] C. K. Williams and C. E. Rasmussen, *Gaussian processes for machine learning*. MIT press Cambridge, MA, 2006, vol. 2, no. 3.
[48] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," *arXiv preprint arXiv:1707.06347*, 2017.

Shangding Gu is currently pursuing the Ph.D. degree in computer science at Technical University of Munich (TUM), Munich, Germany, and he is a member of the Informatics 6-Chair of Robotics, Artificial Intelligence and Real-time Systems, TUM. He is one of the organizers of the 1st International Safe Reinforcement Learning Workshop at IEEE MFI 2022. His main research interests include safe reinforcement learning and motion planning.

Puze Liu is pursuing his Ph. D. degree at Intelligent Autonomous Systems Group, Technical University Darmstadt and German Research Center for AI. Prior to this, Puze received his M. Sc. in Computational Engineering from Technical University Berlin and B. Sc from Tongji University, China. Puze's research interest lies in the interdisciplinary field of robot learning that tries to integrate machine learning techniques into robotics. His prior work focuses on optimization, control, reinforcement learning, and safety in robotics.

Alap Kshirsagar is a postdoctoral researcher in the Intelligent Autonomous Systems Group at Technische Universitaet Darmstadt. He received his Ph.D. in Mechanical Engineering at Cornell University, USA, in 2022. Before his Ph.D., he completed a Master's in Mechanical Engineering at the Indian Institute of Technology (IIT) Madras and a Bachelor's in Mechanical Engineering at IIT Bombay. His research interests include human-robot interaction, robot learning, and robotic manipulation.

Guang Chen is a professor at Tongji University and a senior research associate (guest) at Technical University of Munich. His research interests include 3D vision, intelligent robotics and autonomous driving. He was awarded the program of Shanghai Rising Star 2021, and Shanghai S&T 35U35 2021, the National Distinguished Young Talents 2023. He serves as an Associate Editor for several international journals. He is the program chair of IEEE MFI 2022.

Jan Peters is a full professor (W3) for Intelligent Autonomous Systems at the Computer Science Department of the Technische Universitaet Darmstadt. Jan Peters has received the Dick Volz Best 2007 US Ph.D. Thesis Runner-Up Award, the Robotics: Science & Systems - Early Career Spotlight, the INNS Young Investigator Award, and the IEEE Robotics & Automation Society's Early Career Award as well as numerous best paper awards. In 2015, he received an ERC Starting Grant and in 2019, he was appointed as an IEEE Fellow.

Alois Knoll is a professor at the Department of Informatics, TU Munich (TUM). From 2004 to 2006, he was Executive Director of the Institute of Computer Science at TUM. He was also on the board of directors of the Central Institute of Medical Technology at TUM. His research interests include cognitive, and sensor-based robotics, multi-agent systems, data fusion, adaptive systems, multimedia information retrieval, and model-driven development of embedded systems.