2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Formal Verification of Attitude Control Systems Using Geometric Barrier Functions

Chencheng Xu, Chengcheng Zhao, Zhiguo Shi and Jiming Chen

Abstract— **Compared to safe obstacle avoidance in the position space, ensuring the safety of the attitude system in today's aerial vehicle operations is more challenging due to the non-Euclidean nature of the attitude space and the underactuated nature of the system. To address this issue, we first propose the geometric exponential barrier condition (GEBC) to produce barrier certificates on the manifold, by which attitude safety requirements can be encoded globally into the verification problems of attitude control systems. Then, we use exponential coordinates to characterize GEBCs, which makes them describable in terms of quantifier-free real arithmetic logic (QF-NRA) and efficiently solvable by current satisfiability modulo theories (SMT) solvers. A performance criterion is further discussed where we propose an effective algorithm to construct safe operational regions with different controllers, which can help with nominal controller selection and tuning. Finally, we demonstrate our approach in a quadrotor system and analyze the safe performance of two PD controllers on the proposed safe operation criterion.**

I. INTRODUCTION

Safety is a critical problem in today's aerial vehicle (AV) systems. An efficient tool to integrate safety requirements into system constraints is barrier function (BF) [1], which guarantees safety by proving its forward invariance of a given safe set. BF has been successfully extended to the control literature, leading to the development of control barrier function (CBF) theory [2]. Although many innovative works have been conducted in AV's CBF-based safe controller design [3], [4], we have observed that most of these works construct their barrier functions in the position space. They typically treat the AV rigid body as a mass point and introduce scenario-related CBFs based on its position and velocity states. Control signals are then computed by solving online quadratic program (CBF-QP) problems, thus avoiding collisions with obstacles or other AVs.

On the other hand, it is important to note that attitude safety problems also exist in AV systems. For instance, the angle of attack constraint is a critical factor that prevents loss-of-control (LOC) by guaranteeing the amount of lift generated by AVs. Additionally, attitude requirements such as line-of-sight constraints [5] and keep-out cones [6] are essential for AV's active vision and effective wireless communication. Directly adapting CBF-based methods from position space to attitude space can be challenging since attitude space is non-Euclidean and is expressed by the rotation matrix group SO(3). Although linearization methods can be used to locally describe attitude dynamics, and formal guarantees can then be formulated using Euclidean CBFs [7], it is more practical to construct CBFs in a geometric and global way. In [8], safety constraints on SO(3) are discussed and a group of Gaussian CBFs is proposed to encode safe regions in attitude space. By solving QP problems with Gaussian CBF constraints, safe-enforced moment signals are generated to control the attitude system of a quadrotor.

It is worth noting that to address all the safety concerns discussed above, both Euclidean position constraints and non-Euclidean attitude constraints must be incorporated into the CBF-QP controllers of the attitude system, as most AVs are underactuated. For instance, in the widely used cascaded control framework for quadrotors [3], [9], the attitude control system serves as a subsystem or a low-level control system, and the attitude control signals are used for achieving precise translational motion. Thus, safety requirements for translational distance need to be enforced as additional constraints in the orientation domain. This results in the emergence of multi-domain CBF conditions in attitude, which not only increases the complexity of the CBF-QP problems but also necessitates the guarantee of feasible solutions. One effective way to improve the existence and performance of multi-constraint feasible solutions is to increase the feasible solution regions under each constraint. Due to the complex variability of position safety constraints in various scenarios, the feasible solution regions under attitude conditions are more suitable for analysis and applicable to be enlarged.

To solve the above issue, we first propose a formal verification framework to construct operational regions for nominal controllers under attitude CBF conditions. To further explore how the selection of nominal attitude controllers affects the region of feasible solutions, a safe-operation envelope is designed to compare the performance of different controllers. The proposed method effectively deals with the feasibility issue in a verification way and also provides a new baseline for tuning and evaluating nominal controllers in CBF-QP. To the best of our knowledge, this is the first work that discusses the Multi-domain CBF conditions in attitude.

This work was supported in part by the National Natural Science Foundation of China under Grant 62273305, in part by the Zhejiang Provincial Natural Science Foundation under Grant LZ22F030010, in part by the Young Elite Scientist Sponsorship Program by cast of China Association for Science and Technology under Grant YESS20210158 and in part by the State Key Laboratory of Industrial Control Technology under Grant ICT2023A03.

Chencheng Xu is with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China. Chengcheng Zhao and Jiming Chen are with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, 310027, China. Zhiguo Shi is with the Key Laboratory of Collaborative Sensing and Autonomous Unmanned Systems of Zhejiang Province and Interdisciplinary Motion Dynamics Emulation Platform, Zhejiang University, Hangzhou 310027, China. Emails: {xucc, chengchengzhao, cjm, shizg}@zju.edu.cn

The main contributions are listed as follows.

- Geometric exponential barrier condition (GEBC) is proposed to produce barrier certificates on the manifold, by which attitude safety requirements can be encoded globally into the verification problems of attitude control systems.
- We propose an innovative and practical verification framework for attitude controllers. A class of geometric barrier functions is introduced and formally transformed based on matrix exponential coordinates. The resultant verification problems are then presented in Quantifier Free Real Arithmetic Logic, which could be handled by current SMT solvers.
- A performance criterion is designed based on the safe operational regions generated by the verification process. This performance criterion is graphically represented as a safe flight envelope (SFE), which can help with the selection and fine-tuning of nominal controllers.

The remainder of this paper is organized as follows. Section II introduces some basic concepts of safe control, formal verification, and attitude control systems. Section III presents the methods we adopt to formally verify and generate feasible regions for attitude controllers under attitude constraints. Section IV presents an example case where we compare the performance of two PD controllers based on the generated safe flight envelope.

II. PRELIMINARIES AND PROBLEM FORMULATION

A. Safety and Control Barrier Functions

Consider a control affine dynamic system

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + g(\boldsymbol{x})\boldsymbol{u}, \tag{1}$$

where system state $\boldsymbol{x} = \boldsymbol{x}(t) \in \mathcal{X} \subset \mathbb{R}^n$ and control signal $\boldsymbol{u} = \boldsymbol{u}(t) \in \mathcal{U} \subset \mathbb{R}^m$ are denoted with respect to time $t \geq 0$. The functions $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g : \mathbb{R}^n \to \mathbb{R}^{n\times m}$ are assumed to be Lipschitz continuous.

A safe set in state space $\mathcal{B}$ could be encoded as the zero super-level set of a smooth function $B : \mathcal{X} \subset \mathbb{R}^n \to \mathbb{R}$:

$$\mathcal{B} = \{\boldsymbol{x} \in \mathcal{X} \mid B(\boldsymbol{x}) \geq 0\},$$
$$\partial\mathcal{B} = \{\boldsymbol{x} \in \mathcal{X} \mid B(\boldsymbol{x}) = 0\}.$$

If the safe set is forward invariant, i.e., for any $\boldsymbol{x}(0) \in \mathcal{B}$, $\boldsymbol{x}(t) \in \mathcal{B}$ holds for all $t \geq 0$, then the system is guaranteed to be safe with respect to $\mathcal{B}$. The smooth function B is called barrier function.

Definition 1. (Exponential Control Barrier Function [10]) *Given a control affine system (1) with a safe set $\mathcal{B} = \{\boldsymbol{x} \in \mathcal{X} \mid B(\boldsymbol{x}) \geq 0\}$, which is the super-level set of a smooth function $B : \mathcal{X} \to \mathbb{R}$ with relative degree r, B is an exponential control barrier function if there exists $\boldsymbol{\lambda} \in \mathbb{R}^r$ such that for all $\boldsymbol{x} \in \mathcal{X}$,*

$$\sup_{\boldsymbol{u}\in\mathcal{U}} (L_f^r B(\boldsymbol{x}) + L_g L_f^{r-1} B(\boldsymbol{x})\boldsymbol{u} + \boldsymbol{\lambda}^\top \boldsymbol{\eta}_B) \geq 0, \tag{2}$$

where $\boldsymbol{\eta}_B = [B(\boldsymbol{x}), L_f B(\boldsymbol{x}), \ldots, L_f^{r-1} B(\boldsymbol{x})]^\top$ is a vector of Lie derivatives and the vector $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_r]^\top$ contains the coefficients selected to guarantee forward invariance of ECBF.

Then, we can define a control set that ensures safety with respect to a given state $\boldsymbol{x}$:

$$\mathcal{U}_s(\boldsymbol{x}) = \left\{\boldsymbol{u} \in \mathcal{U} \mid L_f^r B + L_g L_f^{r-1} B\boldsymbol{u} + \boldsymbol{\lambda}^\top \boldsymbol{\eta}_B \geq 0\right\}. \tag{3}$$

Remark 1. The safe control set $\mathcal{U}_s$ here is exactly the feasible solution region of control systems with a single CBF condition. It is evident that as the size of this set increases, there are more available choices for feasible control signals with safe guarantees.

B. Formal Verification using Barrier Certificates

The basic idea of safe verification is to verify that all possible states that a given system can reach starting from an initial set never enter the unsafe region. Although various excellent methods and tools have been developed recently to solve the reachability problem in Euclidean space fast and effectively [11], [12], it remains challenging to conduct non-Euclidean reachability analysis. On the other hand, formal verification methods based on barrier certificates avoid explicit computation of the exact or substantially approximate reachable set [13]. Therefore, we use barrier certificates to verify safety properties in the attitude space.

Lemma 1. (Barrier Condition) Given a system (1) with the state space set $\mathcal{X}$, an initial set Ξ, and an unsafe set $\mathcal{X}_{\text{unsafe}}$, if a smooth barrier function $B : \mathcal{X} \to \mathbb{R}$ satisfies:

$$B(\boldsymbol{x}) < 0, \quad \forall \boldsymbol{x} \in \mathcal{X}_{\text{unsafe}} \tag{4}$$
$$B(\boldsymbol{x}) \geq 0, \quad \forall \boldsymbol{x} \in \Xi \tag{5}$$
$$\dot{B}(\boldsymbol{x}) \geq 0, \quad \forall \boldsymbol{x} \in \partial\mathcal{B} \tag{6}$$

then the safety of the system (1) is guaranteed.

The original barrier conditions give the basic condition that a barrier function should satisfy to render safety. However, condition (6) is non-convex, meaning the problem cannot be solved using convex optimization [14]. Exponential barrier conditions [15] are then proposed where condition (6) is replaced by

$$\dot{B}(\boldsymbol{x}) + \lambda B(\boldsymbol{x}) \geq 0, \quad \forall \boldsymbol{x} \in \mathcal{X}, \tag{7}$$

so that barrier functions can be searched by sum-of-squares (SOS) programming.

C. Attitude Control Systems on SO(3)

Since the attitude space is non-Euclidean, it's better to handle attitude systems in a geometric way [16], [17]. We begin with some basic ideas on Riemannian geometry. Given a smooth manifold Q, the Riemannian metric is an inner product $\|\cdot,\cdot\|_p : T_pQ \times T_pQ \to \mathbb{R}$ on the tangent space T_pQ of any point $p \in Q$. It can also be expressed as a symmetric positive linear operator J_p: $T_pQ \to T_p^*Q$,

satisfying $\|X, X\|_p = \|X_p, X_p\|_p = \langle J_p X_p, X_p \rangle$, where $X_p \in T_p Q$ and $J_p X_p \in T_p^* Q : T_p Q \to \mathbb{R}$. $J_p X_p$ is a one form in the cotangent space. If $f : Q \to \mathbb{R}$ is a smooth function, its Lie derivative with respect to the vector field X is defined as $\mathcal{L}_X f(p) = \langle df, X_p \rangle$, where df is the gradient of f. The tangent bundle $TQ = \{(p, X_p) \mid p \in Q, X_p \in T_p Q\}$.

The attitude control system can be considered as a geometric mechanical system $(\mathrm{SO}(3), J, \boldsymbol{\tau})$ with the following concepts:

- The rotation group $\mathrm{SO}(3)$ is the configuration manifold.
- J is a Riemannian metric on $\mathrm{SO}(3)$, which represents the inertia of this system and describes kinetic energy.
- $\boldsymbol{\tau} = [\tau_1, \tau_2, \tau_3]^\top$ is a collection of one form that describes torque.

We then specify such a system by introducing an AV rigid body and ignoring its position state. The inertial reference frame $\mathcal{F}_o \triangleq \left\{\mathcal{O}, E_o = [\vec{e}_{o1}, \vec{e}_{o2}, \vec{e}_{o3}]^\top\right\}$ is defined with three right-handed orthonormal basis vectors such that any vector in space can be represented as $\vec{v} = \boldsymbol{v}_o^\top E_o = E_o^\top \boldsymbol{v}_o$, where $\boldsymbol{v}_o \triangleq [v_{o1}, v_{o2}, v_{o3}]^\top$ is a column matrix of the coordinates. Similarly, we have body-fixed coordinate frame $\mathcal{F}_b \triangleq \left\{\mathcal{O}, E_b = [\vec{e}_{b1}, \vec{e}_{b2}, \vec{e}_{b3}]^\top\right\}$ and desired coordinate frame $\mathcal{F}_d \triangleq \left\{\mathcal{O}, E_d = [\vec{e}_{d1}, \vec{e}_{d2}, \vec{e}_{d3}]^\top\right\}$. Note that these three frames share the same origin. Now the coordinate transformation between two frames $\mathcal{F}_o$ and $\mathcal{F}_b$ can be expressed as $\boldsymbol{v}_b = R^\top \boldsymbol{v}_o$, where R is rotation matrix of the rigid body on configuration manifold SO(3). Meanwhile, we have R_d as the desired body attitude.

The attitude dynamics is formulated on the configuration manifold SO(3) and its Lie algebra $\mathfrak{so}(3)$:

$$\dot{R} = R\hat{\Omega}, \tag{8}$$

$$J\dot{\Omega} = J\Omega \times \Omega + \boldsymbol{\tau} + \triangle_R, \tag{9}$$

where $\dot{R} \in T_R\mathrm{SO}(3)$ is the tangent vector at R, and $\Omega = [\omega_1, \omega_2, \omega_3]^\top \in \mathbb{R}^3$ denotes the body angular velocity. We have $\hat{\Omega} \in \mathfrak{so}(3)$ satisfies $\hat{\Omega} x = \Omega \times x$ for all $x \in \mathbb{R}^3$, inducing a isomorphism $\hat{\cdot} : \mathbb{R}^3 \to \mathfrak{so}(3)$. In this paper, we assume that the model uncertainty is bounded by $\triangle_R$.

To measure the difference between R_d and R, a configuration error function $\Phi : \mathrm{SO}(3) \to \mathbb{R}$ is introduced with right attitude error $R_e = R_d^\top R$:

$$\Phi(R) = \frac{1}{2}\mathrm{tr}\left[K_p(I_3 - R_e)\right]. \tag{10}$$

Its first and second-order time derivatives are formulated as

$$\dot{\Phi} = \frac{1}{2}(\Omega - {R_e}^\top \Omega_d)^\top \left[K_p R_e - (K_p R_e)^\top\right]^\vee, \tag{11}$$

$$\begin{aligned}\ddot{\Phi} = {} & \frac{1}{2}\mathrm{tr}(K_p R_e){\Omega_e}^\top \Omega_e - \frac{1}{2}{\Omega_e}^\top K_p R_e \Omega_e \\ & + \frac{1}{2}(\dot{\Omega} + \hat{\Omega}{R_e}^\top \Omega_d - {R_e}^\top \dot{\Omega}_d)^\top \left[K_p R_e - (K_p R_e)^\top\right]^\vee,\end{aligned} \tag{12}$$

where $\cdot^\vee$ is the inverse map of $\hat{\cdot}$ and angular velocity error is defined as $\Omega_e = \Omega - {R_e}^\top \Omega_d$. K_p is a symmetric and positive constant matrix.

D. Problem of Interests

Now we can discuss the feasibility problem in CBF-QP attitude controllers. Suppose we have a nominal controller $\boldsymbol{u}_{\mathrm{nom}}(\boldsymbol{x})$, a multi-domain CBF-QP problem in the attitude system can be formulated as:

Multi-domain CBF-QP:

$$\begin{aligned}\boldsymbol{u}(\boldsymbol{x}) = \underset{\boldsymbol{u}\in\mathcal{U}}{\arg\min} \quad & \frac{1}{2}\left\|\boldsymbol{u} - \boldsymbol{u}_{\mathrm{nom}}(\boldsymbol{x})\right\|^2, \\ \text{s.t.} \quad & L_f^{r_a} B_a + L_g L_f^{r_a - 1} B_a \boldsymbol{u} + \boldsymbol{\lambda_a}^\top \boldsymbol{\eta}_{B_a} \geq 0 \\ & L_f^{r_p} B_p + L_g L_f^{r_p - 1} B_p \boldsymbol{u} + \boldsymbol{\lambda_p}^\top \boldsymbol{\eta}_{B_p} \geq 0\end{aligned}$$

---

where B_a and B_p are the control barrier functions defined in attitude space and position space with relative degree r_a and r_b respectively. $\boldsymbol{x}$ is defined to include both attitude and position states. It is possible that these two CBF constraints conflict with each other, which raises the question of whether feasible solutions exist in the whole state space.

We refer to the feasible solution region that satisfies an individual CBF condition as the *operational region* associated with that safe specification. The QP formulation shows that the operational region for attitude safety, before being modified by QP, pre-defines a viable region for position safety. This operational region indicates the allowable degree of aggression in position space. Generally, a larger operational region for attitude safety enables a larger feasible region for QP and thereby indicates more aggressive flight in position space. In this paper, we aim to improve the feasibility from the aspect of analyzing and enlarging operational regions with attitude safety, and address the following problems:

- How to analyze and visualize the operational regions in the attitude space?
- How to implement these non-Euclidean attitude verification problems based on state-of-the-art numerical solvers?
- How to construct an effective and practical criterion where we can compare the safe performance between controllers?

III. Main Results

A. Geometric Barrier Certificates

To formally analyze the safe property of attitude control systems, we first give the following theorem as barrier-certified conditions on manifolds that incorporate control signals and candidate regions.

Theorem 1. (Geometric Exponential Barrier Condition) *Given a geometric mechanical system $(Q, J, \mathcal{F})$ with a candidate state set $\mathcal{X}_c \subset TQ$ and an unsafe set $\mathcal{X}_{\mathrm{unsafe}}$, if a smooth barrier function B on manifold with relative degree r satisfies:*

$$B(q, \dot{q}) < 0, \quad \forall (q, \dot{q}) \in \mathcal{X}_{\mathrm{unsafe}} \tag{13}$$

$$B(q, \dot{q}) \geq 0, \quad \forall (q, \dot{q}) \in \mathcal{X}_c \tag{14}$$

$$L_f^r B + L_g L_f^{r-1} B \boldsymbol{u} + \boldsymbol{\lambda}^\top \boldsymbol{\eta}_B \geq 0, \quad \forall (q, \dot{q}) \in \mathcal{X}_c \tag{15}$$

where $\boldsymbol{u} = \boldsymbol{u}(q, \dot{q})$ is the control input, then the safety of the controlled system (1) is guaranteed.

Proof. Following [10], we define a family of functions on tangent bundle $y_i : TQ \to \mathbb{R}$, for $i = 1, \ldots, r$, satisfying

$$y_i(q, \dot{q}) = \dot{y}_{i-1}(q, \dot{q}) + \mu_i y_{i-1}(q, \dot{q}),$$

where $\mu_i \geq \max(-\frac{\dot{y}_{i-1}(q,\dot{q})}{y_{i-1}(q,\dot{q})}, \delta)$ and $\delta > 0$ for all states in the state space. The super-level set of y_i is defined as $\mathcal{X}_i = \{(q, \dot{q}) \mid y_i(q, \dot{q}) \geq 0\}$. We obtain $\dot{y}_{i-1} + \mu_i y_{i-1} \geq 0$ holds for all states in $\{\mathcal{X}_c \cap \mathcal{X}_i\}$. Consider the worst case when system state $(q(T_w), \dot{q}(T_w)) \in \{\mathcal{X}_c \cap \mathcal{X}_i \cap \mathcal{X}_{i-1}\}$ reaches the boundary of $\mathcal{X}_{i-1}$ at T_w, i.e, when $y_{i-1}(q, \dot{q})|_{t=T_w} = 0$, it holds that $\frac{\mathrm{d}y}{\mathrm{d}t}|_{t=T_w} \geq 0$, which ensures any system trajectory stay in the region $\{\mathcal{X}_c \cap \mathcal{X}_i \cap \mathcal{X}_{i-1}\}$. In other words, $y_{i-1}(q, \dot{q}) \geq 0$ satisfies for any states in $\{\mathcal{X}_c \cap \mathcal{X}_i \cap \mathcal{X}_{i-1}\}$. Usually we suppose that $\mathcal{X}_c \subset \mathcal{X}_i$ holds at every i. The forward invariance of $\mathcal{X}_c$ can then be derived if we prove $y_r(q, \dot{q}) \geq 0$ in this region.

By setting $y_0(q, \dot{q}) = B(q, \dot{q})$, we have the equation $y_i(q, \dot{q}) = \left(\frac{\mathrm{d}}{\mathrm{d}t} + \mu_1\right) \circ \cdots \circ \left(\frac{d}{dt} + \mu_i\right) \circ B(q, \dot{q})$. Condition (15) implies the condition of $y_r(q, \dot{q}) \geq 0$ and the forward invariant condition of $\mathcal{X}_c$. Thus, we have completed the proof.

□

Remark 2. Condition (15) is more focused on the candidate region that we aim to verify than the total state space in condition (7). This helps us to reduce the scale and complexity of verification problems. When constructing these conditions, the entries of $\boldsymbol{\lambda}$, which can also be formulated by $\{\mu_i\}$, need to be chosen carefully so that all the system states rendering safe in the original $\mathcal{X}_0$ will not be excluded during the process of condition recursion strengthening. In other words, $\mathcal{X}_0 \subset \mathcal{X}_r$ need to hold in the state space.

B. Verification Framework for Attitude Controllers

In the attitude space, we present a class of geometric barrier functions based on configuration error functions:

$$B(R, \Omega) = D - \Phi(R), \tag{16}$$

where D is a constant bound and the relative degree of B is 2. The safe set is defined as a region where attitude is close to the desired state R_d. Then, condition (15) can be formulated using (10)-(12):

$$\begin{aligned} &\ddot{B}(R, \Omega) + \lambda_2 \dot{B}(R, \Omega) + \lambda_1 B(R, \Omega) \\ =&-\ddot{\Phi}(R, \Omega) - \lambda_2 \dot{\Phi}(R, \Omega) + \lambda_1 \left[D - \Phi(R)\right] \geq 0. \end{aligned} \tag{17}$$

Satisfiability modulo theories (SMT) solvers are powerful engines that handle these safety verification problems. However, current SMT solvers do not support the theory of arrays with nonlinear constraints like (17). To address this issue, we transform such conditions into supported forms, which are given below.

- Encode (17) into an Euclidean-space equation. We adopt the results from matrix exponential map [16]. The matrix exponential map is a diffeomorphism between $\mathcal{U}_{\mathfrak{so}(3)} = \left\{\widehat{\boldsymbol{\omega}} \in \mathfrak{so}(3) \mid \boldsymbol{\omega} \in \mathbb{R}^3, \|\boldsymbol{\omega}\|_{\mathbb{R}^3} < \pi\right\}$ and $\mathcal{U}_{\mathrm{SO}(3)} = \{R \in \mathrm{SO}(3) \mid \mathrm{tr}(R) \neq -1\}$. Then, we can define a map $\theta(R) : \mathcal{U}_{\mathrm{SO}(3)} \to [0, \pi)$ and a map $\hat{\boldsymbol{\xi}}(R) : \mathcal{U}_{\mathrm{SO}(3)} \to \mathcal{U}_{\mathfrak{so}(3)}$ formulated as:

$$\theta(R) = \arccos\left(\frac{\mathrm{tr}(R) - 1}{2}\right) \in [0, \pi),$$

$$\hat{\boldsymbol{\xi}}(R) = \begin{cases} 0_{3\times 3}, & R = I_3 \\ \frac{1}{2\sin(\phi(R))}\left(R - R^T\right). & R \neq I_3 \end{cases}$$

By setting $K_p = I_{3\times 3}$, (10)-(12) are rewritten as:

$$\Phi = 1 - c_\theta, \tag{18}$$

$$\dot{\Phi} = s_\theta \boldsymbol{\xi}^\top (\Omega - \Omega_d), \tag{19}$$

$$\begin{aligned} \ddot{\Phi} = &\frac{c_\theta + 1}{2}(\Omega^\top \Omega + \Omega_d^\top \Omega_d) + (c_\theta^2 - c_\theta)\Omega_d^\top \boldsymbol{\xi} \Omega^\top \xi \\ &+ \frac{c_\theta - 1}{2}\left[(\Omega^\top \boldsymbol{\xi})^2 + (\Omega_d^\top \boldsymbol{\xi})^2\right] - (c_\theta + c_\theta^2)\Omega_d^\top \Omega \\ &+ s_\theta \Omega^\top \hat{\xi} \Omega_d + s_\theta \boldsymbol{\xi}^\top (\dot{\Omega} - \dot{\Omega}_d) - s_\theta^2 \boldsymbol{\xi}^\top \hat{\Omega} \hat{\boldsymbol{\xi}} \Omega_d, \end{aligned} \tag{20}$$

where $\theta = \theta(R_e)$ and $\boldsymbol{\xi} = \boldsymbol{\xi}(R_e)$. c_θ and s_θ are abbreviations of $\cos\theta$ and $\sin\theta$. Then condition (17) is transformed into a constraint in terms of a real variable θ and a column vector $\boldsymbol{\xi} = [\xi_1, \xi_2, \xi_3]^\top$ with 3 real variables.

- Describe sets in state space $\mathcal{X}$ using real variables θ_c and V_c. The candidate region is defined as follows:

$$\begin{aligned} &\mathcal{X}_c(\theta_c, V_c) \\ =&\mathcal{U}_R(\theta_c) \times \mathcal{U}_\Omega(V_c) \\ =&\left\{(R, \Omega) \mid R \in \mathcal{U}_R(\theta_c), \Omega \in \mathcal{U}_\Omega(V_c)\right\}, \end{aligned} \tag{21, 22}$$

where $\mathcal{U}_R(\theta_c) = \{R \mid \theta(R) \leq \theta_c\}$ is the attitude region described by θ_c and $\mathcal{U}_\Omega(V_c) = \{\Omega \mid \|\Omega\|_{\mathbb{R}^3} \leq V_c\}$ is the angular velocity region described by V_c.

With equations (19)-(22), the verification problem of GEBCs is translated into multiple conditions with real variables. This kind of problem is termed a Quantifier Free Real Arithmetic Logic (QF-NRA) problem and can be solved by current SMT solvers, for example, dReal [18].

Due to the involvement of trigonometric functions, the verification problem in attitude space is quite complicated and takes far too much time. To accelerate the verification process, grid-based partitioning methods are adopted so that the candidate state region is decomposed into smaller regions. The verification problem is the intersection of the corresponding subproblems.

Proposition 2. (State Region Decomposition) *Given a list of grid points $\{(\theta_j, V_j)\}$, $j \in \{1, \cdots, N_g\}$. We get $\theta_{N_g} = \theta_c$, and $V_{N_g} = V_c$. Then the candidate region can be decomposed as*

$$\mathcal{X}_c(\theta_c, V_c) = \sum \mathcal{X}_c([\theta_{a-1}, \theta_a], [V_{b-1}, V_b]), \tag{23}$$

where $a, b \in \{1, \cdots, N_g\}$, $\theta_0 = 0$ and $V_0 = 0$.

C. A Performance Criterion: Safe Flight Envelope

Here, we introduce a performance criterion which is called *safe flight envelope*. We analyze the performance of nominal attitude controllers by giving a standard verification problem. Specifically, we measure the operational region that a nominal controller can reach before being modified by the geometric CBF-QP. In other words, the safety property of controllers with predefined GCBFs is investigated by maximizing the parametric candidate region in (21) under a specific safe scenario.

To begin with, we specify a special requirement where the desired attitude is an identity matrix $R_d \equiv I_{3\times3}$ and $\Omega_d \equiv 0_{3\times1}$. Suppose the unsafe region is $\mathcal{X}_{\text{unsafe}} = \{(R,\Omega) \mid B(R,\Omega) < 0\}$. Then the verification problem is defined as

Problem 1. Given an attitude control system $(\mathrm{SO}(3), J, \boldsymbol{\tau})$ with a nominal controller $\boldsymbol{\tau}(R,\Omega)$, a parametric state set $\mathcal{X}_c(\theta_c, V_c)$ and a geometric CBF designed for attitude safety, if the following conditions are satisfied:

$$B = D - (1 - c_\theta) \geq 0, \quad \forall (R,\Omega) \in \mathcal{X}_c \tag{24}$$

$$\ddot{B} + \lambda_2 \dot{B} + \lambda_1 B \geq 0, \quad \forall (R,\Omega) \in \mathcal{X}_c \tag{25}$$

$$\begin{aligned} \dot{B} &= -s_\theta \xi^\top \Omega, \\ \ddot{B} &= -\frac{c_\theta + 1}{2}\Omega^\top \Omega - \frac{c_\theta - 1}{2}(\Omega^\top \xi)^2, \\ &\quad -s_\theta \xi^\top J^{-1}(J\Omega \times \Omega + \boldsymbol{\tau} + \triangle_R) \end{aligned}$$

then the safety of the controlled system (1) is guaranteed in the candidate region $\mathcal{X}_c(\theta_c, V_c)$.

Note that if we aim to maximize the region $\mathcal{X}_c$, there exists a trade-off between parameters θ_c and V_c. Therefore, we can generate a curve by maximum V_c with respect to θ_c. The algorithm is illustrated in Algorithm 1. We call the curve of the relationship between θ_c and V_c as *safe flight envelope*. The output list of $\{(\theta_n, V_n)\}$ indicates the boundary of the largest GCBF-certified operational region with δ.

Algorithm 1: Safe Flight Envelope Generation

Input: System Model $(J, \triangle_R)$, Nominal controller $\boldsymbol{u}(R,\Omega)$, Physical constraints $(\theta_{\max}, V_{\max})$, Pre-defined parameters $(\lambda_1, \lambda_2, D)$, Sample number N and Precision constant δ

Output: Safe Flight Envolpe $\{(\theta_n, V_n)\}, n \in \{1, \cdots, N\}$

Initialize $\theta_{\min} = 0$, $V_{\text{last}} = V_{\max}$;
for $n = 1; n \leq N; n{+}{+}$ **do**
  $\theta_{\max} = (n/N) * \theta_{\max}$;
  $V'_{\max} = (D - (1 - c_{\theta_{\max}}))/s_{\theta_{\max}}, V'_{\text{last}} = 0$;
  $V_{\min} = 0, V_{\max} = \min\left\{V_{\text{last}}, V'_{\max}\right\}$;
  $d = V_{\max} - V_{\min}$;
  $\tilde{\theta} = [\theta_{\min}, \theta_{\max}], \tilde{V} = [V_{\min}, V_{\max}]$;
  result = $\mathrm{CheckSat}(\tilde{\theta}, \tilde{V}, J, \cdots)$;
  if result **then**
    $(\theta_n, V_n) = (\theta_{\max}, V_{\max}), d = 0$;
  else
    $V'_{\text{last}} = V_{\max}$,;
    $V_{\min} = V_{\min}, V_{\max} = V_{\max} - d/2$;
    $d = V_{\max} - V_{\min}$;
  while $\mathrm{delta} > \delta$ **do**
    result = $\mathrm{CheckSat}(\tilde{\theta}, \tilde{V}, J, \cdots)$;
    if result **then**
      $V_{\min} = V_{\max}, V_{\max} = (V'_{\text{last}} + V_{\max})/2$;
      $d = V_{\max} - V_{\min}$;
    else
      $V'_{\text{last}} = V_{\max}$,;
      $V_{\min} = V_{\min}, V_{\max} = V_{\max} - d/2$;
      $d = V_{\max} - V_{\min}$;
  $(\theta_n, V_n) = (\theta_{\max}, V_{\min})$;
  $\theta_{\min} = \theta_{\max}, V_{\text{last}} = V_{\min}$
return $\{(\theta_n, V_n)\}$;

IV. NUMERICAL EXAMPLES

In this section, we provide a numerical example that compares the safe-related properties of two different nominal controllers using a safe flight envelope. A quadrotor attitude dynamics are considered according to [19][20]:

$$J_{xx} = 0.000906\mathrm{kg}\cdot\mathrm{m}^2, J_{yy} = 0.001242\mathrm{kg}\cdot\mathrm{m}^2,$$
$$J_{zz} = 0.002054\mathrm{kg}\cdot\mathrm{m}^2, J = \mathrm{diag}(J_{xx}, J_{yy}, J_{zz}).$$

We set the modeled uncertainty term $\triangle_R = (0.3\mathrm{rad}\cdot\mathrm{s}^{-2})J$. The GEBC problem in this case can be determined by the parameters: $\lambda_1 = 20, \lambda_2 = 12, D = 0.234$. We use two different PD controllers, which are designed based on the Euler angle representation of attitudes, i.e., $\{\alpha, \beta, \gamma\}$. The structure of controllers $\boldsymbol{\tau} = [\tau_1, \tau_2, \tau_3]^\top$ is defined by

$$\begin{aligned} \tau_1 &= k_{d1}(k_{p1}(\alpha_d - \alpha) - \omega_1), \\ \tau_2 &= k_{d2}(k_{p2}(\beta_d - \beta) - \omega_2), \\ \tau_3 &= k_{d3}(k_{p3}(\gamma_d - \gamma) - \omega_3), \end{aligned}$$

and its parameter set $K = \{k_{d1}, k_{d2}, k_{d3}, k_{p1}, k_{p2}, k_{p3}\}$ with respect to two example controllers are given as

$$K_1 = \{2.0, 2.0, 1.5, 0.025, 0.025, 0.028\},$$
$$K_2 = \{2.5, 2.5, 2.5, 0.016, 0.016, 0.028\}.$$

We use dReal [18] as the SMT solver to solve this safety verification problem. dReal is an automated reasoning tool that deals with nonlinear formulas such as polynomials and trigonometric functions over the reals. Since SMT problems are undecidable when the sine function is involved, every satisfiable result in dReal incorporates a numerical relaxation by a small precision constant δ. With a δ-complete decision framework, it returns either unsatisfied or δ-satisfied input statements with certificates of correctness.

The generated safe flight envelope is shown as Fig 1. Controllers with K_2 (green line) have a larger safe operational region under small attitude errors, which allows more aggressive actions than that with K_1 (blue line) in

the attitude CBF-QP control framework. Also, it is observed that when the attitude error becomes larger, the forward invariant constraint takes effect during operation. The forward invariant constraint in this figure is derived from Theorem 1, where the predefined λ_1 and λ_2 (or μ_1, μ_2) also brings a constraint for this safe operational region. This phenomenon indicates that the design of barrier functions also affects the operational region of nominal attitude controllers, especially when system states are closed to the safe boundary, exerting a strong limit to the controller operations.

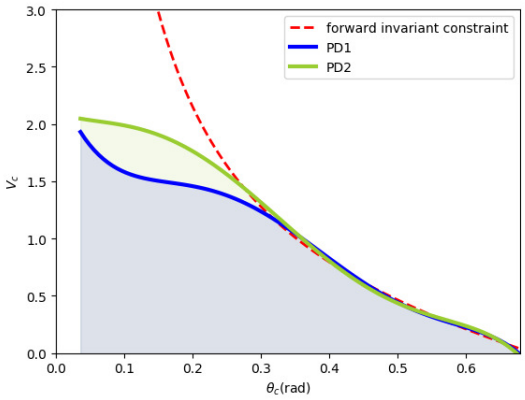

Fig. 1. Safe flight envelopes with respect to two different nominal attitude PD controllers. The blue region is the safe flight envelope of the PD controller with K_1 and the green region represents the one with K_2. The red dotted line refers to the theoretical constraint derived from the forward invariant requirements in Theorem 1.

V. CONCLUSIONS

In this paper, we focuse on the safety problem of attitude controllers. To analyze the safety performance of nominal controllers in general attitude CBF-QP, we introduce geometric barrier certificates and a practical formal verification framework, based on which useful safe performance criteria can be utilized for analysis. By a numerical example, two PD controllers are formally analyzed and compared. For future work, it is worth considering more types of geometric barrier functions to introduce diversity in constructing safe or unsafe attitude regions.

REFERENCES

[1] L. Dai, T. Gan, B. Xia, and N. Zhan, "Barrier certificates revisited," *Journal of Symbolic Computation*, vol. 80, pp. 62–86, 2017.

[2] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *2019 18th European control conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[3] M. Khan, M. Zafar, and A. Chatterjee, "Barrier functions in cascaded controller: Safe quadrotor control," in *2020 American Control Conference (ACC)*. IEEE, 2020, pp. 1737–1742.

[4] A. Ghaffari, "Operational safety control for unmanned aerial vehicles using modular barrier functions," in *2020 American Control Conference (ACC)*. IEEE, 2020, pp. 1719–1724.

[5] M. C. L. Abate, "Mixed monotonicity for efficient reachability with applications to robust safe autonomy," Ph.D. dissertation, Georgia Institute of Technology, 2022.

[6] C. Danielson, J. Kloeppel, and C. Petersen, "Spacecraft attitude control using the invariant-set motion-planner," *IEEE Control Systems Letters*, vol. 6, pp. 1700–1705, 2021.

[7] B. Heersink, P. Sylla, and M. A. Warren, "Formal verification of octorotor flight envelope using barrier functions and satisfiability modulo theories solving," *IEEE Control Systems Letters*, vol. 6, pp. 1507–1512, 2021.

[8] M. Khan and A. Chatterjee, "Gaussian control barrier functions: Safe learning and control," in *2020 59th IEEE Conference on Decision and Control (CDC)*. IEEE, 2020, pp. 3316–3322.

[9] T. P. Nascimento and M. Saska, "Position and attitude control of multi-rotor aerial vehicles: A survey," *Annual Reviews in Control*, vol. 48, pp. 129–146, 2019.

[10] Q. Nguyen and K. Sreenath, "Exponential control barrier functions for enforcing high relative-degree safety-critical constraints," in *2016 American Control Conference (ACC)*. IEEE, 2016, pp. 322–328.

[11] S. Kong, S. Gao, W. Chen, and E. Clarke, "dreach: δ-reachability analysis for hybrid systems," in *Tools and Algorithms for the Construction and Analysis of Systems: 21st International Conference, TACAS 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015, Proceedings 21*. Springer, 2015, pp. 200–205.

[12] C. Fan, B. Qi, S. Mitra, M. Viswanathan, and P. S. Duggirala, "Automatic reachability analysis for nonlinear hybrid models with c2e2," in *Computer Aided Verification: 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part I*. Springer, 2016, pp. 531–538.

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

[14] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *HSCC*, vol. 2993. Springer, 2004, pp. 477–492.

[15] H. Kong, F. He, X. Song, W. N. Hung, and M. Gu, "Exponential-condition-based barrier certificate generation for safety verification of hybrid systems," in *Computer Aided Verification: 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings 25*. Springer, 2013, pp. 242–257.

[16] F. Bullo and A. D. Lewis, *Geometric control of mechanical systems: modeling, analysis, and design for simple mechanical control systems*. Springer, 2019, vol. 49.

[17] F. Bullo and R. M. Murray, "Tracking for fully actuated mechanical systems: a geometric framework," *Automatica*, vol. 35, no. 1, pp. 17–34, 1999.

[18] S. Gao, S. Kong, and E. M. Clarke, "dreal: An smt solver for nonlinear theories over the reals," in *Automated Deduction–CADE-24: 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings 24*. Springer, 2013, pp. 208–214.

[19] S. Sun, R. Schilder, and C. C. de Visser, "Identification of quadrotor aerodynamic model from high speed flight data," in *2018 AIAA Atmospheric Flight Mechanics Conference*, 2018, p. 0523.

[20] S. Sun, C. C. de Visser, and Q. Chu, "Quadrotor gray-box model identification from high-speed flight data," *Journal of Aircraft*, vol. 56, no. 2, pp. 645–661, 2019.