Control Barrier Function Synthesis for Differential-Algebraic Systems

Hongchao Zhang[1], Mohamad H. Kazma[2], Ben Wooding[1], Meiyi Ma[1], Taylor T. Johnson[1] and Ahmad F. Taha[2]

***Abstract*— Control barrier certificates (CBCs) have been extensively studied for ordinary differential equation (ODE) systems, but their synthesis to differential-algebraic equation (DAE) systems has remained an open problem. This paper presents the first CBC synthesis framework for DAE systems, addressing safety for both index-1 and higher-index systems. We transform DAE-CBF synthesis into ODE-CBF synthesis with additional compatibility constraints and develop an alternating synthesis framework. We propose an anchored sum-of-squares (SOS) formulation that guarantees geometric correctness on the constraint manifold by construction. This formulation reduces verification to feasibility certification and enables lifting back to the full DAE state space. The approach is validated on a 24-dimensional three-link manipulator, demonstrating safe operation under algebraic constraints.**

I. Introduction

Safety-critical control of cyber-physical systems requires formal guarantees that the system state remains within a prescribed safe region during operation. Control barrier certificates (CBCs) [1] provide such guarantees by *(i)* synthesizing a Control Barrier Function (CBF) $b(x)$, a scalar function whose superlevel set encodes the safe region, and *(ii)* pairing it with a certificate triple (b, Ξ, γ), where Ξ are Positivstellensatz multipliers and $\gamma > 0$ a certificate margin, to certify forward invariance through an inequality constraint on the control input [2]. The resulting safety filter is computationally efficient, composable with nominal objectives, and extensible to higher relative degrees [3], making CBCs one of the most widely adopted certificate tools for real-time safety enforcement.

Existing CBF synthesis methods, however, assume ordinary differential equation (ODE) models where dynamics evolve over unconstrained differential state space. Many engineering systems are more naturally described by differential-algebraic equations (DAEs), in which differential dynamics are coupled with algebraic constraints that encode physical laws such as kinematic closure in robotic manipulators [4] and power balance in electrical networks [5], [6]. These constraints restrict the state to a manifold and introduce additional structural requirements, such as differentiation index and compatibility conditions, which are absent in ODE models.

Extending CBCs to DAE systems introduces a key technical challenge; the control input must simultaneously satisfy the CBF inequality *and* preserve the algebraic constraint manifold, a *compatibility* requirement absent in ODE formulations. CBFs for DAE systems were first introduced in [4], however without accounting for compatibility, which may drive the state off the manifold and produce certificates that are not physically meaningful. In [7], DAE-aware CBFs are introduced to resolve this challenge through projected dynamics on the constraint manifold, providing necessary and sufficient verification conditions for a given candidate barrier. However, the synthesis problem remains open; that is, given a DAE system and a safe set, it is not clear how to *find* a valid DAE-aware CBF satisfying verification conditions.

Prior work. Existing barrier-certificate work for DAE systems includes safety verification [8] and distributed construction of safety-preserving setpoint policies for power networks [9]. In contrast, CBF-based safe control has been studied primarily for ODE systems, including hybrid systems [2] and higher-relative-degree systems [3]. Synthesis of CBFs has been addressed via sum-of-squares (SOS) programming [10], [11], and neural networks with verification-in-the-loop (counterexample-guided) [12], [13]. However, these methods do not account for algebraic constraints that arise in DAE systems. Safety of DAEs has received comparatively little attention. Reference [4] extends CBFs to DAE systems for a flexible-link manipulator; however, no verification conditions are provided. Furthermore, reference [7] enforces compatibility and provides verification of DAE-aware CBFs, but left the synthesis of such CBFs unexplored.

Contributions. We present the first framework for synthesizing CBCs for DAE systems. The contributions are as follows.

- We propose an anchored SOS formulation (Theorem 3) that structurally guarantees correctness on the constraint manifold, while Positivstellensatz certificates ensure feasibility of a compatible control input.
- We develop an alternating SOS program (Algorithm 1) that jointly synthesizes a polynomial CBF and its certificates for index-1 and index-ν DAEs, initialized by the certified warm start in Proposition 1.
- We prove that a barrier synthesized on a reduced ODE lifts to the full DAE state space while preserving both correctness and feasibility (Corollary 1), and show that each semidefinite program (SDP) can be replaced by a linear program using diagonally dominant sum-of-squares (DSOS) certificates, together mitigating the scalability bottlenecks.
- We validate the framework on a 24-dimensional three-link manipulator DAE demonstrating the proposed DAE-aware CBC ensures safety, whereas an ODE-only baseline violates.

[1] Department of Computer Science, [2] Department of Civil and Environmental Engineering, Vanderbilt University, Nashville, TN 37235 USA. hongchao.zhang@vanderbilt.edu

This work is supported by the NSF under Grants 2220401, 2443803, 2152450 2550934, and the DARPA under Grant FA8750-23-C-0518. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of DARPA or NSF.

II. Problem Formulation

A. DAE System Model

We consider a semi-explicit nonlinear control-affine DAE system with dynamic states $x_d(t) \in \mathbb{R}^{n_d}$, algebraic states $x_a(t) \in \mathbb{R}^{n_a}$, overall state $x(t) = [x_d^T, x_a^T]^T \in \mathbb{R}^{n_x}$ ($n_x = n_d + n_a$), and control input $u(t) \in \mathbb{R}^{n_u}$:

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

$$0 = \phi(x), \tag{1b}$$

where $f : \mathbb{R}^{n_x} \to \mathbb{R}^{n_d}$, $g : \mathbb{R}^{n_x} \to \mathbb{R}^{n_d \times n_u}$, and $\phi : \mathbb{R}^{n_x} \to \mathbb{R}^{n_m}$ with components ϕ_ℓ ($\ell = 1, \dots, n_m$) are smooth. We write $f_d := f$ and $g_d := g$ when emphasizing the differential subsystem. The constraint manifold is $\mathcal{M} := \{x \in \mathbb{R}^{n_x} : \phi(x) = 0\}$. The *differentiation index* [14] ν is the minimum number of differentiations of ϕ required to obtain an ODE. We denote the Jacobians $J_d(x) := \nabla_{x_d}\phi(x)$ and $J_a(x) := \nabla_{x_a}\phi(x)$, and the admissible input set $\mathcal{U} := \{u : A_u u \le r_u\}$ with n_u^c constraints.

B. Safety of DAE Systems

The safe set is $\mathcal{C} := \{x : h(x) \ge 0\}$ for a smooth $h : \mathbb{R}^{n_x} \to \mathbb{R}$. A barrier function $b : \mathbb{R}^{n_x} \to \mathbb{R}$ defines $\mathcal{D} := \{x : b(x) \ge 0\}$. Safety requires positive invariance of $\mathcal{D} \cap \mathcal{M}$, i.e., $x(0) \in \mathcal{D} \cap \mathcal{M}$ implies $x(t) \in \mathcal{D} \cap \mathcal{M}$ for all $t \ge 0$.

For standard ODE systems, a CBF guarantees invariance of $\mathcal{D}$ via the condition $\frac{\partial b}{\partial x}(f(x) + g(x)u) \ge -\alpha(b(x))$, where $\alpha(x)$ is a class-$\mathcal{K}_\infty$ function [2]. For DAE systems, the control input must additionally preserve the constraint manifold, leading to the projected dynamics framework developed in [7].

Differentiating ϕ up to k times along the dynamics yields the k-th level constraint $d^k\phi/dt^k = 0$. We denote the corresponding Jacobians $J_d^{(k)}(x) := \nabla_{x_d}(d^k\phi/dt^k)$ and $J_a^{(k)}(x) := \nabla_{x_a}(d^k\phi/dt^k)$, and write $(\cdot)^\dagger$ for the Moore-Penrose pseudoinverse. The *control influence matrix* at level k is $\eta^{(k)}(x) := (J_d^{(k)}(x) f_d(x))^{d'-1} J_d^{(k)}(x)$, where d' is the relative degree of the differential subsystem. The product $\eta^{(k)} g_d$ is the matrix through which u enters the k-th time derivative of ϕ; it determines whether the control can enforce compatibility at level k. When the differential states are directly actuated ($d' = 1$), $\eta^{(k)} = J_d^{(k)}$.

Assumption 1. *The DAE system* (1) *satisfies: (i) $\phi(x)$ does not depend on u; (ii) the extended Jacobian $\big[J_a^{(\nu)}(x), \eta^{(\nu)}(x) g_d(x)\big]$ has full row rank for all $x \in \mathcal{C} \cap \mathcal{M}$.*

Full row rank ensures compatibility solvability through the algebraic-state rates and input; the guarantees apply only where it holds on $\mathcal{C} \cap \mathcal{M}$ and to the exact model on $\mathcal{M}$, excluding rank loss, plant mismatch, and off-manifold perturbations.

Under Assumption 1, the constrained dynamics on $\mathcal{M}$ admit the control-affine form $\dot{x} = \hat{f}(x) + \hat{g}(x)u$, where the *projected vector fields* are

$$\hat{f}(x) := \begin{bmatrix} f_d \\ -(J_a^{(1)})^\dagger J_d^{(1)} f_d \\ \vdots \\ -(J_a^{(\nu)})^\dagger J_d^{(\nu)} f_d \end{bmatrix}, \quad \hat{g}(x) := \begin{bmatrix} g_d \\ -(J_a^{(1)})^\dagger J_d^{(1)} g_d \\ \vdots \\ -(J_a^{(\nu)})^\dagger J_d^{(\nu)} g_d \end{bmatrix},$$

where all entries depend on x (suppressed for brevity). For index-1 systems, only the $k = 1$ row appears. The projection operator at level k is $P^{(k)}(x) := I_{n_m} - J_a^{(k)}(x)(J_a^{(k)}(x))^\dagger$, and a control u is *compatible* if it satisfies the hierarchy of compatibility conditions for all $k \in \{1, \dots, \nu\}$:

$$P^{(k)}(x)\big(J_d^{(k)}(x) f_d(x) + \eta^{(k)}(x) g_d(x) u\big) = 0. \tag{2}$$

Let $\mathcal{L}_{\hat{f}}\psi(x) := \nabla\psi(x)^\top \hat{f}(x)$ and $\mathcal{L}_{\hat{g}}\psi(x) := \nabla\psi(x)^\top \hat{g}(x)$ for the Lie derivatives along the projected fields. For notational convenience, we use the unified bar notation: $\bar{P}(x)$, $\bar{J}_d(x)$, and $\bar{\eta}(x)$ denote $P^{(1)}(x)$, $J_d^{(1)}(x)$, $\eta^{(1)}(x)$ for index-1, or the stacked quantities $P^{(k)}(x)$, $J_d^{(k)}(x)$, $\eta^{(k)}(x)$ for all $k \in \{1, \dots, \nu\}$ for index-ν systems.

Given a candidate barrier function $b(x)$ and $\alpha(x)$, the *DAE-aware CBF-QP* selects the minimally invasive safe control:

$$\begin{aligned} \min_{u} \quad & \|u - u_{\text{nom}}\|^2 \\ \text{s.t.} \quad & \mathcal{L}_{\hat{f}} b(x) + \alpha(b(x)) + \mathcal{L}_{\hat{g}} b(x)\, u \ge 0, \\ & \bar{P}(x)\big(\bar{J}_d(x) f_d(x) + \bar{\eta}(x) g_d(x)\, u\big) = 0, \\ & A_u u \le r_u, \end{aligned} \tag{3}$$

where u_{nom} is a nominal controller. The first constraint enforces the CBF inequality along the projected dynamics, the second compatibility (2), and the third input bounds.

Definition 1 (DAE-aware CBF [7])**.** *A continuously differentiable function $b(x)$ on $\mathcal{M}$ is a* DAE-aware CBF *if for every $x \in \mathcal{D} \cap \mathcal{M}$, the QP* (3) *is feasible.*

A DAE-aware CBF $b(x)$ is *valid* for $\mathcal{C}$ if it additionally satisfies correctness, $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$. Under these conditions, the following theorem guarantees safety.

Theorem 1 (Safety of DAE systems [7])**.** *Let $b(x)$ be a valid DAE-aware CBF for $\mathcal{C}$. Then $\mathcal{D} \cap \mathcal{M}$ is positively invariant under any control policy solving* (3)*.*

Validity on a DAE requires that the CBF is jointly compatible with the manifold geometry. The positive invariance guarantee of Theorem 1 relies on the feasibility of (3). Appending (2) to an existing ODE-based CBF does not, in general, preserve feasibility, making barrier *synthesis* essential.

C. Problem Statement

Theorem 1 guarantees safety of the DAE system (1) provided a valid DAE-aware CBF (Definition 1) exists. The main problem addressed in this paper is to synthesize such a valid DAE-aware CBF, which can be written as follows.

Problem 1 (DAE CBC Synthesis)**.** *Given* (1)*, $\mathcal{C}$, and a barrier class $\mathcal{B} = \{b(\cdot;\theta) : \theta \in \Theta\}$ with parameter set Θ, find $\theta \in \Theta$, certificate polynomials Ξ, and a certificate margin $\gamma > 0$ such that $b(\cdot;\theta)$ is a valid DAE-aware CBF. The tuple (b, Ξ, γ) is the synthesized CBC.*

The synthesis must produce three tightly coupled objects: a barrier $b(x)$ defining the safe set $\mathcal{D}$, certificates certifying that a compatible control input exists at every $x \in \mathcal{D} \cap \mathcal{M}$, and the resulting safe control policy.

III. CBCs for Differential-Algebraic Systems

Solving Problem 1 requires constructing a barrier $b(x)$ and certificate polynomials Ξ that jointly certify correctness ($\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$) and feasibility (a compatible control input exists at every $x \in \mathcal{D} \cap \mathcal{M}$). The barrier and certificates are coupled bilinearly, so they cannot be optimized in a single

convex program. The correctness guarantee is built into the barrier parameterization itself (the *anchored* formulation), while feasibility is enforced through sum-of-squares (SOS) certificates. This section develops these components and the full synthesis algorithm is presented in Section IV.

Algebraic preliminaries. We recall semi-algebraic tools.

Lemma 1 (Farkas' Lemma [15])**.** *Let $A \in \mathbb{R}^{m\times n}$ and $r \in \mathbb{R}^m$. Exactly one of the following holds: (i) $Au \le r$ has a solution u; or (ii) there exists $\lambda \ge 0$ with $\lambda^\top A = 0^\top$ and $\lambda^\top r < 0$.*

For polynomial set emptiness, we use the Positivstellensatz. Let $\Sigma[x]$ denote the cone of SOS polynomials, $\mathcal{N}[\cdot]$ the monoid, and $\mathbb{I}[\cdot]$ the ideal generated by polynomial families.

Theorem 2 (Positivstellensatz [16])**.** *Let (Φ_i), (χ_j), (Γ_ℓ) be finite families of polynomials. The set $\{x : \Phi_i(x) \ge 0,\ \chi_j(x) \ne 0,\ \Gamma_\ell(x) = 0\}$ is empty if and only if there exist $\Phi \in \Sigma$, $\chi \in \mathcal{N}$, $\Gamma \in \mathbb{I}$ such that $\Phi + \chi^2 + \Gamma = 0$.*

Anchored SOS formulation. The candidate barrier function $b(x)$ is *anchored* to the safe set function $h(x)$ through the following polynomial representation:

$$b(x) = h(x) - s(x)^2 - \mu\,\phi(x)^\top\phi(x), \tag{4}$$

where $s(x)^2 := m_s(x)^\top Q_s\, m_s(x)$ with $m_s(x)$ a monomial basis of degree d_s and $Q_s \succeq 0$ a positive semidefinite (PSD) Gram matrix (the decision variable), and $\mu > 0$ is a fixed scalar hyperparameter. The PSD constraint ensures $s(x)^2 \ge 0$ everywhere, while $\mu\,\|\phi(x)\|^2 \ge 0$ by construction. It enforces

$$b(x) \le h(x) \quad \forall x, \qquad b(x) = h(x) - s(x)^2 \quad \text{on } \mathcal{M},$$

which ensures global correctness $\mathcal{D} \subseteq \mathcal{C}$. The term $\mu\,\phi^\top\phi$ concentrates $\mathcal{D}$ near $\mathcal{M}$ but vanishes on $\mathcal{M}$, so it does not affect the Lie derivatives or feasibility conditions restricted to $\mathcal{M}$. Crucially, $b(x)$ is *linear* in the entries of Q_s (for fixed $\mathbf{x}$), keeping both alternation steps as SDPs. The special choice $Q_s = 0$ gives $b = h$ on $\mathcal{M}$ and is valid when the compatibility-constrained CBF-QP is feasible on $\mathcal{C} \cap \mathcal{M}$; otherwise, the parameterization searches for a smaller $\mathcal{D} \subseteq \mathcal{C}$. It remains to certify feasibility through the SOS constraints.

Dual feasibility conditions. For any $x \in \mathcal{D} \cap \mathcal{M}$, the DAE-aware CBF conditions require a control $u \in \mathcal{U}$ satisfying compatibility, the CBF inequality, and input limits:

$$\begin{aligned} \bar{P}(x)\big(\bar{J}_d(x) f_d(x) + \bar{\eta}(x) g_d(x) u\big) &= 0, \\ \mathcal{L}_{\hat{f}} b(x) + \alpha\big(b(x)\big) + \mathcal{L}_{\hat{g}} b(x)\, u &\ge 0, \\ A_u u &\le r_u. \end{aligned} \tag{5}$$

Encode the compatibility equality by two inequalities and write the resulting input constraints as $A(x)u \le r(x)$. For $x \in \mathrm{int}(\mathcal{D}) \cap \mathcal{M}$, $(A_{\mathrm{int}}, r_{\mathrm{int}})$ contains compatibility and input bounds. For $x \in \partial\mathcal{D} \cap \mathcal{M}$, Nagumo's theorem [17] adds the tangency row, giving $A_{\mathrm{bnd}} = [A_{\mathrm{int}}; -\mathcal{L}_{\hat{g}} b]$ and $r_{\mathrm{bnd}} = [r_{\mathrm{int}}; \mathcal{L}_{\hat{f}} b]$ because $\alpha(b) = 0$ on the boundary.

By Lemma 1, feasibility of each system is equivalent to infeasibility of its dual:

$$\lambda^\top A_{\mathrm{int}}(x) = 0^\top, \qquad \lambda^\top r_{\mathrm{int}}(x) < 0, \tag{6}$$

$$\lambda^\top A_{\mathrm{bnd}}(x) = 0^\top, \qquad \lambda^\top r_{\mathrm{bnd}}(x) < 0, \tag{7}$$

with nonnegative $\lambda = [(\lambda^-)^\top, (\lambda^+)^\top, \lambda^b, (\lambda^u)^\top]^\top$ (the multiplier λ^b is absent in the interior dual). To apply the Positivstellensatz to these dual systems, we impose the following representation condition.

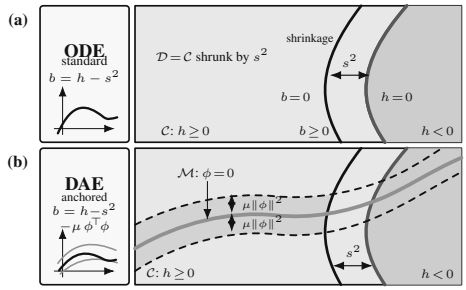

Fig. 1. (a) Standard ODE barrier: the safe set $\mathcal{C}$ is shrunk by s^2 to yield the barrier set $\mathcal{D} \subseteq \mathcal{C}$. (b) DAE anchored barrier: the off-manifold penalty $\mu\|\phi\|^2$ vanishes on $\mathcal{M}$ and grows quadratically away from it, concentrating $\mathcal{D}$ near the constraint manifold while preserving $b \le h$ everywhere.

Assumption 2. *h and ϕ are polynomial, and the entries of A_{int}, r_{int}, A_{bnd}, and r_{bnd} admit polynomial representations on $\mathcal{C} \cap \mathcal{M}$.*

Rational entries with denominators nonzero on $\mathcal{C} \cap \mathcal{M}$ may instead be converted by exact polynomial lifting before forming the certificates.

Positivstellensatz certificates. For a given $b(x)$, feasibility requires that the Farkas dual sets (6)-(7) are empty for all $x \in \mathcal{D} \cap \mathcal{M}$. We certify emptiness via the Positivstellensatz (Theorem 2): for each $\star \in \{\mathrm{int}, \mathrm{bnd}\}$, emptiness holds if there exist a *cone* element $\Phi_\star \in \Sigma$, a *monoid* element $\chi_\star^2$ (with $\chi_\star \in \Sigma$), and an *ideal* element $\varphi_\star \in \mathbb{I}$ satisfying $\Phi_\star + \chi_\star^2 + \varphi_\star = 0$.

The *cone* encodes the nonnegative quantities: multiplier nonnegativity ($[\lambda_\star]_i \ge 0$) and, in the interior, barrier positivity ($b(x) \ge 0$):

$$\Phi_{\mathrm{int}} := \sigma^0_{\mathrm{int}} + \sigma^b_{\mathrm{int}}\, b(x) + \textstyle\sum_i \sigma^{\lambda,i}_{\mathrm{int}}\, [\lambda_{\mathrm{int}}]_i, \tag{8}$$

with all σ-multipliers in $\Sigma[x, \lambda_{\mathrm{int}}]$. The boundary cone Φ_{bnd} has the same form but *omits* the $\sigma^b b$ term, since $b = 0$ on $\partial\mathcal{D}$; instead, $b(x)$ enters the boundary ideal.

The *ideal* encodes the equality constraints, Farkas stationarity ($\lambda_\star^\top A_\star = 0^\top$), the manifold ($\phi = 0$), and the strict-inequality slack ($-\lambda_\star^\top r_\star - \chi_\star^2 - \gamma = 0$, where $\gamma \ge 0$ is the certificate margin):

$$\varphi_\star := (\rho^A_\star)^\top(\lambda_\star^\top A_\star) + (\boldsymbol{\rho}^\phi_\star)^\top\phi + \rho^s_\star(-\lambda_\star^\top r_\star - \chi_\star^2 - \gamma),$$

with an additional term $\rho^b_{\mathrm{bnd}}\, b(x)$ appended for $\star = \mathrm{bnd}$ (since $b = 0$ on $\partial\mathcal{D}$). All ρ are free polynomial multipliers. Let $\Xi := \{\sigma_\star, \chi_\star, \rho_\star\}_{\star\in\{\mathrm{int},\mathrm{bnd}\}}$ collect the certificate polynomials, and let $\gamma > 0$ denote the strict certificate margin. The full SOS certificates are:

$$\Phi_{\mathrm{int}} + \chi^2_{\mathrm{int}} + \varphi_{\mathrm{int}} = 0, \tag{9a}$$

$$\Phi_{\mathrm{bnd}} + \chi^2_{\mathrm{bnd}} + \varphi_{\mathrm{bnd}} = 0. \tag{9b}$$

The constraints in (8)-(9b) are bilinear in the unknown barrier and certificate polynomials, motivating the alternating scheme of Section IV. The following theorem establishes that the anchored formulation together with the Psatz certificates constitutes a valid control barrier certificate.

Theorem 3 (Control barrier certificate for DAEs)**.** *Under*

Assumption 2, let $b(x)$ be defined by (4) *with $Q_s \succeq 0$ and $\mu > 0$. If there exist certificate polynomials Ξ and margin $\gamma > 0$ satisfying* (9a)-(9b)*, then $b(x)$ is a control barrier certificate for DAE system* (1)*, i.e.,*

$$b(x) \geq 0, \quad \forall x \in \mathcal{D} \cap \mathcal{M}, \tag{10a}$$

$$b(x) < 0, \quad \forall x \in (\mathcal{X} \setminus \mathcal{C}) \cap \mathcal{M}, \tag{10b}$$

$$\exists \alpha, u \in \mathcal{U}, \text{ s.t. (5) holds}, \quad \forall x \in \mathcal{D} \cap \mathcal{M}, \tag{10c}$$

and $\mathcal{D} \cap \mathcal{M}$ is positively invariant under policy (3)*.*

Proof. Given anchored form (4) with $Q_s \succeq 0$ and $\mu > 0$, we have $s(x)^2$ and $\mu\phi(x)^T\phi(x)$ nonnegative everywhere. It gives us $\mathcal{D} \subseteq \mathcal{C}$ and $\mathcal{D} \cap \mathcal{M}$ is nonempty, if $\mathcal{D}$ is nonempty, respectively. Hence, it enforces correctness (10a)-(10b) by construction. For each $\star \in \{\mathrm{int}, \mathrm{bnd}\}$, the Positivstellensatz conditions (9a)–(9b) with $\gamma > 0$ certifies that the Farkas dual set (6)-(7) is empty for every $x \in \mathcal{D} \cap \mathcal{M}$. By Lemma 1, the primal system (5) therefore admits a solution $u \in \mathcal{U}$, establishing (10c). Since $b(x)$ is a valid DAE-aware CBF (Definition 1), $\mathcal{D} \cap \mathcal{M}$ is positively invariant under any policy solving (3) by Theorem 1. □

Theorem 3 reduces the CBC synthesis problem to finding a Gram matrix $Q_s \succeq 0$ and certificate polynomials Ξ that jointly satisfy the Psatz identities (9a)-(9b) with $\gamma > 0$. Since (Q_s, Ξ) appear bilinearly in these identities, a single convex program cannot optimize both simultaneously. Section IV presents an alternating SOS algorithm (Algorithm 1) that decouples the search into convex subproblems, together with a Lyapunov-based initialization that provides a certified warm start.

IV. Alternating SOS Synthesis

We first construct a certified initial barrier via a Lyapunov-based SDP (Proposition 1), then present the two alternating convex steps and their assembly into Algorithm 1. The control-influence matrix $\eta^{(k)}$ accounts for higher relative degree in DAE compatibility. The SOS program presents the relative-degree-one barrier condition; the higher-order case is omitted.

Initialization. Let $\dot{\mathbf{z}} = f_{\mathrm{red}}(\mathbf{z}) + g_{\mathrm{red}}(\mathbf{z})u$ denote the reduced ODE in coordinates $\mathbf{z} = Tx_d$. Linearizing it at an equilibrium $(\mathbf{z}^*, u^*)$ gives $A_{\mathrm{red}} := \nabla_{\mathbf{z}}(f_{\mathrm{red}} + g_{\mathrm{red}}u^*)|_{\mathbf{z}^*}$ and $B_{\mathrm{red}} := g_{\mathrm{red}}(\mathbf{z}^*)$. We compute the continuous-time LQR gain K for $(A_{\mathrm{red}}, B_{\mathrm{red}})$ from the algebraic Riccati equation; under $u - u^* = -K(\mathbf{z} - \mathbf{z}^*)$, $A_{\mathrm{cl}} = A_{\mathrm{red}} - B_{\mathrm{red}}K$. The case-study weights are reported in Section V, and the Lyapunov linear matrix inequality (LMI) [18] yields the seed $Q_s^{(0)} \succeq 0$.

Let $V(x; P) = (x - x^*)^\top P\,(x - x^*)$. We jointly optimize a Lyapunov matrix P, the Gram matrix Q_s, and the barrier margin c:

$$\begin{aligned} \max_{P,\,Q_s,\,c} \quad & c \\ \text{s.t.} \quad & P \succ 0,\ Q_s \succeq 0,\ c > 0,\ A_{\mathrm{cl}}^\top P + P\,A_{\mathrm{cl}} \prec 0, \\ & m_s(x)^\top Q_s\, m_s(x) = h(x) - c + V(x; P) \\ & \qquad\qquad - \mu\phi(x)^\top \phi(x). \end{aligned} \tag{11}$$

All constraints are linear in (P, Q_s, c), so (11) is a convex SDP. Since A_{cl} is Hurwitz, the Lyapunov LMI is always feasible [18], and the identity constraint links the barrier shape to a Lyapunov sublevel set. We denote the resulting initial safe set $\mathcal{D}^{(0)} := \{x : b(x; Q_s^{(0)}) \geq 0\}$. The following proposition is straightforward from the construction and guarantees that the initial barrier is a valid DAE-aware CBF near x^*.

Algorithm 1 Alternating SOS Synthesis for DAE-aware CBF

Input: f_d, g_d, h, μ, x^*, polynomial degree deg.
Init: Given x_0, synthesize $Q_s^{(0)}$ via (11) (Prop. 1), $k \leftarrow 0$.
repeat
  $b \leftarrow \textsc{BuildBarrier}(h, \phi; Q_s^{(k)}, \mu)$. (4)
  $(\Xi, \hat{\gamma}) \leftarrow \textsc{SolveCerts}(b, \deg)$. (12)
  $Q_s^{(k+1)} \leftarrow \textsc{SolveBarrier}(\Xi, \deg)$. (13)
  $k \leftarrow k + 1$.
until $\|Q_s^{(k)} - Q_s^{(k-1)}\|_F < \varepsilon$
Output: a verified $(Q_s, \Xi, \hat{\gamma})$ if $Q_s \succeq 0$, $\hat{\gamma} > 0$, and (9a)–(9b) hold after final substitution; otherwise, failure.

Proposition 1. *Given $x^* \in \mathrm{int}(\mathcal{C}) \cap \mathcal{M}$, if* (11) *is feasible with solution $(P^*, Q_s^{(0)}, c^*)$, then the initial barrier $b(x; Q_s^{(0)})$ satisfies* (10) *with $\mathcal{U} = \mathbb{R}^{n_u}$.*

The proof follows from the Lyapunov-based construction. The proof is omitted for brevity. The SDP (11) does not explicitly enforce $u \in \mathcal{U}$. A simple two-stage remedy is to first solve (11), then compute $\bar{c} = \min_j u_{\max,j}^2 / (k_j^\top (P^*)^{-1} k_j)$, and finally re-solve with the additional constraint $c \leq \bar{c}$.

Step 1 (SolveCerts). Fix Q_s (and hence $b(x)$ via (4)) and solve for the certificate polynomials Ξ while maximizing the certificate margin γ:

$$\begin{aligned} \max_{\Xi,\,\gamma} \quad & \gamma \\ \text{s.t.} \quad & \text{identities (9a) and (9b) hold,} \\ & \text{all } \sigma\text{-multipliers} \in \Sigma[x, \lambda]. \end{aligned} \tag{12}$$

The Lie derivatives appearing in A_{bnd} and r_{bnd} are computed from (4). The interior and boundary SDPs can be solved independently (each with its own margin $\gamma_{\mathrm{int}}, \gamma_{\mathrm{bnd}}$), and the reported margin is $\hat{\gamma} := \min\{\gamma_{\mathrm{int}}, \gamma_{\mathrm{bnd}}\}$.

Step 2 (SolveBarrier). Fix the certificate polynomials Ξ (numerical Lagrangians from Step 1) and solve for the Gram matrix Q_s:

$$\begin{aligned} \min_{Q_s} \quad & \|Q_s\|_F^2 \\ \text{s.t.} \quad & \text{identities (9a) and (9b) hold with fixed } \Xi, \\ & Q_s \succeq 0, \quad b(x^*) > 0. \end{aligned} \tag{13}$$

The Frobenius-norm objective regularizes Q_s toward a minimum-norm solution and pushes $b(x)$ toward the geometrical limit $h(x)$ while satisfying the Lagrangian constraints.

We define helper routines: $\textsc{BuildBarrier}(h, \phi; Q_s, \mu)$ returns $b(x)$ via (4); $\textsc{SolveCerts}(b, \deg)$ solves (12) and returns $(\Xi, \hat{\gamma})$; $\textsc{SolveBarrier}(\Xi, \deg)$ solves (13) for Q_s.

ODE-to-DAE lifting. Direct SOS synthesis on high-dimensional DAEs is computationally intractable: the monomial basis grows as $\binom{n_x + d_s}{d_s}$, so increasing the state dimension from n_{red} to n_x inflates the Gram matrix combinatorially. For example, going from 6 to 24 states at degree $d_s = 2$ increases the SDP variable count by a factor of $\approx 130\times$. Instead, one synthesizes on a reduced ODE in minimal coordinates and *lifts* the result to the full DAE state space.

Let $\mathbf{z} = Tx_d$ be a linear coordinate projection whose restriction to the considered component of $\mathcal{M}$ admits a smooth inverse embedding ι, so that each consistent state is represented by $x = \iota(\mathbf{z})$. Assume that every trajectory of the reduced ODE under $u \in \mathcal{U}$ lifts through ι to a consistent DAE trajectory and that $h^{\mathrm{dae}}(\iota(\mathbf{z})) = h^{\mathrm{ode}}(\mathbf{z})$ on this component. Since T is linear, each ODE monomial expands as a linear combination of DAE monomials:

$$m_s^{\mathrm{ode}}(Tx_d) = L\, m_s^{\mathrm{dae}}(x_d), \tag{14}$$

where $L \in \mathbb{R}^{\dim(m_s^{\mathrm{ode}})\times\dim(m_s^{\mathrm{dae}})}$ is the *monomial embedding matrix*. Given a Gram matrix $Q_s^{\mathrm{ode}} \succeq 0$ from Algorithm 1 on the ODE, define the lifted Gram matrix

$$Q_s^{\mathrm{dae}} := L^\top Q_s^{\mathrm{ode}} L, \tag{15}$$

Corollary 1 (ODE-to-DAE lifting)**.** *Under the exact-reduction assumption, if Algorithm 1 returns a reduced-order CBC $(Q_s^{\mathrm{ode}}, \Xi, \hat{\gamma})$ with $Q_s^{\mathrm{ode}} \succeq 0$ and $\hat{\gamma} > 0$, then*

$$b^{\mathrm{dae}}(x) = h^{\mathrm{dae}}(x) - m_s^{\mathrm{ode}}(Tx_d)^\top Q_s^{\mathrm{ode}} m_s^{\mathrm{ode}}(Tx_d) - \mu\phi(x)^\top \phi(x)$$

is a CBC on the considered component of $\mathcal{M}$.

Proof. On $\mathcal{M}$, $\phi = 0$ and $b^{\mathrm{dae}}(\iota(\mathbf{z})) = b^{\mathrm{ode}}(\mathbf{z})$; hence, along corresponding trajectories, $\dot{b}^{\mathrm{dae}} = \dot{b}^{\mathrm{ode}}$, and the same $u \in \mathcal{U}$ satisfies the DAE compatibility and CBF conditions. Substituting $\mathbf{z} = Tx_d$ into the certificate identities completes the proof by Theorem 3. □

Under its coordinate, dynamics-equivalence, and safety-function assumptions, Corollary 1 establishes that a reduced-order CBC returned by Algorithm 1 pulls back to a valid CBC on the considered component of $\mathcal{M}$. This avoids the combinatorial growth of the SDP variables with state dimension. We note that Algorithm 1 has no claimed convergence or global-optimality guarantee. A returned tuple is a CBC only if the final $(Q_s, \Xi, \hat{\gamma})$ satisfies the Positivstellensatz identities with $Q_s \succeq 0$ and $\hat{\gamma} > 0$; otherwise, the algorithm returns no certificate and makes no safety claim. Furthermore, Algorithm 1 can be further accelerated by replacing every SOS constraint with its diagonally dominant SOS (DSOS) relaxation. Concretely, the Positive Semi-Definite (PSD) constraint $Q_s \succeq 0$ is replaced by diagonal dominance ($[Q_s]_{ii} \geq \sum_{j\neq i} |[Q_s]_{ij}|$), and each SOS cone multiplier $\sigma \in \Sigma$ is restricted to have a diagonally dominant Gram matrix. Since diagonal dominance implies PSD, any returned DSOS certificate remains sound under Theorem 3. DSOS can be more conservative than SOS, and we make no safe-set optimality claim.

V. Case Study

We validate the proposed framework on a planar three-link manipulator [19] operating near an obstacle, and we pose the following research questions.

RQ1 Does the proposed DAE-aware CBC ensure safety where an ODE-CBC fails?

RQ2 How scalable is the proposed synthesis algorithm?

The experiments are conducted in a simulation environment using Python and are performed on a machine with an Apple M2 Max with 32 GB RAM running macOS. The solver for the SOS programs is Drake [20] and the code is available[1].

A. System Model

We consider a three-link manipulator with link lengths $L_1 = 1.0$, $L_2 = 0.7$, $L_3 = 0.5\,\mathrm{m}$, masses $m_1 = 1.0$, $m_2 = 0.7$, $m_3 = 0.3\,\mathrm{kg}$, and moments of inertia $I_i = \frac{1}{12} m_i L_i^2$, under gravity $g = 9.81\,\mathrm{m/s^2}$. The base is pinned at the origin, a point obstacle lies at $p_{\mathrm{obs}} = (1.2, 0.5)\,\mathrm{m}$ with safety radius $d_{\mathrm{safe}} = 0.3\,\mathrm{m}$, and joint torques $u = [\tau_1, \tau_2, \tau_3]^\top$ satisfy $|\tau_i| \leq \tau_{\max}$. The equilibrium is $\theta_1^* = \pi/2$, $\theta_2^* = \theta_3^* = 0$. We model the system as a Newton-Euler DAE: each link has center-of-mass position $r_i = (x_i, y_i)$, orientation θ_i, and velocities $(\dot{x}_i, \dot{y}_i, \omega_i)$, giving $x_d \in \mathbb{R}^{18}$; the algebraic state $x_a \in \mathbb{R}^6$ collects the pin-joint constraint forces. The dynamics are

$$M_i \ddot{r}_i = F_i^{\mathrm{ext}}(x_a), \tag{16a}$$

$$I_i \dot{\omega}_i = T_i^{\mathrm{ext}}(x_a, u), \tag{16b}$$

$$0 = \phi(x_d), \tag{16c}$$

for $i = 1, 2, 3$, where F_i^{ext} collects gravity and constraint forces, and T_i^{ext} is the net torque from constraints and actuation. The six constraints (16c) enforce pin-joint connectivity: each joint coincides with the endpoints of its adjacent links via $\phi(x_d) = 0$, where ϕ depends only on x_d. Hence $\nabla_{x_a}\phi = 0$, $\bar{P} = I_6$ (maximally nontrivial compatibility), and the system is index-3 with 3 true degrees of freedom.

Safety function. The i-th link segment ℓ_i runs between $r_i \pm \frac{L_i}{2} e(\theta_i)$ with $e(\theta_i) = (\cos\theta_i, \sin\theta_i)^\top$. The safe set is $\mathcal{C} = \{x : h(x) \geq 0\}$, with whole-body safety function $h(x)$:

$$h(x) = \min_{i\in\{1,2,3\}} \mathrm{dist}(\ell_i, p_{\mathrm{obs}})^2 - d_{\mathrm{safe}}^2. \tag{17}$$

Since (17) is non-polynomial, SOS synthesis uses a degree-4 surrogate h_{poly} and the polynomial set $\mathcal{C}_{\mathrm{poly}} := \{x : h_{\mathrm{poly}}(x) \geq 0\}$. The formal CBC guarantee is $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C}_{\mathrm{poly}} \cap \mathcal{M}$; whole-body safety with respect to (17) is evaluated in simulation because $\mathcal{C}_{\mathrm{poly}} \subseteq \mathcal{C}$ is not certified here.

Reduced ODE. The Lagrangian formulation eliminates x_a, yielding a 6D ODE in $q = [\theta_1, \theta_2, \theta_3]^\top$:

$$M(q)\ddot{q} + C(q, \dot{q})\dot{q} + G(q) = u, \tag{18}$$

which preserves the dynamics but discards link geometry; for SOS synthesis, the reduced and Newton-Euler representations use polynomial models in deviation coordinates and satisfy Assumption 2.

B. Experimental Results

We initialize the synthesis on the DAE system (16) via (11), which linearizes about the equilibrium under LQR control ($Q = \mathrm{diag}(10, 1, 10, 1, 10, 1)$, $R = 0.1\,I$) and yields a Lyapunov-based seed with margin $c = 0.086$. We compare two synthesis strategies in Table I: direct synthesis (DAE), and projection to the reduced ODE (18) followed by lifting (Red.). The anchored form (4) uses h_{poly}; the monomial basis ($d_s = 2$, 6 states) gives a 28×28 Gram matrix Q_s^{ode}. Algorithm 1 meets its stopping and final-certificate checks after 2 SOS iterations and 8 DSOS iterations. The ODE Gram matrix is then lifted via (15) back to a 190×190 DAE Gram matrix of rank 12.

[1] https://github.com/HongchaoZhang-HZ/CBCDAE

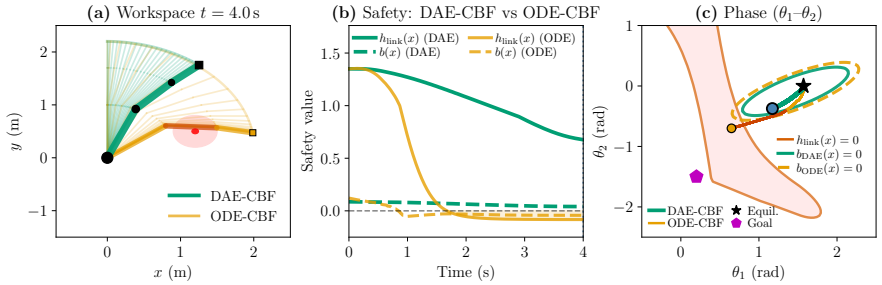

Fig. 2. Closed-loop simulation of the three-link planar comparing DAE-aware CBC (green) and ODE-only CBC (orange). (a) Workspace at $t = 4.0\,\mathrm{s}$: the DAE-aware CBF keeps all links avoiding the obstacle (red circle), while the ODE-only CBF results in collision. (b) Safety function h_{link} (17) and barrier $b(x)$ over time: both remain nonnegative under DAE-CBC, whereas h_{link} drops to zero under ODE-CBC. (c) Phase portrait in (θ_1, θ_2): the collision boundary ($h_{\mathrm{link}} = 0$, red), the DAE barrier zero-level set ($b_{\mathrm{DAE}} = 0$, green), the ODE barrier zero-level set ($b_{\mathrm{ODE}} = 0$, orange). The DAE-CBC trajectory remains inside $\{b_{\mathrm{DAE}} \geq 0\} \subset \{h_{\mathrm{link}} \geq 0\}$, while the ODE-CBC trajectory exits the safe region.

TABLE I

COMPARISON OF PER-ITERATION SOLVE TIME AND PROBLEM SIZE FOR SOS AND DSOS SYNTHESIS ON THE REDUCED ODE VS. THE FULL DAE.

	n_d	$\dim(m_s)$	Q_s vars	Constraints	Time (s)
Red. (SOS)	6	28	406	LMI (28×28)	41.0
Red. (DSOS)	6	28	406	Linear (378)	40.2
DAE (SOS)	18	190	18,145	LMI (190×190)	N/A
DAE (DSOS)	18	190	18,145	Linear (17,955)	655.6

Under the assumptions of Corollary 1, the result is a valid CBC for $\mathcal{C}_{\mathrm{poly}}$ on the considered component of $\mathcal{M}$. Whole-body safety with respect to (17) is observed in simulation.

RQ1: DAE-aware vs. ODE-only CBC (RQ1). The control policy derived from the DAE-aware CBC maintains $h_{\mathrm{wb}}(x(t)) \geq 0$ throughout with zero violations and no QP infeasibility. As a baseline, we compare against an ODE-only CBC following [11], synthesized on (18) without verifying the feasibility of (3). The ODE-only CBC trajectory violates $h_{\mathrm{wb}} < 0$, i.e., physical link-obstacle penetration (Fig. 2(a), (b)). Enforcing DAE compatibility prevents the safety violation observed with the ODE-only baseline.

RQ2: Scalability (RQ2). Table I compares the per-iteration solve time and problem size. The ODE-to-DAE lifting reduces SDP variables from $18,145$ to 406. Each iteration of the reduced SOS solves in $41.0\,\mathrm{s}$, while direct SOS on the full DAE exceeds the solver's memory limit. The DSOS relaxation makes the full DAE tractable at $655.6\,\mathrm{s}$ per iteration but remains $16\times$ slower than the reduced ODE. Thus, ODE-to-DAE lifting improves scalability while preserving certificate validity on the considered component of $\mathcal{M}$ under Corollary 1.

VI. CONCLUSION

This paper presented a synthesis framework for DAE control barrier certificates that combines an anchored SOS barrier with Positivstellensatz certificates for compatible-input feasibility. The resulting compatibility condition ensures that safety and algebraic consistency are satisfied simultaneously for both index-1 and higher-index systems. A case study on a 24-dimensional three-link manipulator DAE illustrates safety without link violations. Future work includes improving scalability on higher-dimensional DAEs and extending the framework to neural CBFs.

REFERENCES

[1] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International workshop on hybrid systems: Computation and control*. Springer, 2004, pp. 477–492.

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

[3] W. Xiao and C. Belta, "High-order control barrier functions," *IEEE Transactions on Automatic Control*, vol. 67, no. 7, pp. 3655–3662, 2021.

[4] Y. Park and C. Sloth, "Differential-Algebraic Equation Control Barrier Function for Flexible Link Manipulator," *IEEE International Conference on Intelligent Robots and Systems*, pp. 12 408–12 413, 2024.

[5] P. Kundur *et al.*, "Power System Stability," *Power system stability and control*, vol. 10, no. 1, pp. 7–1, 2007.

[6] T. Groß, S. Trenn, and A. Wirsen, "Solvability and stability of a power system DAE model," *Systems and Control Letters*, vol. 97, pp. 12–17, 2016.

[7] H. Zhang, M. H. Kazma, M. Ma, T. T. Johnson, and A. F. Taha, "Verification and forward invariance of control barrier functions for differential-algebraic systems," 2026. [Online]. Available: https://arxiv.org/abs/2603.13509

[8] R. Pedersen, C. Sloth, and R. Wisniewski, "Verification of power grid voltage constraint satisfaction—a barrier certificate approach," in *2016 European Control Conference (ECC)*. IEEE, 2016, pp. 447–452.

[9] S. Kundu, S. Geng, S. P. Nandanoori, I. A. Hiskens, and K. Kalsi, "Distributed barrier certificates for safe operation of inverter-based microgrids," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 1042–1047.

[10] Z. Jarvis-Wloszek, R. Feeley, W. Tan, K. Sun, and A. Packard, "Control of nonlinear systems with area-preserving SOS programming," in *IEEE Conference on Decision and Control*. IEEE, 2003, pp. 3567–3572.

[11] A. Clark, "A semialgebraic framework for verification and synthesis of control barrier functions," *IEEE Transactions on Automatic Control*, vol. 70, no. 5, pp. 3101–3116, 2024.

[12] A. Edwards, A. Peruffo, and A. Abate, "Fossil 2.0: Formal Certificate Synthesis for the Verification and Control of Dynamical Models," *HSCC 2024 - Proceedings of the 27th ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2024, part of CPS-IoT Week*, no. May 2024, 2024.

[13] H. Zhang, Z. Qin, S. Gao, and A. Clark, "Seev: Synthesis with efficient exact verification for relu neural barrier functions," *Advances in Neural Information Processing Systems*, vol. 37, pp. 101 367–101 392, 2024.

[14] P. Kunkel and V. Mehrmann, *Differential-Algebraic Equations: analysis and Numerical Solution*. EMS Press, 2005.

[15] J. Matoušek and B. Gärtner, *Understanding and Using Linear Programming*. Springer, 2007, vol. 1.

[16] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical programming*, vol. 96, pp. 293–320, 2003.

[17] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*. Springer, 2008, vol. 78.

[18] S. Boyd, V. Balakrishnan, E. Feron, and L. ElGhaoui, "Control system analysis and synthesis via linear matrix inequalities," in *1993 American Control Conference*. IEEE, 1993, pp. 2147–2154.

[19] X. Lai, Y. Wang, M. Wu, and W. Cao, "Stable control strategy for planar three-link underactuated mechanical system," *IEEE/ASME Transactions on Mechatronics*, vol. 21, no. 3, pp. 1345–1356, 2016.

[20] R. Tedrake and the Drake Development Team, "Drake: Model-based design and verification for robotics," 2019. [Online]. Available: https://drake.mit.edu