A Scenario Approach for Synthesizing k-Inductive Barrier Certificates

Vishnu Murali, *Student Member, IEEE*, Ashutosh Trivedi, and Majid Zamani, *Senior Member, IEEE*

***Abstract*— The notion of k-inductive barrier certificates generalize the idea of k-induction to verification of discrete-time continuous-state dynamical systems by requiring restrictions over k-grams (sequence of k-states in evolution) of the system transitions. The promise of k-inductive barrier certificates is in the simplicity of the form of barrier certificates (lower-degree of polynomials) at the cost of more complex non-convex constraints involving logical implications. Recent breakthroughs in convex robust programming via the *scenario approach* deliver a sampling-based randomized algorithm for the computation of barrier certificates. In the absence of system dynamics (a.k.a. black box models), extending scenario approach to k-inductive barrier certificates faces challenges due to the resulting lack of convexity. This paper overcomes non-convexity challenges by providing a sound approach for data-driven computation of k-inductive barrier certificates. We present computational methods to solve the resulting scenario programs for k-inductive barrier certificates, provide out-of-sample performance guarantees, and experimentally demonstrate the effectiveness of the proposed results.**

***Index Terms*— barrier certificates, control systems, data-driven verification, safety, reachability**

I. Introduction

SCENARIO-based approach to optimization and synthesis [1] is a statistical learning based paradigm that provides probabilistic guarantees on the quality of the solution based on a finite number of samples or scenarios chosen i.i.d. over the uncertainty space. Scenario-based approach is naturally related to robust convex programming [2] and chance-constrained programming [1]. By leveraging a connection between barrier certificates and robust convex programming, scenario-based approach has been applied [3], [4] to construct barrier certificates for unknown systems. A key obstacle to scalability in computing the barrier certificates via scenario-based approach is the complexity of the concept class (polynomial degree for barrier certificates). The k-inductive barrier certificates [5], [6] provide a trade-off in the complexity of concept class at the cost of non-convexity in the robust programming problem.

Contributions. This paper presents a scenario-based approach to design k-inductive barrier certificates for discrete-time continuous-space dynamical systems for both safety and reachability requirements. While the barrier certificates demonstrate a decrease in system potential along the transitions starting from states with negative potential, the k-inductive barrier certificates weaken this condition by requiring a decrease only when the last k-transitions remain within the states with negative potential. While this weakening may result in lower-degree barrier certificates, expressing their constraints require logical implications that, via S-procedural reduction, lead to a bilinear robust programming problem. Due to the resulting non-convexity, the existing scenario-based approach to robust convex programming [2] is not applicable. Analyzing the form of the bilinear program, we provide a litmus test on the solution of the scenario program to identify if it is a k-inductive barrier certificate with high probability. This litmus test indicates towards three hyperparameters to adjust when the scenario program fails to provide the k-inductive barrier certificate: 1) increase the bound k for k-inductive barrier certificate; 2) increase number of scenarios; and 3) search for a higher degree of polynomial for barrier certificates. Our experimental results indicate that increasing the bound k is a sample-efficient and computationally attractive option.

We consider two notions of k-inductive barrier certificates (for reachability and safety) and provide a sampling-based approach for a given confidence bound. While our results are presented in the context of k-inductive barrier certificates, the established connection between the robust bilinear program and the scenario program may be of general interest itself.

Related Literature. *Discretization*-based approaches have been proposed to guarantee safety and reachability [7], [8], but they suffer from the curse of dimensionality. Barrier certificates [9] provide discretization-free approaches for safety, reachability [10], as well as for richer classes of specifications such as Linear Temporal Logic [11]–[13]. The notion of k-induction has been extended to t-barrier certificates [14] and k-inductive barrier certificates [5], [6], [15]. Prominent techniques to synthesize barrier certificates include sum-of-squares approach [9], counterexample guided inductive synthesis [16], and Satisfiablity Modulo Theory solvers [17], [18]. These approaches are inapplicable when the system is unknown.

When the system is unknown, a scenario approach [1] can be used [3], [4] to compute barrier certificates based on the connection between robust convex programs, chance-constrained programs and scenario programs [2]. While connections exist between non-convex scenario programs and non-convex chance-constrained programs [19], their connection to

This work was supported by the NSF under Grants ECCS-2015403 and CNS-2145184.

Vishnu Murali, Ashutosh Trivedi and Majid Zamani are with the Department of Computer Science at the University of Colorado, Boulder, USA. Majid Zamani is also with the Computer Science Department, Ludwig Maximillian University, Munich, Germany. Emails: {vishnu.murali, ashutosh.trivedi, majid.zamani}@colorado.edu

non-convex robust programs is still unknown.

II. Problem Definition

We write $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$ for the set of reals, integers, and natural numbers. For $a \in \mathbb{R}$, we write $\mathbb{R}_{\geq a}$ and $\mathbb{R}_{>a}$ for the intervals $[a, \infty)$ and (a, ∞) For a function $f{:}A{\to}A$ we write f^n as the n-th iterate of f, where f^0 is the identity function. We use $\bigwedge$ to indicate the logical "and" operation. This allows us to represent conjunction of constraints succinctly.

A. Optimization under Uncertainty

In the sampling based view of the unknown system, a practically useful stance is to view the system as not fixed but rather subject to uncertainty characterized by a fixed probability space $(Q, B(Q), \mathbb{P})$, where $B(Q)$ denotes the Borel sigma algebra over the sample space Q. Given the design space $Y \subseteq \mathbb{R}^l$ and a measurable constraint function $g : Y{\times}Q{\to}\mathbb{R}$, there are three prevalent views of the optimization problem concerning the search for design parameter $y \in Y$ that satisfy the constraints $g(y, q) \leq 0$ "reliably" with respect to perturbation in the system uncertainty.

- **Robust Programs (RP)** consider reliability as the worst-case resolution of Q, *i.e.* for $\zeta \in \mathbb{R}_{\geq 0}$:

$$\text{RP} : \begin{cases} \min\limits_{y} & c^T y \\ \text{s.t.} & g(y, q) \leq \zeta \quad \text{for all } q \in Q. \end{cases}$$

- **Chance-Constraint Program (CCP)** consider reliability as the probabilistic resolution of Q, *i.e.* for $\epsilon \in [0, 1)$:

$$\text{CCP}_\epsilon : \begin{cases} \min\limits_{y} & c^T y \\ \text{s.t.} & \mathbb{P}[g(y, q) \leq 0] \geq 1 - \varepsilon. \end{cases}$$

- **Scenario Program (SP)** consider reliability as random selection of scenarios $q_1, \ldots, q_N \in Q$:

$$\text{SP} : \begin{cases} \min\limits_{y} & c^T y \\ \text{s.t.} & g(y, q_i) \leq 0 \quad \text{for } q_1, \ldots, q_N \in Q. \end{cases}$$

In an SP, we say that a constraint $g(y, q_i)$ is a *support constraint* if removing it changes the optimal value of the objective function. Similarly, we say that a set of constraints $S = \{g(y, q_1), \ldots, g(y, q_j)\}$ is a *support subsample* if the optimal solution of the SP is the same as the optimal solution of the SP with only the constraints present in S.

B. Discrete-time Dynamical System

A discrete-time dynamical system (or simply, a system) $\mathfrak{S}$ is a tuple $(\mathcal{X}, f)$, where $\mathcal{X} \subseteq \mathbb{R}^n$ denotes the state set of the system and $f : \mathcal{X} \to \mathcal{X}$ denotes the state transition function. The state evolution of the system is given by

$$\mathfrak{S} : x(t + 1) = f(x(t)). \tag{1}$$

A *trace* or *state sequence* of the system starting from a state x_0 is an infinite sequence $\langle x_0, x_1, \ldots \rangle$ such that $x_{i+1} = f(x_i)$ for all $i \in \mathbb{N}$. Throughout the rest of the paper, we assume that the state set $\mathcal{X}$ is uncountable but compact. We assume the system $\mathfrak{S}$ to be "unknown" in that the information about its transition function $f : \mathcal{X}{\to}\mathcal{X}$ is available only through samples.

C. Safety Verification and Barrier Certificates

A system $\mathfrak{S}$ is *safe* with respect to a set of initial states $\mathcal{X}_0$ and a set of unsafe states $\mathcal{X}_u$ if every trace starting from $\mathcal{X}_0$ never reaches $\mathcal{X}_u$, *i.e.*, for any trace $\langle x_0, x_1 \ldots \rangle$ from $\mathcal{X}_0$, we have that $x_i \notin \mathcal{X}_u$ for any $i \geq 0$. Given a system $\mathfrak{S}$ with initial states $\mathcal{X}_0$, and unsafe states $\mathcal{X}_u$, the *safety verification problem* is to determine whether the system is safe.

Definition 2.1 (Safety Barrier): A function $\mathcal{B} : \mathcal{X}{\to}\mathbb{R}$ is a *safety barrier certificate* for a system $\mathfrak{S}$ with initial states $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$ if there exists $\gamma < \lambda$ satisfying:

$$\mathcal{B}(x) \leq \gamma, \qquad \forall x \in \mathcal{X}_0, \tag{2}$$

$$\mathcal{B}(x) \geq \lambda, \qquad \forall x \in \mathcal{X}_u, \text{ and} \tag{3}$$

$$\mathcal{B}(f(x)) - \mathcal{B}(x) \leq 0, \qquad \forall x \in \mathcal{X}. \tag{4}$$

The existence of barrier certificates provide an inductive proof of the safety of the system.

Theorem 1 (Existence Implies Safety [9]): A system $\mathfrak{S}$ is safe if there exists a safety barrier certificate $\mathcal{B} : \mathcal{X} \to \mathbb{R}$ with respect to initial states $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$.

The k-inductive barrier certificates (k-BCs) are touted to expand the class of functions guaranteeing safety as, for a fixed template of barrier certificates, one may find k-BCs even when standard barrier certificates may not exist.

Definition 2.2 (k-Inductive Safety Barrier): A function $\mathcal{B} : \mathcal{X}{\to}\mathbb{R}$ is a k-inductive safety barrier certificate (k-SBC) for a system $\mathfrak{S}$ with initial states $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$, if there exists $\gamma < \lambda$ satisfying:

$$\bigwedge_{1 \leq i \leq k} (\mathcal{B}(f^i(x)) \leq \gamma), \quad \forall x \in \mathcal{X}_0, \tag{5}$$

$$\mathcal{B}(x) \geq \lambda, \quad \forall x \in \mathcal{X}_u, \tag{6}$$

$$\bigwedge_{1 \leq i < k} (\mathcal{B}(f^i(x)) \leq \gamma) \implies (\mathcal{B}(f^k(x)) \leq \gamma), \quad \forall x \in \mathcal{X}. \tag{7}$$

Similar to barrier certificates, the existence of k-BCs provides a k-inductive proof of the safety of the system.

Theorem 2 (Existence Implies Safety [5]): A system $\mathfrak{S}$ is safe if there exists a k-BC $\mathcal{B} : \mathcal{X} \to \mathbb{R}$ with respect to a set of initial states $\mathcal{X}_0$, and set of unsafe states $\mathcal{X}_u$.

D. Reachability Verification and Barrier Certificates

A trace $\langle x_0, x_1, \ldots \rangle$ is said to *reach* a target $\mathcal{X}_R$ if $x_i \in \mathcal{X}_R$ for some $i \geq 0$. Alternatively, we say that a target set $\mathcal{X}_R$ can be reached from $\mathcal{X}_0$ if every trace starting from $\mathcal{X}_0$ reaches $\mathcal{X}_R$. Given a system $\mathfrak{S}$ with initial states $\mathcal{X}_0$ and target states $\mathcal{X}_R$, the *reachability verification problem* is to decide whether all traces of $\mathfrak{S}$ from $\mathcal{X}_0$ reach $\mathcal{X}_R$.

Barrier certificates and k-BCs can also be used to verify reachability as described in [10] and [6]. We consider a formulation of barrier certificates and k-BCs that verify reachability adapted from [6, Definition 18]. We rely on the following assumption to ensure reachability.

Assumption 1 (Forward Invariance Under $\mathcal{X}$): The state transition function $f : \mathcal{X} \to \mathcal{X}$ is forward invariant in $\mathcal{X}$. Observe that this can be verified by considering sets $\mathcal{X}_0 = \mathcal{X}$ and $\mathcal{X}_u = \mathbb{R}^n \setminus \mathcal{X}$ and trying to find a barrier certificate or k-SBC as in Definition 2.1 or 2.2.

Definition 2.3 (Reachability Barrier): A continuous function $\mathcal{B} : \mathcal{X} \to \mathbb{R}$ is a *reachability barrier certificate* for a

system $\mathfrak{S}$ with initial states $\mathcal{X}_0$ and target states $\mathcal{X}_R$, if there exist $\gamma \in \mathbb{R}_{\geq 0}$ and $\delta \in \mathbb{R}_{>0}$ satisfying:

$$\mathcal{B}(x) \leq \gamma, \quad \forall x \in \mathcal{X}_0 \text{ and} \tag{8}$$

$$\mathcal{B}(f(x)) - \mathcal{B}(x) \leq -\delta, \quad \forall x \in \mathcal{X} \setminus \mathcal{X}_R. \tag{9}$$

The proof connecting the existence of reachability barrier to the satisfaction of the reachability property is immediate.

Theorem 3 (Existence Implies Reachability): A system $\mathfrak{S}$ under Assumption 1 satisfies the reachability property if there exists a reachability barrier certificate.

Proof: Let us assume that there exists some trace $\langle x_0, x_1, \ldots \rangle$ starting from $\mathcal{X}_0$ that never reaches $\mathcal{X}_R$. From condition (8), we have $\mathcal{B}(x_0) \leq \gamma$. From condition (9), Assumption 1, and the fact that the trace never reaches $\mathcal{X}_R$, we have $\mathcal{B}(x_{i+1}) \leq \mathcal{B}(x_i) - \delta$ for every $i \in \mathbb{N}$. We thus have $\mathcal{B}(x_i) \leq \gamma - i\delta$ for every $i \in \mathbb{N}$. The value $\mathcal{B}(x_i)$ approaches $-\infty$ as i approaches ∞. Note, however, that the set $\mathcal{X}$ is compact and the function $\mathcal{B}$ is continuous hence the value of $\mathcal{B}$ is bounded over $\mathcal{X}$ and can never be $-\infty$. ∎

The k-inductive reachability barrier certificates can be defined in a straightforward manner.

Definition 2.4 (k-Inductive Reachability Barrier): A continuous function $\mathcal{B} : \mathcal{X} \to \mathbb{R}$ is a k-inductive reachability barrier certificate (k-RBC) with initial states $\mathcal{X}_0$ and target states $\mathcal{X}_R$, if there exists $\gamma \in \mathbb{R}_{\geq 0}$, $\delta \in \mathbb{R}_{>0}$ satisfying:

$$\mathcal{B}(x) \leq \gamma, \quad \forall x \in \mathcal{X}_0, \tag{10}$$

$$\mathcal{B}(x) \leq \gamma \implies \mathcal{B}(f^k(x)) - \mathcal{B}(x) \leq -\delta, \quad \forall x \in \mathcal{X} \setminus \mathcal{X}_R. \tag{11}$$

Theorem 4: A system $\mathfrak{S}$ under Assumption 1 satisfies the reachability property if there exists a k-RBC.

The proof of Theorem 4 follows that of Theorem 3, except that we have $\mathcal{B}(x_{i+k}) \leq \mathcal{B}(x_i) - i\delta$ instead of $\mathcal{B}(x_{i+1}) \leq \mathcal{B}(x_i) - \delta$, leading again to a contradiction.

E. Barrier Certificates for Unknown Systems

We consider barrier certificates and k-BCs to be weighted sums of m non-linear basis functions $p_1(x), \ldots, p_m(x)$, *i.e.*, $\mathcal{B}(b, x) = \sum_{j=1}^{m} b_j p_j(x)$. For simple presentation, we assume the barrier certificate to be polynomial and, hence, functions $p_j(x)$ to be monomials. Given a fixed template, the search for k-BCs as in Definition 2.2 and 2.4, reduces to a search for the values $b_1, \ldots, b_m$ that satisfy the above conditions. To do so, however, one is required to know the values of $f(x)$ for every state $x \in \mathcal{X}$ or every $x \in \mathcal{X} \setminus \mathcal{X}_R$ due to conditions (7) and (11). Since the system is unknown, we recourse to scenario-based approach.

Problem 1 (k-SBC for Unknown Systems): Given an unknown system $\mathfrak{S}$, initial states $\mathcal{X}_0$, and unsafe states $\mathcal{X}_u$, find a k-SBC as in Definition 2.2 using a finite number of samples that can ensure the system is safe with a given confidence of at least $1 - \beta$, with $\beta \in [0, 1)$.

Problem 2 (k-RBC for Unknown Systems): Given an unknown system $\mathfrak{S}$, initial states $\mathcal{X}_0$, target states $\mathcal{X}_R$, find a k-RBC as in Definition 2.4 using a finite number of samples that can ensure the system reaches the target states with a given confidence of at least $1 - \beta$, with $\beta \in [0, 1)$.

III. A Scenario-Based Approach to k-BCs

A. k-Inductive Safety Barrier Certificates

Recall the k-inductive safety barrier certificate characterization from Definition 2.2. In order to use the scenario program to compute k-SBC, let us recast conditions (5)-(7) as an optimization problem. Note that condition (7) has an implication, and so we first replace this with a sufficient condition via the S-procedure [20].

Lemma 1 (S-procedure): Consider the constraint:

$$(\gamma - \mathcal{B}(b, f^k(x))) - \sum_{0 \leq i < k} \tau_i (\gamma - \mathcal{B}(b, f^i(x))) \geq 0, \forall x \in \mathcal{X}. \tag{12}$$

The existence of values $\tau_0, \ldots, \tau_{k-1} \in \mathbb{R}_{\geq 0}$ satisfying condition (12), imply the satisfaction of condition (7).

Remark 1: Note that condition (12) is sufficient for ensuring condition (7).

Lemma 1 allows us to reformulate the search for a k-SBC as a search for a solution to the following robust program.

$$\text{RP}^k : \begin{cases} \min\limits_{d} \quad \eta \\ \text{s.t.} \ \max\limits_{1 \leq j \leq 4} \{g_j(d, x)\} \leq \eta, \forall x \in \mathcal{X} \\ \quad d = [\eta; \gamma; \lambda; \tau; b] \in \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}^k_{\geq 0} \times \mathbb{R}^m, \end{cases}$$

where,

$$g_1(d, x) = \big(\max_{0 \leq i \leq k} \{(\mathcal{B}(b, f^i(x)) - \gamma)\} \big) \mathbf{I}_0(x), \tag{13}$$

$$g_2(d, x) = \big(-\mathcal{B}(b, x) + \lambda \big) \mathbf{I}_u(x), \tag{14}$$

$$g_3(d, x) = \sum_{i=0}^{k-1} \tau_i (\gamma - \mathcal{B}(b, f^i(x))) - (\gamma - \mathcal{B}(b, f^k(x))), \tag{15}$$

$$g_4(d, x) = \gamma + \epsilon - \lambda. \tag{16}$$

Here, functions $\mathbf{I}_0(x)$ and $\mathbf{I}_u(x)$ are indicator functions for the initial and unsafe sets, $\epsilon \in \mathbb{R}_{>0}$ is a small positive value, and variables τ_i indicate the decision variables added by the use of the S-procedure.

Let a feasible solution of RP^k be η^*_{RP}. If $\eta^*_{\text{RP}} \leq 0$, then condition (13) implies the satisfaction of condition (5), while conditions (14)-(15) imply conditions (6)-(7) and condition (16) ensures that $\gamma < \lambda$. Thus a solution to the above RP with $\eta^*_{\text{RP}} \leq 0$ gives us a k-SBC and a proof that the system is safe. Unfortunately, the above RP has uncountably many constraints as the set $\mathcal{X}$ is uncountable and cannot be solved directly. Furthermore it relies on knowing the function f (which is unknown), to satisfy conditions (13)-(16), and hence one cannot use techniques such as semidefinite programming [21].

To adopt a sampling-based approach, we instead consider a scenario program [1] by drawing $3N$ samples and simulate the system for k-steps.

Assumption 2: We assume that we can draw $3N$ independent and identically distributed (i.i.d.) sample states and can simulate the system initiated from them and for some fixed number of time-steps to construct the following sets:

$$\mathcal{I} = \big\{ \big(\hat{x}_i, f(\hat{x}_i), \ldots, f^k(\hat{x}_i)\big) \mid \hat{x}_i \in \mathcal{X}_0 \big\}_{i=1}^{N},$$

$$\mathcal{U} = \big\{ \hat{x}_i \mid \hat{x}_i \in \mathcal{X}_u \big\}_{i=1}^{N}, \text{ and}$$

$$\mathcal{E} = \big\{ \big(\hat{x}_i, f(\hat{x}_i), \ldots, f^k(\hat{x}_i)\big) \mid \hat{x}_i \in \mathcal{X} \big\}_{i=1}^{N}$$

This allows us to construct the scenario program SP^k as follows:

$$\text{SP}^k: \begin{cases} \min\limits_{d} \quad \eta \\ \text{subject to} \quad g_1(d,\hat{x}_i) \le \eta, \forall(\hat{x}_i,\dots,f^k(\hat{x}_i)) \in \mathcal{I} \\ \qquad\qquad g_2(d,\hat{x}_i) \le \eta, \forall \hat{x}_i \in \mathcal{U}, \\ \qquad\qquad g_3(d,\hat{x}_i) \le \eta, \forall(\hat{x}_i,\dots,f^k(\hat{x}_i)) \in \mathcal{E}, \\ \qquad\qquad g_4(d,\hat{x}_i) \le \eta, \forall(\hat{x}_i,\dots,f^k(\hat{x}_i)) \in \mathcal{E}, \\ \qquad d = [\eta;\gamma;\lambda;\tau;b] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^k_{\ge 0}\times\mathbb{R}^m, \end{cases}$$

where functions g_j are the same as in conditions (13)-(16) for all $1 \le j \le 4$. Let the sub-optimal value of SP^k be η^*, the values of the decision variables be d^*_{SP}, and the number of support subsamples be s^*. Note that the programs RP^k and SP^k are non-convex due to the bilinear terms present in $g_3(d,x)$ and $g_3(d,\hat{x}_i)$, $\forall i \in \{1,\dots,N\}$, respectively. This is due to the multiplication of the decision variables τ_i, with the coefficients of the k-SBC b and the constant γ. Thus, we cannot extend earlier results from [3], [4] directly because they only deal with convex programs.

To determine whether a solution to SP^k is also a feasible solution to RP^k such that $\eta^*_{\text{RP}} \le 0$, we make use of a function $\varepsilon : \{0,1,\dots,N\} \to [0,1]$ taken from [19]. Let $\beta \in [0,1)$ and $N \in \mathbb{N}$ be fixed a priori, then $\varepsilon(r)$ is defined as[1]:

$$\varepsilon(r) = \begin{cases} 1 & \text{if } r = N, \\ 1 - \sqrt[N-r]{\frac{\beta}{N\binom{N}{r}}} & \text{otherwise.} \end{cases} \tag{17}$$

Furthermore, we assume functions g_1, g_2, g_3, and g_4 to be Lipschitz-continuous in x over the sets $\mathcal{X}_0$, $\mathcal{X}_u$, $\mathcal{X}$, and $\mathcal{X}$, respectively, with constants bounded from above by $\mathcal{L}'$.

We now state the main theorem we obtain for safety.

Theorem 5 (Safety: Correctness): Consider an unknown system $\mathfrak{S} = (\mathcal{X}, f)$ with an initial states $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$. Let SP^k be constructed by drawing $3N$ i.i.d. samples as specified in Assumption 2. Let the values of the decision variables for a sub-optimal solution of SP^k be $d^*_{\text{SP}} = [\eta^*;\gamma^*;\lambda^*;\tau^*;b^*]$ and the number of support samples be s^*. Let $\beta \in [0,1)$ be fixed a priori, ε be defined as in equation (17) and $\nu = \mathcal{L}'(\sqrt[n]{\varepsilon(s^*)})$. If

$$\eta^* + \nu \le 0, \qquad \text{(Litmus Test)}$$

then the system is safe with a confidence of $1 - 3\beta$.

Proof: To relate the sub-optimal value of SP^k to a feasible value of RP^k, we construct three RPs: $\text{RP}^{k(1)}$, $\text{RP}^{k(2)}$, and $\text{RP}^{k(3)}$ as follows.

$$\text{RP}^{k(1)}: \begin{cases} \min\limits_{d} \quad \eta \\ \text{subject to: } g_1(d,x) \le \eta, \forall x \in \mathcal{X}_0 \qquad (\ddagger) \\ \qquad d = [\eta;\gamma;\lambda;\tau;b] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^k_{\ge 0}\times\mathbb{R}^m. \end{cases}$$

Similarly, we construct $\text{RP}^{k(2)}$ by replacing the constraint marked with $(\ddagger)$ with

$$g_2(d,x) \le \eta, \forall x \in \mathcal{X}_u,$$

while $\text{RP}^{k(3)}$ is constructed by replacing $(\ddagger)$ with

$$\max_{3\le j\le 4}\{g_j(d,x)\} \le \eta, \forall x \in \mathcal{X}.$$

Let a *common* feasible solution for $\text{RP}^{k(1)}$, $\text{RP}^{k(2)}$, and $\text{RP}^{k(3)}$ be d^*_{RP}, such that the cost function $\eta^*_{\text{RP}} \le 0$, then this is also a solution to RP^k. Further, we can split SP^k into three scenario programs $\text{SP}^{k(1)}$, $\text{SP}^{k(2)}$, and $\text{SP}^{k(3)}$ corresponding to $\text{RP}^{k(1)}$, $\text{RP}^{k(2)}$, and $\text{RP}^{k(3)}$, respectively. Observe that any feasible solution to SP^k is also a feasible solution to each of the three SPs. Further, note that the number of support constraints for each of these SPs is at most s^*. Define three chance-constraint programs [1] $\text{CCP}^{k(1)}_{\varepsilon(s^*)}$, $\text{CCP}^{k(2)}_{\varepsilon(s^*)}$, and $\text{CCP}^{k(3)}_{\varepsilon(s^*)}$ from the three RPs:

$$\text{CCP}^{k(1)}_{\varepsilon(s^*)}: \begin{cases} \min\limits_{d} \quad \eta \\ \text{s.t.} \quad \mathbb{P}\left[g_1(d,x) \le \eta\right] \ge 1 - \varepsilon(s^*), \\ \qquad d = [\eta;\gamma;\lambda;\tau;b] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^k_{\ge 0}\times\mathbb{R}^m. \end{cases}$$

$\text{CCP}^{k(2)}_{\varepsilon(s^*)}$ and $\text{CCP}^{k(3)}_{\varepsilon(s^*)}$ are constructed similarly and their details are omitted. According to [19, Theorem 1] a feasible solution d^*_{SP} of $\text{SP}^{k(i)}$ is NOT a feasible solution to $\text{CCP}^{k(i)}_{\varepsilon(s^*)}$ with a confidence of at most β for all $i \in \{1,2,3\}$. Define events indicating that d^*_{SP} is not a feasible solution for $\text{CCP}^{k(i)}_{\varepsilon(s^*)}$. Then, the probability that this solution fails to satisfy at least one of the CCPs is upper bounded by the sum of the probabilities via a union-bound argument and is hence 3β. Thus, d^*_{SP} is a feasible solution to the three CCPs with a confidence of at least $1 - 3\beta$. Let $h : [0,1] \to \mathbb{R}_{\ge 0}$ be a uniform-level set bound (ULB) as defined in [2, Definition 3.1]. We can consider the function $h(\xi)$ to be $\mathcal{L}'\sqrt[n]{\xi}$ from [2, Proposition 3.8] and [2, Remark 3.9 (ii)]. Let $\nu = \mathcal{L}'\sqrt[n]{\varepsilon(s^*)}$ and consider the three RPs $\text{RP}^{k(1)}_\nu$, $\text{RP}^{k(2)}_\nu$, and $\text{RP}^{k(3)}_\nu$:

$$\text{RP}^{k(1)}_\nu: \begin{cases} \min\limits_{d} \quad \eta \\ \text{s.t.} \quad g_1(d,x) \le \eta + \nu, \ \ \forall x \in \mathcal{X}_0, \\ \qquad d = [\eta;\gamma;\lambda;\tau;b] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^k_{\ge 0}\times\mathbb{R}^m. \end{cases}$$

$\text{RP}^{k(2)}_\nu$ and $\text{RP}^{k(3)}_\nu$ are constructed in a similar way and their details are omitted due to lack of space. According to [2, Lemma 3.2], a feasible solution of $\text{CCP}^{k(i)}_{\varepsilon(s^*)}$ is also a feasible solution to RP^i_ν for all $i \in \{1,2,3\}$. Thus, we have $g_j(d^*_{\text{SP}},x) \le \eta^* + \nu$ for all $1 \le j \le 4$ and for all $x \in \mathcal{X}_0$, $\mathcal{X}_u$, or $\mathcal{X}$ respectively, with a confidence of at least $1 - 3\beta$. We observe that the variable η is not present in functions g_j. Consider $d^*_r = [\eta^* + \nu;\gamma^*;\lambda^*;\tau^*;b^*]$. This is a common feasible solution to all three RPs with a confidence of at least $1 - 3\beta$. Using Lemma 1, as well as the fact that $\eta^* + \nu \le 0$, we conclude the function $\mathcal{B}(b^*,x)$ to be a k-SBC with a confidence of at least $1 - 3\beta$. Using Theorem 2, we infer the system to be safe with a confidence of $1 - 3\beta$. ■

B. k-Inductive Reachability Barrier Certificate

The problem of finding k-RBCs can similarly be posed as an RP and SP denoted by RP^r and SP^r, respectively.

Theorem 6 (Reachability: Correctness): Consider an unknown system $\mathfrak{S} = (\mathcal{X}, f)$ with initial states $\mathcal{X}_0$ and target

[1] As usual, $\binom{N}{r}$ represents the number of ways of choosing r elements from a set of N elements.

states $\mathcal{X}_R$. Let SP^r be constructed by drawing $3N$ i.i.d. samples and simulating the system for k-units of time from these points. Let the values of the decision variables for a sub-optimal solution of SP^r be $d^*_{\text{SP}} = [\eta^*; \gamma^*; \lambda^*; \tau^*; b^*]$ and the number of support samples be s^*. Let $\beta \in [0, 1)$ be fixed a priori, ε be defined as in equation (17) and $\nu = \mathcal{L}'(\sqrt[n]{\varepsilon(s^*)})$. If $\eta^* + \nu \leq 0$, then the system satisfies reachability with the confidence of at least $1 - 3\beta$.

The proof of Theorem 6 is similar to that of Theorem 5 and is omitted here due to lack of space.

Remark 2: In some cases (c.f. Case Study IV-B) increasing the value of k, leads to the value of $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)}$ to be more negative (increase in absolute value). When one fails to find a standard barrier approach using the above sampling-based technique, *i.e.*, the value of $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)} > 0$, one usually increases N to decrease the value of $\sqrt[n]{\varepsilon(s^*)}$. Instead, one may choose to increase the value of k to make the value of η^* to become more negative and still find a k-SBC without having to increase N.

C. Computing k-BCs and Lipschitz Constants

To determine the k-inductive barrier certificate as well as solve the SP^k, we make use of the idea of V-K iteration [22]. First we consider a template for the barrier certificate by restricting the degree of the polynomial. We then take an initial guess for the values of variables $\tau_0, \ldots, \tau_{k-1}$. This reduces the bilinear programming problem to a linear programming problem. We then use a solver such as Gurobi [23] to find the values of the coefficients of the candidate polynomial, as well as γ, μ, and λ. We now consider the coefficients of the barrier certificate to be fixed and then solve a linear programming problem over the variables $\tau_0, \ldots, \tau_{k-1}$. We repeat this process until the difference in the sub-optimal values is negligible and consider the values of the decision variables at this point to be the sub-optimal values which we denote as $d^* = [\eta^*; \gamma^*; \lambda^*; \tau^*; b^*]$. If $\eta^* + \nu \leq 0$, then the values of b^* correspond to the coefficients of our k-SBC, and so we have $\mathcal{B}(x) = \sum_{j=1}^{m} b^*_j p_j(x)$.

To find the value of $\varepsilon(s^*)$, we first use the algorithm presented in [19, Section II] to find the number of support constraints s^*. The procedure to do so is as follows. We remove constraints from the SP one by one and check if the sub-optimal value changes more than a given threshold (cf. 10^{-6} in the case studies). If the removal of a constraint causes the sub-optimal value to change, we consider the corresponding constraint as a support constraint and add it back. If not we continue by removing the next constraint. We repeat this procedure until we consider all the constraints. We denote the number of support constraints as s^*. We then calculate the value of $\sqrt[n]{\varepsilon(s^*)}$. To determine the Lipschitz-constants of the functions $g_j(d, x)$, we follow the proposed method in [24, Section 2]. We now compute the value of $\mathcal{L}' \sqrt[n]{\varepsilon(s^*)}$ and determine if $\eta + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)} \leq 0$. If so, we conclude that the system is safe with a confidence of $1 - 3\beta$, and otherwise it is inconclusive.

We consider the estimation technique for the Lipschitz constants to be accurate and neglect the confidence involved in their calculations. We summarize our approach for safety verification in Algorithm 1. The algorithm for reachability verification is analogous, and hence omitted.

Algorithm 1 Scenario-Based Design of k-Barrier Certificates

procedure SAFETY VERIFICATION(N, β)
  Input: Number of samples N, threshold β
  Sample N points from $\mathcal{X}$.
  Simulate $\mathfrak{S}$ for k-steps from these points.
  Collect the data and build SP^k.
  Solve SP^k using V-K iteration.
  Let η^* be the value of the objective function.
  Compute the number of support constraints s^*.
  Calculate $\sqrt[n]{\varepsilon(s^*)}$.
  Estimate the Lipschitz constants of functions g_j.
  Consider the largest to be $\mathcal{L}'$.
  if $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)} \leq 0$
    return system safe with a confidence of $1 - 3\beta$
  else return inconclusive
end procedure

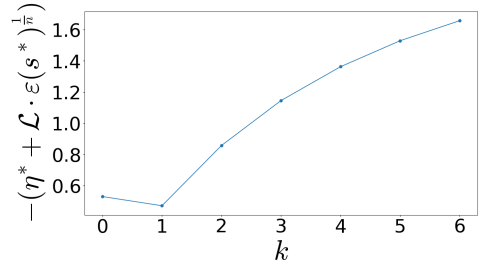
IV. Case Studies

A. Verification of Safety for an RLC circuit

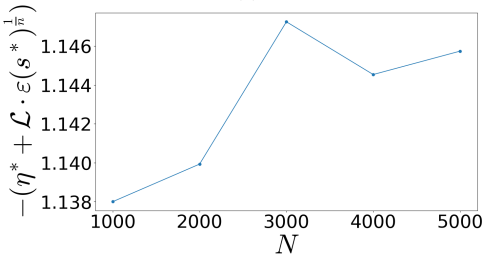
As a case study to experimentally demonstrate the effectiveness of our approach we consider the problem of demonstrating the safety of an RLC circuit. The dynamics of the system are described as follows and are adapted from [5].

$$\mathfrak{S} : \begin{cases} i(t+1) = i(t) + t_s(-\frac{R}{L} i(t) + -\frac{1}{L} v(t)), \\ v(t+1) = v(t) + t_s \frac{1}{C} i(t), \end{cases} \tag{18}$$

where $i(t)$ and $v(t)$ indicate the current and voltage of the system at time t, $t_s = 0.5s$ indicates the sampling time, $R = 3\Omega$, $L = 8$H, and $C = 0.5$F. We consider the state space of the system $\mathcal{X} = [-1, 2] \times [-4, 4]$, with the initial set of states $\mathcal{X}_0 = [0, 0.5] \times [0, 1]$ and the unsafe set of states $\mathcal{X}_u = [1, 2] \times [-4, 4]$. We consider the k-SBC to be of the form $\mathcal{B}(i, v) = b_1 i^2 + b_2 v^2 + b_3$. Let $k = 6$, fix $\gamma = 0$, $\lambda = 0.01$, $\epsilon = 0.01$, and sample $N = 60000$ points to formulate an SP^k. We solve SP^k via V-K iteration assuming the initial values of τ_i to be 0.001 and then make use of the linear programming solver Gurobi [23] to find the values of the decision variables as we alternate the V-K iterations. We find the sub-optimal value to be $\eta^* = -6.431$ and the equation of the barrier certificate to be $\mathcal{B}(i, v) = 100.0 \cdot i^2 - 1.834 \cdot v^2 - 64.2006$. We compute the number of support constraints $s^* = 3$, fix $\beta = 0.0001$, and find the value of $\varepsilon(s^*) = 0.000856$. We finally estimate the Lipschitz Constant as $\mathcal{L}' = 190$ and verify that $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)} \leq 0$. This informs us that the the system is safe with a confidence of at least 0.9997. Note that the corresponding scenario program to find a safety barrier certificate of the same template is *infeasible*. The computation takes around 120 minutes on a machine running MacOS 11.2 (Intel i9-9980HK with 64 GB of RAM).



(a)



(b)

Fig. 1: (a) Change in the value of $-(\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)})$ for different values of k with $N = 10000$ samples. (b) Change in the value of $-(\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)})$ for different values of N with $k = 3$, η^* is non-decreasing as N increases, however $\varepsilon(s^*)$ always decreases as N increases.

B. Verification of Reachability for a Room-Temperature

To demonstrate our approach for reachability, we consider the problem of verifying reachability for a room-temperature model. The model we consider is a non-stochastic version of the one considered in [6] with the following dynamics.

$$\mathfrak{S} : T(t+1) = (1 - t_s\alpha)T(t) + t_s\alpha T_e,$$

where $T(t)$ indicates the temperature at time t, $t_s = 5$ minutes is the sampling time, $\alpha = 0.04$ is the heat-exchange coefficient and $T_e = 15$C is the ambient temperature. We consider $\mathcal{X} = [18, 45]$ as the state space, $\mathcal{X}_0 = [23, 24]$ as the initial set, $\mathcal{X}_R = [18, 22]$ as the target set, and consider the template of the barrier certificate as $\mathcal{B}(T) = b_1 T + b_2$. We consider $N = 10000$ samples, $\beta = 0.0001$, $\delta = 0.02$, $\gamma = 0$, and the values of $k \in \{0, 1, \ldots, 6\}$, where we consider barrier certificates as in Definition 2.3 for $k = 0$. We observe that we can find reachability barrier certificates satisfying the template but note that the value of $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)}$ first increases as we increase k, and then decreases and becomes more negative as the value of k increases as shown in Figure 1a. Thus, it is easier to satisfy the conditions of Theorem 6 by increasing k while keeping N fixed.

The time to solve SP^r (the scenario program for k-RBCs as specified in Section III-B) increases from 0.7 to 4.23 seconds as k increases from 0 to 6. We also consider the change in the value of $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)}$ as N increases, for fixed $k = 3$ as shown in Figure 1b. While η^* may increase as N increases, $\varepsilon(s^*)$ decreases and so we notice $\eta^* + \mathcal{L}' \sqrt[n]{\varepsilon(s^*)}$ is not non-increasing or non-decreasing.

V. Conclusion

This paper extended the scenario-based approach to guarantee safety and reachability of a system with unknown dynamics for k-inductive barrier certificates. To do so, it reformulated the search for a k-inductive barrier certificate as a robust program, and considered an analogous scenario program by taking finitely many samples from the system. The scenario approach enables one to establish an out-of-sample performance guarantee based on the number of samples. We will investigate data-driven controller synthesis problem via barrier certificates in the future.

References

[1] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE TAC*, pp. 742–753, 2006.

[2] P. M. Esfahani, T. Sutter, and J. Lygeros, "Performance bounds for the scenario approach and an extension to a class of non-convex programs," *IEEE Transactions on Automatic Control*, pp. 46–58, 2014.

[3] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates," *IFAC-PapersOnLine*, pp. 7–12, 2021.

[4] A. Salamati and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach," *The 4th Annual Learning for Dynamics and Control Conference*, 2022.

[5] M. Anand, V. Murali, A. Trivedi, and M. Zamani, "Safety verification of dynamical systems via k-inductive barrier certificates," in *60th Conference on Decision and Control*, 2021.

[6] ——, "k-inductive barrier certificates for stochastic dynamical systems," in *25th International Conference on Hybrid Systems: Computation and Control*, 2022.

[7] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, "Hytech: A model checker for hybrid systems," *International Journal on STTT*, 1997.

[8] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer Science & Business Media, 2009.

[9] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International Workshop on Hybrid Systems: Computation and Control*, 2004, pp. 477–492.

[10] S. Prajna and A. Rantzer, "Convex programs for temporal verification of nonlinear dynamical systems," *SIAM Journal on Control and Optimization*, pp. 999–1021, 2007.

[11] P. Jagtap, S. Soudjani, and M. Zamani, "Temporal logic verification of stochastic systems using barrier certificates," in *ATVA*, 2018, pp. 177–193.

[12] ——, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, 2020.

[13] T. Wongpiromsarn, U. Topcu, and A. Lamperski, "Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems," *IEEE Transactions on Automatic Control*, 2015.

[14] S. Bak, "t-Barrier certificates: a continuous analogy to k-induction," in *6th IFAC Conference on ADHS*, 2018, pp. 145–150.

[15] S. Gao, J. Kapinski, J. Deshmukh, N. Roohi, A. Solar-Lezama, N. Arechiga, and S. Kong, "Numerically-robust inductive proof rules for continuous dynamical systems," in *CAV*, 2019, pp. 137–154.

[16] A. Solar-Lezama, *Program Synthesis by Sketching*, ser. PhD thesis, University of California, Berkeley, 2008.

[17] S. Gao, J. Avigad, and E. M. Clarke, "δ-complete decision procedures for satisfiability over the reals," in *Automated Reasoning*, B. Gramlich, D. Miller, and U. Sattler, Eds., 2012, pp. 286–300.

[18] S. Gao, S. Kong, and E. M. Clarke, "dReal: An SMT solver for nonlinear theories over the reals," in *Automated Deduction – CADE-24*, 2013, pp. 208–214.

[19] M. C. Campi, S. Garatti, and F. A. Ramponi, "A general scenario theory for nonconvex optimization and decision making," *IEEE Transactions on Automatic Control*, pp. 4067–4078, 2018.

[20] S. V. Gusev and A. L. Likhtarnikov, "Kalman-Popov-Yakubovich lemma and the S-procedure: A historical essay," *Automation and Remote Control*, 2006.

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

[22] A. Hassibi, S. Boyd, and J. How, "Control of asynchronous dynamical systems with rate constraints on events," in *38th IEEE Conference on Decision and Control*, 1999, pp. 1345–1351.

[23] Gurobi Optimization, LLC, "Gurobi Optimizer Reference Manual," 2021. [Online]. Available: https://www.gurobi.com

[24] G. Wood and B. Zhang, "Estimation of the lipschitz constant of a function," *Journal of Global Optimization*, pp. 91–103, 1996.