Safety Verification of Dynamical Systems via $k$-Inductive Barrier Certificates

Mahathi Anand, Vishnu Murali, Ashutosh Trivedi and Majid Zamani

Abstract—Safety verification of dynamical systems via barrier certificates has recently gained considerable attention. A barrier certificate is typically a real-valued function over states of the system such that its value over the unsafe states is strictly greater than its value at the initial states. Moreover, the system dynamics must guarantee a decrease in the value of the barrier certificate in time with each transition. The existence of a barrier certificate thus ensures that the system trajectories never reach unsafe regions. Unfortunately, these conditions are often restrictive as they require barrier certificates to be non-increasing at every time step. Inspired by the success of $k$-induction in software verification, we propose two refinements of the notion of barrier certificates. In our first refinement of $k$-inductive barrier certificates, we relax the strict non-increment requirement to a net non-increment in $k$-steps with a potential (bounded) increment in each step. On the other hand, the second refinement of $k$-inductive barrier certificates relaxes the strict non-increment requirement at each step to a strict safety requirement under the assumption that the previous $k$-steps remained safe. We present two computational methods based on sum-of-squares (SOS) programming and SMT solvers to synthesize suitable $k$-inductive barrier certificates and demonstrate their effectiveness over a case study.

I. INTRODUCTION

The control of safety-critical systems demands a rigorous proof of the correctness of its behaviors under some given initial conditions. The safety verification problem, a canonical verification objective for safety-critical systems, is to certify that all of the system trajectories avoid visiting unsafe or undesirable configurations. While over finite state spaces, the safety verification reduces to graph reachability, it is computationally hard for complex systems evolving over continuous state spaces. The recent proliferation of cyber-physical systems (CPS)—systems with integrated physical and software components—across a wide range of safety-critical applications including air traffic control, power systems, and medical devices, has spurred great interest in the safety verification of systems with complex dynamics [1].

A leading approach for safety verification for discrete systems, such as digital hardware and software systems, is based on the idea of inductive invariants [2], [3]. An inductive invariant is a property over the state space which can be shown to hold universally along the reachable state space via structural induction over syntactic program structure.

Barrier certificates, introduced by Prajna and Jadabai [4], encapsulate the spirit of inductive invariants for continuous-state spaces and have been initially proposed for the safety verification of nonlinear dynamical systems. Barrier certificates are real-valued functions that act as a barrier between the safe and the unsafe regions of the state space and provide sufficient conditions to verify whether the barrier is crossed by the system trajectories. Since their introduction, the barrier certificates approach for safety verification has been extended to hybrid [5] and stochastic systems [6], [7].

Unfortunately, the conditions presented in the aforementioned literature are restrictive as they require the inductive invariant to hold with every single transition step and the value of barrier certificates to be decaying at each time step. Therefore, in cases where these conditions cannot be met, one may not be able to prove safety using these approaches, even when the system is safe. The $k$-induction principle—by Sheeran et. al [8]—aims to alleviate these issues in the safety verification of finite-state systems as well as software programs [9], [10]. This paper extends $k$-induction principle to barrier certificates by introducing $k$-inductive barrier certificates for discrete-time dynamical systems.

Contributions. We propose two different notions of $k$-inductive barrier certificates which relax the traditional conditions such that a larger class of functions can behave as $k$-inductive barrier certificates, while still ensuring safety specifications. We motivate these notions via simple finite-state illustrative example (cf. Example 2.2) and show that the second notion of $k$-inductive barrier certificates are more expressive than the first (cf. Example 3.5) for a given template class of barrier functions. Additionally, under some mild assumptions on the dynamics of the system as well as the regions of interest, we present two computational methods based on sum-of-squares (SOS) optimization and Satisfiability Modulo Theory (SMT) solvers to compute $k$-inductive barrier certificates. We demonstrate the effectiveness of our proposed notions over a numerical case study.

Related Work. A generalization of barrier certificates utilizing the $k$-induction principle has recently been proposed in [11]. Our proposal differs from this work in three main directions. First, the result in [11] considers continuous-time dynamical systems while our paper targets and exploits the properties of discrete-time systems. Second, the conditions presented in [11] rely on a time-bounded reachability analysis along the barrier in order to verify safety, whereas we do not have such requirements. Lastly, the implementation technique presented in [11] assumes the barrier certificate

This work was supported in part by the NSF under grant ECCS-2015403 and the German Research Foundation (DFG) through the Research Training Group 2428.

Mahathi Anand and Majid Zamani are with the Computer Science Department, LMU Munich, Germany. Vishnu Murali, Ashutosh Trivedi, and Majid Zamani are with the Computer Science Department, University of Colorado Boulder, USA. Emails: mahathi.anand@lmu.de, {vishnu.murali,ashutosh.trivedi,majid.zamani}@colorado.edu
is given as input data and utilizes reachability analysis to verify a posteriori whether the barrier certificate satisfies the required conditions. On the other hand, in this paper, we present different computational approaches to search for suitable barrier certificates of specified parametric forms (e.g. polynomial functions). The first definition of $k$-inductive barrier certificates presented in this paper (cf. Definition 3.1) is similar to the Type 2 barrier functions studied in [12]. However, our formulation is in the context of discrete-time systems rather than continuous-time ones as in [12]. Moreover, conditions in [12] require strict contraction of the barrier certificates from the initial set after a certain time period, whereas our conditions are more relaxed.

**Organization.** The paper is structured as follows. Section II discusses some preliminary concepts relevant to the paper. The main theoretical results are presented in Section III, followed by implementation techniques in Section IV. Finally, we discuss a case study demonstrating the effectiveness of our results in Section V, followed by a brief conclusion.

II. PRELIMINARIES

A. Notations

We denote the set of real, positive real and non-negative real numbers by $\mathbb{R}$, $\mathbb{R}_{>0}$ and $\mathbb{R}_{\geq 0}$, respectively. Similarly, the set of non-negative integers and positive integers are denoted by $\mathbb{N}$ and $\mathbb{N}_{>1}$, respectively. The $n$-dimensional Euclidean space is denoted by $\mathbb{R}^n$.

For two sets $A$ and $B$, a function $f : A \rightarrow B$ is a mapping from $A$ to $B$. The identity function on the set $A$ is denoted by $\text{id}_A$. Given three sets $A, B, C$ and functions $f : A \rightarrow B$ and $g : B \rightarrow C$, the composition of functions $f$ and $g$ is denoted by $g \circ f : A \rightarrow C$. For a function $f : A \rightarrow A$ and $n \in \mathbb{N}$, we use $f^n$ to denote the $n$th iterate of the function $f$ defined as $f^0 = \text{id}_A$ and $f^{n+1} = f \circ f^n$ when $n > 0$.

We use logical operators $\land$, $\lor$ and $\implies$ for conjunction, disjunction and implication, respectively. Similarly, we use quantifiers $\exists$ and $\forall$ to denote the existential and universal quantification, respectively.

B. Barrier Certificates for Discrete-time Dynamical Systems

We consider the discrete-time dynamical system:

$$\mathcal{S} : x(t+1) = f(x(t)), \quad (II.1)$$

where $x(t) \in X$, $X \subseteq \mathbb{R}^n$, is the state of the system at time step $t \in \mathbb{N}$ and $f : X \rightarrow X$ is the transition function that characterizes the state evolution of the system. We use $x_{x_0} = (x(0), x(1), \ldots)$ to denote the state sequence of the system $\mathcal{S}$ starting from the initial state $x(0) = x_0$.

We are interested in verifying safety specifications for the system $\mathcal{S}$ such that state sequences $x_{x_0}$ of $\mathcal{S}$ do not visit given unsafe regions. Barrier certificates separate safe and unsafe states of the system by acting as a barrier between them, thereby providing sufficient conditions for safety.

**Definition 2.1 (Barrier Certificate):** We say that a function $B : X \rightarrow \mathbb{R}$ is a barrier certificate for the system $\mathcal{S}$ with respect to a set of initial states $X_0 \subseteq X$ and a set of unsafe states $X_u \subseteq X$, if the following conditions hold:

$$B(x) \leq 0, \quad \text{for all } x \in X_0, \quad (II.2)$$

$$B(x) > 0, \quad \text{for all } x \in X_u, \quad (II.3)$$

$$B(f(x)) - B(x) \leq 0, \quad \text{for all } x \in X. \quad (II.4)$$

It is straightforward to see that barrier certificates provide sufficient conditions ensuring that the state sequences started in the initial set $X_0 \subseteq X$ never reach the unsafe region $X_u \subseteq X$. Since the condition (II.4) requires the barrier certificate to be non-increasing at every time step, it ensures that the state sequences never cross the level set $B(x) = 0$. In other words, the state sequences of the system $\mathcal{S}$ always remain in the safe regions. Figure 1 demonstrates the safety verification using barrier certificates. For additional information and detailed proofs, we refer the interested readers to [4].

In order to prove that a system is safe, it suffices to discover a barrier certificate. The search for a barrier certificate can be performed in a principled fashion by restricting the search space to a given template (e.g. polynomial functions of a specified degree) and then employing appropriate search techniques such as sum-of-squares (SOS) programming [13] or satisfiability modulo theory (SMT) solvers [14] to compute barrier certificates satisfying conditions (II.2)-(II.4).

However, condition (II.4) can be quite conservative as it requires the desired barrier certificate to decay at every time step/transition. Therefore, in many cases, no suitable barrier certificate with a given template can be found for a system $\mathcal{S}$ even if the system is safe as shown in the following example.

**Example 2.2:** Consider a finite system $\mathcal{S}$ as shown in Figure 2 with $x \in X = \{0, 1, 1.25, 1.5, 1.75, 2, 2.25, 2.75\}$.
as the states of the system with \( x = 1 \) as the initial state and \( x = 2.75 \) as the unsafe state. We want to verify that the unsafe state \( x = 2.75 \) is never visited by any state sequence of the system. One can immediately see that this property trivially holds, as there is no way to reach the state \( x = 2.75 \) from the initial state \( x = 1 \). Unfortunately, we cannot utilize barrier certificates provided in Definition 2.1 to obtain safety guarantees for the system, when, for instance, the template of barrier certificates is fixed to be linear, i.e., \( B(x) = ax + b \).

This can be shown as follows. From condition (II.2) for the initial state \( x = 1 \), we have \( a + b < 0 \). Similarly, from condition (II.3) for the unsafe state \( x = 2.75 \), we have that \( 2.75a + b > 0 \). Now, utilizing condition (II.4) for the transition from the state \( x = 2 \) to \( x = 0 \), we get the inequality \( a \geq 0 \). Similarly, for the transition from the state \( x = 2.75 \), we obtain \( a \leq 0 \). The only possible solution is \( a = 0 \), from which we obtain the barrier certificate as \( B(x) = b \). But this results in a contradiction between conditions (II.2) and (II.3). Therefore, no linear barrier certificate exists for this system, even though the system satisfies the safety property.

In the following sections, we show that one can leverage the \( k \)-induction principle, often used in software verification [15], [16], to formulate a modified notion of barrier certificates that we dub \( k \)-inductive barrier certificates. The constraints for these barrier certificates are more relaxed, and their existence implies safety. Therefore, a system \( S \) that does not admit a standard barrier certificate according to Definition 2.1 may admit a \( k \)-inductive barrier certificate satisfying a set of conditions such that the state sequences of the system remain in the safe regions. For instance, we show that Example 2.2 admits a \( k \)-inductive linear barrier certificate even though it does not admit a standard one. In the next section, we first describe in detail the \( k \)-induction principle and then introduce the notion of \( k \)-inductive barrier certificates that utilize this principle to provide sufficient conditions for ensuring safety.

III. \( k \)-INDUCTIVE BARRIER CERTIFICATES

A. The \( k \)-Induction Principle

An inductive proof for a property \( P \) consists of a base case, an inductive hypothesis and an inductive step. In a standard inductive proof, also called as weak induction, the inductive hypothesis consists of an assumption that the property \( P \) holds at any given step, which is used to imply that the property also holds in the next step. Formally, the induction for property \( P \) is formulated as follows:

\[
\begin{align*}
& P(0) \text{ and } \\
& P(n) \implies P(n+1) \text{ for every } n \in \mathbb{N} \quad \text{(base)} \\
& \implies P(n) \text{ for every } n \in \mathbb{N} \text{. (induction)}
\end{align*}
\]

In contrast, \( k \)-induction assumes a stronger inductive hypothesis that the property \( P \) holds at all steps until the \( k \)th step. The stronger hypothesis makes the property \( P \) easier to prove in the inductive step due to the availability of more information. Mathematically, \( k \)-induction for property \( P \) is formulated as follows:

\[
\begin{align*}
& \bigwedge_{0 \leq i < k} P(i) \text{ and } \\
& P(n) \implies P(n+k), \text{ for every } n \in \mathbb{N} \text{ (induction)} \\
& \implies P(n) \text{ for every } n \in \mathbb{N}.
\end{align*}
\]

As it can be seen, the property \( P \) needs to be shown to hold true in the first \( k \) steps as the base case. The inductive hypothesis is essentially the antecedent of the inductive step, where the property \( P \) is assumed to hold true in the first \( k \) steps to show that the consequent \( P(n+k) \) also holds.

Barrier certificates for safety properties, as presented in Definition 2.1, are comparable to standard inductive proofs. To clarify this, condition (II.2) presents the base case, where the values of the barrier certificate at initial states of the system are such that the state sequence always begins from the safe set. Then, condition (II.4) is analogous to the inductive step which ensures that the value of barrier certificate is non-increasing at each time step, so that the state sequence never reaches unsafe set due to condition (II.3). However, due to the weaker construction of the inductive hypothesis, condition (II.4) is difficult to satisfy. One could relax these conditions by utilizing \( k \)-inductive proofs rather than standard induction. In the following subsection, we introduce \( k \)-inductive barrier certificates based on \( k \)-inductive proofs that can potentially relax conditions (II.2)-(II.4) while still providing sufficient conditions for safety verification.

B. \( k \)-Inductive Barrier Certificates

Next, we introduce two different notions of \( k \)-inductive barrier certificates and illustrate their merits with examples.

Definition 3.1: We say that a function \( B : X \to \mathbb{R} \) is a \( k \)-inductive barrier certificate for the system \( S \) with respect to a set of initial states \( X_0 \subseteq X \) and a set of unsafe states \( X_u \subseteq X \), if there exist \( k \in \mathbb{N}_>1 \), \( \epsilon \in \mathbb{R}_{\geq 0} \), and \( d > k\epsilon \) such that the following conditions hold:

\[
\begin{align*}
& B(x) \leq 0, \quad \text{for all } x \in X_0, \quad \text{(III.1)} \\
& B(x) \geq d, \quad \text{for all } x \in X_u, \quad \text{(III.2)} \\
& B(f(x)) - B(x) \leq \epsilon, \quad \text{for all } x \in X, \quad \text{(III.3)} \\
& B(f^k(x)) - B(x) \leq 0, \quad \text{for all } x \in X. \quad \text{(III.4)}
\end{align*}
\]

Now, we present the first result of the paper on the safety verification of systems \( S \) based on the existence of barrier certificates as in Definition 3.1.

Theorem 3.2: Consider a discrete-time dynamical system \( S \). If there exists a \( k \)-inductive barrier certificate \( B : X \to \mathbb{R} \) for \( S \) such that it is a \( k \)-inductive barrier certificate as in Definition 3.1 with respect to initial set \( X_0 \subseteq X \) and unsafe set \( X_u \subseteq X \), then state sequences \( x_{x_0} \) of \( S \) starting from \( x_0 \in X_0 \) never reach the unsafe region \( X_u \).

Proof: We begin the proof by assuming that there exists a function \( B : X \to \mathbb{R} \) such that conditions (III.1)-(III.4) hold but the system is not safe, i.e., there exists some time \( T \in \mathbb{N} \) such that \( x(T) \in X_u \). Let \( T = ik + k' \), for some
\[ B = d \quad B = 0 \]

Fig. 3. Safety verification using k-inductive barrier certificates presented in Definition 3.1.

\[ i \in \mathbb{N} \text{ and } k' < k. \quad \text{From conditions (III.1) and (III.2), we have } B(x_0) \leq 0 \text{ and } B(x(ik + k')) \geq d. \quad \text{From condition (III.3) and induction, we have that} \]

\[ B(x(ik + k')) \leq B(x(ik)) + k'\epsilon \leq B(x(ik)) + k\epsilon. \]

From (III.4) and induction, we get \( B(x(ik)) \leq B(x_0). \) From the two inequalities and condition (III.1), we obtain

\[ B(x(ik + k')) - B(x_0) \leq k\epsilon < d. \]

This is a contradiction to (II.3), implying that \( x(T) \notin X_u. \) Therefore, the state sequences \( x_{x_0} \) of \( \mathcal{S} \) that begin from \( x_0 \in X_0 \) remain in the safe regions.

In condition (III.4), the value of barrier certificate needs to be non-increasing only at every \( k \) time steps rather than at each time step. However, the additional condition (III.3) is required to ensure that state sequences do not reach unsafe regions within \( k \) time steps. Safety verification utilizing \( k \)-inductive barrier certificates presented in Definition 3.1 is demonstrated in Figure 3. Note that when \( k = 1, \epsilon = 0, \text{ and } d \in \mathbb{R}_{>0} \) is a small positive number, conditions (III.1)-(III.4) reduce to standard barrier certificate conditions (II.2)-(II.4). We now illustrate \( k \)-inductive barrier certificates as in Definition 3.1 by utilizing the finite system considered in Example 2.2.

Example 2.2 (Continued): Consider the finite system shown in Figure 2. In the previous section, we proved that no linear barrier certificate satisfying (II.2)-(II.4) exists for the system. Now, we show that we can instead utilize \( k \)-inductive barrier certificates to guarantee that the system indeed satisfies safety specifications. Consider a linear \( k \)-inductive barrier certificate as in Definition 3.1 given by \( B(x) = x - 1 \) with \( k = 3 \). Then, by assigning \( \epsilon = 0.5 \) and \( d = 1.6 \), it can be immediately observed that condition (III.1) is satisfied for initial state \( x = 1 \) and similarly, (III.2) is satisfied for unsafe state \( x = 2.75 \). Moreover, for all 1-step transitions possible in the system, we can verify that condition (III.3) also holds. Similarly, for all the possible 3-step transitions from the initial state to the unsafe state, condition (III.4) is valid. Therefore, it can be inferred that \( B(x) = x - 1 \) is indeed a 3-inductive barrier certificate as in Definition 3.1 that verifies the safety of the system.

As required by the \( k \)-induction principle, \( k \)-inductive barrier certificates in Definition 3.1 ensure the safety of the system for \( k \) consecutive steps by ensuring only a bounded increase at every step via condition (III.3). The non-increase of \( B(x) \) after every \( k \) steps via condition (III.3) is required to ensure the safety of the system at the \((k + 1)^{th}\) step, thus capturing the inductive step of the proof. Note that the system remains safe as long as the barrier certificate remains in the set \( B(x) < d \) for all time. However, due to condition (III.4), the barrier certificate cannot stay in the set \( B(x) < d \) forever and must eventually return to the set \( B(x) \leq 0 \), leading to some conservatism in the approach.

To better capture the requirements of \( k \)-induction, we present a different notion of \( k \)-inductive barrier certificates which provides us with less conservative conditions.

Definition 3.3: We say that a function \( B : X \to \mathbb{R} \) is a \( k \)-inductive barrier certificate for the system \( \mathcal{S} \) with respect to a set of initial states \( X_0 \subseteq X \) and a set of unsafe states \( X_u \subseteq X \), if there exists \( k \in \mathbb{N}_{\geq 1} \) such that following holds:

\[
\bigwedge_{0 \leq i < k} B(f^i(x)) \leq 0 \quad \text{for all } x \in X_0, \quad \text{(III.5)}
\]

\[
B(x) > 0 \quad \text{for all } x \in X_u, \quad \text{(III.6)}
\]

\[
\bigwedge_{0 \leq i < k} (B(f^i(x)) \leq 0) \implies B(f^k(x)) \leq 0 \quad \text{for all } x \in X. \quad \text{(III.7)}
\]

Now, we present the second result of the paper on the safety verification of systems \( \mathcal{S} \) based on the existence of barrier certificates as in Definition 3.3.

Theorem 3.4: Consider a discrete-time dynamical system \( \mathcal{S} \). If there exists a function \( B : X \to \mathbb{R} \) for \( \mathcal{S} \) such that it is a \( k \)-inductive barrier certificate as in Definition 3.3 with respect to initial set \( X_0 \subseteq X \) and unsafe set \( X_u \subseteq X \), then the state sequences \( x_{x_0} \) of \( \mathcal{S} \) starting from \( x_0 \in X_0 \) never reach the unsafe region \( X_u \).

Proof: Assume that \( k \)-inductive barrier certificate as in Definition 3.3 exists for the system \( \mathcal{S} \) but it is not safe, i.e., there exists some \( T \in \mathbb{N} \) such that \( B(x(T)) \in X_u \). Then, from condition (III.6), we must have \( B(x(T)) > 0 \). Condition (III.5) implies that \( B(x(0)) \leq 0, B(x(1)) \leq 0, \ldots, B(x(k - 1)) \leq 0 \), which means that the state sequences starting from the safe set will definitely stay in the safe set for the next \( k - 1 \) consecutive time steps. From condition (III.7), we have that for any given \( k \) consecutive time steps, if the system is safe, then the system will remain safe in the \((k + 1)^{th}\) time step. Then, by applying the \( k \)-induction proof rule with (III.5) as the base case and (III.7) as the inductive hypothesis, we have that \( B(x(t)) \leq 0 \) for all \( t \in \mathbb{N} \). This is contradictory to condition (III.6). Therefore, the state sequences \( x_{x_0} \) of system \( \mathcal{S} \) starting from \( x_0 \in X_0 \) remain safe for all time.

Note that Definition 3.3 is similar to \( t \)-barrier certificates presented in [11] for continuous-time systems, except the latter uses the contrapositive equivalent of the logical implication in the inductive step in combination with backwards reachability analysis. We observe that for the value of \( k = 1 \), any \( k \)-inductive barrier certificate satisfying (III.1)-(III.4) also satisfies (III.5)-(III.7). Furthermore, unlike
conditions (II.4) or (III.3), condition (III.7) does not impose a non-increasing or bounded increase requirement between $B(f(x))$ and $B(x)$. We now illustrate $k$-inductive barrier certificates as in Definition 3.3 by once again considering the finite system in Example 2.2.

**Example 2.2 (Continued):** Consider the finite system shown in Figure 2. We now utilize $k$-inductive barrier certificates as in Definition 3.3 to show that the system satisfies the required safety specification. Let $B$ be a linear function defined as $B(x) = x - 2$. We show that $B$ is a $k$-inductive barrier certificate as in Definition 3.3 with $k = 2$ as follows. Condition (III.5) is shown to be satisfied because $B(x) \leq 0$ for the state $x = 1$ and its consecutive states $x = 1.5$ and $x = 2$. Similarly, condition (III.6) is true as $B(x) > 0$ at the unsafe state $x = 2.75$. In order to show condition (III.7), we first consider all states $x$ where $B(x) \leq 0$. The set of states which satisfy this condition are $\{0, 1, 1.25, 1.5, 1.75, 2\}$. For any two-step transitions from the states in the set $\{0, 1, 1.25, 1.5, 2\}$, we see that the antecedent of (III.7) holds, and so does the consequent. Hence, the logical implication in condition (III.7) holds. For the state $x = 1.75$, even though $B(x) \leq 0$, after one transition we have $B(f(x)) > 0$. Therefore, the antecedent automatically fails to hold and condition (III.7) is satisfied. Finally for the remaining states in $S$, since $B(x) > 0$, the antecedent is false and so condition (III.7) is true. The logical implication is valid in all the cases which proves that the function $B(x) = x - 2$ is indeed a 2-inductive barrier certificate that guarantees the safety of the system.

We now illustrate the merits of $k$-inductive barrier certificates as in Definition 3.3 over those of Definition 3.1 by showing that there exist systems that do not admit linear $k$-inductive barrier certificates satisfying conditions (III.1)-(III.4) for any $k \in \mathbb{N}_{\geq 1}$, but admit linear $k$-inductive barrier certificates satisfying conditions (III.5)-(III.7) for some $k \in \mathbb{N}_{\geq 1}$.

**Example 3.5:** Let us consider the finite system $S'$ shown in Figure 4 with $x \in X = \{1, 2, 3, 5, 6, 7\}$ as the states of the system, $x = 2$ as the initial state and $x = 6$ as the unsafe state. Similar to Example 2.2, we see that the system is trivially safe. Suppose that a $k$-inductive barrier certificate as in Definition 3.1 of the form $B(x) = ax + b$ exists for the system. When $k = 1$, there exists no such $k$-inductive barrier certificate based on the discussion in Example 2.2. Therefore, we assume that $k \geq 2$. We let $d$ and $\epsilon$ take any value in $\mathbb{R}_{>0}$ such that $d > k\epsilon$. Due to the self-loop at the state $x = 3$, we have $f^k(3) = 3$ for any $k$. By applying condition (III.1) at the initial state $x = 2$, we get $B(x = 2) = 2a + b \leq 0$. Similarly, by applying condition (III.2) at the unsafe state $x = 6$, we have $6a + b \geq d > 0$. From the above inequalities, we get $a \geq 0$. Now, from condition (III.4) for a $k$-step transition from $x = 2$ to $x = 3$ for any $k \geq 2$, we have $B(3) - B(2) = a \leq 0$. This results in a contradiction, concluding that there exists no linear $k$-inductive barrier certificate as in Definition 3.1 for the system $S'$ and therefore, safety cannot be verified. Now, we show that formulating $k$-inductive barrier certificates via Definition 3.3 allows us to provide safety guarantees. Let $B(x) = x - 5$ and $k = 2$. One can see that conditions (III.5) and (III.6) are trivially satisfied. For $x \in \{2, 3, 5\}$, we have $B(x) \leq 0$ and, hence, (III.7) is satisfied. For $x \in \{6, 7\}$, the antecedent of the implication is false which validates (III.7). Similarly, for the state $x = 1$, we have $B(x) \leq 0$, but since $B(f(x)) = B(7) > 0$, the antecedent of the implication is once again false due to which (III.7) is true. Thus, the above system is shown to be safe using a linear $k$-inductive barrier certificates according to Definition 3.3.

**IV. Computation of $k$-Inductive Barrier Certificates**

In this section, we provide suitable computational approaches for synthesizing $k$-inductive barrier certificates. We propose two different systematic methods for computing $k$-inductive barrier certificates as presented in Definition 3.1 and Definition 3.3, respectively. The first one is based on sum-of-squares (SOS) optimization, while the second one utilizes the $\delta$-complete procedures over the reals [17].

**A. Sum-of-Squares Optimization**

For the synthesis of suitable $k$-inductive barrier certificates based on Definition 3.1, one can reformulate conditions (III.1)-(III.4) as an SOS optimization problem [13]. When the underlying dynamics of the system $S$ is polynomial and the initial set $X_0$ and unsafe set $X_u$ are semi-algebraic [18], one can cast conditions (III.1)-(III.4) as a collection of SOS constraints in order to compute a suitable polynomial $k$-inductive barrier certificate of a predefined degree.

**Assumption 4.1:** The system $S$ has a continuous state set $X \subseteq \mathbb{R}^n$, and its transition function $f : X \to X$ is a polynomial function of the state $x$.

Under Assumption 4.1, conditions (III.1)-(III.4) can be formulated as a set of SOS constraints, which is given by the following lemma.

**Lemma 4.2:** Suppose Assumption 4.1 holds for the system $S$ and sets $X$, $X_0$ and $X_u$ are semi-algebraic and can be described as vectors of polynomial inequalities: $X = \{x \in \mathbb{R}^n \mid g(x) \geq 0\}$, $X_0 = \{x \in \mathbb{R}^n \mid g_0(x) \geq 0\}$, and $X_u = \{x \in \mathbb{R}^n \mid g_u(x) \geq 0\}$, respectively, where the inequalities are provided element-wise. Suppose there exists a polynomial $B(x)$, constants $k \in \mathbb{N}_{\geq 1}$, $\epsilon \geq 0$, and $d > k\epsilon$ and sum-of-squares polynomials $\lambda(x), \hat{\lambda}(x), \lambda_0(x)$,
and $\lambda_u(x)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:

$$-B(x) - \lambda^T u(x) g_0(x),$$

$$B(x) - \lambda^T u(x) g_0(x) - d,$$

$$B(f_i(x)) + B(x) - \lambda^T u(x) g_i(x) + \epsilon,$$

$$-B(f^k(x)) + B(x) - \lambda^T u(x) g_i(x).$$

Then, function $B(x)$ is a k-inductive barrier certificate as in Definition 3.1 satisfying conditions (III.1)-(III.4).

**B. $\delta$-Complete Decision Procedures over Reals (dReal)**

The SOS optimization problem described in the previous subsection requires the set of constraints to be in conjunctive form. In other words, SOS handles optimization problems when the constraints are written as conjunctions (logical AND) of one another. However, k-inductive barrier certificates as defined in Definition 3.3 requires the satisfaction of a logical implication (condition (III.7)), which cannot be checked using the SOS approach. Therefore, in order to synthesize suitable k-inductive barrier certificates as in Definition 3.3, we reformulate conditions (III.5)-(III.7) as a feasibility expression with an existential and universal quantifier and make use of the satisfiability modulo theory (SMT) solver dReal [19] and the universal clause pruning approach used in [20] to handle this quantifier alternation.

**Assumption 4.3:** The system $\mathcal{S}$ is a compact set $X \subseteq \mathbb{R}^n$, and the initial and unsafe sets $X_0$ and $X_u$, respectively, are bounded semi-algebraic sets.

Under Assumption 4.3, one can reformulate conditions (III.5)-(III.7) as a feasibility formula whose satisfaction by an SMT solver returns a suitable parametric k-inductive barrier certificate. We define a parametric k-inductive barrier certificate with unknown coefficients $c_i \in \mathbb{R}$ and basis function $b_i(x)$ as $B(c, x) = \sum_{i=1}^{m} c_i b_i(x)$. For a polynomial k-inductive barrier certificate, the basis functions $b_i(x)$ are monomials over $x$. We encode conditions (III.5)-(III.7) with the help of the following formulas:

$$\psi_{ante}(c, x) = \left( \bigwedge_{0 \leq i < k} (B(c, f^i(x)) + \delta \leq 0) \right),$$

$$\psi_{unsafe}(c, x) = B(c, x) - \delta > 0,$$

$$\psi_{cons}(c, x) = B(c, f^k(x)) + \delta \leq 0,$$

$$\psi_{c1}(c, x) = (x \in X_0 \implies \psi_{ante}(c, x)),$$

$$\psi_{c2}(c, x) = (x \in X_u \implies \psi_{unsafe}(c, x)),$$

$$\psi_{c3}(c, x) = (\psi_{ante}(c, x) \implies \psi_{cons}(c, x)),$$

$$\psi_{cond1}(c) = \forall x \in X(\psi_{c1}(c, x)),$$

$$\psi_{cond2}(c) = \forall x \in X(\psi_{c2}(c, x)),$$

$$\psi_{cond3}(c) = \forall x \in X(\psi_{c3}(c, x)),$$

$$\psi_{bar}(c) = (\psi_{cond1}(c) \land \psi_{cond2}(c) \land \psi_{cond3}(c)).$$

where $\delta \in \mathbb{R}_{>0}$ is a tolerance parameter to ensure the satisfaction of conditions (III.5)-(III.7) via $\delta$-complete decision procedures. Then, a function $B(x)$ is a k-inductive barrier certificate if the formula $\phi = \exists c \psi_{bar}(c)$ is satisfiable. In other words, there must exist coefficients $c_i \in \mathbb{R}, i \in \{1, \ldots, m\}$, of the k-inductive barrier certificate such that the formula $\psi_{bar}(c)$ holds over the bounded state set. We note that $\phi$ is a formula with one quantifier alternation where a universal quantifier over state variables $x$ follows the existential quantifier over coefficients $c$, and the state variables are in a bounded domain. To ensure all variables are in a bounded domain, we also bound the coefficients $c$ to lie in a fixed interval. Finally, to determine the satisfiability of $\phi$ and compute the coefficients $c$, one can utilize the branch-and-prune algorithm of dReal [19] in conjunction with the universal clause pruning approach presented in [20] to handle the quantifier alternation.

**V. CASE STUDY**

For our case study, we consider the discrete-time model of a source-free series RLC circuit with state variables $i, v$ denoting the inductor current and capacitor voltage. The dynamics can be given by the following difference equations:

$$\mathcal{S} : \begin{cases}
i(t+1) = i(t) + \tau_s \left(-\frac{R}{L} i(t) - \frac{1}{L} v(t)\right), \\
v(t+1) = v(t) + \tau_e \frac{1}{C} i(t),
\end{cases}$$

where $\tau_s = 0.5s$ is the sampling time, $R = 3\Omega$ is the series resistance, $L = 8H$ is the series inductance, and $C = 0.5F$ is the capacitance of the circuit. Let the state set be $X = [-1, 5] \times [-4, 4]$. The initial set and the unsafe set are given by $X_0 = [0, 0.5] \times [0, 1]$ and $X_u = [1.5] \times [-4, 4]$, respectively. We consider a function of the parametric form $B(i, v) = c_1 i^2 + c_2 v^2 + c_3$ and attempt to compute suitable coefficients $c_1, c_2, c_3 \in \mathbb{R}$ such that $B(i, v)$ is a standard barrier certificate as defined in Definition 2.1. To do so, we utilize SOSTools [21] in conjunction with SeDuMi [22] on MATLAB to reformulate conditions (II.2)-(II.4) as an SOS optimization problem. However, we see that there exist no values of $c_1, c_2, c_3$ such that $B(i, v)$ satisfies conditions (II.2)-(II.4). Therefore, using standard barrier certificate approach, one cannot verify the safety of system $\mathcal{S}$.

**A. Using Sum-of-Squares Optimization**

We now compute coefficients $c_1, c_2, c_3$ such that $B(i, v)$ is a k-inductive barrier certificate as in Definition 3.1. Once again, we utilize SOSTools and SeDuMi to reformulate conditions (III.1)-(III.4) as an SOS problem via Lemma 4.2. By considering $k = 6, \epsilon = 0.06$ and $d = 0.361$, we obtain $B(i, v) = 0.71271^2 + 0.04319v^2 - 0.2957$ as the k-inductive barrier certificate as described in Definition 3.1. Therefore, by using Theorem 3.2, one can conclude that system $\mathcal{S}$ indeed satisfies the safety objective with respect to the initial set $X_0$ and unsafe set $X_u$. We shall mention that the computation time for this approach using the mentioned tools is about 20 seconds on a machine running with Linux Ubuntu OS (Intel i7-8665U CPU with 32 GB of RAM).
B. Using δ-complete Decision Procedures over Reals

We now demonstrate the computation of k-inductive barrier certificates as in Definition 3.3 for the same dynamics and regions of interest considered above. We formulate a parametric k-inductive barrier certificate \( B(i, v) = c_1 i^2 + c_2 v^2 + c_3 \) and compute the coefficients \( c_1, c_2, c_3 \in \mathbb{R} \) such that \( B(i, v) \) is a k-inductive barrier certificate as defined in Definition 3.3 by utilizing dReal in conjunction with universal clause pruning. To do so, we first bound the coefficients \( c_1, c_2 \in [0, 1, 6] \) and \( c_3 \in [-6, 6] \). We consider \( \delta + 0.2 \) as the constant in equation (IV.6) to ensure the k-inductive barrier certificate is strictly positive in the unsafe region. Similarly we consider \( \delta + 0.1 \) instead of \( \delta \) in equations (IV.5) and (IV.7) to ensure that the k-inductive barrier certificate is strictly negative in the safe regions. By setting \( k = 3 \) and \( \delta = 0.05 \), we obtain \( B(i, v) = 1.403317i^2 + 0.104829v^2 - 1.128599 \) as the k-inductive barrier certificate as in Definition 3.3. By utilizing Theorem 3.4, one can conclude that the set \( \mathcal{S} \) satisfies the safety objective with respect to the initial set \( X_0 \) and unsafe set \( X_u \). The computation time is around 15 seconds on a machine running MacOS 11.2 (Intel i9-9980HK with 64 GB of RAM). Figure 5 shows the state sequences of the system starting from different initial conditions inside \( X_0 \). As it can be observed, the state sequences always stay away from the unsafe region \( X_u \).

VI. CONCLUSION

We proposed two different notions of k-inductive barrier certificates for discrete-time systems which generalize the traditional notion of barrier certificate for providing safety guarantees by establishing stronger inductive proofs via k-induction. Using an illustrative example, we showed that for a given template of barrier certificates, one may be able to show the existence of k-inductive barrier certificates even when the classical ones may not exist. We also compared the two formulations of k-inductive barrier certificates via a simple example. We presented two approaches based on sum-of-squares programming and δ-complete decision procedures over the reals (using dReal) for the computation of suitable k-inductive barrier certificates under some mild assumptions on the systems. We demonstrated the effectiveness of the proposed approaches on a numerical case study.

REFERENCES