ON THE COMPLETENESS AND ORDERING OF PATH-COMPLETE BARRIER FUNCTIONS

MAHATHI ANAND[1], RAPHAËL JUNGERS[2], MAJID ZAMANI[3], AND FRANK ALLGÖWER[4]

Abstract. This paper is concerned with path-complete barrier functions which offer a graph-based methodology for verifying safety properties in switched systems. The path-complete framework leverages algebraic (barrier functions) as well as combinatorial (graph) components to characterize a set of safety conditions for switched systems, thus offering high flexibility (two degrees of freedom) in searching for suitable safety certificates. In this paper, we do not propose any new safety criteria. Instead, we further investigate the role that the combinatorial component plays in the safety verification problem. First, we prove that *path-completeness*, which is a property on a graph that describes the switching sequences, is *necessary* to obtain a set of valid safety conditions. As a result, the path-complete framework is able to provide a complete characterization of safety conditions for switched systems. Furthermore, we provide a systematic methodology for comparing two path-complete graphs and the conservatism associated with the resulting safety conditions. Specifically, we prove that under some conditions, such as when there exists a simulation relation between two path-complete graphs, it is possible to conclude that one graph is always able to provide less conservative safety conditions than another, independent of the algebraic properties of the switched system and the template of the barrier function under consideration. Such a result paves the way for a systematic use of the path-complete framework with barrier functions, as one can then consistently choose the appropriate graph that provides less conservative safety conditions.

1. Introduction

Traditionally, control theorists have focused on studying systems with purely continuous or discrete behaviors. However, many physical systems behave in a hybrid manner. Examples include chemical processes and energy systems [1], robotics [2], biological systems [3], and air traffic management systems [4]. On the other hand, switched systems [5] exhibit continuous-time behavior with isolated discrete switching modes and can be used as abstractions for more complex hybrid systems. However, their analysis is still a challenging problem [6, 7] that requires careful consideration.

An important problem concerning switched systems is the analysis of safety properties. The safety verification problem entails ascertaining whether all the behaviors of the switched system avoid visiting some unsafe or undesirable configurations. One way to solve this problem is to construct simpler finite abstractions and analyze the abstract systems, e.g., in [8–10], however, they suffer severely from the curse of dimensionality. More recently, discretization-free methods using barrier functions [11, 12] have shown great promises in proving safety properties effectively and efficiently. They are real-valued functions that assign higher values to the unsafe states than the initial states, thus serving as a *barrier* between reachable and unsafe regions. Hence, the safety verification problem is reduced to finding suitable barrier functions.

Related Literature. Several results in the literature utilize barrier functions in the context of switched and hybrid systems [11, 13–21]. The existing approaches can be divided in two groups. The first one is the use of common barrier functions [13, 14], where a single barrier function is used to guarantee safety for all the discrete operating modes of the switched system. Unfortunately, the conditions imposed on the barrier function are quite restrictive, and one may not be able to find suitable common barrier functions even when the system is safe. To alleviate the conservatism, multiple barrier functions were proposed in [11, 15–17]. Here, a barrier function is assigned to each operating mode of the switched (hybrid) system, and safety guarantees are obtained by ensuring not only mode safety but also safety at switching instances.

More recently, inspired by path-complete Lyapunov functions for stability analysis [22–27], we introduced in [28] a new framework for the safety of *linear* switched systems under arbitrary switching, based on a notion of *path-complete barrier functions*. This approach extends and generalizes the common and multiple barrier functions framework by introducing a combinatorial component to the safety verification problem via a graph. In particular, a so-called *path-complete graph* is used to encode the arbitrary switching sequences occurring in the system. Then, path-complete barrier functions are defined as a collection of functions so that each node of the graph is assigned a distinct barrier function. The edges within the graph enable algebraic conditions imposed on the barrier functions, such that the structure of the graph, together with the algebraic conditions, provide sufficient conditions for safety. It was also shown in [28] that depending on the choice of path-complete graphs, the approach provides less conservative results compared to the existing common and multiple barrier function framework. However, some unresolved questions regarding the path-complete framework remain. In this paper, we investigate in detail the special role that the choice of graphs plays in solving the safety verification problem. In this context, we address important questions concerning the completeness and ordering of path-complete barrier functions.

Contributions. The contributions of this paper in comparison to [28] are three-fold. First, while [28] focused primarily on linear switched systems, we remove in this paper any such restrictions and provide results for general nonlinear systems. Second, we provide completeness arguments for the path-complete framework proposed in [28]. It is known that path-complete barrier functions only provide sufficient conditions for safety. In other words, given a system and a suitable path-complete graph, failure to find a barrier function does not mean that the system is unsafe. However, it is not yet clear whether the chosen graph is required to be path-complete to begin with. Therefore, in this paper, we ask whether path-completeness is necessary for proving safety properties, and answer this question affirmatively by constructing appropriate counterexamples, i.e., by constructing suitable unsafe systems where the lack of the path-completeness property in graphs may lead to invalid safety certificates. This enables us to prove that the path-complete framework encapsulates the complete set of graph-based conditions for the safety verification of switched systems.

Thirdly, we investigate how the choice of graphs can influence the conservatism of the resulting safety conditions. In general, for a given system, the choice of a path-complete graph over which safety conditions are defined is not unique. As a result, different path-complete graphs lead to different algebraic conditions for safety verification, and the conservatism of the resulting conditions may differ. In this paper, we leverage techniques from graph theory to compare two path-complete graphs in terms of the conservatism of the resulting safety conditions. In particular, we define some simulation relations on the graphs under which one can order two path-complete graphs according to their conservatism, independently of the system or the barrier function template under consideration. Then, for any two path-complete graphs with some simulation relation, it is possible to objectively conclude in a complete manner, which graph results in less conservative safety certificates. This allows to consistently choose an appropriate graph that provides less conservative safety conditions, thus bridging the existing gap in the path-complete framework and making the approach more useful for verifying safety properties for switched systems systematically.

In addition, we support our theoretical results with several illustrative examples and experiments. First, we utilize a nonlinear two-car platoon system to demonstrate the applicability of path-complete barrier functions for the safety of switched nonlinear systems. Then, to illustrate the completeness of the path-complete barrier function framework, we construct counterexamples, both linear and nonlinear, to demonstrate that unsafe systems can yield invalid safety guarantees when graphs are chosen to be non path-complete. Finally, we conduct experiments to investigate the consequences of the choice of graphs in the resulting safety certificates. We show that in the presence of a simulation relation between two path-complete graphs, one graph always performs better than the other.

We note that our results echo similar existing ones in the context of path-complete Lyapunov functions presented in [24, 25, 29]. Particularly, in [29], the necessity of path-completeness for stability criteria were provided, and [24, 25] tackled the comparison between path-complete Lyapunov functions. Though our results are analogous to these, we point out that there is no reason (to the best of our knowledge) to assume that

these results can be extended directly from the stability to the safety framework. Indeed, it turns out that the proofs are significantly different, even though they are based on similar intuition. This is due to the fact that the algebraic conditions for stability and safety are also quite different.

Outline. In Section 2, we first highlight the necessary notations and then present the required background on switched systems as well as the safety verification problem. Consequently, in Section 3, we summarize briefly the path-complete framework for the safety verification of switched systems that was first proposed in [28], and extend the framework to general nonlinear systems. Section 4 presents the first main result of this paper. Here, we address the completeness of the path-complete barrier function framework and construct counterexamples which show that path-completeness of graphs is indeed a necessary condition for safety verification. Section 5 then addresses the ordering of path-complete barrier functions. Here, necessary and sufficient conditions on any two graphs are presented in order to compare the conservatism of the safety conditions resulting from the graphs. In Section 6, we present some case studies and experiments to validate the theoretical results obtained in the paper. Finally, we summarize our results and raise a few open questions in Section 7.

2. Notations and Problem Statement

2.1. **Notations.** Throughout the article, the set of real and non-negative integers are denoted by $\mathbb{R}$ and $\mathbb{N}$, respectively. In addition, appropriate subscripts are used to refer to subsets of $\mathbb{R}$, and $\mathbb{N}$, respectively, e.g., $\mathbb{N}_{\geq 1}$ for representing the set of positive integers. The notation $\mathbb{R}^n$ denotes a real space of dimension n and $\mathbb{R}^{m\times n}$ denotes a real space of dimension $m \times n$. For a vector (denoted in lowercase) $x \in \mathbb{R}^n$, $x[i]$ denotes the i^{th} element of x, $1 \leq i \leq n$. Similarly, for a matrix (denoted in uppercase) $X \in \mathbb{R}^{m\times n}$, the $(i,j)^{\text{th}}$ element is represented by $X[i,j]$, where $1 \leq i,j \leq n$. For a square matrix $X \in \mathbb{R}^{2n\times 2n}$, we write the i^{th} 2×2 diagonal block of X as $X[i] = \begin{bmatrix} X[2i-1,2i-1] & X[2i-1,2i] \\ X[2i,2i-1] & X[2i,2i] \end{bmatrix}$. Given a vector $x \in \mathbb{R}^n$, $\text{diag}(x) \in \mathbb{R}^{n\times n}$ is the diagonal matrix with diagonal elements $X[i,i] = x[i]$, $1 \leq i \leq n$. The inequality $A \geq 0$ (resp $\leq$) is element-wise. Moreover, $A^\top$ denotes the transpose of A. The set of all continuous functions with domain $\mathbb{R}^n$ and co-domain $\mathbb{R}$ are denoted by $\mathcal{C}(\mathbb{R}^n, \mathbb{R})$.

Finally, an alphabet Σ is a finite set of letters, and a sequence (denoted by bold symbols) $\mathbf{w} = (w_0 w_1 \ldots) \in \Sigma^\omega$ is an infinite concatenation of letters, i.e., $w_i \in \Sigma$, for all $i \geq 0$. Similarly, a finite sequence of length k is a sequence $\mathbf{w}_k = (w_0 w_1 \ldots w_{k-1}) \in \Sigma^k$. We use $\mathbf{w}(i) = w_i$ to denote the i^{th} position of the sequence $\mathbf{w}$.

2.2. **Problem Definition.** In this work, we consider nonlinear discrete-time switched dynamical systems (dt-SwS) of the form

$$S := \mathbf{x}(t+1) = f_{\boldsymbol{\sigma}(t)}(\mathbf{x}(t)), \tag{2.1}$$

where $\mathbf{x}(t) \in X \subseteq \mathbb{R}^n$ and $\boldsymbol{\sigma}(t) \in \Sigma = \{1, \ldots, m\}$, $m \in \mathbb{N}_{\geq 1}$, denote the state of the system as well the switching mode at time $t \in \mathbb{N}$, such that each mode corresponds to the dynamics $f_{\boldsymbol{\sigma}(t)} \in \{f_1, \ldots, f_m\}$. We call $\boldsymbol{\sigma} = (\sigma_0 \sigma_1 \ldots)$ a switching sequence of the system S, and we denote by $\mathbf{x}_{x_0,\boldsymbol{\sigma}} = (x_0 \mathbf{x}(1)\mathbf{x}(2)\ldots)$ the infinite sequence generated from the initial condition $\mathbf{x}(0) = x_0$ under the switching sequence $\boldsymbol{\sigma}$.

This article deals with the safety verification problem for dt-SwS under arbitrary switching sequences, i.e., to ensure that the dt-SwS S starting from a given initial set does not reach an unsafe set for any possible arbitrary switching sequence $\boldsymbol{\sigma}$. We present the formal definition of safety as follows.

Definition 2.1 (System Safety)**.** *Given an initial set $X_0 \subseteq X$ and an unsafe set $X_u \subseteq X$ such that $X_0 \cap X_u \neq \varnothing$, a dt-SwS S as in* (2.1) *defined over Σ is said to satisfy the safety specification denoted by* $\text{Safe}(X_0, X_u)$ *if for any $x_0 \in X_0$ and any $\boldsymbol{\sigma} \in \Sigma^\omega$, one has that $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(t) \notin X_u$, $\forall t \in \mathbb{N}$.*

The safety verification problem can then be formulated as follows.

Problem 2.2 (Safety Verification)**.** *Given a dt-SwS as in* (2.1) *over Σ, an initial set X_0, and an unsafe set X_u, verify that S satisfies* $\text{Safe}(X_0, X_u)$.

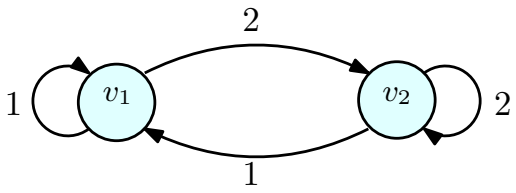

FIGURE 1. Example for a path-complete graph for a dt-SwS S with $\Sigma = \{1, 2\}$.

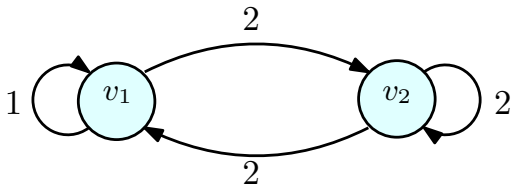

FIGURE 2. Example for a non path-complete graph for a dt-SwS S with $\Sigma = \{1, 2\}$. The sequence $\boldsymbol{\sigma}_3 = (121)$ cannot be accepted.

In our previous work [28], we addressed Problem 2.2 by proposing a new barrier function-based approach, called path-complete barrier functions. This approach leverages algebraic (barrier functions) as well as combinatorial (graph) components to characterize a set of safety conditions for dt-SwS. In the following section, for the sake of completeness, we briefly review the path-complete framework via suitable descriptions of graph-based barrier functions.

3. Path-Complete Framework for Safety Verification

In this section, we discuss the combinatorial and algebraic components that constitute the path-complete framework for the safety verification of dt-SwS. The combinatorial component is a graph that allows encoding the switching sequences occurring in the dt-SwS. In particular, a graph is a pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ defined on the alphabet Σ, where $\mathcal{V}$ is the set of vertices with cardinality $|\mathcal{V}|$, and $\mathcal{E}$ is the set of edges $(v, \sigma, v') \in \mathcal{E}$, with $v, v' \in \mathcal{V}$, and $\sigma \in \Sigma$. We say that a sequence $\boldsymbol{\sigma} = (\sigma_0 \sigma_1 \ldots) \in \Sigma^\omega$ is accepted by $\mathcal{G}$ if one can match this sequence to a path in $\mathcal{G}$, i.e., there exists corresponding sequence of edges $\boldsymbol{\pi} = \big((v_0, \sigma_0, v_1)(v_1, \sigma_1, v_2), \ldots\big)$ such that $(v_i, \sigma_i, v_{i+1}) \in \mathcal{E}$, for all $i \in \mathbb{N}$. Now, one may also consider a finite sequence $\boldsymbol{\sigma}_k = (\sigma_0 \ldots \sigma_{k-1})$ of length k and extend the definition of acceptance to finite paths. Then, it is not difficult to see that if there exists a finite sequence $\boldsymbol{\sigma}_k$ that cannot be accepted by $\mathcal{G}$, then any infinite sequence $\boldsymbol{\sigma}$ containing $\boldsymbol{\sigma}_k$ cannot be accepted by $\mathcal{G}$. We now present the definition of path-complete graphs that encode the arbitrary switching sequences possible in a dt-SwS S.

Definition 3.1 (Path-Complete Graphs)**.** *A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ over the alphabet Σ is said to be path-complete (PC) if any finite sequence $\boldsymbol{\sigma}_k$ of any length $k \in \mathbb{N}_{\geq 1}$ is accepted by $\mathcal{G}$.*

An example of a path-complete graph for $\Sigma = \{1, 2\}$ is shown in Figure 1. On the other hand, Figure 2 shows a graph that is not path-complete since it cannot accept any switching sequence $\boldsymbol{\sigma}$ containing the finite sequence $\boldsymbol{\sigma}_3 = (121)$.

Remark 3.2. *Note that given an alphabet Σ, the choice of a path-complete graph is in general non-unique. For example, reversing the direction of the edges $(v_1, 2, v_2)$ and $(v_2, 1, v_1)$ in Figure 1 results in a new path-complete graph.*

The algebraic component of our framework is a set of real-valued functions that allows to characterize a set of inequalities via graphs. The following definition formalizes the notion of graph-based barrier functions, and as an extension, path-complete barrier functions, which are vital for addressing the safety verification problem (Problem 2.2).

Definition 3.3 (Graph-Based Barrier Function)**.** *Consider a dt-SwS S over Σ as in Definition 2.1, an initial set X_0, and an unsafe set X_u. A graph-based barrier function is a pair $\big(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\big)$, where $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and $\mathrm{B}_v : X \to \mathbb{R}$ such that the following conditions are satisfied:*

$$\mathrm{B}_v(x) \leq 0, \qquad \forall x \in X_0,\ \forall v \in \mathcal{V}, \tag{3.1}$$

$$\mathrm{B}_v(x) > 0, \qquad \forall x \in X_u,\ \forall v \in \mathcal{V}, \tag{3.2}$$

$$\mathrm{B}_{v'}(f_\sigma(x)) \leq \mathrm{B}_v(x), \qquad \forall x \in X,\ \forall (v, \sigma, v') \in \mathcal{E}. \tag{3.3}$$

In addition, $\big(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\big)$ is said to be admissible for $\mathcal{G}$ and S if conditions (3.1)-(3.3) *are satisfied by $\{\mathrm{B}_v, v \in \mathcal{V}\}$.*

Moreover, a graph-based barrier function $\big(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\big)$ is said to be a *path-complete barrier function* if the associated graph $\mathcal{G}$ is path-complete. In the following, we show that path-complete barrier functions can guarantee the satisfaction of safety specifications.

Theorem 3.4. *Consider a dt-SwS S as in* (2.1) *over Σ, an initial set X_0 and unsafe set X_u, respectively. Suppose there exists a path-complete barrier function $\big(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\big)$ according to Definition 3.3 for some path-complete graph $\mathcal{G}$. Then, S satisfies* $\mathrm{Safe}(X_0, X_u)$.

Proof. The proof is established by contradiction. Assume that S is not safe, i.e., $\exists t \in \mathbb{N}$ such that $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(t) \in X_u$ for some $x_0 \in X_0$ and a sequence $\boldsymbol{\sigma} = (\sigma_0\sigma_1\ldots)$. Suppose that a PCBF $\big(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\big)$ also exists for some path-complete graph $\mathcal{G}$ such that the switching sequence $\boldsymbol{\sigma}$ up to length t generates the path $\boldsymbol{\pi}_t = \big((v(0)\sigma(0)v(1))\ldots(v(t-1), \sigma(t-1), v(t))\big)$, where $v(i) \in \mathcal{V}$, $0 \leq i \leq t-1$ is the node reached in $\mathcal{G}$ at time t. Then from condition (3.1), $\mathrm{B}_{v(0)}(x_0) \leq 0$. Moreover, due to Definition 3.1 and from condition (3.3), we can generate the sequence $\boldsymbol{\sigma}$ for which we get $\mathrm{B}_{v(t)}(x(t)) = \mathrm{B}_{v(t)}(A_{\sigma(t-1)}x(t-1)) \leq \mathrm{B}_{v(t-1)}(A_{\sigma(t-2)}x(t-2)) \leq \ldots \leq \mathrm{B}_{v(0)}(x_0) \leq 0$. This is in contradiction with condition (3.2), which requires that for all $v(t) \in \mathcal{V}$, $\mathrm{B}_{v(t)}(x(t)) > 0$. So the system must satisfy $\mathrm{Safe}(X_0, X_u)$. ■

The existence of path-complete barrier functions is in general only sufficient for safety, but not necessary. This means that given a dt-SwS S and a path-complete graph $\mathcal{G}$ over the alphabet Σ, failure to find a path-complete barrier function does not necessarily mean that S is unsafe. However, it is not yet clear whether the requirement for the graph $\mathcal{G}$ to be path-complete is a necessary condition for safety. In other words, we ask whether the existence of a graph-based barrier function as in Definition 3.3 can guarantee safety satisfaction for S even if the associated graph is not path-complete. Answering this question allows us to provide a complete set of graph-based safety criteria for switched systems via our proposed path-complete framework.

4. Necessity of Path-Completeness

In this section, we show that for any non path-complete graph $\mathcal{G}_{np}$, there exists a dt-SwS S and a safety specification $\mathrm{Safe}(X_0, X_u)$ such that there exists an admissible graph-based barrier function for $\mathcal{G}_{np}$ and S even when S is unsafe. That is, $\mathcal{G}_{np}$ cannot lead to a valid safety certificate. We now formally present the main result of the section.

Theorem 4.1 (Necessity of Path-Completeness)**.** *For any non path-complete graph $\mathcal{G}_{np} = (\mathcal{V}_{np}, \mathcal{E}_{np})$ over Σ, there exists a dt-SwS S_{np} as in* (2.1) *and a safety specification* $\mathrm{Safe}(X_0, X_u)$ *such that the following holds:*

(1) S_{np} violates $\mathrm{Safe}(X_0, X_u)$*,*
(2) There exists an admissible graph-based barrier function $\big(\mathcal{G}_{np}, \{\mathrm{B}_v, v \in \mathcal{V}_{np}\}\big)$.

The proof of Theorem 4.1 can be established by suitably constructing a dt-SwS S_{np} and a specification $\mathrm{Safe}(X_0, X_u)$ by leveraging the structure of $\mathcal{G}_{np}$. In particular, since $\mathcal{G}_{np}$ is not path-complete, there exists a sequence $\boldsymbol{\sigma}_k = (\sigma_0 \ldots \sigma_{k-1})$ of length k that cannot be accepted by $\mathcal{G}_{np}$. Using this, we construct S_{np} and sets X_0, X_u such that S_{np} violates $\mathrm{Safe}(X_0, X_u)$ upon encountering the switching sequence $\boldsymbol{\sigma} = (\boldsymbol{\sigma}_k\sigma_k\sigma_{k+1}\ldots)$,

where $\boldsymbol{\sigma}$ is the sequence obtained by concatenating $\boldsymbol{\sigma}_k$ with an arbitrary sequence $(\sigma_k\sigma_{k+1}\ldots)$. In the following, we first provide a step-wise approach to the construction, and then conclude the section by summarizing the final proof of Theorem 4.1.

4.1. **Construction of System and Specification.** Similar to the approach presented in [29] in the context of stability, we start our construction with a non path-complete graph $\mathcal{G}_{np} = (\mathcal{V}_{np}, \mathcal{E}_{np})$ over Σ and identify a sequence $\boldsymbol{\sigma}_k = (\sigma_0 \ldots \sigma_{k-1})$ of length k that cannot be accepted by $\mathcal{G}_{np}$. Having this, we construct a dt-SwS S_{np} as in (2.1) with linear dynamics, i.e., $f_{\boldsymbol{\sigma}(t)} \in \{A_{\sigma_1}, \ldots, A_{\sigma_m}\}$ for all $t \in \mathbb{N}, \forall \sigma \in \Sigma$, and a corresponding safety specification $\text{Safe}(X_0, X_u)$ as follows.

Definition 4.2 (dt-SwS Construction)**.** *For a non path-complete graph $\mathcal{G}_{np}$, consider a finite sequence $\boldsymbol{\sigma}_k \in \Sigma^k$, of length $k \in \mathbb{N}_{\geq 1}$ that is not accepted by $\mathcal{G}_{np}$. Define binary matrices $\hat{A}_\sigma \in \mathbb{R}^{n\times n}$, where $n = k+1$, such that $\hat{A}_\sigma[i,j] = 1$ if and only if $\boldsymbol{\sigma}_k(j-1) = \sigma$ and $i = j+1$, and all other elements of $\hat{A}_\sigma$ are identically zero. Then, define $A_\sigma = 2\hat{A}_\sigma$, $\forall \sigma \in \Sigma$. The linear dt-SwS S_{np} may be obtained as*

$$S_{np} \coloneqq \mathbf{x}(t+1) = A_{\sigma(t)}\mathbf{x}(t), \tag{4.1}$$

where $\mathbf{x}(t) \in \mathbb{R}^n$, and $\boldsymbol{\sigma}(t) \in \Sigma, \forall t \in \mathbb{N}$. Moreover, define safety specification as $\text{Safe}(X_0, X_u)$ with

$$X_0 \coloneqq \{x \in \mathbb{R}^n \mid \sum_{i=1}^{n} x[i]^2 \leq \frac{1}{4^k}\}, \tag{4.2}$$

$$X_u \coloneqq \{x \in \mathbb{R}^n \mid \sum_{i=1}^{n} x[i]^2 \geq 1\}. \tag{4.3}$$

Clearly, by the construction in Definition 4.2, statement (1) of Theorem 4.1 is true, since for the initial condition $x_0 = [\frac{1}{2^k}\ 0\ \ldots\ 0]^\top \in X_0$ and the extended switching sequence $\boldsymbol{\sigma} = (\boldsymbol{\sigma}_k\sigma_k\sigma_{k+1}\ldots)$, we have that $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(k) = [0\ 0\ \ldots\ 1]^\top \in X_u$, and as a result, $\text{Safe}(X_0, X_u)$ is violated. We now state the following lemma which is later used for proving statement (2) of Theorem 4.1.

Lemma 4.3. *Let $\boldsymbol{\sigma}_k$ be a finite sequence over Σ^k, $k \in \mathbb{N}_{\geq 1}$. Consider the corresponding linear dt-SwS S_{np} as in (4.1) as well as the safety specification $\text{Safe}(X_0, X_u)$ as in (4.2)-(4.3). Consider a product of matrices from Σ obtained as $A_{\boldsymbol{\sigma}'_l} = A_{\sigma'_{l-1}} \cdots A_{\sigma'_0}$, corresponding to a finite switching sequence $\boldsymbol{\sigma}'_l$, $l \in \mathbb{N}_{\geq 1}$. Then, $A_{\boldsymbol{\sigma}'_l} \neq 0$ if and only if $\boldsymbol{\sigma}'_l \in \boldsymbol{\sigma}_k$, i.e., there exist sequences $\boldsymbol{\sigma_m}, \boldsymbol{\sigma_n}$ of appropriate lengths such that $\boldsymbol{\sigma}_k = (\boldsymbol{\sigma}_m\boldsymbol{\sigma}'_l\boldsymbol{\sigma}_n)$.*

Proof. This statement can be directly verified from the construction of S_{np} via Definition 4.2.

Now, to show the validity of Statement 2 of Theorem 4.1, we seek to construct a suitable graph-based barrier function $\big(\mathcal{G}_{np}, \{\text{B}_v, v \in \mathcal{V}_{np}\}\big)$ for S_{np} that satisfies conditions (3.1)-(3.3). For this purpose, we consider our barrier functions to be quadratic, so that for each $v \in \mathcal{V}_{np}$, we have $B_v : \mathbb{R}^n \to \mathbb{R}$ as

$$\text{B}_v(x) \coloneqq \sum_{i=1}^{n} p_v[i]x[i]^2 - 1. \tag{4.4}$$

Moreover, we let $p_v[i]$ be any real value satisfying

$$1 < p_v[i] \leq 4^k, \tag{4.5}$$

for all $v \in \mathcal{V}_{np}$ and $1 \leq i \leq n$. Note that condition (4.5) is required for the satisfaction of (3.1)-(3.2), as we will see later.

Now, it remains to show that the graph-based barrier function $\big(\mathcal{G}_{np}, \{\text{B}_v, v \in \mathcal{V}_{np}\}\big)$ satisfies conditions (3.1)-(3.3) in order to prove statement (2) of Theorem 4.1.

4.2. **Admissibility of Graph-Based Barrier Function.** In this section, we show that there exists a graph-based barrier function with the template (4.4) satisfying conditions (3.1)-(3.3) for S_{np} with respect to the corresponding safety specification $\text{Safe}(X_0, X_u)$ as in Definition 4.2. In particular, we first show that for S_{np}, condition (3.3) can be represented as simple vector inequalities over the coefficients p_v in equation (4.4). Then, we utilize some interesting properties of the graph $\mathcal{G}_{np}$ to find the coefficients p_v that lead to the satisfaction of inequalities (3.1)-(3.3).

Proposition 4.4. *Consider the dt-SwS S_{np} as in Definition 4.2 and the corresponding safety specification $\text{Safe}(X_0, X_u)$, and a non path-complete graph $\mathcal{G}_{np}$. The graph-based barrier function $\big(\mathcal{G}_{np}, \{\text{B}_v, v \in \mathcal{V}_{np}\}\big)$ with B_v as in (4.4)-(4.5) satisfies conditions (3.1)-(3.2). Moreover, condition (3.3) is satisfied if and only if for all $(v, \sigma, v') \in \mathcal{E}_{np}$:*

$$4\hat{A}_\sigma^\top p_{v'} \leq p_v. \tag{4.6}$$

Proof. We first show the satisfaction of condition (3.1). For $x \in X_0$ as in (4.2), we have from (4.5) that for all $v \in \mathcal{V}_{np}$, $\text{B}_v(x) = \sum_{i=1}^n p_v[i]x[i]^2 - 1 \leq 4^k \sum_{i=1}^n x[i]^2 - 1 \leq 0$. Similarly, one can show the satisfaction of condition (3.2). Now we show that condition (3.3) is satisfied if and only if the vector inequality (4.6) holds. To do so, we first show the direction (3.3) $\implies$ (4.6). By applying condition (3.3) to the dt-SwS S_{np}, we have that for all $(v, \sigma, v') \in \mathcal{E}_{np}$ and all $x \in \mathbb{R}^n$, $\text{B}_{v'}(A_\sigma x) \leq \text{B}_v(x)$. For an arbitrary index $0 \leq i' \leq n$, consider the i'^{th} row of the inequality (4.6). If the i'^{th} row of A_σ is the 0 vector, then we get $0 \leq p_v[i']$, which is automatically satisfied due to (4.5). If not, take any index $0 \leq i, i' \leq n$ such that $\hat{A}_\sigma[i', i] = 1$ (note that for any i, there exists at most one i' such that this holds) and fix $x = e_i$, which is the i^{th} canonical basis vector. By applying condition (3.3), we get

$$4p_{v'}[i'] \leq p_v[i].$$

Combining the inequalities and putting it in a matrix form, we get (4.6).

To show that (4.6) $\implies$ (3.3), write for all $v \in \mathcal{V}_{np}$, $P_v = \text{diag}(p_v)$. Then, we have

$$\begin{aligned}
\text{B}_{v'}(A_\sigma x) &= ((A_\sigma x)^\top P_{v'}(A_\sigma x)) - 1 \\
&= x^\top (2\hat{A}_\sigma)^\top P_{v'}(2\hat{A}_\sigma)x - 1 \\
&= 4x^\top \hat{A}_\sigma^\top \Big(\sum_{i'} p_{v'}[i'] e_{i'} e_{i'}^\top\Big)\hat{A}_\sigma x - 1 \\
&= 4x^\top \Big(\sum_{i'} p_v[i'](\hat{A}_\sigma^\top e_{i'})(\hat{A}_\sigma e_{i'}^\top)\Big)x - 1 \\
&\leq x^\top \sum_i p_v[i] e_i e_i^\top x - 1 \\
&= x^\top P_v x - 1 = B_v(x),
\end{aligned}$$

where the inequality arises from condition (4.6). ■

Proposition 4.4 allows us to show that the graph-based barrier function constructed in Section 4.1 satisfies conditions (3.1)-(3.2). As the last step in constructing the proof of statement 2 of Theorem 4.1, we show that for the non path-complete graph $\mathcal{G}_{np}$, the construction also satisfies (3.3), which can be shown by proving that the vector inequality (4.6) holds. To do so, we utilize an auxiliary graph $\hat{\mathcal{G}}_{np} = (\hat{\mathcal{V}}_{np}, \hat{\mathcal{E}}_{np})$, whose edges describe the element-wise inequalities of (4.6). The nodes of $\hat{\mathcal{G}}_{np}$ are defined as

$$\hat{\mathcal{V}}_{np} \coloneqq \{(v, i) \mid v \in \mathcal{V}_{np}, 1 \leq i \leq n\},$$

i.e., they are pairs of the nodes of $\mathcal{G}_{np}$ and the i^{th} dimension of the dt-SwS S_{np}, such that each node represents a particular coefficient of the graph-based barrier function $p_v[i]$. Now, we construct the edge in $\hat{\mathcal{E}}_{np}$ from (v, i) to (v', i') if and only if

(1) There is an edge $(v, \sigma, v') \in \mathcal{V}$ for some $\sigma \in \Sigma$, and
(2) The corresponding matrix A_σ is such that $A_\sigma(i', i) \neq 0$.

Correspondingly, we label the edge σ, i.e., $\big((v,i),\sigma,(v',i')\big) \in \hat{\mathcal{E}}_{np}$. The graph $\hat{\mathcal{G}}_{np}$ enjoys some interesting properties, as shown in the following proposition, which we will leverage to show the satisfaction of (4.6).

Proposition 4.5. *Given a non path-complete graph $\mathcal{G}_{np}$ over the alphabet Σ, the corresponding auxiliary graph $\hat{\mathcal{G}}_{np}$ is acyclic with at most $k-1$ consecutive edges.*

Proof. A cycle in the graph $\hat{\mathcal{G}}_{np}$ corresponds to a path $\boldsymbol{\pi}_l = \big(\big((v,i),\sigma_0,(v_1,i_i)\big)\dots\big((v_{l-1},i_{l-1}),\sigma_{l-1},(v,i)\big)\big)$. Such a cycle can exist only if the $[i,i]$ element of the matrix product $A_{\boldsymbol{\sigma}_l} = A_{\sigma_{l-1}}\cdots A_{\sigma_0}$ is non-zero, where $\boldsymbol{\sigma}_l = (\sigma_0\dots\sigma_{l-1})$. Moreover, we have that $A_{\boldsymbol{\sigma}_l}[i,i] = \sum_{j_{l-2},\dots,j_0=1}^{n} A_{\sigma_{l-1}}[i,j_{l-2}]\cdots A_{\sigma_0}[j_0,i]$. By the construction of A_σ by Definition 4.2, we have that $A_\sigma[0,j] = 0$ for any $1 \le j \le n$ and any $\sigma \in \Sigma$, so, $A_{\boldsymbol{\sigma}_l}[0,0] = 0$. For any other i, again from Definition 4.2, we have that for any $\sigma \in \Sigma$, $A_\sigma[i,j] = 0$ whenever $i \neq j+1$. Therefore, for $A_{\boldsymbol{\sigma}_l}[i,i] \neq 0$, one needs $i = j_{k-2}+1 = j_{k-3}+2\cdots = i+(k-1)$, which is impossible. Therefore, $A_{\boldsymbol{\sigma}_l}[i,i] = 0$ for all $1 \le i \le n$, and thus, $\hat{\mathcal{G}}_{np}$ is acyclic.

Now, if $\hat{\mathcal{G}}_{np}$ consists of k consecutive edges, then it corresponds to a path $\boldsymbol{\pi}_k = \big(\big((v,i),\sigma_0,(v_1,i_1)\big)\dots\big((v_{k-1},i_{k-1}),\sigma_{k-1},(v',i')\big)$. Then, from Lemma 4.3, the product $A_{\boldsymbol{\sigma}_k} \neq 0$ if and only if $\boldsymbol{\sigma}_k$ exists in $\hat{\mathcal{G}}_{np}$, and correspondingly $\boldsymbol{\sigma}_k$ is accepted by $\mathcal{G}_{np}$. But this is not possible since $\mathcal{G}_{np}$ is non path-complete and cannot accept $\boldsymbol{\sigma}_k$. Therefore, $\hat{\mathcal{G}}_{np}$ can have at most $k-1$ edges. ■

We now have all the prerequisites to show the existence of an admissible graph-based barrier function $(\mathcal{G}_{np},\{\mathrm{B}_v, v \in \mathcal{V}_{np}\})$ as defined in (4.4) such that it satisfies conditions (3.1)-(3.3), for the constructed dt-SwS S_{np} and the given non path-complete graph $\mathcal{G}_{np}$.

Proof of Theorem 4.1. Statement 1 of Theorem 4.1 follows directly from the construction of the dt-SwS S_{np} and $\mathrm{Safe}(X_0,X_u)$ in Definition 4.2, as S_{np} violates $\mathrm{Safe}(X_0,X_u)$ in k time steps with $\mathbf{x}_{\mathbf{x_0}},\boldsymbol{\sigma}(k) \in X_u$ for the sequence $\boldsymbol{\sigma_k}$ that is not accepted by $\mathcal{G}_{np}$. So we focus on the proof of statement (2). Note that every directed acyclic graph has a topological ordering of its nodes [30, Chapter 1]. This implies that the nodes of $\hat{\mathcal{V}}_{\mathrm{np}}$ can be re-numbered, i.e., $(v,i) \to s$, $1 \le s \le |\mathcal{V}_{np}|$, such that there exists a path from s to s' only if $s' > s$, $1 \le s,s' \le |\mathcal{V}_{np}|$. Furthermore, for each node $(v,i) \in \hat{\mathcal{V}}_{np}$ numbered s, assign the coefficient of the graph-based barrier function as

$$p_v(i) = 4^{a_s}.$$

We determine a_s as follows. If there exists an edge $\big((v,i),\sigma,(v',i')\big) \in \hat{\mathcal{E}}_{np}$ for some $\sigma \in \Sigma$, and the nodes $(v,i),(v',i')$ are numbered s,s' respectively, then $a_s = a_{s'}+1$. Otherwise, for all nodes $(v,i) \in \mathcal{E}_{np}$ with no outgoing edge, $a_s = 4$. Then, since the graph has no more than $k-1$ consecutive edges, one has that for all $(v,i) \in \mathcal{E}_{np}$, $4 \le p_v(i) \le 4^k$, satisfying condition (4.5). Therefore, using Proposition 4.4, we can show the satisfaction of conditions (3.1)-(3.2).

Now, we have to show that for every edge $(v,\sigma,v') \in \mathcal{E}_{np}$ of $\mathcal{G}_{np}$, condition (3.3) holds. By Proposition 4.4, we instead show the satisfaction of condition (4.6). Consider the i^{th} component of inequality (4.6). This corresponds to the term $4\hat{A}_\sigma^\top p_{v'}[i]$. If this is zero, then (4.6) automatically holds at the i^{th} component. In the case that $\hat{A}_\sigma^\top[i,i'] = 1$ for some index i', this corresponds to an edge $\big((v,i),\sigma,(v',i')\big) \in \hat{\mathcal{E}}_{np}$ of $\hat{\mathcal{G}}_{np}$. As a result, we have that $4p_{v'}[i'] = 4^{a_{s'}+1} \le p_v[i]$. Therefore, condition (4.6) is satisfied at all components $1 \le i \le n$. Thus, the graph-based barrier function $(\mathcal{G}_{np},\{\mathrm{B}_v, v \in \mathcal{V}_{np}\})$ is indeed admissible, and the proof is complete. ■

In the following, we illustrate a simple counterexample obtained via the construction described above.

Example 4.6. *Consider the non path-complete graph $\mathcal{G}_{np} = (\mathcal{V}_{np},\mathcal{E}_{np})$ over $\Sigma = \{1,2\}$ as shown in Figure 2. The corresponding finite sequence of length $k = 3$ that cannot be accepted by $\mathcal{G}_{np}$ is given by $\boldsymbol{\sigma}_k = (121)$. Using this, we first construct a suitable dt-SwS S_{np}. By Definition 4.2, we obtain $\hat{A}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and*

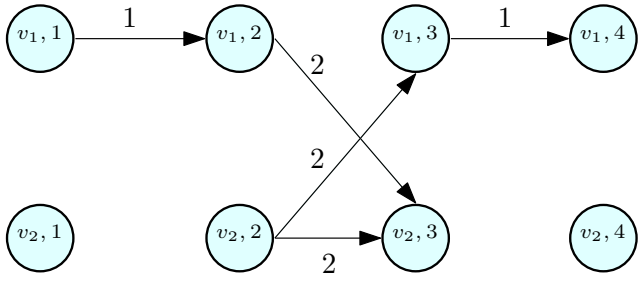

FIGURE 3. $\hat{\mathcal{G}}_{np}$ corresponding to graph $\mathcal{G}_{np}$ for Example 4.6

$\hat{A}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. *Consequently, we have* $A_1 = 2\hat{A}_1$, $A_2 = 2\hat{A}_2$, *and* S_{np} *given by* (4.1), *with state set* $X = \mathbb{R}^n$, $X_0 = \{x \in \mathbb{R}^n \mid \sum_{i=1}^n x[i]^2 \leq \frac{1}{64}\}$, $X_u = \{x \in \mathbb{R}^n \mid \sum_{i=1}^n x[i]^2 \geq 1\}$, *and safety specification* $\mathrm{Safe}(X_0, X_u)$.

Clearly, statement 1 of Theorem 4.1 is correct, since for the initial condition $x_0 = [\frac{1}{64}\ 0\ 0\ 0]^\top$ *and switching sequence* $\boldsymbol{\sigma} = (121\ldots)$, *we have* $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(3) = [0\ 0\ 0\ 1] \in X_u$. *Now, consider the graph-based barrier function* $(\mathcal{G}_{np}, \{\mathrm{B}_v : v \in \{v_1, v_2\}\})$ *of* $\mathcal{G}_{np}$, *where* $\mathrm{B}_{v_1}(x) = 64x[1]^2 + 16x[2]^2 + 16x[3]^2 + 4x[4] - 1$, *and* $\mathrm{B}_{v_2}(x) = 4x[1]^2 + 64x[2]^2 + 4x[3]^2 + 4x[4]^2 - 1$. *Note that these functions are obtained by utilizing the topological ordering of auxiliary graph* $\hat{\mathcal{G}}_{np}$ *corresponding to* $\mathcal{G}_{np}$, *shown in Figure 3. Indeed, the set of functions are admissible for* S_{np} *and* $\mathcal{G}_{np}$, *since conditions* (4.5) *and* (4.6) *are satisfied. Therefore,* $(\mathcal{G}_{np}, \{\mathrm{B}_v : v \in \{v_1, v_2\}\})$ *cannot provide a valid set of safety certificates when* $\mathcal{G}_{np}$ *is not path-complete.*

5. Comparison of Path Complete Barrier Functions

In the previous section, we showed that graph-based barrier functions do not provide valid safety certificates unless they are path-complete. In general, given an alphabet Σ, the choice of a suitable path-complete graph for defining the safety conditions is not unique. As a result, the path-complete framework provides two degrees of freedom for the computation of suitable PCBFs. The first one is through the algebraic component, i.e., the template of barrier functions. For instance, one may change the template of the PCBF (e.g., from quadratic functions to general polynomial functions [31, 32], or even neural network parameterizations [33, 34]) to improve conservatism of the safety certificates and making the safety verification problem less restrictive. Secondly, one can leverage the flexibility offered by the combinatorial component, i.e., the path-complete graph. While it was shown in [28] that path-complete barrier functions are generally less conservative than common and multiple barrier function frameworks [11, 13, 14], it is not clear how the choice of different path-complete graphs may affect the conservatism. In this section, we aim to address this problem by leveraging techniques from graph theory to compare two path-complete graphs and order them according to the conservatism offered by their corresponding safety conditions. We would like to note that the results here have been inspired from [24, 25] which present approaches for systematically comparing the conservatism of Lyapunov functions and joint spectral radius for switched systems via path-complete Lyapunov functions.

Consider a dt-SwS S defined as in (2.1). For S, suppose that $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a path-complete graph over Σ, and $(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\})$ is the corresponding PCBF. By a slight abuse of notation, we say that the PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\})$ belongs to the template $\mathcal{B}$, denoted by $\mathrm{B} \in \mathcal{B}$, if for all $v \in \mathcal{V}$, $\mathrm{B}_v \in \mathcal{B}$. For instance, when $\mathcal{B}$ is the set of quadratic functions, we want B_v to be a quadratic function for each v. Then, we define the ordering relation between any two path-complete graphs over Σ as follows.

Definition 5.1 (Ordering of PCBFs)**.** *Consider two path-complete graphs* $\mathcal{G}$ *and* $\bar{\mathcal{G}}$. *We say that* $\mathcal{G} \preceq \bar{\mathcal{G}}$ *if for any dt-SwS* S *over* Σ *as in* (2.1), *any safety specification* $\mathrm{Safe}(X_0, X_u)$, *and any template* $\mathcal{B}$, *the existence*

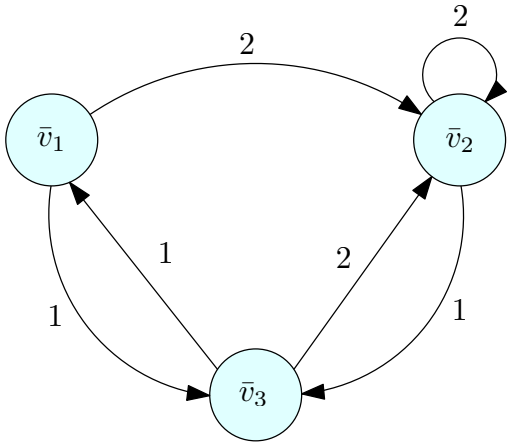

FIGURE 4. Path-complete graph $\bar{\mathcal{G}}$ that is simulated by the graph $\mathcal{G}$ in Figure 1.

of a suitable PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}) \in \mathcal{B}$ *implies the existence of a PCBF* $\bar{\mathrm{B}} = (\bar{\mathcal{G}}, \{\bar{\mathrm{B}}_{\bar{v}}, \bar{v} \in \bar{\mathcal{V}}\}) \in \mathcal{B}$. *Moreover, if the relation holds only for a particular template* $\mathcal{B}$, *we write* $\mathcal{G} \preceq_{\mathcal{B}} \bar{\mathcal{G}}$.

One observes that the ordering relation $\mathcal{G} \preceq \bar{\mathcal{G}}$ means that the graph $\bar{\mathcal{G}}$ leads to potentially less conservative PCBFs in comparison with $\mathcal{G}$, since one may be able to find a PCBF corresponding to $\bar{\mathcal{G}}$ even when those corresponding to $\mathcal{G}$ do not exist. In the following, we focus on determining the ordering relation between two path-complete graphs $\mathcal{G}$ and $\bar{\mathcal{G}}$, by utilizing the notion of simulation relations, defined below.

Definition 5.2 (Simulation Relation)**.** *Consider two path-complete graphs* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ *and* $\bar{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$ *defined over the same alphabet* Σ. *We say that* $\mathcal{G}$ *simulates* $\bar{\mathcal{G}}$ *if there exists a function* $R : \bar{\mathcal{V}} \to \mathcal{V}$ *such that*

$$(\bar{v}, \sigma, \bar{v}') \in \bar{\mathcal{E}} \implies \big(R(\bar{v}), \sigma, R(\bar{v}')\big) \in \mathcal{E}. \tag{5.1}$$

As an example, consider the path-complete graph $\bar{\mathcal{G}}$ in Figure 4 and the path-complete graph $\mathcal{G}$ as shown in Figure 1. It is evident that $\mathcal{G}$ simulates $\bar{\mathcal{G}}$ with the relation $R(\bar{v}_1) = R(\bar{v}_3) = v_1$, and $R(\bar{v}_2) = v_2$. Now, we show the main result of this section, i.e., we prove that a simulation relation between graphs is both necessary and sufficient for determining the ordering relation between two path-complete graphs independent of the class of the systems and the considered template of the barrier functions.

Theorem 5.3 (Ordering of PCBFs via Simulation)**.** *Consider two path-complete graphs* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ *and* $\bar{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$ *over the same alphabet* Σ. *Then the following statements are equivalent:*

(1) $\mathcal{G}$ *simulates* $\bar{\mathcal{G}}$
(2) $\mathcal{G} \preceq \bar{\mathcal{G}}$ *in the sense of Definition 5.1*

The proof of Theorem 5.3 is more involved. In fact, it relies on showing that for any given graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, adding another edge not already in the graph may lead to the violation of inequalities (3.1)-(3.3). This is formally stated as follows.

Lemma 5.4. *For any graph* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ *over an alphabet* Σ, *there exists a dt-SwS* S *over* Σ *as in* (2.1), *a safety specification* $\mathrm{Safe}(X_0, X_u)$, *and a suitable graph-based barrier function* $(\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\})$ *such that the following hold:*

$$\forall (v, \sigma, v') \in \mathcal{E}, \forall x \in X: \quad \mathrm{B}_{v'}(f_\sigma(x)) \leq \mathrm{B}_v(x), \tag{5.2}$$

$$\forall (v, \sigma, v') \notin \mathcal{E}, \exists x \in X: \quad \mathrm{B}_{v'}(f_\sigma(x)) > \mathrm{B}_v(x). \tag{5.3}$$

Proof. The proof is by construction, i.e., for a given graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, we build a suitable switched system S and a safety specification $\mathrm{Safe}(X_0, X_u)$, and correspondingly also construct a graph-based barrier

function $\{\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\}$ that satisfies conditions (5.2)-(5.3). Consider $\tilde{\mathcal{E}}$ to consist of all edges not in $\mathcal{E}$, i.e., $\tilde{\mathcal{E}} = (\mathcal{V} \times \Sigma \times \mathcal{V}) \setminus \mathcal{E}$. For notational clarity throughout the proof, we distinguish edges in $\bar{\mathcal{E}}$ from those in $\mathcal{E}$ by using the symbol e to denote the edges in $\bar{\mathcal{E}}$. Moreover, for each edge $e = (v, \sigma, v') \in \tilde{\mathcal{E}}$, we assign an index $1 \leq \tilde{e} \leq |\tilde{\mathcal{E}}|$. Now, we build a system S of dimension n and state set $X = \mathbb{R}^n$, where $n = 2|\tilde{\mathcal{E}}|$, as follows. For each $\sigma \in \Sigma$, consider $f_\sigma(x) = A_\sigma x$, where A_σ is defined block-wise, with $|\tilde{\mathcal{E}}|$ blocks of 2×2 entries on the diagonal, and zero everywhere else. Then, for each $\tilde{e} \in \{1, \ldots, |\mathcal{E}|\}$, we set the $\tilde{e}^{\text{th}}$ diagonal block of A_σ as $A_\sigma[\tilde{e}] = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. Then, we consider the safety specification $\mathrm{Safe}(X_0, X_u)$ with $X_0 \coloneqq \{x \in \mathbb{R}^n \mid \sum_{i=1}^n x_i^2 \leq 1\}$, and $X_u = \{x \in \mathbb{R}^n \mid \sum_{i=1}^n x_i^2 \geq 3\}$.

Now, we build an appropriate graph-based barrier function $\{\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\}$ corresponding to S, $\mathrm{Safe}(X_0, X_u)$, and $\mathcal{G}$. Suppose that $\mathrm{B}_v(x) = \sum_{i=1}^n q_v(i) x_i^2 - 1$, where $\frac{1}{3} \leq q_v(i) \leq 1$. One can readily observe that conditions (3.1)-(3.2) are satisfied, making $\{\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}\}$ a suitable graph-based barrier function as long as (3.3), and correspondingly, (5.2) is satisfied. Now, we need to assign coefficients q_v that satisfy conditions (5.2)-(5.3). To do this, let $Q_v = \mathrm{diag}(q_v)$, then we can write $\mathrm{B}_v(x) = x^\top Q_v x$. The matrix Q_v is then defined to be block-wise such that each diagonal block $Q_v[\tilde{e}]$ consists of coefficients $q_v[2\tilde{e}-1]$ and $q_v[2\tilde{e}]$. With some abuse of notation, we rewrite each block diagonal matrix $Q_v[\tilde{e}]$ as a vector $Q_v[\tilde{e}] = \begin{bmatrix} q_v[2\tilde{e}-1] & q_v[2\tilde{e}] \end{bmatrix}^\top$. Remark that for any $(v, \sigma, v') \in \mathcal{E} \cup \tilde{\mathcal{E}}$, the following holds:

$$\mathrm{B}_{v'}(A_\sigma x) \leq \mathrm{B}_v(x),\ \forall x \in \mathbb{R}^n,\ \iff\ \forall e = (\tilde{v}, \sigma, \tilde{v}') \in \tilde{\mathcal{E}} : Q_{v'}^\top[\tilde{e}] \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \leq Q_v^\top[\tilde{e}]. \tag{5.4}$$

The above relation is due to the construction of the dt-SwS S. Inequality (5.4) means that the second element of $Q_{\tilde{v}'}[\tilde{e}]$ must be less than or equal to the first element of $Q_{\tilde{v}}[\tilde{e}]$. On the other hand, the second entry of $Q_v[\tilde{e}]$ can be arbitrary as long as it takes a value between $\frac{1}{3}$ and 1, since the corresponding entry on the left hand-side is zero, and thus the lower part of inequality (5.4) is automatically satisfied.

Now, we are ready to formally obtain the elements $Q_v[\tilde{e}]$, for all $1 \leq \tilde{e} \leq |\tilde{\mathcal{E}}|$, which consequently define the coefficients of $\mathrm{B}_v(x)$. For each $v \in \mathcal{V}$ of $\mathcal{G}$, we decide the coefficients based on the indices $1 \leq \tilde{e} \leq |\tilde{\mathcal{E}}|$ and its corresponding edges $e = (\tilde{v}, \sigma, \tilde{v}') \in \tilde{\mathcal{E}}$, using the following cases:

(1) $v = \tilde{v} = \tilde{v}'$ (e is a self-loop from v): $Q_v[\tilde{e}] = [\frac{1}{3}\ \frac{1}{2}]^\top$,
(2) $v = \tilde{v}$ and $\tilde{v} \neq \tilde{v}'$ (e is an outgoing edge from v): $Q_v[\tilde{e}] = [\frac{1}{3}\ \frac{1}{3}]^\top$,
(3) $v = \tilde{v}'$ and $\tilde{v} \neq \tilde{v}'$ (e is an incoming edge to v): $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{2}]^\top$,
(4) otherwise: $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$.

Now, we proceed by showing that the construction satisfies condition (5.2) for any edge $(v, \sigma, v') \in \mathcal{E}$, by equivalently checking condition (5.4) for all $e = (\tilde{v}, \sigma, \tilde{v}') \in \tilde{\mathcal{E}}$. The following scenarios are considered:

- Case 1: $v = v'$. We clearly cannot consider $v = \tilde{v} = \tilde{v}'$ since we get $e \in \mathcal{E}$, leading to a contradiction. In all other possible scenarios, the second term of $Q_v[\tilde{e}]$ is at least as small as the first term of $Q_v[\tilde{e}]$, so (5.2) is satisfied.
- Case 2: $v \neq v'$. This case can be further divided into the following scenarios, out of which the possible ones are summarized in Table 1.
  (2.1): $v = \tilde{v} \neq v' = \tilde{v}'$. Then, once again, we have $e \in \mathcal{E}$, so we can rule out this scenario.
  (2.2): $v = \tilde{v}' \neq v' = \tilde{v}$. Then, e is an incoming edge for the node v and outgoing for the node v'. As a result, $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{2}]^\top$, and $Q_{v'} = [\frac{1}{3}\ \frac{1}{3}]^\top$.
  (2.3): $v = \tilde{v}' \neq \tilde{v} \neq v'$. Then, e is an incoming edge to v and for $\tilde{v}'$ it is neither. So $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{2}]^\top$, and $Q_{v'}[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$.
  (2.4): $v = \tilde{v}' = \tilde{v} \neq v'$. Then, e is a self-loop for v and for $\tilde{v}'$ it is neither. So $Q_v[\tilde{e}] = [\frac{1}{3}\ \frac{1}{2}]^\top$, and $Q_{v'}[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$.
  (2.5): $v = \tilde{v} \neq \tilde{v}' \neq v'$. Then, e is an outgoing edge for v, and neither an incoming nor an outgoing one for v'. Therefore, $Q_v[\tilde{e}] = [\frac{1}{3}\ \frac{1}{3}]^\top$ and $Q_{v'}[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$.

(2.6): $v \neq \tilde{v} \neq v' = \tilde{v}'$. Then e is outgoing for v' and neither for v. In this case, $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$ and $Q_{v'}[\tilde{e}] = [\frac{1}{3}\ \frac{1}{3}]^\top$.
(2.7): $v \neq \tilde{v} = v' = \tilde{v}'$. Then e is a self-loop for v' and neither for v. In this case, $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$ and $Q_{v'}[\tilde{e}] = [\frac{1}{3}\ \frac{1}{2}]^\top$.
(2.8): $v \neq \tilde{v} \neq v' = \tilde{v}'$. Then e is incoming for v' and neither for v. We have $Q_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$, and $Q_{v'}[\tilde{e}] = [\frac{1}{2}\ \frac{1}{2}]^\top$.
(2.9): $v \neq \tilde{v} \neq v' \neq \tilde{v}'$. Then e is neither an incoming nor an outgoing edge for v, v'. Then, we have $Q_v[\tilde{e}] = Q_{v'}[\tilde{e}] = [\frac{1}{2}\ \frac{1}{3}]^\top$.
Clearly, in all of these cases, the second element of $Q_{v'}[\tilde{e}]$ is at least as small as the first element of $Q_v[\tilde{e}]$. Therefore, condition (5.4), and correspondingy condition (5.2) follows.

TABLE 1. The eight possible scenarios considered when checking for condition (5.4).

$e = (\tilde{v}, \sigma, \tilde{v}') \in \tilde{\mathcal{E}}$	$Q_v[\tilde{e}]$	$Q_{v'}[\tilde{e}]$
$v = \tilde{v}' \neq v' = \tilde{v}$	$[\frac{1}{2}\ \frac{1}{2}]^\top$	$[\frac{1}{3}\ \frac{1}{3}]^\top$
$v = \tilde{v}' \neq \tilde{v} \neq v'$	$[\frac{1}{2}\ \frac{1}{2}]^\top$	$[\frac{1}{2}\ \frac{1}{3}]^\top$
$v = \tilde{v}' \neq \tilde{v} \neq v'$	$[\frac{1}{3}\ \frac{1}{2}]^\top$	$[\frac{1}{2}\ \frac{1}{3}]^\top$
$v = \tilde{v} \neq \tilde{v}' \neq v'$	$[\frac{1}{3}\ \frac{1}{3}]^\top$	$[\frac{1}{2}\ \frac{1}{3}]^\top$
$v \neq \tilde{v} \neq v' = \tilde{v}'$	$[\frac{1}{2}\ \frac{1}{3}]^\top$	$[\frac{1}{3}\ \frac{1}{3}]^\top$
$v \neq \tilde{v} = v' = \tilde{v}'$	$[\frac{1}{2}\ \frac{1}{3}]^\top$	$[\frac{1}{3}\ \frac{1}{3}]^\top$
$v \neq \tilde{v} \neq v' = \tilde{v}'$	$[\frac{1}{2}\ \frac{1}{3}]^\top$	$[\frac{1}{2}\ \frac{1}{2}]^\top$
$v \neq \tilde{v} \neq v' \neq \tilde{v}'$	$[\frac{1}{2}\ \frac{1}{3}]^\top$	$[\frac{1}{2}\ \frac{1}{3}]^\top$

Finally, we want to show the satisfaction of condition (5.3), by showing that for some $e = (\tilde{v}, \sigma, \tilde{v}')$, (5.4) is violated. For any $(v, \sigma, v') \in \tilde{\mathcal{E}}$, consider the following cases by picking a suitable $e = (v, \sigma, v')$:

- Case 1: $v = v'$. Then, we have $Q_v[\tilde{e}] = Q_{v'}[\tilde{e}] = [\frac{1}{3}\ \frac{1}{2}]^\top$. The second element here is greater than the first one, so condition (5.4), and thus (5.3) is violated.
- Case 2: $v \neq v'$. In this case, e is an outgoing edge for v and an incoming one for v'. Then, $Q_v[\tilde{e}] = [\frac{1}{3}\ \frac{1}{3}]^\top$ and $Q'_v[\tilde{e}] = [\frac{1}{2}\ \frac{1}{2}]^\top$. Then, (5.4) and correspondingly, (5.3) are violated. ■

We now have the required ingredients to prove Theorem 5.3.

Proof of Theorem 5.3. We first show that if statement (1) of Theorem 5.3 holds, then statement (2) holds as well. Suppose that $R : \bar{\mathcal{V}} \to \mathcal{V}$ is a simulation relation between $\mathcal{G}$ and $\tilde{\mathcal{G}}$. Moreover, suppose that for a given dt-SwS S as in (2.1) and the graph $\mathcal{G}$, a suitable PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\})$ of some arbitrary template $\mathcal{B}$ exists. From this, one can easily construct a PCBF $\bar{\mathrm{B}} = (\bar{\mathcal{G}}, \{\bar{\mathrm{B}}_{\bar{v}}, \bar{v} \in \bar{\mathcal{V}}\})$ corresponding to $\bar{\mathcal{G}}$ by simply assigning to each node $\bar{v} \in \bar{\mathcal{V}}$, a corresponding function $\bar{\mathrm{B}}_{\bar{v}} = \mathrm{B}_{R(\bar{v})}$. Note that such a function automatically satisfies conditions (3.1)-(3.2). Moreover, since R is a simulation relation, for every edge $(\bar{v}, \sigma, \bar{v}') \in \bar{\mathcal{E}}$, one has that $\bar{\mathrm{B}}_{\bar{v}'}(f_\sigma(x)) = \mathrm{B}_{R(\bar{v}')}(f_\sigma(x)) \leq \mathrm{B}_{R(\bar{v})}(x) = \bar{\mathrm{B}}_{\bar{v}}(x)$, where the inequality is due to (5.1) and the fact that $\{\mathrm{B}_v, v \in \mathcal{V}\}$ corresponds to the PCBF for $\mathcal{G}$ which satisfies condition (3.3). Therefore, one has the guarantee that existence of PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}) \in \mathcal{B}$ implies the existence of PCBF $\bar{\mathrm{B}} = (\mathcal{G}, \{\bar{\mathrm{B}}_{\bar{v}}, \bar{v} \in \bar{\mathcal{V}}\}) \in \mathcal{B}$, and statement (2) holds.

Then, we proceed to prove the converse statement, i.e., show that if statement (2) holds, then (1) also holds. Suppose that $\mathcal{G} \preceq \bar{\mathcal{G}}$, i.e., regardless of the template $\mathcal{B}$ and the system S, existence of PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\}) \in \mathcal{B}$ implies the existence of $\bar{\mathrm{B}} = (\mathcal{G}, \{\bar{\mathrm{B}}_{\bar{v}}, \bar{v} \in \bar{\mathcal{V}}\}) \in \mathcal{B}$. To show that $\mathcal{G}$ simulates $\bar{\mathcal{G}}$, we first apply Lemma 5.4 to $\mathcal{G}$ and obtain a dt-SwS S and a PCBF $\mathrm{B} = (\mathcal{G}, \{\mathrm{B}_v, v \in \mathcal{V}\})$ such that conditions (5.2)-(5.3) are satisfied. Now choose the template $\mathcal{B} = \{B_v, v \in \mathcal{V}\}$. Since $\mathcal{G} \preceq \bar{\mathcal{G}}$, there must also exist a PCBF $\bar{\mathrm{B}} = (\mathcal{G}, \{\bar{\mathrm{B}}_{\bar{v}}, \bar{v} \in \bar{\mathcal{V}}\}) \in \mathcal{B}$. Now, define a function $R : \bar{\mathcal{V}} \to \mathcal{V}$ such that $\bar{\mathrm{B}}_{\bar{v}} = \mathrm{B}_{R(\bar{v})}$, for all $\bar{v} \in \bar{\mathcal{V}}$. Note that this is always possible since the considered barrier function template $\mathcal{B}$ consists of the functions B_v, $v \in \mathcal{V}$.

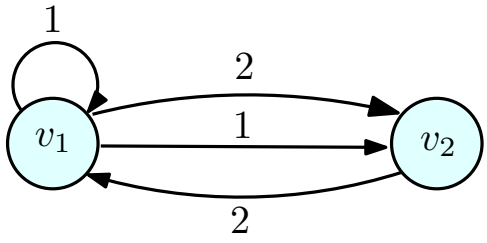

FIGURE 5. PC graph $\mathcal{G}$ utilized for the examples in Section 6.1 and Section 6.3.

So we can write

$$\forall(\bar{v},\sigma,\bar{v}') \in \bar{\mathcal{E}} : \mathrm{B}_{R(\bar{v}')}(f_\sigma(x)) \leq \mathrm{B}_{R(\bar{v})}(x), \forall x \in X. \tag{5.5}$$

We claim that such a function is a simulation relation, i.e., it satisfies condition (5.1). Suppose that it is not, i.e., for some $(\bar{v},\sigma,\bar{v}') \in \bar{\mathcal{E}}$, we have that $\big(R(\bar{v}),\sigma,R(\bar{v}')\big) \notin \mathcal{E}$. Then, by Lemma 5.4, we know that there exists some $x \in X$ such that $\mathrm{B}_{R(\bar{v}')}(f_\sigma(x)) > \mathrm{B}_{R(\bar{v})}(x)$. However, this is a contradiction with equation (5.5). The proof is now complete. ■

6. Case Studies and Experiments

6.1. **Nonlinear Switched Systems.** This case study aims to demonstrate the applicability of the path-complete framework for the safety verification of nonlinear switched dynamical systems. Specifically, we consider a two-car platoon example that exhibits polynomial dynamics, enabling us to utilize the sum-of-squares (SOS) algorithm [35] to compute suitable polynomial PCBFs. Note that for the sake of brevity, we do not present the SOS algorithm in our paper. However, we refer the interested reader to some prior works [31, 32, 36], and note that the computation of PCBF follows similarly. Consider two cars moving in a platoon formation with the following discrete-time system dynamics, adapted from [37]:

$$\begin{aligned} x_1(t+1) =& x_1(t) - \beta_1 x_1(t) - \alpha_1 x_1^2(t) + u_1, \\ x_2(t+1) =& x_2(t) - \beta_1 x_2(t) - \alpha_1 x_2^2(t) + u_2, \end{aligned}$$

where x_1, x_2 are the velocities of the vehicles 1 and 2, respectively, and u_1, u_2 are the forces normalized by the vehicle mass. Moreover, $\alpha_1 = 0.02, \alpha_2 = 0.04$ and $\beta_1 = 0.1, \beta_2 = 0.2$ are the rolling and aerodynamic-drag friction coefficients of the vehicles, respectively. Suppose that the second car, i.e., car corresponding to x_2 is the leader and communicates its state with the first car corresponding to x_1 at every time instant, and the corresponding inputs $u_1 = 0.01x_2, u_2 = 2$ are applied to the cars, respectively. However, occasionally and randomly, the communication between the cars breaks which results in $u_1 = 0$. This corresponds to a switched system as in equation (2.1) with two operating modes, given by the dynamics

$$\begin{aligned} f_1(x) &= \begin{bmatrix} 0.01x_2 + 0.9x_1 - 0.02x_1^2, \\ 2 + 0.8x_2 - 0.04x_2^2 \end{bmatrix}, \\ f_2(x) &= \begin{bmatrix} 0.9x_1 - 0.02x_1^2, \\ 2 + 0.8x_2 - 0.04x_2^2 \end{bmatrix}. \end{aligned}$$

Furthermore, we define the safety specification by sets $X = [0,10]^2$, $X_0 = \{x_1 \in [0,3], x_2 \in X \mid 1 \leq x_2 - x_1 \leq 2\}$, and $X_u = \{x_1, x_2 \in X \mid x_2 - x_1 \geq 0.2\}$. Now, we try to find a suitable PCBF by a priori choosing the path-complete graph given in Figure 5 and a quadratic barrier function template. By casting the PCBF conditions as sum-of-squares constraints and utilizing the YALMIP optimization toolbox [38] with sedumi [39] as the underlying solver, we are able to find a PCBF $(\mathcal{G}, \{\mathrm{B}_v, v \in V\}$ where $B_{v_1}(x) = 7.24 + 3.35x_1 - 8.91x_2 + 1.23x_1^2 + 0.91x_2^2 - 0.76x_1x_2$ and $B_{v_2}(x) = 6.19 + 3.96x_1 - 8.47x_2 + 1.18x_1^2 + 0.86x_2^2 - 0.9x_1x_2$. The simulations shown in Figure 6 also demonstrate the satisfaction of the safety specifications, thus illustrating our theoretical results.

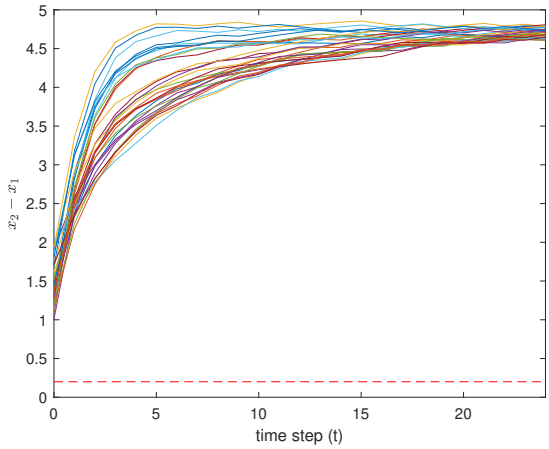

FIGURE 6. Simulation corresponding to the platoon example in Subsection 6.1. The value of $x_2 - x_1$ is plotted against the time step t. The area below the red dotted line indicates the unsafe set.

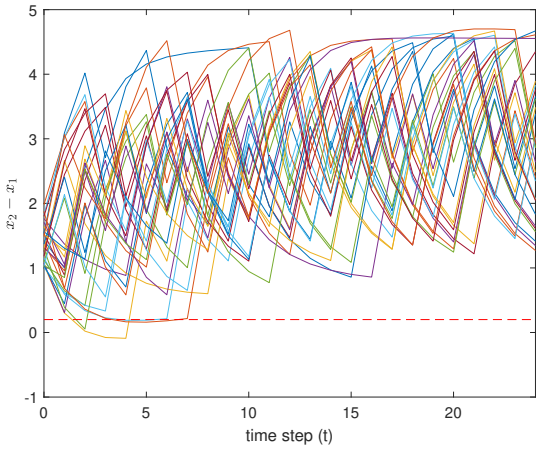

FIGURE 7. Simulations corresponding to the platoon example in Subsection 6.2. The simulations indicate the violation of safety specification.

6.2. **Necessity of Path-Completeness.** Now for the two-car platoon example above, suppose that a control input of $u_1, u_2 = 0$ is applied when there is a communication breakdown, resulting in the modified second mode dynamics given by

$$f_2(x) = \begin{bmatrix} 0.9x_1 - 0.02x_1^2, \\ 0.8x_2 - 0.04x_2^2 \end{bmatrix},$$

while f_1 remains the same. We consider the same safety specification as considered above. Clearly, the simulations in Figure 7 show that the switched system is unsafe. Now consider the non-path complete graph $\mathcal{G}_{np}$ obtained by removing the edge $(v_2, 2, v_1)$ from the graph $\mathcal{G}$ in Figure 5. We attempt to find a quadratic graph-based barrier function $(\mathcal{G}_{np}, \{\mathrm{B}_v, v \in \mathcal{V}_{np})$ corresponding to the system using YALMIP. The obtained functions are given by $B_{v_1}(x) = 1.89 + 5.72x_1 - 6.45x_2 + 0.8x_1^2 + 0.86x_2^2 - 1.43x_1x_2$, and $B_{v_2}(x) = 3.93 + 4.94x_1 - 5.30x_2 + 0.51x_1^2 + 0.48x_2^2 - 0.82x_1x_2$. This means we risk obtaining invalid safety certificates even when the system is unsafe by utilizing non path-complete graphs instead of path-complete ones.

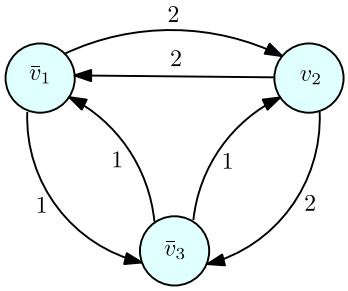

FIGURE 8. PC graph $\bar{\mathcal{G}}$ utilized for the example in Section 6.3.

6.3. **Comparison of Path-Complete Barrier Functions.** To illustrate the comparison of two path-complete graphs that are related to each other via a simulation relation, we consider two path-complete graphs $\mathcal{G}$ and $\bar{\mathcal{G}}$, as shown in Figures 5 and 8, respectively. Observe that $\mathcal{G}$ simulates $\bar{\mathcal{G}}$ via a simulation relation R with $R(\bar{v}_1) = v_1, R(\bar{v}_2) = v_2$ and $R(\bar{v}_3) = v_1$. Now, we randomly sample 3000 switched systems with two operating modes to examine the conservativeness of the PCBFs corresponding to $\mathcal{G}$ and $\bar{\mathcal{G}}$ respectively. To do so, we restrict ourselves to three-dimensional switched linear systems as in (2.1) given by $f_\sigma(x) = A_\sigma x$, $\sigma = \{1, 2\}$. We consider sets $X = \mathbb{R}^3$, $X_0 = \{x \in \mathbb{R}^n \mid \sum_{i=1}^3 x_i^2 \leq 4\}$ and $X_u = \{x \in \mathbb{R}^n \mid \sum_{i=1}^3 x_i^2 \geq 9\}$. Moreover, we consider quadratic barrier functions in order to cast the PCBF conditions (3.1)-(3.3) as linear matrix inequalities (LMIs) [28]. For each system and each mode $\sigma \in \{1, 2\}$, we randomly generate $A_\sigma \in \mathbb{R}^{3\times 3}$ such that its eigenvalues are less than 1 to ensure stability. Specifically, the elements of the 3×3 matrices are obtained randomly from a uniform distribution. If the eigenvalues of are computed to be greater than 1, the matrices are divided by a factor of 1.05 until the eigenvalues are close to, but still less than, 1. While stability in general is not required for safety verification, we restrict ourselves to stable systems to maximize the chances of finding PCBFs.

Then, by solving the LMIs for each of the 3000 systems we report that for 1435 systems, we were not able to find suitable PCBFs corresponding to neither $\mathcal{G}$ nor $\bar{\mathcal{G}}$, and for 1511 systems, we were able to find PCBFs corresponding to both graphs. However, there were 54 cases for which we were able to find a PCBF corresponding to $\bar{\mathcal{G}}$ while the computation of PCBFs for $\mathcal{G}$ resulted in an infeasible optimization problem. On the other hand, there were no cases where we could find a PCBF corresponding to $\mathcal{G}$ when the computation for $\bar{\mathcal{G}}$ led to infeasibility. This shows that the graph $\bar{\mathcal{G}}$ tends to perform better in comparison to $\mathcal{G}$, and this is because $\bar{\mathcal{G}}$ consistently leads to less conservative PCBFs. This is a direct consequence of Theorem 5.3 because $\mathcal{G}$ simulates $\bar{\mathcal{G}}$. Note that the computations were performed using the YALMIP optimization toolbox [38] with sedumi [39] as the underlying solver.

7. Conclusion and Discussion

In this paper, we addressed some important questions regarding the graph-based methodology for the safety verification of switched systems via path-complete barrier functions. We showed that it is necessary that a graph is path-complete to ensure the validity of the resulting safety certificates via barrier functions. As a consequence, our framework provides a complete set of graph-based safety criteria for switched systems. Moreover, we proposed a systematic methodology for comparing two different path-complete graphs and the conservatism associated with the resulting safety conditions. In particular, we leveraged a notion of simulation relation between two graphs and showed that if this relation holds, one graph always performs better than the other and leads to less conservative results. This result is independent of the class of systems considered (i.e., linear, polynomial, etc.) as well as the algebraic templates of the barrier functions (quadratic, polynomial, etc.). Correspondingly, we demonstrated the soundness of our theoretical results with several case studies and experiments.

Although the paper significantly advances the applicability of the path-complete framework for safety verification, there are still some gaps to be addressed. In particular, this paper proved that when two graphs

are related by a simulation relation, one can characterize the relative conservatism of the resulting safety conditions irrespective of the considered system and the barrier function template. However, it is unclear how to compare the resulting conditions when two graphs are unrelated. For example, consider the experiment performed in Section 6.3. Suppose that we modify the graph $\bar{\mathcal{G}}$ in Figure 8 slightly by reversing the edges $(\bar{v}_3, 1, \bar{v}_2)$ and $(\bar{v}_2, 2, \bar{v}_3)$. Then, we see that $\bar{\mathcal{G}}$ no longer simulates the graph $\mathcal{G}$ in Figure 5 due to the presence of the edge $(\bar{v}_2, 1, \bar{v}_3)$ that can no longer be matched by $\mathcal{G}$ which has no outgoing edge labeled 1 from v_2. However, we observed results similar to that of the experiment in this case, i.e., $\bar{\mathcal{G}}$ consistently provided less conservative results than $\mathcal{G}$. The reason for this is not yet clear. However, we postulate that there may be some specific system classes and barrier function templates for which one may characterize an ordering relation between graphs even when no simulation relation exists. Some results in this direction have been presented in the context of path-complete Lyapunov functions [26, 27, 40].

Finally, another interesting question is about the *quality* of the computed safe set, i.e, the invariant set: while the stability problem is essentially a 'yes or no' answer, for safety analysis, the quality of the computed invariant set (e.g. its volume) may matter in practice. The relationship between the properties of a particular path-complete graph and the invariant set quantified by the corresponding PCBF is far from clear to us and would deserve further investigation.

References

[1] B. Lennartson, M. Tittus, B. Egardt, and S. Pettersson, "Hybrid systems in process control," *IEEE Control Systems Magazine*, vol. 16, no. 5, pp. 45–56, 1996.

[2] J. Ding, J. H. Gillula, H. Huang, M. P. Vitus, W. Zhang, and C. J. Tomlin, "Hybrid systems in robotics," *IEEE Robotics & Automation Magazine*, vol. 18, no. 3, pp. 33–43, 2011.

[3] K. Aihara and H. Suzuki, "Theory of hybrid dynamical systems and its applications to biological and medical systems," vol. 368, no. 1930, pp. 4893–4914, 2010.

[4] C. Tomlin, G. Pappas, J. Lygeros, D. Godbole, S. Sastry, and G. Meyer, "Hybrid Control in Air Traffic Management Systems1," vol. 29, no. 1, pp. 5512–5517, 1996.

[5] D. Liberzon, "Switching in systems and control," in *Systems & Control: Foundations & Applications*, 2003.

[6] F. Zhu and P. J. Antsaklis, "Optimal control of hybrid switched systems: A brief survey," *Discrete Event Dynamic Systems*, vol. 25, no. 3, pp. 345–364, 2015.

[7] R. Shorten, F. Wirth, O. Mason, K. Wulff, and C. King, "Stability criteria for switched and hybrid systems," *SIAM Review*, vol. 49, no. 4, pp. 545–592, 2007.

[8] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2010.

[9] J. Camara, A. Girard, and G. Gössler, "Safety controller synthesis for switched systems using multi-scale symbolic models," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 2011, pp. 520–525.

[10] M. Zamani, A. Abate, and A. Girard, "Symbolic models for stochastic switched systems: A discretization and a discretization-free approach," *Automatica*, vol. 55, pp. 183–196, 2015.

[11] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Proceedings of the 7th ACM International Conference on Hybrid Systems: Computation and Control*, 2004, pp. 477–492.

[12] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117–126, 2006.

[13] A. Kıvılcım, O. Karabacak, and R. Wisniewski, "Safety verification of nonlinear switched systems via barrier functions and barrier densities," in *18th European Control Conference*, 2019, pp. 776–780.

[14] ——, "Safe reachability verification of nonlinear switched systems via a barrier density," in *58th Conference on Decision and Control (CDC)*, 2019, pp. 2368–2372.

[15] Q. Liu and L. Long, "Asymptotic stability with guaranteed safety for switched nonlinear systems: A multiple barrier functions method," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 6, pp. 3581–3590, 2022.

[16] H. Kong, X. Song, D. Han, M. Gu, and J. Sun, "A new barrier certificate for safety verification of hybrid systems," *The Computer Journal*, vol. 57, no. 7, pp. 1033–1045, 2014.

[17] G. Wang, J. Liu, H. Sun, J. Liu, Z. Ding, and M. Zhang, "Safety verification of state/time-driven hybrid systems using barrier certificates," in *35th Chinese Control Conference (CCC)*, 2016, pp. 2483–2489.

[18] M. Anand, P. Jagtap, and M. Zamani, "Verification of switched stochastic systems via barrier certificates," in *58th Conference on Decision and Control*, 2019, pp. 4373–4378.

[19] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier certificates for large-scale stochastic switched systems," *IEEE Control Systems Letters*, vol. 4, no. 4, pp. 845–850, 2020.

[20] A. Lavaei, S. Soudjani, and E. Frazzoli, "Safety barrier certificates for stochastic hybrid systems," in *American Control Conference*, 2022, pp. 880–885.

[21] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier functions for continuous-time stochastic hybrid systems," *Automatica*, vol. 145, p. 110513, 2024.
[22] A. A. Ahmadi, R. Jungers, P. A. Parrilo, and M. Roozbehani, "Analysis of the joint spectral radius via lyapunov functions on path-complete graphs," in *Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control*, 2011, p. 13–22.
[23] D. Angeli, N. Athanasopoulos, R. M. Jungers, and M. Philippe, "Path-complete graphs and common lyapunov functions," in *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, 2017, p. 81–90.
[24] M. Philippe, N. Athanasopoulos, D. Angeli, and R. M. Jungers, "On path-complete lyapunov functions: Geometry and comparison," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 1947–1957, 2019.
[25] M. Philippe and R. M. Jungers, "A complete characterization of the ordering of path-complete methods," in *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, 2019, p. 138–146.
[26] V. Debauche, M. Della Rossa, and R. M. Jungers, "Necessary and sufficient conditions for template-dependent ordering of path-complete lyapunov methods," in *Proceedings of the 25th ACM International Conference on Hybrid Systems: Computation and Control*, 2022.
[27] ——, "Comparison of path-complete Lyapunov functions via template-dependent lifts," *Nonlinear Analysis: Hybrid Systems*, vol. 46, p. 101237, 2022.
[28] M. Anand, R. Jungers, M. Zamani, and F. Allgöwer, "Path-complete barrier functions for safety of switched linear systems," in *63rd Conference on Decision and Control (CDC)*, 2024, pp. 7423–7428.
[29] R. M. Jungers, A. A. Ahmadi, P. A. Parrilo, and M. Roozbehani, "A characterization of lyapunov inequalities for stability of switched systems," vol. 62, no. 6, pp. 3062–3067, 2025.
[30] J. Bang-Jensen and G. Z. Gutin, *Digraphs: Theory, Algorithms and Applications*, ser. Springer Monographs in Mathematics. Springer.
[31] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE TAC*, vol. 52, no. 8, pp. 1415–1428, 2007.
[32] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, vol. 66, no. 7, pp. 3097–3110, 2021.
[33] H. Zhao, X. Zeng, T. Chen, Z. Liu, and J. Woodcock, "Learning safe neural network controllers with barrier certificates," *Formal Aspects of Computing*, vol. 33, no. 3, pp. 437–455, 2021.
[34] M. Anand and M. Zamani, "Formally verified neural network control barrier certificates for unknown systems," in *22nd IFAC World Congress*, vol. 56, no. 2, 2023, pp. 2431–2436.
[35] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical Programming*, vol. 96, no. 2, pp. 293–320, 2003.
[36] M. Anand, A. Lavaei, and M. Zamani, "Compositional synthesis of control barrier certificates for networks of stochastic systems against ω-regular specifications," vol. 51, p. 101427, 2024.
[37] A. Luppi, A. Bisoffi, C. De Persis, and P. Tesi, "Data-driven design of safe control for polynomial systems," in *European Journal of Control*, vol. 75, 2024, p. 100914. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0947358023001425
[38] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in matlab," in *IEEE International Conference on Robotics and Automation*, 2004, pp. 284–289.
[39] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization methods and software*, vol. 11, pp. 625–653, 1999.
[40] R. M. Jungers, "Statistical comparison of path-complete lyapunov functions: a discrete-event systems perspective," in *17th IFAC Workshop on discrete Event Systems (WODES)*, vol. 58, no. 1, 2024, pp. 258–263. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896324001228

[1]Munich Institute of Robotics and Machine Intelligence (MIRMI), Technical University of Munich (TUM), Germany

Email address: mahathi.anand@tum.de

[2]Department of Mathematical Engineering, Université catholique de Louvain.

Email address: raphael.jungers@uclouvain.be

[3]University of Colorado Boulder, USA

Email address: majid.zamani@colorado.edu

[4]Institute for Systems Theory and Automatic Control, University of Stuttgart, Germany.

Email address: frank.allgower@ist.uni-stuttgart.de