Path-Complete Barrier Functions for Safety of Switched Linear Systems

Mahathi Anand, Raphaël Jungers, Majid Zamani, and Frank Allgöwer

***Abstract*— In this paper, we address the safety verification problem of switched linear dynamical systems under arbitrary switching via barrier functions. Our approach is based on a notion of path-complete barrier functions, which utilizes a collection of barrier functions associated with a directed labeled graph that can encode all the possible switching sequences. We show that path-complete barrier functions effectively generalize notions of common and multiple barrier functions studied in existing literature, and can potentially provide less conservative conditions for safety verification. We demonstrate that, for switched linear systems, the inequalities imposed via path-complete barrier functions can be easily encoded into simple linear matrix inequalities under some assumptions on the regions of interest and appropriately chosen templates for the barrier functions. We also study the relationship between path-complete barrier functions and common barrier functions, and show that for any path-complete graph with an admissible path-complete barrier function, one can derive a suitable (possibly non-smooth) common barrier function by utilizing the path-complete barrier function. Finally, we utilize several examples to illustrate the effectiveness of our approach, and briefly discuss the challenges that lay foundations for future research.**

I. Introduction

The ubiquity of safety-critical systems in engineering applications has significantly elevated the importance of safety verification in the field of systems theory. The safety verification problem is to rigorously certify that all the system trajectories avoid visiting some unsafe or undesirable configurations. While the problem is generally hard to solve for complex dynamical systems, barrier functions [1, 2] have recently shown great promise in providing an efficient mechanism for safety certification. Specifically, barrier functions are real-valued functions that serve as a *barrier* between reachable and unsafe regions by giving higher values to the unsafe states compared to the initial states. They guarantee that their values decrease along the system trajectories, thereby avoiding entry into unsafe states. Hence, the safety verification problem is reduced to finding suitable barrier functions. Many physical systems can be described by hybrid or switched dynamics [3] and their analysis presents several theoretical challenges [4, 5] that contribute to the complexity of the safety verification problem. Barrier function-based approaches for safety verification have previously been adapted to such systems. Related results include safety verification of switched systems with common barrier functions [6, 7], safety and stability verification via multiple barrier functions and Lyapunov functions for switched systems [8], safety verification of hybrid systems via multiple barrier functions [1] and exponential barrier functions [9], and safety verification of state and time-dependent hybrid systems [10]. Moreover, control barrier functions have also been used for the verification and synthesis of switched stochastic control systems [11, 12] and stochastic hybrid systems [13, 14].

Contributions. Inspired by path-complete Lyapunov functions in the context of stability analysis [15]–[20], we introduce a graph-theoretical methodology via path-complete barrier functions (PCBFs) for the safety verification of switched dynamical systems under arbitrary switching. Specifically, a path-complete graph is utilized to encode the arbitrary switching sequences occurring in the switched system. Consequently, PCBFs may be defined as a collection of barrier functions, wherein each node in the graph corresponds to a distinct barrier function. Moreover, the edges within the graph enable the encoding of various barrier function inequalities, ensuring safety not only within the operating modes but also during the transition between these modes.

Our framework builds upon common barrier functions (CoBFs) and multiple barrier functions (MBFs) utilized in the aforementioned literature [1, 6, 7]. Particularly, the path-complete framework for safety verification unifies and generalizes both CoBFs and MBFs. It provides less conservative conditions for safety, depending on the choice of the path-complete graph, which is in general non-unique. We illustrate the effectiveness of our approach by showing via examples that for some systems, one may be able to find PCBFs corresponding to suitable graphs even when CoBFs or MBFs of a given template do not exist. We also illustrate the connections between PCBFs and CoBFs by showing that for any path-complete graph and its corresponding PCBF, one can extract a (possibly non-smooth) CoBF as a $\min$-$\max$ combination of the distinct pieces of the path-complete barrier function. Finally, we briefly demonstrate the challenges associated with our framework and discuss the possible future research to expand the scope of our approach.

Note that although our path-complete framework for safety may be applied to general switched nonlinear systems, we limit our focus to switched linear systems for ease of exposition. Particularly, by restricting ourselves to linear systems and quadratic barrier functions, we are able to search for suitable (path-complete) barrier functions by utilizing simple linear matrix inequalities.

II. Preliminaries

A. Notations

We denote the set of real numbers and non-negative integers by $\mathbb{R}$ and $\mathbb{N}$, respectively. Moreover, we use appropriate subscripts to refer to a subset of $\mathbb{R}$ and $\mathbb{N}$, respectively, e.g. $\mathbb{N}_{\geq 1}$ denotes the set of positive integers. $\mathbb{R}^n$ denotes a real space of dimension n and $\mathbb{R}^{m\times n}$ denotes a real space of dimension $m \times n$. We represent the set of all continuous functions with domain $\mathbb{R}^n$ and co-domain $\mathbb{R}$ as $\mathcal{C}(\mathbb{R}^n, \mathbb{R})$. For a matrix $A \in \mathbb{R}^{n\times n}$, the inequality $A \geq 0$ (resp $\leq$) is element-wise, whereas the inequality $A \succeq 0$ (resp. $\preceq$) means that A is positive (resp. negative) semi-definite. Similarly, a strict inequality implies positive (resp. negative) definiteness. Moreover, $A^\top$ denotes the transpose of A.

B. Problem Definition

In this work, we consider discrete-time switched linear dynamical systems of the form

$$\Sigma := x(t+1) = A_{\boldsymbol{\sigma}(t)}(x(t)), \tag{II.1}$$

where $x(t) \in X \subseteq \mathbb{R}^n$, and $\boldsymbol{\sigma}(t) \in \{1, \ldots, M\}$, $M \in \mathbb{N}_{\geq 1}$ $\forall t \in \mathbb{N}$, denote the state and the switching mode of the system such that each mode corresponds to a set of M matrices $\{A_1, \ldots, A_M\}$. We call $\boldsymbol{\sigma} = (\sigma(0), \sigma(1), \ldots)$ a switching sequence. Given an initial state $x(0) = x_0$, and a switching sequence $\boldsymbol{\sigma} = (\sigma(0), \sigma(1), \ldots)$, we denote by $\mathbf{x}_{x_0,\boldsymbol{\sigma}} = (x_0, x(1), x(2), \ldots)$ the infinite state sequence generated by applying the dynamics corresponding to $A_{\boldsymbol{\sigma}(t)}$ at each step t. The aim of this paper is to verify safety properties of the system Σ under arbitrary switching sequences, *i.e.*, to ensure that the system Σ starting from a given initial set does not reach an unsafe region, for any possible switching sequence $\boldsymbol{\sigma}$. This can be formally defined as follows.

Problem 2.1: Given a switched linear dynamical system Σ as in (II.1) with M switching modes, an initial set $X_0 \subseteq X$, an unsafe set $X_u \subseteq X$, verify that the state sequences $\mathbf{x}_{x_0,\boldsymbol{\sigma}}$ for any $x_0 \in X_0$ and any $\boldsymbol{\sigma}$ do not reach X_u for all time t, *i.e.*, $\mathbf{x}(t) \notin X_u, \forall t \in \mathbb{N}$.

C. Barrier Functions for Safety

Barrier functions [2] are an effective tool for safety analysis. They are real-valued functions $\mathrm{B} : X \to \mathbb{R}$ defined over the state set X such that the level set $\mathrm{B} = 0$ acts as a *barrier* between the reachable and the unsafe regions. For switched dynamical systems, one generally utilizes a common barrier function to guarantee safety for all operating modes $\sigma \in \{1, \ldots, M\}$, as well as at switching instants. We now provide the following definition, adopted from [6, Theorem 1].

Definition 2.2: Consider the switched dynamical system Σ as in (II.1) and the initial and unsafe sets given by $X_0, X_u \subseteq X$, respectively. Then, $\mathrm{B} : X \to \mathbb{R}$ is a common barrier function (CoBF) for Σ if the following conditions hold for all $\sigma \in \{1, \ldots, M\}$:

$$\mathrm{B}(x) \leq 0, \qquad \forall x \in X_0, \tag{II.2}$$

$$\mathrm{B}(x) > 0, \qquad \forall x \in X_u, \tag{II.3}$$

$$\mathrm{B}(A_\sigma x) \leq \mathrm{B}(x), \quad \forall x \in X. \tag{II.4}$$

It is easy to see that due to conditions (II.2) and (II.4), one can ensure that $\mathrm{B}(x) \leq 0$, $\forall t \in \mathbb{N}$, guaranteeing that Σ never reaches the unsafe regions where condition (II.3) holds. As a result, the safety verification problem is reduced to finding suitable CoBFs as in Definition (2.2). For linear switched systems, one can reduce this search to a set of linear matrix inequalities (LMIs) by considering quadratic CoBFs, and assuming that the sets of interest can be outer-approximated by quadratic inequalities.

Assumption 2.3: For a system as in (II.1), the initial set $X_0 \subseteq X$ and unsafe set $X_u \subseteq X$ are represented by quadratic inequalities, *i.e.,* there exist symmetric matrices S_0 and S_u such that

$$\begin{bmatrix} x \\ 1 \end{bmatrix}^\top S_0 \begin{bmatrix} x \\ 1 \end{bmatrix} \geq 0, \quad \forall x \in X_0, \tag{II.5}$$

$$\begin{bmatrix} x \\ 1 \end{bmatrix}^\top S_u \begin{bmatrix} x \\ 1 \end{bmatrix} \geq 0, \quad \forall x \in X_u. \tag{II.6}$$

Remark 2.4: In general, S_0 and S_u can appear as decision variables so that one can optimize the outer-approximation of the sets X_0 and X_u, respectively, to minimize the conservatism of the barrier function conditions. Sets such as hyper-rectangles, polytopes, and ellipsoids can be outer-approximated by (II.5)-(II.6). For example, initial set as a hyper-rectangle defined by $X_0 = \{x \in \mathbb{R}^n \mid x_l \leq x \leq x_u\}$ satisfies inequality (II.5) with $S_0 = \begin{bmatrix} -2\Lambda & \Lambda(x_l + x_u) \\ (x_l + x_u)^\top \Lambda & -2x_l^\top \Lambda x_u \end{bmatrix}$, where $\Lambda \in \mathbb{R}^{n\times n}$ is diagonal and non-negative. For additional information, see [21].

Under Assumption 2.3, the conditions (II.2)-(II.4) can be reduced to the following LMIs [22].

Proposition 2.5: Consider a switched dynamical system Σ as in (II.1) and the initial and unsafe sets are given by $X_0, X_u \subseteq X$, respectively. Suppose that Assumption 2.3 holds with matrices S_0, and S_u, respectively. Then, $\mathrm{B}(x) = \begin{bmatrix} x \\ 1 \end{bmatrix}^\top P \begin{bmatrix} x \\ 1 \end{bmatrix}$ is a quadratic CoBF for some symmetric indefinite matrix P if there exist some $\gamma_0, \gamma_u \geq 0$ such that the following conditions hold for all $\sigma \in \{1, \ldots, M\}$:

$$P + \gamma_0 S_0 \preceq 0 \tag{II.7}$$

$$P - \gamma_u S_u \succ 0 \tag{II.8}$$

$$P - \begin{bmatrix} A_\sigma & 0 \\ 0 & 1 \end{bmatrix}^\top P \begin{bmatrix} A_\sigma & 0 \\ 0 & 1 \end{bmatrix} \succeq 0. \tag{II.9}$$

Remark 2.6: Note that conditions (II.2) and (II.3) are equivalent to conditions (II.7) and (II.8), respectively, and can be proved using $\mathcal{S}$-procedure [22]. However, the equivalence between conditions (II.4) and (II.9) does not hold due to the fact that condition (II.9) is more conservative than (II.4) (*i.e.*, the decrease condition is checked for all $x \in \mathbb{R}^n$ instead of the state set X). While $\mathcal{S}$-procedure may be used also for (II.4), we choose not to do so for ease of computations.

Remark 2.7: From Remark 2.4, it is understood that matrices S_0, S_u may appear as decision variables in equations (II.7)-(II.8), especially when considering non-ellipsoidal sets of interest such as hyper-rectangles, polytopes, etc. This leads to bilinearity of the conditions. However, without loss of generality, one may simply consider $\gamma_0, \gamma_u = 1$, as these variables can be encoded by scaling the matrices S_0 and S_u, respectively.

Remark that even for simple switched linear systems, it may not be trivial to find the existence of quadratic barrier functions with the above linear matrix inequalities, even if there exists some barrier function. This is because of the conservatism of conditions in Definition 2.2, where one function B needs to act as a quadratic barrier function for all the modes of the system. One could utilize complex parameterizations of barrier functions (*e.g.*, polynomial functions of a higher degree), but this comes at a greater computational cost, (*e.g.*, using sum-of-squares (SOS) programming [23]). Another alternative would be to utilize multiple barrier functions (MBFs), where one barrier function is assigned per mode, and safety guarantees are obtained by (i) ensuring mode safety by allowing the barrier function of a given mode to decrease along its dynamics, and (ii) ensuring safe switching by allowing the barrier function of one mode to decrease with respect to the other during switching. We now define MBFs, adapted from [1, Theorem 2].

Definition 2.8: Consider a switched dynamical system Σ as in (II.1) and the initial and unsafe sets $X_0, X_u \subseteq X$, respectively. Then a collection of barrier functions $\mathrm{B}_\sigma : X \to \mathbb{R}$ is a multiple barrier function (MBF) for Σ under arbitrary switching sequences σ if the following conditions hold for all $\sigma, \sigma' \in \{1, \ldots, M\}$:

$$\mathrm{B}_\sigma(x) \leq 0, \qquad \forall x \in X_0, \tag{II.10}$$

$$\mathrm{B}_\sigma(x) > 0, \qquad \forall x \in X_u, \tag{II.11}$$

$$\mathrm{B}_{\sigma'}(A_{\sigma'} x) \leq \mathrm{B}_\sigma(x), \quad \forall x \in X. \tag{II.12}$$

Similar to CoBFs, one can encode quadratic MBFs as a set of linear matrix inequalities with M unknown matrices $P_i, i \in \{1, \ldots, M\}$, under Assumption 2.3. While MBFs are less conservative than CoBFs, it is not clear if utilizing MBFs with one barrier function assigned to each mode is the least conservative formulation for analyzing safety of switched stochastic systems. To answer this question, we unify and generalize the MBF framework via PCBFs, a framework under which MBFs are represented by a class of directed and labeled graphs known as path-complete graphs.

D. Path-Complete Graphs

Consider a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of vertices with cardinality $|\mathcal{V}|$ and $\mathcal{E}$ is the set of edges $(v, \sigma, v') \in \mathcal{E}$, where $v, v' \in \mathcal{V}$, and the label $\sigma \in \{1, \ldots, M\}$ denotes the possible modes for Σ as in (II.1). We call an infinite sequence $\pi = (v^1, \sigma_1, v^2, \ldots)$ a path of $\mathcal{G}$ if $(v^i, \sigma_i, v^{i+1}) \in \mathcal{E}$ for all $i \in \mathbb{N}_{\geq 1}$. A truncated *finite path* is then obtained as $\pi_k = (v^1, \sigma_1, v^2, \ldots, v^{k-1}, \sigma_{k-1}, v^k)$, $k \in \mathbb{N}_{\geq 2}$, where $(v^i, \sigma_i, v^{i+1}) \in \mathcal{E}$ for all $i \in \{1, \ldots, k-1\}$. We now define the notion of path-complete graphs [15] which encodes the set of all possible switching sequences of a dynamical system Σ.

Definition 2.9: A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is path-complete if for any $k \in \mathbb{N}_{\geq 2}$, and for any sequence $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_{k-1})$, $\sigma_i \in \{1, \ldots, M\}$, there exists a path $\pi_k = (v^1, \sigma_1, v^2, \ldots, v^{k-1}, \sigma_{k-1}, v^k)$ in $\mathcal{G}$, *i.e.*, for all $i \in \{1, \ldots, k-1\}$, we have $(v^i, \sigma_i, v^{i+1}) \in \mathcal{E}$.

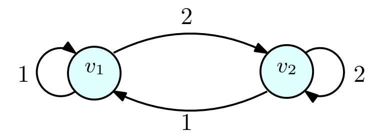

Fig. 1: Path-complete graph $\mathcal{G}_1$ corresponding to a system with 2 modes. The graph represents a valid PCBF with 2 barrier functions and 4 inequalities represented by the 4 edges.

One can see an illustration of a path-complete graph for a system with $\sigma \in \{1, 2\}$ in Figure 1. Note that in this particular example, removal of any edge of the graph makes the graph not path-complete. Furthermore, note that for a given set of M switching modes, path-complete graph is not unique. For instance, switching the direction of edges corresponding to $(v_1, 2, v_2)$ and $(v_2, 1, v_1)$ in Figure 1 would still render the graph path-complete. Moreover, one can have path-complete graphs with more than M nodes for the same system. We now introduce (co)-complete graphs, which form a subset of path-complete graphs [16].

Definition 2.10: A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is complete[1] if for all $v \in \mathcal{V}$, and all $\sigma \in \{1, \ldots, M\}$, there exists at least one edge $(v, \sigma, v') \in \mathcal{E}$. Graph $\mathcal{G}$ is co-complete if for all $v' \in \mathcal{V}$, and all $\sigma \in \{1, \ldots, M\}$, there exists at least one edge $(v, \sigma, v') \in \mathcal{E}$.

It can be readily seen that graph $\mathcal{G}_1$ in Figure 1 is complete. Similarly, the graph $\mathcal{G}_3$ in Figure 3 is co-complete.

III. Path-Complete Barrier Functions

In this section, we unify and generalize the notion of CoBFs and MBFs presented in Section II-C and introduce path-complete barrier functions. Note that the result presented in this section is inspired from the notion of path-complete Lyapunov functions first introduced in [15]. We first present a collection of barrier functions in a vector form, *i.e.*, $\mathrm{B} : X \to \mathbb{R}^N$ for some $N \in \mathbb{N}_{\geq 1}$, where each element B_i of B is a barrier function $\mathrm{B}_i = X \to \mathbb{R}$.

Definition 3.1: Consider a switched dynamical system Σ as in (II.1) and let $X_0, X_u \subseteq X$ be the initial and unsafe sets, respectively. Moreover, let $\mathcal{G}$ be a path-complete graph defined over M modes. A path-complete barrier function (PCBF) for Σ and $\mathcal{G}$, is given by $\mathrm{B} : X \to \mathbb{R}^{|\mathcal{V}|}$, where for all $(v, \sigma, v') \in \mathcal{E}$:

$$\mathrm{B}(x) \leq 0, \qquad \forall x \in X_0, \tag{III.1}$$

$$\mathrm{B}(x) > 0, \qquad \forall x \in X_u, \tag{III.2}$$

$$\mathrm{B}_{v'}(A_\sigma(x)) \leq \mathrm{B}_v(x), \qquad \forall x \in X. \tag{III.3}$$

Theorem 3.2: For a given switched dynamical system Σ and a path-complete graph $\mathcal{G}$ defined over M modes, suppose there exists a PCBF $\mathrm{B} : X \to \mathbb{R}^{|\mathcal{V}|}$ with respect to initial and unsafe sets $X_0, X_u \subseteq X$, respectively, that satisfies conditions (III.1)-(III.3). Then, Σ is safe, *i.e.*, for any sequence $\mathbf{x}_{x_0,\boldsymbol{\sigma}}$ starting from $x_0 \in X_0$ under any switching sequence $\boldsymbol{\sigma}$, one has $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(t) \notin X_u, \forall t \in \mathbb{N}$.

Proof. The proof is established by contradiction. Assume

[1] This terminology is borrowed from automata theory and should not be confused with the notion of completeness used in graph theory.

there exists a PCBF B corresponding to $\mathcal{G}$ satisfying conditions (III.1)-(III.3). Moreover, suppose that the system is unsafe, *i.e.*, there exists a state sequence $\mathbf{x}_{x_0,\boldsymbol{\sigma}}$ for some $x_0 \in X_0$ and some $\boldsymbol{\sigma} = (\sigma(0), \sigma(1), \ldots)$ such that $\mathbf{x}_{x_0,\boldsymbol{\sigma}}(t) \in X_u$, for some $t \in \mathbb{N}$. Consider a path-complete graph $\mathcal{G}$ over M modes, such that the switching sequence $\boldsymbol{\sigma}$ up to time t generates the path $\pi_t = (v(0), \sigma(0), v(1), \ldots, v(t-1), \sigma(t-1), v(t))$, where $v(i) \in \mathcal{V}$, $i \in \{1, \ldots, t\}$ is the node reached in $\mathcal{G}$ at time t. Then from condition (III.1), $\mathrm{B}_{v(0)}(x_0) \leq 0$, $\forall v(0) \in \mathcal{V}$. Moreover, due to the definition of path-complete graph $\mathcal{G}$, and from condition (III.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 contradicts condition (III.2), which requires that for all $v(t) \in \mathcal{V}$, $\mathrm{B}_{v(t)}(x(t)) > 0$. So the system must be safe. ∎

Remark 3.3: Proposition 2.5 may be readily extended to PCBFs. Here, one considers $|\mathcal{V}|$ functions $\mathrm{B}_v(x) = \begin{bmatrix} x \\ 1 \end{bmatrix}^\top P_v \begin{bmatrix} x \\ 1 \end{bmatrix}$, $v \in \mathcal{V}$. Then, conditions (II.7)-(II.8) are formulated for each matrix P_v in order to satisfy conditions (III.1)-(III.3), as

$$P_v + \gamma_{0v} S_0 \preceq 0, \qquad \text{(III.4)}$$

$$P_v - \gamma_{uv} S_u \succ 0, \qquad \text{(III.5)}$$

where $\gamma_{0v}, \gamma_{uv} \geq 0$, for all $v \in \mathcal{V}$. Then, for each edge $(v, \sigma, v') \in \mathcal{E}$, one ensures the satisfaction of the LMI

$$P_v - \begin{bmatrix} A_\sigma & 0 \\ 0 & 1 \end{bmatrix}^\top P_{v'} \begin{bmatrix} A_\sigma & 0 \\ 0 & 1 \end{bmatrix} \succeq 0. \qquad \text{(III.6)}$$

Remark 3.4: While quadratic CoBFs require to solve 3 LMI constraints consisting of at most $3n+1$ decision variables, quadratic PCBFs require to solve $2|\mathcal{V}|+|\mathcal{E}|$ constraints consisting of $|\mathcal{V}|(3n+1)$ decision variables, where $|\mathcal{V}|$ and $|\mathcal{E}|$ denote the number of nodes and edges of the graph $\mathcal{G}$, respectively. Clearly, the computational complexity of our framework increases linearly with the size of the graph.

PCBFs unify both CoBFs and MBFs. To see this, consider path-complete graphs $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ as shown in Figures 1-3. All of these graphs correspond to Σ with $M = 2$. Using $\mathcal{G}_2$, one is able to encode a single barrier function that satisfies conditions (II.2)-(II.4), thus defining common barrier functions. Similarly, $\mathcal{G}_1$ encodes conditions (II.10)-(II.12), thus defining multiple barrier functions. By choosing other suitable path-complete graphs for a given system Σ, such as $\mathcal{G}_3$, one may be able to achieve potentially less conservative conditions via (III.1)-(III.3), thus allowing more flexibility in finding suitable barrier functions.

An important question that naturally arises from the above formulation is whether there are further connections between path-complete barrier functions and common barrier functions. Specifically, one could ask whether one can deduce a (possibly non-smooth) common barrier function as in Definition 2.2 for a PCBF corresponding to any arbitrary graph. This is straightforward in the case of path-complete graphs with only one node, like $\mathcal{G}_1$ in Figure 1. In this case, the associated common barrier function is equivalent to the path-complete barrier function. However, in other cases, this

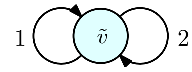

Fig. 2: Graph $\mathcal{G}_2$ for a system with 2 modes. The graph represents the inequalities imposed by common barrier functions.

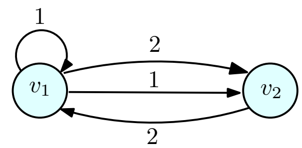

Fig. 3: Graph $\mathcal{G}_3$ for a system with 2 modes. The graph is co-complete and represents a valid PCBF with 2 barrier functions and 4 inequalities represented by the 4 edges.

connection is not trivial. We now address this question by utilizing some classical tools from automata theory.

IV. Extracting CoBFs from PCBFs

In this section, we show that one can obtain a (possibly non-smooth) common barrier function as in Definition 2.2 from a path-complete graph and its corresponding path-complete barrier function. To do so, we exploit the structure of path-complete graph and make use of the so-called observer graph [24] that is obtained from path-complete graphs as in Definition 2.9.

Definition 4.1: For a path-complete graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, the observer graph $\mathcal{G}_o = (\mathcal{V}_o, \mathcal{E}_o)$ is defined such that $\mathcal{V}_o \subseteq 2^{\mathcal{V}}$, *i.e.*, each node of $\mathcal{G}_o$ is a subset of $\mathcal{V}$, and is constructed as follows:

1) Initialize with $\mathcal{V}_0 = \{\mathcal{V}\}$, $\mathcal{E}_o = \varnothing$.
2) Set $S := \varnothing$. For each pair $(V, \sigma) \in \mathcal{V} \times \{1, \ldots, M\}$:
   a) Compute $V' := \bigcup_{v \in V} \{v' \mid (v, \sigma, v') \in \mathcal{E}\}$.
   b) If $V' \neq \varnothing$, set $\mathcal{E}_o := \mathcal{E}_o \bigcup \{(V, \sigma, V')\}$, and $S := S \bigcup V'$.
3) If $S \subseteq \mathcal{V}_o$, then terminate and obtain $\mathcal{G}_o$. Else, set $\mathcal{V}_o = \mathcal{V}_o \bigcup S$, and return to step 2.

We now present the following proposition which we will later use in conjunction with the observer graph to show the main result of this section. The result is inspired from the connections between path-complete Lyapunov functions and common Lyapunov functions for the stability of linear switched systems [16].

Proposition 4.2: Consider a switched system Σ and a corresponding path-complete graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ over M modes. Suppose that there exists a PCBF B for Σ corresponding to $\mathcal{G}$. Consider two non-empty subsets $V, V' \subseteq \mathcal{V}$ and a fixed mode $\sigma \in \{1, \ldots, M\}$. Then, the following results hold:

- If $\forall v \in V, \exists v' \in V'$ with $(v, \sigma, v') \in \mathcal{E}$, then
$$\min_{v' \in V'} \mathrm{B}_{v'}(A_\sigma(x)) \leq \min_{v \in V} \mathrm{B}_v(x), \quad \forall x \in X. \qquad \text{(IV.1)}$$
- If $\forall v' \in V', \exists v \in V$ with $(v, \sigma, v') \in \mathcal{E}$, then
$$\max_{v' \in V'} \mathrm{B}_{v'}(A_\sigma(x)) \leq \max_{v \in V} \mathrm{B}_v(x), \quad \forall x \in X. \qquad \text{(IV.2)}$$

Proof. Consider a system Σ, graph $\mathcal{G}$ and a mode $\sigma \in \{1, \ldots, M\}$. Since B is a PCBF, and for all $v \in V$, there exists some $v' \in V'$ with $(v, \sigma, v') \in \mathcal{E}$, it must be from condition (III.3) that for all $v \in V$, $x \in X$, $\mathrm{B}_{v'}(A_\sigma x) \leq \mathrm{B}_v(x)$ holds. From this, we get $\mathrm{B}_{v'}(A_\sigma x) \leq \min_{v \in V} \mathrm{B}_v(x)$,

$\forall x \in X$. Since this inequality must hold for at least one $v' \in V'$, we can replace the left hand side of the inequality with a minimum over $v' \in V'$, to obtain (IV.1). The proof of (IV.2) follows similarly. ■

We now present the main result for constructing CoBFs from any given path-complete graph and its corresponding PCBF.

Theorem 4.3: Consider a switched dynamical system Σ with $X_0, X_u \subseteq X$ as the initial and unsafe sets, respectively. Consider an appropriate path-complete graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ for Σ, and its corresponding observer graph $\mathcal{G}_o = (\mathcal{V}_o, \mathcal{E}_o)$. Suppose that $\mathrm{B} : X \to \mathbb{R}^{|\mathcal{V}|}$ is a PCBF with respect to Σ and $\mathcal{G}$. Then, the function

$$\mathrm{B}'(x) = \min_{V \in \mathcal{V}_o} \big(\max_{v \in V} \mathrm{B}_v(x) \big), \tag{IV.3}$$

is a CoBF for Σ.

Proof. Consider a system Σ and a corresponding path-complete graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and its corresponding observer graph $\mathcal{G}_o = (\mathcal{V}_o, \mathcal{E}_o)$. We first show that B' satisfies conditions (II.2)-(II.3). By construction of $\mathcal{G}_0$, any node in $\mathcal{V}_o$ is a set of nodes in $\mathcal{V}$. Since B is a PCBF corresponding to $\mathcal{G}$, from (III.1), for all $v \in \mathcal{V}$ we have that $\forall x \in X_0, \mathrm{B}_v(x) \leq 0$. As a result, for any subset $V \subseteq \mathcal{V}$, $\max_{v \in V} \mathrm{B}_v(x) \leq 0, \forall x \in X_0$. Similarly, by applying a minimum over nodes $V \in \mathcal{V}_0$, we get $\forall x \in X_0, \mathrm{B}'(x) \leq 0$, thus satisfying condition (II.2). Satisfaction of condition (II.3) follows similarly.

We now show the satisfaction of condition (II.4). By construction of $\mathcal{G}_o$ via Definition 4.1, there exists an edge (V, σ, V') in $\mathcal{G}_o$ if and only if for any $v' \in V'$, there exists some $v \in V$ such that $(v, \sigma, v') \in \mathcal{E}$. Therefore, (IV.2) holds, and as a result we have for all $(V, \sigma, V') \in \mathcal{E}_o$:

$$\max_{v' \in V'} \mathrm{B}_{v'}(A_\sigma(x)) \leq \max_{v \in V} \mathrm{B}_v(x), \forall x \in X.$$

Now consider $\bar{\mathrm{B}}_V(x) = \max_{v \in V} \mathrm{B}_v(x)$, for all $V \subseteq \mathcal{V}$. Then, we get for all $(V, \sigma, V') \in \mathcal{E}_o$:

$$\bar{\mathrm{B}}_{V'}(A_\sigma(x)) \leq \bar{\mathrm{B}}_V(x), \forall x \in X,$$

implying that these functions satisfy inequalities (III.3) encoded in $\mathcal{G}_o$.

Now, we claim that the observer graph $\mathcal{G}_o$ of any path-complete graph $\mathcal{G}$ is complete. To show this, we prove the contrapositive statement, *i.e.*, if $\mathcal{G}_o$ is not complete, then $\mathcal{G}_o$ is not path-complete. Since $\mathcal{G}_o$ is not complete, there must exist for some $V \in \mathcal{V}_o$ and some label $\sigma^* \in \{1, \ldots, M\}$, no edges $(V, \sigma^*, V') \in \mathcal{E}_o$. By construction, $\mathcal{G}_o$ has directed paths from the node $\mathcal{V} \in \mathcal{V}_o$ to the node V, so there must exist some sequence $(\sigma_1, \ldots, \sigma_k)$ following which one can reach V. Moreover, V consists of the set of nodes that can be reached by following the sequence $(\sigma_1, \ldots, \sigma_k)$ in $\mathcal{G}$. Now, since $(V, \sigma^*, V') \notin \mathcal{E}_o$, it must be that there exists no sequence $(\sigma_1, \ldots, \sigma_k, \sigma^*)$ that can be encoded in $\mathcal{G}$, so $\mathcal{G}$ is not path-complete. This proves the original statement, and thus $\mathcal{G}_o$ must be complete.

Finally, since $\mathcal{G}_o$ is complete, for any $\sigma \in \{1, \ldots, M\}$ and for any $V \in \mathcal{V}_o$ there exists $V' \in V_o$ such that $(V, \sigma, V') \in \mathcal{E}_o$. By using Proposition 4.2, we can show that $\min_{V \in \mathcal{V}_o} \bar{\mathrm{B}}_V(A_\sigma x) \leq \min_{V \in \mathcal{V}_o} \bar{\mathrm{B}}_V(x)$, $\forall x \in X$, and $\forall \sigma \in \{1, \ldots, M\}$, satisfying condition (II.4). This implies that $\mathrm{B}'(x)$ of (IV.3) is a CoBF for Σ. ■

Corollary 4.4: Consider a switched dynamical system Σ with $X_0, X_u \subseteq X$ as the initial and unsafe sets, respectively. Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a path-complete graph, and $\mathrm{B} : X \to \mathbb{R}^{|\mathcal{V}|}$ be the corresponding PCBF. Then,

- If $\mathcal{G}$ is complete, then $\mathrm{B}'(x) = \min_{v \in \mathcal{V}} \mathrm{B}_v(x)$ is a common barrier function for Σ.
- If $\mathcal{G}$ is co-complete, then $\mathrm{B}'(x) = \max_{v \in \mathcal{V}} \mathrm{B}_v(x)$ is a common barrier function for Σ.

V. Discussion on the Comparison of PCBFs

The aforementioned discussion makes it evident that employing PCBFs in switched systems might offer greater flexibility in validating safety specifications, as they might present less conservative safety conditions compared to CoBFs and MBFs. The PCBF framework generally provides two degrees of freedom in computing appropriate PCBFs for a system. Firstly, one must choose a suitable path-complete graph. Secondly, an appropriate parameterization (or template) for control barrier functions must be selected, along with employing suitable search tools for computing PCBFs. It is widely understood that selecting a larger function template provides greater flexibility in the search for PCBFs. Nevertheless, the impact of chosen path-complete graphs on the conservatism of safety verification remains unexplored, and we defer this investigation to future work.

VI. Examples

As our first example, we consider a 2D switched linear system Σ_1 with states $x = [x_1; x_2]$, operating on two modes $\sigma = \{1, 2\}$, given by the system matrices $A_1 = \begin{bmatrix} 0.7 & 0.77 \\ -0.49 & 0.84 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 0.7 & 0.77 \\ -0.49 & 0.56 \end{bmatrix}$. We consider the state set $X = \mathbb{R}^2$, the initial set $X_0 = \{x_1, x_2 \mid x_1^2 + x_2^2 \leq 16\}$, and the unsafe set $X_u = \{x_1, x_2 \mid x_1^2 + x_2^2 \geq 36\}$. Note that here, the sets of interest are ellipsoidal, and can be represented as quadratic inequalities in (II.5)-(II.5) with $S_0 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 16 \end{bmatrix}$, and $S_u = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -36 \end{bmatrix}$, respectively. To verify safety using PCBFs, we consider the graphs $\mathcal{G}_1$-$\mathcal{G}_3$ from Figures 1-3, respectively. We fix the PCBFs $\mathrm{B}_{\mathcal{G}_i} : X \to \mathbb{R}^{|\mathcal{V}_i|}$ to be quadratic for each graph $\mathcal{G}_i$ with $i = \{1, 2, 3\}$, and search for the functions using linear matrix inequalities presented in Remark 3.3. We see that the system does not admit any PCBF corresponding to $\mathcal{G}_2$, which represents the graph corresponding to CoBF. As a result, it does not admit any quadratic CoBF as in Definition 2.2. However, we were able to find a PCBF corresponding to both $\mathcal{G}_1$ (graph corresponding to MBF) and $\mathcal{G}_3$, thus providing safety guarantees for the system even in the absence of a quadratic CoBF. Figure 4 illustrates the PCBF corresponding to $\mathcal{G}_1$. One can see in the figure the zero level sets of the pieces B_{v_1} and B_{v_2} corresponding to nodes v_1 and v_2 in $\mathcal{G}_1$, respectively. Since $\mathcal{G}_1$ is a complete graph, the corresponding (non-smooth) CoBF is obtained via Corollary 4.4 by $\mathrm{B}' = \min(\mathrm{B}_{v_1}, \mathrm{B}_{v_2})$.

As our second example, we consider a 2D system Σ_2 operating on two modes $\sigma = \{1, 2\}$ with $A_1 = \alpha^{-1} \begin{bmatrix} 0 & -0.1 \\ 0.8 & 0 \end{bmatrix}$

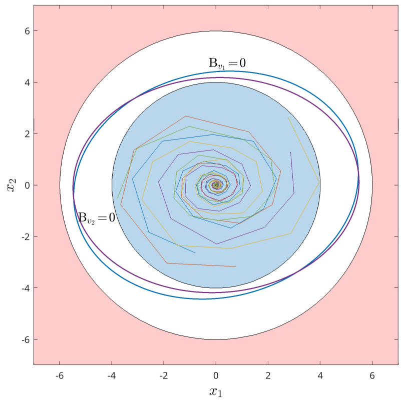

Fig. 4: Illustration of PCBF corresponding to $\mathcal{G}_1$ for system Σ_1. The blue region indicates the set X_0 whereas the red region indicates the set X_u. The 0 level sets of the pieces of the PCBF B_{v_1} and B_{v_2} corresponding to nodes v_1 and v_2 in $\mathcal{G}_1$ are labeled accordingly. The plot also shows some sample trajectories starting from X_0 under arbitrary switching sequences, indicating that the system is safe.

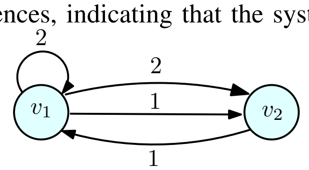

Fig. 5: Graph $\mathcal{G}_4$ corresponding to a system with 2 modes of operation. The graph represents a valid PCBF with 2 barrier functions and 4 inequalities corresponding to 4 edges.

and $A_2 = \alpha^{-1}\begin{bmatrix}0.25 & 0.4\\ 0.1 & 0.3\end{bmatrix}$, where $\alpha = 0.577$. Consider the state set $X = [-10, 10]^2$, initial set $X_0 = [0, 4]^2$ and unsafe set $X_u = [5, 10]^2$. To represent the hyper-rectangular sets, we utilize Remark 2.4 and characterize corresponding matrices S_0 and S_u as decision variables. We fix the template of the barrier functions to be quadratic, but fail to find PCBFs corresponding to graphs $\mathcal{G}_1$-$\mathcal{G}_3$ in Figures 1-3, respectively. However, by considering the path-complete graph $\mathcal{G}_4$ in Figure 5, we were able to find a suitable PCBF that guarantees that Σ_2 remains safe with respect to X_0 and X_u. This example clearly shows that the choice of the graph influences the obtained safety verification guarantees, and as a result, illustrates the need for a comparison framework for understanding the conservatism between different path-complete graphs. Note that the optimization problems (corresponding to conditions (III.4)-(III.6)) were solved by using YALMIP [25] with SeDuMi [26] as the underlying semi-definite programming solver on a Linux operating system with 32 GB RAM and AMD Ryzen 7 Pro processor.

References

[1] 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.

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

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

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] ——, "Comparison of path-complete Lyapunov functions via template-dependent lifts," *Nonlinear Analysis: Hybrid Systems*, vol. 46, p. 101237, 2022.

[21] M. Fazlyab, M. Morari, and G. J. Pappas, "Safety verification and robustness analysis of neural networks via quadratic constraints and semidefinite programming," *IEEE Transactions on Automatic Control*, vol. 67, no. 1, pp. 1–15, 2022.

[22] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Society for Industrial and Applied Mathematics, 1994.

[23] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical Programming*, vol. 96, no. 2, pp. 293–320, 2003.

[24] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Springer US, 2008.

[25] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in matlab," in *IEEE International Conference on Robotics and Automation*, 2004, pp. 284–289.

[26] 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.