

A Model Checking Framework for Linear Time Invariant Switching Systems using Structural Systems Analysis

Guilherme Ramos [†] Sérgio Pequito ^{†,‡} A. Pedro Aguiar ^{†,◊} Jaime Ramos [§] Soumya Kar [‡]

Abstract—This paper introduces the concept of structural hybrid systems to address, as a particular case, the model checking problem of switching (possible large scale) linear time invariant systems. Within the proposed setup, we provide necessary conditions to ensure properties such as controllability, at each time. We show that such model checking controllability properties can be implemented using efficient algorithms (with polynomial complexity). An example, based on the IEEE 5-bus power system, is presented which illustrates our model checking and design methodologies.

I. INTRODUCTION

This paper is motivated by the lack of efficient and scalable methods to design and verify properties of hybrid dynamical systems, commonly referred to as *model checking* [1]. In particular, we focus on the important subclass corresponding to *switching systems* that can model the behavior of several physical phenomena, including circumstances where a control module has to switch [2-4], with examples ranging from simple thermostats to an electrical power grid.

Informally, model checking consists of two main steps: first, a possible design of the dynamic system of interest, i.e., the *model*; second, the procedure of *checking* if a desired property of the model holds or not; if not, the design step is revisited and a new model is constructed. The majority of the tools for model checking are computationally cumbersome and, in particular, the hybrid automata (i.e., a common tool used to do model checking for hybrid dynamical systems) is, in general, undecidable [2]. In fact, even approximation methods exhibit numerical instabilities and suffer from the curse of dimensionality, see [3], [4] and references therein.

Common properties of interest in model checking include (but are not restricted to) *reachability* and *safety* [5]. In this paper, we focus on controllability, i.e., the ability of driving the system state toward a goal, by proper selection of the system's inputs. From the design point of view, the problem of finding the minimum number of inputs (actuators) to ensure system's controllability has recently been shown to be an NP-hard problem [6], which implies that designing the

minimum number of inputs that ensure a switching system to be controllable is at least as difficult. Therefore, alternative design approaches have been proposed, see, for example, [7]. In this paper, using structured systems theory [8], we obtain necessary conditions to ensure controllability for switching linear systems. Such property is of fundamental interest in several critical systems, such as the electric power grid, where it is critical to ensure that the system state stays within imposed standards in the face of dynamic mode changes often triggered by uncertain events like transmission line failures or faults.

To achieve this, we propose the concept of a *structural hybrid system*, hinged on the graph theoretic representation of a structural switching system [8], in which each mode system operating corresponds to a directed graph (digraph), and mode transitions are captured by switching between distinct digraph representations. We demonstrate that the above concept enables efficient model checking for switching systems and, in particular, provides easy-to-verify necessary conditions that ensure controllability.

Formally, we would like to address the following problem: \mathcal{P}_1

Given $A(\sigma(t))$, where $A \in \mathbb{R}^{n \times n}$ and $\sigma(t) : [0, +\infty[\rightarrow \mathbb{R}$ is a piecewise switching signal, that may only switch at most once in a given dwell-time $[t, t + \varepsilon[$, $\varepsilon > 0$, for all $t \geq 0$, we are interested in obtaining $B(\sigma(t)) \in \mathbb{R}^{n \times p}$ such that

$$\dot{x}(t) = A(\sigma(t))x(t) + B(\sigma(t))u(t), \quad (1)$$

is controllable for all $t \geq 0$ and $B(\sigma(t))$ comprises at most one non-zero entry for each column, i.e., uses *dedicated inputs* only. \diamond

Given that this problem is hard to solve (see [6], for example), hereafter we focus on addressing its *structural* reformulation \mathcal{P}_2 , which provides necessary conditions for the all-time controllability requirement in \mathcal{P}_1 .

Problem Statement

\mathcal{P}_2

Given structural matrices $\bar{A}(\sigma(t))$, with $\bar{A} \in \{0, \star\}^{n \times n}$, where \star stands for a non-zero entry, and $\sigma(t) : [0, +\infty[\rightarrow \mathbb{R}$ is a piecewise constant switching signal satisfying the dwell-time property for some $\varepsilon > 0$, find $\bar{B}(\sigma(t)) \in \{0, \star\}^{n \times p}$ such that the (structural) dynamical system

$$\dot{x}(t) = \bar{A}(\sigma(t))x(t) + \bar{B}(\sigma(t))u(t), \quad (2)$$

is structurally controllable (to be defined precisely soon) for all $t \geq 0$ and $\bar{B}(\sigma(t))$ comprises at most one non-zero entry for each column, i.e., uses dedicated inputs only. \diamond

This work was partially supported by grant SFRH/BD/33779/2009, from Fundação para a Ciência e a Tecnologia (FCT) and the CMU-Portugal (ICTI) program, and by projects CONAV/FCT-PT (PTDC/EEACRO/113820/2009), FCT (PEst-OE/EEI/LA0008/2013) and MORPH (EU FP7 No. 288704).

[†] Institute for System and Robotics, Instituto Superior Técnico, Technical University of Lisbon, Lisbon, Portugal.

[‡] Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213.

[◊] Department of Electrical and Computer Engineering, Faculty of Engineering, University of Porto (FEUP), Portugal.

[§] SQIG-Instituto de Telecomunicações, Department of Mathematics, Instituto Superior Técnico, Technical University of Lisbon, Portugal.

In addition, in this paper, we restrict the analysis of problem \mathcal{P}_2 to the case where \bar{A} satisfies a specific structural constraint, to be made precise in Assumption \mathbf{A}_1 , that is consistent with several practical physical systems, such as the electric power grid as modeled in [9]. Such structural treatment of dynamical properties of switching systems (i.e. switching systems where only its structure is considered) and, in particular, obtaining necessary conditions to ensure structural controllability, has been considered in prior work, see [10], [11], for instance. In [10] a (vector) dynamical system was modeled as a multi-agent network with each agent corresponding to a single scalar state variable of the dynamical system, and the design goal was to obtain the minimal placement of sensors such that system structural observability (the dual of structural controllability) is retained in the face of arbitrary agent departures (such departure events correspond to mode changes and are captured by deleting all the edges in the nominal system digraph incident to the departed agent). Similarly, in [11] a similar multi-agent networked system setting, mode changes consisted of potential removal of bi-directional edges between physically coupled agents (states), and the minimal placement of actuators necessary to retain structural controllability was sought. However, both the approaches were limited to systems in which the digraph representation had the special structure of being the disjoint union of strongly connected components, i.e., with no edge between the components. In contrast, the design and verification methodologies introduced in this paper are more general, include as instances the scenarios studied in [11], [12], and, in particular, applicable to systems in which the digraph representation may consist of several strongly connected components with directed edges between them.

The main contributions of this paper are twofold: first, we introduce the concept of structural hybrid system; second we provide an efficient model checker (i.e., with polynomial time complexity) to ensure the system's structural controllability at all times.

The rest of this paper is organized as follows. Section II reviews and introduces some concepts in structural systems theory, establishing their relations with graph theory and review basic definitions of hybrid systems. Section III presents the main contributions of this paper. In Section IV we discuss possible extensions to other properties for model checking, followed by an illustrative example in Section V. Finally, Section VI concludes the paper and discusses avenues for further research.

II. PRELIMINARIES AND TERMINOLOGY

In this section, we review some concepts of structural systems [12] and some basic concepts of hybrid dynamical systems and hybrid automata [2] in connection with linear switching systems.

A. Structural Systems Theory

Consider a linear time invariant system (LTI) described as

$$\dot{x}(t) = Ax(t) + Bu(t), \quad (3)$$

where $x \in \mathbb{R}^n$ represents the state and $u \in \mathbb{R}^p$ denotes the input. The system (3) is controllable *if and only if* the controllability matrix

$$C = [B \quad AB \quad A^2B \quad \dots \quad A^{n-1}B] \quad (4)$$

has full rank, i.e., $\text{rank}(C) = n$. Informally, a structural system consists of an equivalence class of systems, where *generic* properties are studied based only on the zero/non-zero pattern of the matrices in (3). The structural version of controllability is as follows:

Definition 1: Given a pair (\bar{A}, \bar{B}) of structural matrices, we say that the pair (\bar{A}, \bar{B}) is structurally controllable, if and only if there exists a controllable system (3) such that (\bar{A}, \bar{B}) is a numerical realization of (\bar{A}, \bar{B}) , i.e., has the same structural pattern as (\bar{A}, \bar{B}) . \diamond

Definition 2: Given specific numerical instances of the non-zero entries in (\bar{A}, \bar{B}) , we say that we have a *realization* (A, B) with the same structural pattern of (\bar{A}, \bar{B}) . \diamond

Structural systems provide an efficient representation of the system as a directed graph (digraph). Each digraph is associated with a set of *vertices* V and a set of *directed edges* E of the form (v_i, v_j) where $v_i, v_j \in V$. We represent the state digraph by $\mathcal{D}(\bar{A}) = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ i.e. the digraph that comprises only the state variables as vertices denoted by $\mathcal{X} = \{x_1, \dots, x_n\}$ and a set of directed edges between the state vertices denoted by $\mathcal{E}_{\mathcal{X}, \mathcal{X}} = \{(x_i, x_j) : x_i, x_j \in \mathcal{X} \text{ and } \bar{A}_{j,i} \neq 0\}$. Similarly, we represent the system digraph by $\mathcal{D}(\bar{A}, \bar{B}) = (\mathcal{X} \cup \mathcal{U}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \cup \mathcal{E}_{\mathcal{U}, \mathcal{X}})$, where $\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ are given as in the state digraph and $\mathcal{U} = \{u_1, \dots, u_p\}$ and $\mathcal{E}_{\mathcal{U}, \mathcal{X}} = \{(u_i, x_j) : u_i \in \mathcal{U}, x_j \in \mathcal{X} \text{ and } \bar{B}_{i,j} \neq 0\}$.

Given a digraph \mathcal{D} , a digraph $\mathcal{D}_s = (V_s, E_s)$ such that $V_s \subset V$ and $E_s \subset E$ is said to be *subgraph* of \mathcal{D} . If $V_s = V$, \mathcal{D}_s is said to *span* \mathcal{D} . A sequence of edges $\{(v_1, v_2), (v_2, v_3), \dots, (v_{k-1}, v_k)\}$ is an *elementary path* if all the vertices are distinct. If only $v_k = v_1$, the sequence is called a *cycle*.

In addition, given a collection of digraphs $\mathcal{D}_i = (\mathcal{X}_i, \mathcal{E}_{\mathcal{X}_i, \mathcal{X}_i})$, $i \in \{1, \dots, m\}$, the union digraph of these digraphs is given by $\mathcal{D} = (\bigcup_{i=1}^m \mathcal{X}_i, \bigcup_{i=1}^m \mathcal{E}_{\mathcal{X}_i, \mathcal{X}_i})$.

We also require the following graph theoretic notions [13]: A digraph \mathcal{D} is said to be strongly connected if there exists a directed path between any two pairs of vertices. A *strongly connected component* (SCC) is a maximal subgraph (there is no other subgraph, containing it, with the same property) $\mathcal{D}_S = (V_S, E_S)$ of \mathcal{D} such that for every $u, v \in V_S$ there exists a path from u to v and from v to u . Remark that a path from u to v on an SCC may not be unique and it may be composed by some vertices that are not in the path from v to u . We can create a *directed acyclic graph* (DAG) by visualizing each SCC as a virtual node, where there is a directed edge between vertices belonging to two SCCs if and only if there exists a directed edge connecting the corresponding SCCs in the digraph $\mathcal{D} = (V, E)$, the original digraph. The DAG associated with $\mathcal{D}(\bar{A})$ can be

computed efficiently in $\mathcal{O}(|V| + |E|)$ [13]. The SCCs in the DAG may be further categorized as follows.

Definition 3: [12] An SCC is said to be linked if it has at least one incoming/outgoing edge from another SCC. In particular, an SCC is *non-top/non-bottom linked* if it has no incoming/outgoing edges to/from its vertices from/to the vertices of another SCC. \diamond

Given $\mathcal{D} = (V, E)$ we can associate it with the *bipartite graph* $\mathcal{B}(S_1, S_2, E_{S_1, S_2})$, where $S_1, S_2 \subset V$ and the edge set $E_{S_1, S_2} = \{(s_1, s_2) \in E : s_1 \in S_1, s_2 \in S_2\}$.

A matching M , with respect to the bipartite graph $\mathcal{B}(S_1, S_2, E_{S_1, S_2})$, is a subset of edges in E_{S_1, S_2} , where there are not two edges sharing vertices in neither S_1 nor S_2 . Therefore, a maximum matching M^* is a matching M with the largest number of edges among all possible matchings. Note that in general it may not be unique. The maximum matching problem can be solved efficiently in $\mathcal{O}(\sqrt{|S_1 \cup S_2|} |E_{S_1, S_2}|)$ using, for instance, the Hopcroft-karp algorithm [13]. A vertex in S_1/S_2 is a *left/right-matched vertex* if it belongs to an edge in M^* , otherwise, it is an *left/right-unmatched vertex*. A maximum matching where there are no unmatched vertices is called a *perfect match*.

Remark that due to the equivalence between the system digraph and the pair of matrices (\bar{A}, \bar{B}) of the system (3), given the state digraph $\mathcal{D}(\bar{A}) = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$, we say that a subset of state variables $\mathcal{S}_u \subset \mathcal{X}$ is a *feasible dedicated input configuration* (FDIC) if, by assigning *dedicated inputs* (i.e., an input that is assign to a single state variable) to the state variables in \mathcal{S}_u , and denoting by $\mathcal{U}, \mathcal{E}_{\mathcal{U}, \mathcal{X}}$ the dedicated inputs and its corresponding assignments, then we have that $\mathcal{D}(\bar{A}, \bar{B}) = (\mathcal{X}, \mathcal{U}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \cup \mathcal{E}_{\mathcal{U}, \mathcal{X}})$ corresponds to the digraph representation of a structurally controllable system associated with (\bar{A}, \bar{B}) . The following result may be used to characterize minimal FDICs [12].

Theorem 1 (Minimal FDIC): Let $\mathcal{D}(\bar{A}) = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ denote the system digraph and $\mathcal{B} \equiv \mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ its bipartite representation. A set $\mathcal{S}_u \subset \mathcal{X}$ is a minimal feasible dedicated input configuration if and only if there exist two disjoint subsets \mathcal{U}_R and \mathcal{A}_u^c such that $\mathcal{S}_u = \mathcal{U}_R \cup \mathcal{A}_u^c$, \mathcal{U}_R corresponds to the set of right-unmatched vertices of some maximum matching of \mathcal{B} with maximum number of right-unmatched vertices in different SCCs, and \mathcal{A}_u^c comprising only one state variable from each non-top linked SCC of $\mathcal{D}(\bar{A})$ without a right-unmatched vertex from \mathcal{U}_R . \diamond

Therefore, it is easy to see that any FDIC contains a set of right-unmatched vertices with respect to (w.r.t.) a maximum matching of the state bipartite graph \mathcal{B} and at least one state variable from each non-top linked SCC. To illustrate Theorem 1 we have the example depicted in Figure 1.

B. Hybrid Dynamical Systems

We now provide some basic definitions and properties of hybrid dynamical systems to be used later in the paper, mainly, to discuss possible extensions of the proposed model checker to verify other properties of interest, for instance, the ability to keep the state of the system within a prespecified set of values, commonly known as the *safety problem*.

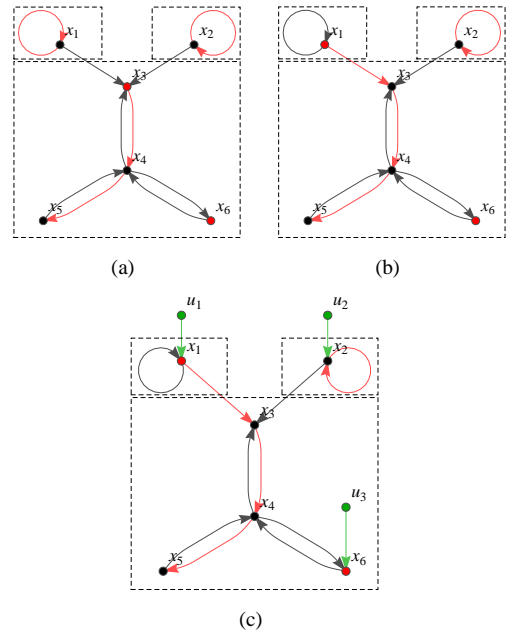


Fig. 1. (a) represents $\mathcal{D}(\bar{A}) = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and its SCCs represented by the dashed rectangles, where the red edges correspond to M^* , a maximum matching associated with $\mathcal{B} = \mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and the red vertices the corresponding \mathcal{U}_R set of right-unmatched vertices. (b) depicts the set of right-unmatched vertices of some maximum matching of \mathcal{B} with maximum number of right-unmatched vertices in different SCCs, the vertices and edges in red, respectively. (c) reproduces $\mathcal{D}(\bar{A}, \bar{B})$, where the green vertices are the input variables connected with the green edges to the set \mathcal{S}_u of Theorem 1.

A hybrid dynamical system is a dynamical system that exhibits both continuous and discrete behavior, that is, a system that alternates between flows and jumps (see [14] for instance).

A particularization of the notion of hybrid dynamical system leads to the useful concept of hybrid automaton, which consists of: a continuous state space \mathbb{R}^n ; a finite directed graph: vertices Q (modes), edges E (control switches); the *flows* φ_q , where $\varphi_q(t; x) \in \mathbb{R}^n$ is the state reached after staying in mode $q \in Q$ for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$; the evolution domain constraints $inv_q \subseteq \mathbb{R}^n$ (invariants) for $q \in Q$; jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$ usually comprising guard on current state and reset relations.

A particular class of hybrid dynamical systems for which we are interested in ensuring certain properties is the one of switching systems. These properties can be, for instance, restrictions of the state to certain domains or constraints in the quantitative behavior of the dynamical system.

A collection of techniques for the automatic analysis and verification of the system properties is often called *model checking*.

Recall that most of the available model checking tools are, in general, undecidable [2], and even approximation methods exhibit numerical instabilities and suffer from the curse of dimensionality, see [3], [4] and references therein.

C. Controllability and Structural Controllability of Switching Systems

We now provide some results about the controllability and structural controllability of switching systems. In what follows we assume that the switching signal σ satisfies the dwell time property. First, if a system is controllable in each state, then it follows that it is controllable, formally, we have:

Proposition 1 ([15]): Given a switching system (2), if each mode of the switching system is controllable, then the switching system is controllable. \diamond

The next result relates Proposition 1 with structural controllability, and follows by definition of structural controllability.

Corollary 1: Given a switching systems (2), if each mode of the switching system is structurally controllable, then the switching system is structurally controllable. \diamond

An alternative interpretation may be obtained as follows:

Proposition 2 ([8]): A switching linear system (2) with state digraphs $\mathcal{D}_i, i \in \{1, \dots, m\}$ is structurally controllable if its union graph \mathcal{D} is structurally controllable. \diamond

Therefore, if a mode in the structural switching system is structurally controllable, it follows that the union of the digraphs corresponding to the states of the structural switching system is structurally controllable. Once again, recall that our goal consists in ensuring that each state of the structural switching system is structurally controllable, hence the system is structurally controllable at all times.

Next, in Section III we present the concept of *structural hybrid systems* that leads to an efficient model checker that ensures properties, of interest, as for example, structural controllability at all times.

III. MAIN RESULTS

In this section we introduce the main results of the paper, that are two fold: we start by introducing the concept of *structural hybrid system*; second, we explore the procedure to model check necessary controllability properties of the structural hybrid system, i.e., design the input matrix that solves \mathcal{P}_2 . Informally, structural hybrid system stands for a linear switching system as (2), where each state consists of a digraph $\mathcal{D}(\bar{A}(\sigma(t)), \bar{B}(\sigma(t)))$, associated with system represented by the pair $(\bar{A}(\sigma(t)), \bar{B}(\sigma(t)))$, that changes over time.

To motivate the notion of structural hybrid system, consider a simple switching system with two modes and its structural representation. By recalling the definition of structural controllability, and its application to each of the modes of the switching system and their structural representations, some properties can be established, as depicted in Figure 2.

In particular, we have the following result:

Proposition 3: A switched system is structurally controllable if for each mode q the digraph $\mathcal{D}(\bar{A}_q, \bar{B}_q)$ (or equivalently, the pair (\bar{A}_q, \bar{B}_q)) is structurally controllable. \diamond

Proof: The result follows immediately by Proposition 2. \blacksquare

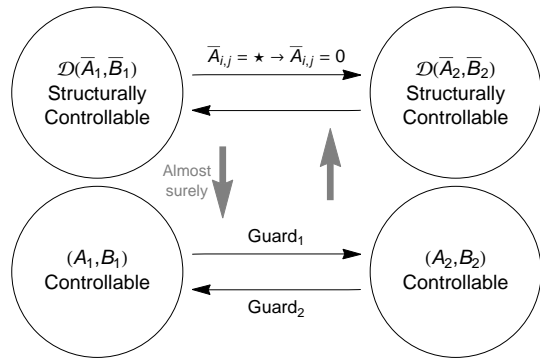


Fig. 2. In bottom we depict a switching system with two controllable states and in the top its structural correspondence. In addition, the digraph representation of the structural representation in the bottom corresponds to a structural hybrid system with two states, where possible transition is identified, by a change in the structure of the dynamic system matrix, i.e., $\bar{A}_{i,j} = * \rightarrow \bar{A}_{i,j} = 0$.

Formally, a *structural hybrid system* can be defined as follows.

Definition 4: [Structural Hybrid System] A structural hybrid system is a hybrid dynamical system constituted by:

- a state space:
a set of structural directed graphs with n state vertices and p input vertices
- $$\mathcal{D}_n = \{\mathcal{D}(\bar{A}, \bar{B}) : \bar{A} \in \{0, *\}^{n \times n}, \bar{B} \in \{0, *\}^{n \times p}\};$$
- a finite directed graph:
vertices Q (modes, which are directed graphs), edges E (switches);
 - jump relations $jump_e \subseteq \mathcal{D}_n \times \mathcal{D}_n$ for edges $e \in E$:
if $q_1 = \mathcal{D}(\bar{A}_1, \bar{B}_1) \in Q$ and $q_2 = \mathcal{D}(\bar{A}_2, \bar{B}_2) \in Q$, then $(q_1, q_2) \in jump_e$ if (\bar{A}_1, \bar{B}_1) differs from (\bar{A}_2, \bar{B}_2) in, at least, one entry. \diamond

Observe that in a structural hybrid system, each change of mode corresponds to a change in the digraph representation. An example is depicted in Figure 5, where we depict two possible transitions from the initial mode described by the digraph $\mathcal{D}(\bar{A}, \bar{B})$, where

$$\bar{A} = \begin{bmatrix} 0 & * & 0 & 0 \\ * & 0 & * & * \\ 0 & * & 0 & 0 \\ 0 & * & 0 & 0 \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} * & 0 \\ 0 & 0 \\ 0 & * \\ 0 & 0 \end{bmatrix}$$

and 1) only the system's dynamic matrix structure changes but the input configuration (i.e., the input matrix structure) remains the same; and 2) both system's dynamic matrix and input matrix structure changes.

A more interesting question to ask, from a system designer point of view is: What should be \bar{B} such that at each mode, the system digraph associated with (\bar{A}, \bar{B}) is structurally controllable. In other words, what is the solution to problem \mathcal{P}_2 ? We address this problem in a restricted setting, more

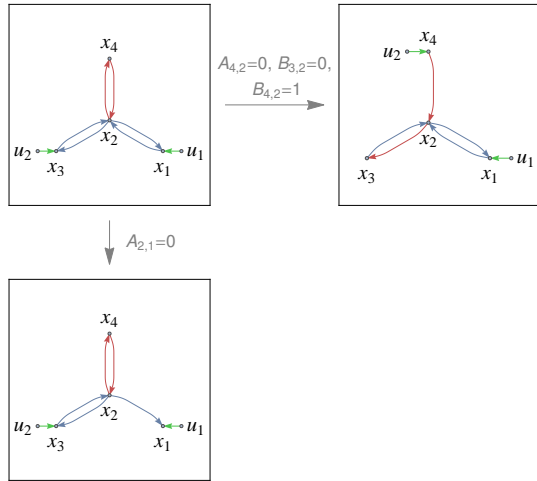


Fig. 3. Structural hybrid system representation of some discrete transitions from the initial directed graph, in the top-left, 1) only the system's dynamic matrix structure changes but the input configuration (i.e., the input matrix structure) remains the same; and 2) both system's dynamic matrix and input matrix structure changes.

precisely, we only consider systems whose associated DAG representations always consist of the same non-top linked SCC across mode changes, and the remaining SCCs satisfy an additional constraint. Otherwise, the edge set of each SCC may vary with mode (structural) transitions, caused, for instance, by failures or natural switches.

Specifically, from this point onwards we consider the following additional assumption:

- A₁** The DAG representation of $\mathcal{D}(\bar{A})$ has only one non-top linked SCC and all the other SCCs originate¹ a perfect matching.

There are several physical systems with this property, in particular, electric power grids as modeled in [9], which we explore later in the paper (see Proposition 4). Also, note that requiring an SCC to originate a perfect matching is not a very restrictive assumption, since, in practice, most of the diagonal entries in the system matrix are non-zero, which correspond to self-loops in the system's digraph and may contribute edges to the maximum matching. In particular, if all states in an SCC have self-loops, it readily follows that such an SCC originates a perfect matching.

Now, we show the feasibility of assumption **A₁** in the electrical power grid as modeled in [9], where a single loss of a transmission line corresponds to the loss of two edges on the system digraph, and where the DAG representation of the system remains the same.

Proposition 4: For any power electrical grid modeled as in [9] and for any single transmission line failure, we have that the system digraph is composed of several SCCs, where only one is a non-top linked SCC and the others SCCs originate perfect matchings. \diamond

Under assumption **A₁**, we now obtain a set of results that provide an understanding of why the solution to \mathcal{P}_2 can be

¹We say that a subgraph $\mathcal{D}_S = (\mathcal{X}_S, \mathcal{E}_{\mathcal{X}_S, \mathcal{X}_S})$ originates a perfect match if the maximum matching associated with the bipartite graph $\mathcal{B}(\mathcal{X}_S, \mathcal{X}_S, \mathcal{E}_{\mathcal{X}_S, \mathcal{X}_S})$ has no right-unmatched vertices.

restricted to the analysis of a single (non-top linked) SCC and a maximum matching problem on the bipartite graph, associated with the system digraph. Such understanding will constitute the basis of the design procedure in our model checker, stated in Theorem 2.

Proposition 5: Given $\mathcal{D}(\bar{A})$ with its DAG representation, constituted by $\{\mathcal{N}_i\}_{i=0}^{n-1}$ SCCs, where $\mathcal{N}_i = (\mathcal{X}_i, \mathcal{E}_{\mathcal{X}_i, \mathcal{X}_i})$. Let \mathcal{N}_0 be the only non-top linked SCC and $\mathcal{B}_i \equiv \mathcal{B}(\mathcal{X}_i, \mathcal{X}_i, \mathcal{E}_{\mathcal{X}_i, \mathcal{X}_i})$ the bipartite graph associated with \mathcal{N}_i , $i = 0, \dots, n-1$. If M_i^* is a maximum matching associated with \mathcal{B}_i ($i = 0, \dots, n-1$) and M_i^* is a perfect matching for $i = 1, \dots, n-1$, then $M^* = \bigcup_{i=0}^{n-1} M_i^*$ is a maximum matching of $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$. \diamond

The previous Proposition follows immediately by noticing that if the matching M^* was not maximum, then some of the M_i^* was not maximum, which leads to a contradiction. Consequently, we have the following result.

Corollary 2: Under the same assumptions of Proposition 5, to computing the set of right-unmatched vertices we only need to compute a maximum matching M_0^* of \mathcal{B}_0 . \diamond

Corollary 2 states that if a system fulfills the conditions of Proposition 5, then, to construct \bar{B} , we just need to consider the design of dedicated inputs restricted to the non-top linked SCC, where the system become structural controllable, by noticing that set of right-unmatched vertices is a FDIC, as stated in Theorem 1.

Now, suppose we consider a transition between modes in the structural hybrid system. If a structural change in the digraph occurs, two scenarios are possible: 1) the placement of inputs previously considered ensures structural controllability; or 2) a new placement of inputs needs to be considered, i.e., the system must be redesigned to ensure structural controllability. Next, we explore the implications of the structure change in the system's dynamics, through the edges present in the non-top linked SCC, and corresponding maximum matching.

Proposition 6: Let \mathfrak{S} be a structural hybrid system with at least two modes, one associated with the directed graph $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and the other to $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$, where $(u, v) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ and let $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ be their bipartite representations, respectively. Additionally let $M \subseteq \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ be a set of edges corresponding to a maximum matching on $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and U_R the set of its associated right-unmatched vertices. If $(u, v) \notin M$, then M is also a maximum matching with respect to $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ and, consequently, the set of its associated right-unmatched vertices is also U_R . \diamond

As an immediate consequence we have the following result.

Corollary 3: Let \mathfrak{S} be a structural hybrid system with at least two modes, associated with the strongly connected directed graphs $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$, where $(u, v) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ and let $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ be their bipartite representations, respectively. Additionally, let $M \subseteq \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ be a set of edges corresponding to a maximum matching on $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$

and U_R the set of its associated right-unmatched vertices. If $(u, v) \notin M$, then $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ is also structurally controllable with the same set of inputs U_R . \diamond

If the eliminated edge belongs to a specific maximum matching of the non-top linked SCC, we obtain the following result.

Proposition 7: Let \mathfrak{S} be a structural hybrid system with at least two modes, one associated with the directed graph $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and the other to $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$, where $(u, v) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ and let $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ be their bipartite representations, respectively. Additionally let $M \subseteq \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ be a set of edges corresponding to a maximum matching on $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and U_R the set of its associated right-unmatched vertices. If $(u, v) \in M$, then there exists a maximum matching \hat{M} with respect to $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ such that $U_R \subseteq \hat{U}_R$ (set of right unmatched vertices with respect to \hat{M}) iff $\hat{M} = M \setminus \{(u, v)\}$ is a maximum matching for $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ or there exists an augmenting path in $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$, with respect to $M \setminus \{(u, v)\}$ ending in v . \diamond

Now, recall that the complexity of finding an augmenting path has complexity $\mathcal{O}(|\mathcal{E}_{\mathcal{X}, \mathcal{X}}|)$, which implies an efficient method to verify which edges jeopardize the structural controllability.

As a particular case of the previous Proposition 3 we have the following.

Corollary 4: Let \mathfrak{S} be a structural hybrid system with at least two modes, associated with the strongly connected directed graphs $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$, where $(u, v) \in \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ and let $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ be their bipartite representations, respectively. Additionally, let $M \subseteq \mathcal{E}_{\mathcal{X}, \mathcal{X}}$ be a set of edges corresponding to a maximum matching on $\mathcal{B}(\mathcal{X}, \mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and U_R the set of its associated right-unmatched vertices. If $(u, v) \in M$ and there exists an augmenting path with respect to $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ ending in v , then $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus \{(u, v)\})$ is also structurally controllable with the same set of inputs U_R . \diamond

Recall that verifying if a graph is strongly connected has complexity $\mathcal{O}(|\mathcal{X}| + |\mathcal{E}_{\mathcal{X}, \mathcal{X}}|)$ using the Tarjan's strongly connected components algorithm [13].

Theorem 2: Let $\bar{A}(\sigma(I_l))$ represent the structure of $A(\sigma(I_l))$ on the time interval $I_l = [t_l, t_{l+1}[$, $(\bar{A}(\sigma(I_l)), \bar{B}(\sigma(I_l)))$ denote the l -th state of the structural hybrid system, $\mathcal{D}(\bar{A}) = (\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}})$ and $\Sigma = \{\sigma(I_l), l = 0, 1, \dots\}$ such that $|\Sigma| \leq p(|\mathcal{X}|)$, where p is a polynomial on the number of state variables $|\mathcal{X}|$. The solution of \mathcal{P}_2 can be found with the following procedure: First, consider the initial state of the structural hybrid system and find $\bar{B}(\sigma(I_0))$ that ensures structural controllability by the following steps

- 1) Create the DAG representation of $\mathcal{D}(\bar{A})$;
- 2) Compute the maximum matching M^* for the non-top linked SCC;
- 3) Construct $\bar{B}(\sigma(I_0))$ as corresponding to assign dedicated inputs to the right-unmatched vertices associated with M^* ;

For each possible state corresponding to the system with $\bar{A}(\sigma(I_{l+1}))$ determine $\bar{B}(\sigma(I_{l+1}))$ as

- 1) Detect the set of removed edges from $(\bar{A}(\sigma(I_l)), \bar{B}(\sigma(I_l)))$, denoted by \mathcal{E}_l ;
- 2) For each $e \in \mathcal{E}_l$ use the results of Proposition 7 and 6 for designing $\bar{B}(\sigma(I_{l+1}))$.

The complexity of this procedure is $\mathcal{O}((\sqrt{|\mathcal{X}|}|\mathcal{E}_{\mathcal{X}, \mathcal{X}}| + |\mathcal{E}_{\mathcal{X}, \mathcal{X}}|)|\mathcal{E}_{\mathcal{X}, \mathcal{X}}|p(|\mathcal{X}|))$. \diamond

In the above, we only considered the case where one edge in the directed graph fails, however, the results can be readily extended to the case with multiple edge failures. In the latter case, if n edges fail simultaneously, for analysis purposes, the failures may be viewed as happening sequentially one at a time and the previous results are applicable. Specifically, under the assumptions of Proposition 7, if we lose a set of edges $E \subseteq M$, if there is a maximum matching with respect to $\mathcal{D}(\mathcal{X}, \mathcal{E}_{\mathcal{X}, \mathcal{X}} \setminus E)$ with the same right unmatched vertices, then it is structurally controllable with the same set of inputs U_R , otherwise we have a new set of right unmatched vertices \hat{U}_R with $|\hat{U}_R| \leq |U_R|$.

In the next section, we explore how to extend the concept of structural hybrid system to verify other properties.

IV. EXTENSION TO OTHER PROPERTIES FOR MODEL CHECKING

Additionally, structural hybrid systems can be used to perform model checking for other properties, such as *safety*, i.e., if a system can keep its state within certain values. In order to do such reasoning, we start with a comparison between the structural hybrid system and hybrid automaton.

Now, suppose that the evolutions of the hybrid automaton imposes changes on the domain of the system. For instance, suppose that we have a linear system with continuous time $\dot{x}(t) = A_1x(t) + B_1u(t)$, $x \in \Omega_1$ it can evolve to another linear system $\dot{x}(t) = A_2x(t) + B_2u(t)$, $x \in \Omega_2$, with the transition of the system given by a guard on the state variable $x(t)$, depicted in Figure 4.

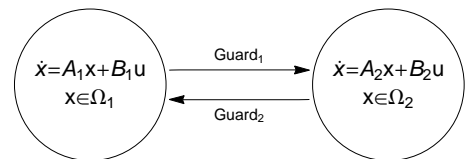


Fig. 4. Hybrid system with two states and two discrete jumps, where each state represents a SLS system with the state variable on a certain domain.

Proposition 8: Consider a linear system $\dot{x}(t) = Ax(t) + Bu(t)$, let Ω be an open and connected set. If the pair of matrices (A, B) is controllable then we can ensure that $x(t) \in \Omega$. \diamond

The next results follows immediately.

Corollary 5: Given a switching system (2), using Proposition 8 applied to each mode, the result holds for the switching entire system. \diamond

Observe that, if the structural hybrid system is structurally controllable, then, almost surely, using Corollary 5, it is controllable.

Now, with Proposition 8 in mind, we can abstract our previous model and reasoning about the controllability of the pair of matrices (A_1, B_1) and (A_2, B_2) where the system transition is, once again, a guard on the state variable $x(t)$. We refer the reader to Figure 5 for a graphical representation of the new aforementioned abstraction.

Nevertheless, notice that the reverse implication is not true, as depicted in Figure 8. The following counter-example illustrates a case where the implication does not hold. Consider the following dynamic system:

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(0) = 0$$

with $B = 0$ and $\Omega = B_\varepsilon(0)$, $\varepsilon > 0$. The controllability matrix of the dynamic system is

$$\mathcal{C} = [B \ AB \ \dots \ A^n B] = 0$$

and $\text{rank}(\mathcal{C}) \neq n$. Therefore, the system is not controllable.

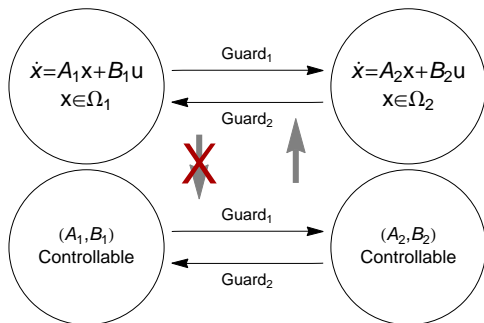


Fig. 5. Relationship between the hybrid system abstraction based on the pair of matrices (A, B) of the linear systems and the original hybrid system.

V. ILLUSTRATIVE EXAMPLE

In this section we provide an illustrative example of the structural hybrid systems in the context of power electrical grids, where link failures, may occur due to fatigue and over heat of transmission lines.

The IEEE 5-bus power system, depicted in Figure 9, is a standard benchmark model used as proof-of-concept for different methodologies suggested in power systems. It corresponds to a electric power grid composed by 5 buses (depicted by black rectangles), interconnected through transmission lines (depicted by solid lines), and which represents the network topology. Here, we consider three power generators, denoted by G_i ($i = 1, 2, 3$) and two power loads L_i ($i = 1, 2$), coupled through the network topology. Additionally, we adopt the cyber-physical modeling of the generators (as Steam-Turbine-Generators) and loads (as induction machines), similar to the proposed approach in [16], where the linear system is obtained by linearization. For the complete description of our model, see [17].

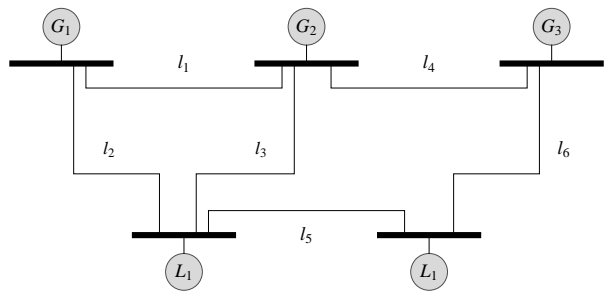


Fig. 6. Graph representation of a 5-bus system.

TABLE I
STATE VARIABLES OF THE GENERATORS AND LOADS

Descriptions	Node Number
frequency of $G1$ (ω_{G_1})	1
turbine output mechanical power of $G1$ (P_{T_1})	2
steam valve opening position of $G1$ (a_1)	3
frequency of $G2$ (ω_{G_2})	4
turbine output mechanical power of $G2$ (P_{T_2})	5
steam valve opening position of $G2$ (a_2)	6
frequency of $G3$ (ω_{G_3})	7
turbine output mechanical power of $G3$ (P_{T_3})	8
steam valve opening position of $G3$ (a_3)	9
random noise of $L1$ (ω_{L_1})	15
load consumed of $L1$ (L_1)	16
random noise of $L2$ (ω_{L_2})	17
load consumed of $L2$ (L_2)	18

In Table II, we describe the variables of interest, i.e., the variables of the generators and loads, of the system digraph corresponding to the system's structure as depicted in Figure 7 and 8. Remark that the remaining variables/nodes in the system digraph correspond to the interaction variables interconnecting the different bus/generators/loads.

Now we want to solve \mathcal{P}_2 , given the dynamic system derived by considering the IEEE 5-bus power system depicted in Figure 6, and assuming that only a single transmission line failure can occur. First, notice that assumption \mathbf{A}_1 holds for the original system digraph, as well as for the system digraph where one transmission line fails, accordingly with Proposition 4. For illustrative purpose, consider Figure 7 and Figure 8, that depict the system's original digraph and under the failure of transmission line l_1 .

Now, let us consider the design/selection of the dedicated inputs ensuring the structural controllability of the system. Therefore, we can use the procedure of Theorem 2 in order to design the matrix \bar{B} . Since for each possible connection line failure the SCCs of the system digraph still have a perfect matching, by Theorem 1, we only need to assign one input to any state variable belonging to the non-top link SCC in order to ensure structural controllability. However, from the physical point of view, we can only actuate the variables ω_{G_i} ($i = 1, 2, 3$) of the generators. Hence, we can design \bar{B} as one of the canonical vectors in $\{e_1, e_4, e_7\}$, where $e_i \in \{0, \star\}$ ¹⁸ is a vector with \star in the i -th position and zero elsewhere.

To complement the proposed analysis, in [17] we consid-

