Reachability Analysis for High-Index Linear Differential Algebraic Equations

Hoang-Dung Tran[1], Luan Viet Nguyen[2], Nathaniel Hamilton[1], Weiming Xiang[1][0000−0001−9065−8428], and Taylor T. Johnson[1][0000−0001−8021−9923]

[1] Institute for Software Integrated Systems, Vanderbilt University, TN, USA
[2] University of Pennsylvania, PA, USA

Abstract. Reachability analysis is a fundamental problem for safety verification and falsification of Cyber-Physical Systems (CPS) whose dynamics follow physical laws usually represented as differential equations. In the last two decades, numerous reachability analysis methods and tools have been proposed for a common class of dynamics in CPS known as ordinary differential equations (ODE). However, there is lack of methods dealing with differential algebraic equations (DAE), which is a more general class of dynamics that is widely used to describe a variety of problems from engineering and science, such as multibody mechanics, electrical circuit design, incompressible fluids, molecular dynamics, and chemical process control. Reachability analysis for DAE systems is more complex than ODE systems, especially for *high-index* DAEs because they contain both a *differential part* (i.e., ODE) and *algebraic constraints (AC)*. In this paper, we propose a scalable reachability analysis for a class of high-index large linear DAEs. In our approach, a high-index linear DAE is first decoupled into one ODE and one or several AC subsystems based on the well-known Marz decoupling method utilizing *admissible projectors*. Then, the *discrete* reachable set of the DAE, represented as a list of *star-sets*, is computed using simulation. Unlike ODE reachability analysis where the initial condition is freely defined by a user, in DAE cases, the consistency of the initial condition is an essential requirement to guarantee a feasible solution. Therefore, a thorough check for the consistency is invoked before computing the discrete reachable set. Our approach successfully verifies (or falsifies) a wide range of practical, high-index linear DAE systems in which the number of state variables varies from several to thousands.

1 Introduction

Reachability analysis for continuous and hybrid systems has been an attractive research topic for the last two decades since it is an essential problem for verification of safety-critical CPS. In this context, numerous techniques and tools have been proposed. Reachability analysis using zonotopes [2, 21] and support functions [19, 22] are efficient approaches when dealing with linear, continuous and hybrid systems. For nonlinear, continuous and hybrid systems, dReal [25] using

$\delta-$reachability analysis and Flow* [10] using Taylor model are well-known and efficient approaches. However, these over-approximation based approaches can only conduct a reachability analysis for small and medium scale systems. To deal with large-scale systems, other simulation-based methods have been proposed recently. For linear cases, the simulation-equivalent reachability analysis [5, 16] utilizing the *generalized star-set* as the state-set representation has shown an impressive result by successfully dealing with linear systems up to $10,000$ state variables. In this approach, the *discrete simulation-equivalent* reachable set of a linear ODE system can be computed efficiently using standard ODE solvers by taking advantage of the superposition property. Another technique applies order-reduction abstraction [23, 32, 33] in which a large system can be abstracted to a smaller system with bounded error. For nonlinear cases, C2E2 [15, 18] utilizing simulation has shown significant improvement on time performance and scalability in comparison with other methods. Recently, a new numerical verification approach has been proposed to verify/falsify the safety properties of CPS with physical dynamics described by partial differential equations [31, 34].

Although many methods have been developed for reachability analysis of CPS, most of them mentioned above focus on CPS with ODE dynamics. There is a lack of methodology in analyzing systems with high-index DAE dynamics. It is because the reachability analysis for DAE systems is more complex than ODE systems, especially for *high-index* DAEs because they contain both a *differential part* (i.e., ODE) and *algebraic constraints* (AC). It should be emphasized that there are efficient reachability analysis approaches for DAE systems with index-1 [1, 11, 13, 28]. Dealing with index-1 DAE is slightly different from coping with pure ODE because, with a consistent initial condition, a semi-explicit index-1 DAE can be converted to an ODE. As CPS involving high-index DAE dynamics appear extensively in engineering and science such as multi-body mechanics, electrical circuit design, heat and gas transfer, chemical process, atmospheric physics, thermodynamic systems, and water distribution network [8, 17], there is an urgent need for novel reachability analysis methods and tools that can either verify or falsify the safety properties of such CPS. Solving this challenging problem is the main contribution of this research.

The novelty of our approach comes from its objective in dealing with high-index DAE which is a popular class of dynamics that has not been addressed in the existing literature. In this paper, we investigate the reachability analysis for large linear DAE systems with the index up to 3, which appear widely in practice. There are a variety of definitions for the index of a linear DAE. However, throughout the paper, we use the concept of *tractability index* proposed in [26] to determine the index of a linear DAE system. Our approach consists of three main steps (a) decoupling and consistency checking, (b) reachable set computation, and (c) safety verification or falsification; that can be summarized as follows.

The first step is to use the Marz decoupling method [7, 26] to decouple a high-index DAE into one ODE subsystem and one or several algebraic constraint (AC) subsystems. The core step in decoupling is constructing a set of admissible projectors which has not previously been discussed deeply in the existing literature.

In this paper, *we propose a novel algorithm that can construct such admissible projectors for a linear DAE system with the index up to* 3 *(most of DAE systems in practice have index from 1 to 3)*. Additionally, we define a *consistent space* for the DAE because, unlike ODE reachability analysis where the initial set of states can be freely defined by a user, to guarantee a numerical solution for the DAE system, the initial state and inputs of such DAE system must be consistent and satisfy certain constraints. It is important to emphasize that the decoupling and consistency checking methods used in our approach can be combined with existing over-approximation reachability analysis methods [2,19] to compute the over-approximated reachable sets for high-index, linear DAE systems with small to medium dimensions.

The second step in our approach is reachable set computation. Since our main objective is to verify or falsify large linear DAEs, we extend ODE simulation-based reachability analysis to DAEs. In particular, we modify the *generalized star-set* proposed in [5] to enhance the efficiency in checking the initial condition consistency and safety for DAEs. From a consistent initial set of states and inputs, the reachable set of a DAE system can be constructed by combining the reachable sets of its subsystems. It is also worth pointing out that the piecewise constant inputs assumption for ODE with inputs used in [5] may lead a DAE system to *impulsive behavior*. Therefore, in this paper, we assume the inputs applied to the system are *smooth functions*. Such the inputs can be obtained by *smoothing* piecewise constant inputs with filters.

The last step in our approach is to verify or falsify the safety properties of the DAE system using the constructed reachable set computed in the second step. In this paper, we consider linear safety specifications. We are interested in checking the safety of the system in a specific direction defined using a directional matrix. Using the modified star-set and the directional matrix, checking the safety property can be solved efficiently as a low-dimensional feasibility linear programming problem. In the case of violation, our approach generates a counterexample trace that falsifies the system safety.

Contribution. The main contributions of the paper are as follows.

1. A novel reachability analysis approach for high-index linear DAE systems developed based on the effective combination of a decoupling method and a reachable set computation using star-set. To the best of our knowledge, this problem has not been addressed in the existing literature.
2. An end-to-end design and implementation of the approach in a Python toolbox, called *Daev*, which is publicly available for verifying high-index linear DAE systems.
3. An extensive evaluation that demonstrates the capability of our approach in verifying/falsifying a wide range of practical, high-index linear DAE systems where the number of state variables varies from several to thousands.

We note that our reachability analysis approach for high-index DAEs based on combining the decoupling technique and existing ODE reachability analysis is extensible and generic. Instead of using star-set, one can use the decoupling technique in a combination of other state-of-the-art ODE reachability analysis

tool like SpaceEx and Flow* for specific application purposes. We choose star-set to handle high-index large linear DAEs because of its scalability advantage compared to other ODE reachability analysis tools.

Outline of paper. The remainder of the paper is structured as follows. Section 2 reviews the relevant definitions of a high-index large linear DAE system, and the concept of a modified star-set used to represent its reachable set. Section 3 describes our decoupling approach that can effectively decouple a high-index DAE system into ODE and AC subsystems. Section 4 discusses the consistent condition for the initial states and inputs of a DAE system. Section 5 presents the core algorithms that can efficiently compute reachable set and perform a safety verification/falsification for a high-index large linear DAE system. Sections 6 describes the verification results of our approach through a collection of high-index linear DAE system benchmarks. Section 7 concludes the paper and presents future research directions for the proposed work.

2 Preliminaries

2.1 Linear DAE system

We are interested in the reachability analysis of a high-index large linear DAE system described as follows:

$$\Delta: \ E\dot{x}(t) = Ax(t) + Bu(t), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector of the system; $E, A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ are the system's matrices in which E is *singular*; and $u(t) \in \mathbb{R}^m$ is the input of the system. Let I_n be the n-dimensional identity matrix. The regularity, the tractability index, the admissible projectors, the fixed-step bounded-time simulation, and the bounded-time simulation-equivalent reachable set of the system are defined below.

Definition 1 (Regularity [12]). *The pair (E, A) is said to be regular if $det(sE-A)$ is not identically zero.*

Remark 1. For *any specified initial conditions*, the regularity of the pair (E, A) guarantees the existence and uniqueness of a solution of the system (1).

Definition 2 (Tractability index [26]). *Assume that the DAE system (1) is solvable, i.e., the matrix pair (E, A) is regular. A matrix chain is defined by:*

$$\begin{aligned} &E_0 = E, \ A_0 = A, \\ &E_{j+1} = E_j - A_jQ_j, \quad A_{j+1} = A_jP_j, \ \textit{for } j \geq 0, \end{aligned} \tag{2}$$

where Q_j are projectors onto $Ker(E_j)$, i.e., $E_jQ_j = 0$, $Q_j^2 = Q_j$, and $P_j = I_n - Q_j$. Then, there exists an index μ such that E_μ is nonsingular and all E_j are singular for $0 \leq j < \mu-1$. It is said that the system (1) has tractability index-μ. In the rest of the paper, we use the term "index" to state for the "tractability index" of the system.

Definition 3 (Admissible projectors [26]). *Given a DAE with tractability index-μ, the projectors $Q_0, Q_1, \cdots, Q_{\mu-1}$ in Definition 2 are called admissible if and only if they satisfy the following property: $\forall j > i$, $Q_jQ_i = 0$.*

Definition 4 (Fixed-step, bounded-time simulation). *Given consistent initial state x_0 and input $u(t)$, a time bound T, and a time step h, the finite sequence:*

$$\rho(x_0, u(t), h, T = Nh) = x_0 \xrightarrow[0\le t<h]{u(t)} x_1 \xrightarrow[h\le t<2h]{u(t)} x_2 \cdots \xrightarrow[(N-1)h\le t<Nh]{u(t)} x_N,$$

is a $(x_0, u(t), h, T)$-simulation of the DAE system (1) if and only if for all $0 \le i \le N-1$, x_{i+1} is the state of the system trajectory starting from x_i when provided with input function $u(t)$ for $ih \le t < (i+1)h$. If there is no input, $u(t) = 0$.

The consistent condition for the initial state x_0 and input $u(t)$ will be discussed in detail in Section 4. From the fixed-step, bounded-time simulation of a DAE system, we define the following bounded-time, simulation-equivalent reachable set of the DAE system.

Definition 5 (Bounded-time, simulation-equivalent reachable set). *Given sets of consistent initial state X_0 and input U, the bounded-time, simulation-equivalent reachable set $R_{[0,T]}(\Delta)$ of the system (1) is the set of all states that can be encountered by any $(x_0, u(t), h, T)$-simulation starting from any $x_0 \in \mathcal{X}_0$ and input $u(t) \in U$.*

Let $Unsafe(\Delta) \triangleq Gx \le f$ be the unsafe set of the DAE system (1) in which $x \in \mathbb{R}^n$ is the state vector of the system, $G \in \mathbb{R}^{k\times n}$ is the *unsafe matrix* and $f \in \mathbb{R}^k$ is the *unsafe vector*. Given sets of consistent initial state X_0 and input U, the simulation-based safety verification and falsification problem is defined in the following.

Definition 6 (Simulation-based safety verification and falsification). *The DAE system (1) is said to be "simulationally safe" up to time T if and only if its simulation-equivalent reachable set, $R_{[0,T]}(\Delta)$, and the unsafe set, $Unsafe(\Delta)$, are disjoint, i.e., $R_{[0,T]}(\Delta) \cap Unsafe(\Delta) = \emptyset$. Otherwise, it is simulationally unsafe.*

The DAE system is said to be "simulationally falsifiable" if and only if it is simulationally unsafe and there exists a simulation, $(x_0, u(t), h, T)$, that leads the initial state, x_0, of the system to an unsafe state, $x_{unsafe} \in Unsafe(\Delta)$.

The main objective of the paper is to compute the simulation-equivalent reachable set, $R_{[0,T]}(\Delta)$, of the DAE system and use it to verify or falsify the safety property of the system. In the rest of the paper, we use the term *reachable set* to stand for *simulation-equivalent reachable set*. Next, we define a *modified star set* which is used as the state-set representation of the DAE system.

2.2 Modified star set

In our approach, we use a modified star set to represent the reachable set of the DAE system. The modified star set is slightly different from the generalized star set [5] because it does not have a *center vector* and is only defined on a star's $n \times k$ basis matrix.

Definition 7 (Modified star set). *A modified star set (or simply star) Θ is a tuple $\langle V, P\rangle$ where $V = [v_1, v_2, \cdots, v_k] \in \mathbb{R}^{n\times k}$ is a star basis matrix and P is a linear predicate. The set of states represented by the star is given by:*

$$[\![\Theta]\!] = \{x \mid x = \Sigma_{i=1}^{k}(\alpha_i v_i) = V \times \alpha,\ P(\alpha) \triangleq C\alpha \leq d\}, \tag{3}$$

where $\alpha = [\alpha_1, \alpha_2, \cdots, \alpha_k]^{\boldsymbol{T}}$, $C \in \mathbb{R}^{p\times k}$, $d \in \mathbb{R}^p$ and p is the number of linear constraints.

The benefit of the modified star set come from its form given as a *matrix-vector product* which is convenient (in next sections) for checking initial condition consistency and safety properties. In the rest of the paper, we will refer to both the tuple Θ and the set of states $[\![\Theta]\!]$ as Θ.

To construct the reachable set of the DAE system (1), we decouple the system into $\mu + 1$ subsystems where μ is the index of the DAE system. The underlining technique used in our approach is the Marz decoupling method utilizing admissible projectors which is presented in detail in the following section.

3 Decoupling

In this section, we discuss how to decouple a high-index DAE system into one ODE subsystem and one or several AC subsystems using the matrix chain and admissible projectors defined in the previous section with noticing that the decoupled system and the original one are equivalent, i.e., they have the same solutions. Since we are particularly interested in DAE systems with index up to 3 which happen in most of DAE systems in practice, the proofs of decoupling process for index-1, -2, and -3 are given in detail in the appendix. A generalization of decoupling for a DAE with arbitrary index is presented in [26]. As the construction of admissible projectors used in decoupling has not been discussed clearly in existing literature, in this section, we propose a method and an algorithm to solve this problem.

Lemma 1 (Index-1 DAE decoupling [7, 26]). *An index-1 DAE system described by (1) can be decoupled using the matrix chain defined by Equation (2) as follows:*

$$\begin{aligned}
\Delta_1 :\quad & \dot{x}_1(t) = N_1 x_1(t) + M_1 u(t),\ \textit{ODE subsystem},\\
\Delta_2 :\quad & x_2(t) = N_2 x_1(t) + M_2 u(t),\ \textit{AC subsystem},\\
& x(t) = x_1(t) + x_2(t),\\
& x_1(t) = P_0 x(t),\ N_1 = P_0 E_1^{-1} A_0,\ M_1 = P_0 E_1^{-1} B,\\
& x_2(t) = Q_0 x(t),\ N_2 = Q_0 E_1^{-1} A_0,\ M_2 = Q_0 E_1^{-1} B.
\end{aligned}$$

Proof is given in Appendix C.1.

Lemma 2 (Index-2 DAE decoupling [7, 26]). *An index-2 DAE system described by (1) can be decoupled into a decoupled system using the matrix chain*

defined by Equation (2) and the admissible projectors in Definition 3 as follows:

$$
\begin{aligned}
\Delta_1: &\quad \dot{x}_1(t) = N_1 x_1(t) + M_1 u(t),\ \textit{ODE subsystem},\\
\Delta_2: &\quad x_2(t) = N_2 x_1(t) + M_2 u(t),\ \textit{AC subsystem 1},\\
\Delta_3: &\quad x_3(t) = N_3 x_1(t) + M_3 u(t) + L_3 \dot{x}_2(t),\ \textit{AC subsystem 2},\\
&\quad x(t) = x_1(t) + x_2(t) + x_3(t),\\
&\quad x_1(t) = P_0P_1x(t),\ N_1 = P_0P_1E_2^{-1}A_2,\ M_1 = P_0P_1E_2^{-1}B,\\
&\quad x_2(t) = P_0Q_1x(t),\ N_2 = P_0Q_1E_2^{-1}A_2,\ M_2 = P_0Q_1E_2^{-1}B,\\
&\quad x_3(t) = Q_0x(t),\ N_3 = Q_0P_1E_2^{-1}A_2,\ M_3 = Q_0P_1E_2^{-1}B,\ L_3 = Q_0Q_1.
\end{aligned}
$$

Proof is given in Appendix C.2.

Lemma 3 (Index-3 DAE decoupling [7, 26]). *An index-3 DAE system described by (1) can be decoupled into a decoupled system using the matrix chain defined by Equation (2) and the admissible projectors in Definition 3 as follows:*

$$
\begin{aligned}
\Delta_1: &\quad \dot{x}_1(t) = N_1 x_1(t) + M_1 u(t),\ \textit{ODE subsystem},\\
\Delta_2: &\quad x_2(t) = N_2 x_1(t) + M_2 u(t),\ \textit{AC subsystem 1},\\
\Delta_3: &\quad x_3(t) = N_3 x_1(t) + M_3 u(t) + L_3 \dot{x}_2(t),\ \textit{AC subsystem 2}\\
\Delta_4: &\quad x_4(t) = N_4 x_1(t) + M_4 u(t) + L_4 \dot{x}_3(t) + Z_4 \dot{x}_2(t),\ \textit{AC subsystem 3}\\
&\quad x(t) = x_1(t) + x_2(t) + x_3(t) + x_4(t),\ \textit{where:}\\
x_1(t) &= P_0P_1P_2x(t),\ N_1 = P_0P_1P_2E_3^{-1}A_3,\ M_1 = P_0P_1P_2E_3^{-1}B,\\
x_2(t) &= P_0P_1Q_2x(t),\ N_2 = P_0P_1Q_2E_3^{-1}A_3,\ M_2 = P_0P_1Q_2E_3^{-1}B,\\
x_3(t) &= P_0Q_1x(t),\ N_3 = P_0Q_1P_2E_3^{-1}A_3,\ M_3 = P_0Q_1P_2E_3^{-1}B,\ L_3 = P_0Q_1Q_2,\\
x_4(t) &= Q_0x(t),\ N_4 = Q_0P_1P_2E_3^{-1}A_3,\ M_4 = Q_0P_1P_2E_3^{-1}B,\ L_4 = Q_0Q_1,\\
&\quad Z_4 = Q_0P_1Q_2.
\end{aligned}
$$

Proof is given in Appendix C.3.

It should be noted that the AC subsystems Δ_3 and Δ_4 in Lemma 2 and 3 are called algebraic constraints, though they contain the derivatives of $x_2(t)$ and $x_3(t)$. This is because the explicit forms of these algebraic constraints can be obtained if we further extend the derivatives using the corresponding ODE subsystems. In addition, one can see that for a DAE system with index-2 or -3, a set of admissible projectors need to be constructed for decoupling. In the following, we give a Proposition and Lemmas that are used to construct such admissible projectors.

Proposition 1 (Orthogonal projector on a subspace). *Given a real matrix $Z \in \mathbb{R}^{n\times n}$ such that $rank(Z) = r < n$, the Singular-Value Decomposition (SVD) of Z has the form:*

$$
Z = [L_1\ L_2] \begin{bmatrix} S_{r\times r} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} K_1^T \\ K_2^T \end{bmatrix}, \tag{4}
$$

where $L_1, K_1 \in \mathbb{R}^{n\times r}$ and $L_2, K_2 \in \mathbb{R}^{n\times n-r}$. Then, the matrix $Q = K_2K_2^T$ is an orthogonal projector on $Ker(Z)$, i.e., $ZQ = 0$, $Q = Q^T$ and $Q^2 = Q$.

Proof is given in Appendix C.4.

For an index-2 or -3 DAE system, using Proposition 1, we can construct a set of projectors of the matrix chain defined in Equation (2). However, these projectors are not yet admissible, because $Q_j Q_i \neq 0, j > i$. Instead, the admissible projectors can be constructed based on these inadmissible projectors using the following Lemmas.

Lemma 4 (Admissible projectors for an index-2 DAE system). *Given an index-2 DAE system described by (1), let Q_0 and Q_1 respectively be the orthogonal projectors of E_0 and E_1 of the matrix chain defined in Equation (2). The following projectors Q_0^* and Q_1^* are admissible: $Q_0^* = Q_0,\ Q_1^* = -Q_1 E_2^{-1} A_1$.*

Proof is given in Appendix C.5.

Lemma 5 (Admissible projectors for an index-3 DAE system). *Given an index-3 DAE system described by (1), let Q_0, Q_1 and Q_2 respectively be the orthogonal projectors of E_0, E_1 and E_2 of the matrix chain defined in Equation (2). We define the following projectors and the corresponding new matrices for the matrix chain as:*

$$Q_2' = -Q_2 E_3^{-1} A_2,\ Q_1' = -Q_1 P_2' E_3^{-1} A_1,\ E_2' = E_1 - A_1 Q_1',\ A_2' = A_1 P_1'$$

where $P_2' = I_n - Q_2'$ and $P_1' = I_n - Q_1'$. Let Q_2'' be the orthogonal projector on E_2' and $E_3'' = E_2' - A_2' Q_2''$, then the following projectors Q_0^*, Q_1^* and Q_2^* are admissible: $Q_0^* = Q_0,\ Q_1^* = Q_1',\ Q_2^* = -Q_2''(E_3'')^{-1} A_2'$.

Proof is given in Appendix C.6.

Lemmas 4 and 5 are the constructions of admissible projectors for index-2 and -3 DAE systems. The details of the admissible projectors construction are summarized in Algorithm A.1. Next, based on the decoupled DAE system, we discuss the consistent condition of the system and analyze the system behavior under the effect of input functions.

4 Consistency

In this section, we discuss the consistent condition for a DAE system. Using the decoupled DAE system, the consistent condition for the initial state and inputs is derived. Additionally, the piecewise constant assumption on the inputs used in [5] for ODE systems may lead to *impulsive behavior* in high-index DAE systems. To avoid this, we limit our problem to *smooth* and *specific-user-defined* inputs. As a result, DAE systems with inputs can be converted to autonomous DAE systems, where *consistent spaces* for the initial states and inputs can be conveniently defined and checked. Furthermore, the reachable set computation is executed efficiently using a decoupled autonomous DAE system.

Using Lemmas 1, 2, and 3, to guarantee a solution for the DAE system, the initial states and inputs must satisfy the following conditions:

$$\begin{aligned}
&\text{Index-1 DAE}: \quad x_2(0) = N_2 x_1(0) + M_2 u(0),\\
&\text{Index-2 DAE}: \quad x_2(0) = N_2 x_1(0) + M_2 u(0),\\
&\qquad\qquad\quad\; x_3(0) = N_3 x_1(0) + M_3 u(0) + L_3 \dot{x}_2(0),\\
&\text{Index-3 DAE}: \quad x_2(0) = N_2 x_1(0) + M_2 u(0),\\
&\qquad\qquad\quad\; x_3(0) = N_3 x_1(0) + M_3 u(0) + L_3 \dot{x}_2(0),\\
&\qquad\qquad\quad\; x_4(0) = N_4 x_1(0) + M_4 u(0) + L_4 \dot{x}_3(0) + Z_4 \dot{x}_2(0).
\end{aligned} \tag{5}$$

Assuming that the consistent condition is satisfied, Lemmas 2 and 3 indicate the solution of the system involves the derivatives of the input functions $\dot{x}_2(t) = N_2\dot{x}_1(t) + M_2\dot{u}(t)$ and $\dot{x}_3(t) = N_3\dot{x}_1(t) + M_4\dot{u}(t) + L_3[N_2\ddot{x}_1(t) + M_2\ddot{u}(t)]$. In cases where we apply piecewise constant inputs to a high-index DAE system, the impulsive behavior may appear in the system at an exact discrete time point t_k. For example, let $u(t)$ be a step function in $[t_k, t_{k+1})$, then $\dot{u}(t_k) = \delta(t_k)$, where $\delta(t_k)$ is the Dirac function describing an impulse. To avoid such impulsive behavior and do reachability analysis for high-index DAE systems, we limit our approach to smooth inputs which are governed by the following ODE: $\dot{u}(t) = A_u u(t),\ u(0) = u_0 \in U_0$, where $A_u \in \mathbb{R}^{m\times m}$ is the user-defined input matrix, and U_0 is the set of initial inputs.

Remark 2. By introducing the input matrix A_u, we limit the safety verification and falsification of a high-index DAE system to a class of *specific-user-defined* inputs. If $A_u = 0$, then the input set is a set of constant inputs. We note that designing the input matrix A_u can be seen as the last step in designing a controller for a DAE system to eliminate the impulsive behavior of the closed-loop system which is a fundamental problem in DAE control system [14].

Given a user-defined input matrix A_u, a DAE system described by (1) can be converted to an equivalent autonomous DAE system of the following form:

$$\bar{E}\dot{\bar{x}}(t) = \bar{A}\bar{x}(t), \tag{6}$$

where $\bar{x}(t) = \begin{bmatrix} x(t) \\ u(t) \end{bmatrix} \in \mathbb{R}^{n+m}$, $\bar{E} = \begin{bmatrix} E & 0 \\ 0 & I_m \end{bmatrix}$, $\bar{A} = \begin{bmatrix} A & B \\ 0 & A_u \end{bmatrix} \in \mathbb{R}^{(n+m)\times(n+m)}$ and the state of the original DAE is: $x(t) = [I_n \ \ 0]\bar{x}(t)$.

Similar to the original DAE system, the autonomous DAE system (6) can be decoupled to form one autonomous ODE subsystem and one or several AC subsystems. It should be noted that the autonomous DAE system has the same index as the original one.

We have discussed the conversion of a DAE system with user-defined input to an autonomous DAE system. Next, we derive the *consistent space* for the initial condition of an autonomous DAE system. All previous results apply to these systems given that $u(t) = 0$.

Definition 8 (Consistent Space for an autonomous DAE system). *Consider an autonomous DAE system (Δ) defined in Equation (1) by letting $u(t) = 0$. From this, we define in the following a "consistent matrix" Γ as:*

$$\textit{Index-1 } \Delta: \ \Gamma = Q_0 - N_2P_0, \ (Q_0, P_0, N_2) \textit{are defined in Lemma 1},$$

$$\textit{Index-2 } \Delta: \ \Gamma = \begin{bmatrix} P_0Q_1 - N_2P_0P_1 \\ Q_0 - (N_3 + L_3N_2N_1)P_0P_1 \end{bmatrix},$$
$$(Q_i, P_i, N_i, L_i) \textit{are defined in Lemma 2},$$

$$\textit{Index-3 } \Delta: \ \Gamma = \begin{bmatrix} P_0P_1Q_2 - N_2P_0P_1P_2 \\ P_0Q_1 - (N_3 + L_3N_2N_1)P_0P_1P_2 \\ Q_0 - [N_4 + L_4(N_3N_1 + L_3N_2N_1^2) + Z_4N_2N_1]P_0P_1P_2 \end{bmatrix},$$
$$(Q_i, P_i, N_i, L_i, Z_4) \textit{are defined in Lemma 3},$$

then, $Ker(\Gamma)$ is the consistent space of the system Δ, where $Ker(\Gamma)$ denotes the null space of the matrix Γ.

An initial state x_0 is consistent if it is in the consistent space, i.e., $\Gamma x_0 = 0$. The consistent matrix and consistent space is introduced because it is useful and convenient for checking the consistency of an initial set of states represented using a star set. For example, assume that the initial set of states is defined by $\Theta(0) = \langle V(0), P \rangle$, then this set is consistent for all α satisfying the predicate P if $\Gamma V(0) = 0$. This means that we require consistency for all points in the initial set. With a consistent initial set of states, we investigate the reachable set computation and safety verification/falsification of an autonomous DAE system in the next section.

5 Reachability Analysis

5.1 Reachable Set Computation

The reachable set of an autonomous DAE system is constructed by combining the reachable set of all of its decoupled subsystems. The reachable set of all AC subsystems can be derived from the reachable set of the ODE subsystem, which can be computed efficiently using existing ODE solvers. We first discuss the reachable set computation of the ODE subsystem by exploiting its *superposition property*. Then, the reachable set of the autonomous DAE system is constructed conveniently using only matrix addition and multiplication.

Let $\Theta(0) = \langle V(0), P \rangle$ be the initial set of states of an autonomous DAE system defined in (1) by letting $u(t) = 0$. Assume that the initial set of states, $X(0)$, satisfies the consistent condition. After decoupling, the initial set of states of the ODE subsystem $\Theta_1(0)$ is obtained as follows: $\Theta_1(0) = \langle V_1(0), P \rangle$ where $V_1(0) = (\prod_{i=0}^{\mu-1} P_0 \cdots P_{\mu-1})V(0) = [v_1^1(0) \ v_2^1(0) \ \cdots \ v_k^1(0)]$, μ is the index of the DAE system, and $P_i, (i = 0, \cdots, \mu - 1)$, are defined in Lemma 1 or 2 or 3 corresponding to the index μ.

Then, for any $x_1(0) \in \Theta_1(0)$, we have $x_1(0) = \Sigma_{i=1}^{k} \alpha_i v_i^1(0)$. The solution of the ODE subsystem at time t is given by: $x_1(t) = \Sigma_{i=1}^{k} \alpha_i v_i^1(t) = V_1(t)\alpha$, where $v_i^1(t) = e^{N_1 t} v_i^1(0)$ and $V_1(t) = [v_1^1(t) \ v_2^1(t) \ \cdots \ v_k^1(t)]$. Therefore, the reachable set of the ODE subsystem at anytime t is also a star set defined by $\Theta_1(t) = V_1(t)\alpha$.

Using existing ode solvers, we can construct the matrix $V_1(t)$ at anytime t. From $\Theta_1(t)$, the reachable set of the autonomous DAE system can be obtained using the following Lemma.

Lemma 6 (Reachable Set Construction). *Given an autonomous DAE system defined in Equation (1) where $u(t) = 0$ and a consistent initial set of states $\Theta(0) = \langle V(0), P\rangle$, let $\Theta_1(t) = \langle V_1(t), P\rangle$ be the reachable set at time t of the corresponding ODE subsystem after decoupling. Then, the reachable set $\Theta(t)$ at time t of the system is given by $\Theta(t) = \langle V(t) = \Psi V_1(t), P\rangle$, where Ψ is a "reachable set projector" defined below.*

$$
\begin{aligned}
&\textit{Index-1}: \ \Psi = (I_n + N_2), \ N_2 \textit{ is defined in Lemma 1},\\
&\textit{Index-2}: \ \Psi = (I_n + N_2 + N_3 + L_3N_2N_1),\\
&\qquad\qquad (N_{i=1,2,3}, L_3) \textit{ are defined in Lemma 2},\\
&\textit{Index-3}: \ \Psi = (I_n + N_2 + N_3 + N_4 + L_3N_2N_1 +\\
&\qquad\qquad\qquad L_4N_3N_1 + L_4L_3N_2N_1^2 + Z_4N_2N_1),\\
&\qquad (N_{i=1,2,3,4}, L_{i=3,4}, Z_4) \textit{ are defined in Lemma 3}.
\end{aligned}
\tag{7}
$$

Proof is given in Appendix D.1.

The reachable set construction of an autonomous DAE system is summarized in Algorithm A.2. Next, from the constructed reachable set, we discuss how to verify or falsify the safety property.

5.2 Safety Verification and Falsification

By utilizing the star set to represent the reachable set of a DAE system, the safety verification and falsification problem is solved in the following manner. Let $Unsafe(\Delta) \triangleq Gx \leq f$ be the unsafe set of an autonomous DAE system and assume that we want to check the safety of the system at the time step $t_j = jh$. This is equivalent to checking $GV(jh)\alpha \leq f$ subject to $P(\alpha) \triangleq C\alpha \leq d$, where $V(jh)$ is the basic matrix of the reachable set $\Theta(jh)$ of the system at time jh computed using the reachable set construction algorithm in Algorithm A.2. Combining these constraints, the problem changes to checking the feasibility of the following linear predicate: $\bar{P} \triangleq \bar{G}\alpha \leq \bar{f}$, where $\bar{G} = [(GV(jh))^T \ \ C^T]^T$ and $\bar{f} = [f^T \ \ d^T]^T$. This can be solved efficiently using existing linear programming algorithms. The verification and falsification algorithm in Algorithm A.3 in the appendix summarizes the steps of verifying or falsifying the safety property of an autonomous DAE system. In the next section, we evaluate our approach using a set of DAE benchmarks with several thousand states.

6 Experimental Results

In this section, we first demonstrate the effectiveness and scalability of our approach via the verification results for several DAE benchmarks [29]. Then, we analyze the time performance of our approach using the index-2, two-dimensional

semi-discretized Stokes Equation benchmark [27]. It is worthy of noting that our reachability analysis approach for high-index DAEs is extensible and generic, in the sense that we can combine a decoupling method with other ODE reachability analysis tools such as SpaceEx and Flow*. The verification results of all benchmarks using such combinations with SpaceEx are presented in Appendix B , which demonstrates the limitations in both timing and scalability performances. Our approach based on the combination of a decoupling method and a reachable set computation using star-set is implemented in a tool called *Daev*[3] using Python and its standard packages numpy, scipy, and mathplotlib. All experiments were done on a computer with the following configuration: Intel Core i7-6700 CPU @ 3.4GHz 8 Processor, 62.8 GiB Memory, 64-bit Ubuntu 16.04.3 LTS OS.

6.1 Scalability Performance

Table 1 presents the verification results for all high-index DAE system benchmarks using Daev. From the table, we can see that Daev is scalable in verifying large DAE systems with thousands of state variables where the over-approximation approach is not applicable. Moreover, our approach can produce an unsafe trace in the case that a DAE system violates its safety property. An example of unsafe traces of the index-2, interconnected rotating masses system [30] is shown in Figure 2(a) in Appendix E. Therefore, our approach is practically useful for falsification of large, linear DAE systems.

6.2 Timing Performance

Next, we investigate the time performance of our approach through the reachability analysis of the index-2, two-dimensional semi-discretized Stokes Equation benchmark.

Example 1 (Semi-discretized Stokes Equation [27]). This example studies the safety of a Stokes equation that describes the flow of an incompressible fluid in a two-dimensional spatial domain Ω. The mathematical description of the Stokes-equation is given in Appendix F. An index-2 DAE system is derived from the Stokes-equation by discretizing the domain Ω by a number of uniform square cells. Let n be the number of discretized segments of the domain on the x- or y-axes, then the dimension of the DAE system is $3n^2 + 2n$. Additionally, we are interested in the velocity along the x- and y- axes, $v_x^c(t)$ and $v_y^c(t)$, of the fluid in the *central cell* of the domain Ω. The unsafe set of the system is defined: $Unsafe \triangleq -v_x^c(t) - v_y^c(t) \leq 0.04$. By increasing the number of cells used to discretize the domain Ω, we can produce an index-2 DAE system with arbitrarily large dimension. We evaluate the time performance of our approach via three scenarios. First, we discuss how the times for decoupling, reachable set computation, and safety checking are affected by changes in the system dimension.

[3] https://github.com/verivital/daev/releases/tag/formats2019

Table 1. Verification results for all benchmarks using Daev.

Benchmarks	n	Index	Unsafe Set	Result	V-T(s)
RL network [24]	3	2	$x_1 \leq -0.2 \wedge x_2 \leq -0.1$	unsafe	0.184
			$x_1 \geq 0.2$	safe	0.44
RLC circuit [12]	4	1	$x_1 + x_3 \geq 0.2$	unsafe	0.224
			$x_4 \leq -0.3$	safe	1.37
Interconnected rotating mass [30]	4	2	$x_3 \leq -0.9$	unsafe	0.37
			$x_4 \leq -1.0$	safe	0.114
Generator [20]	9	3	$x_9 \geq 0.01$	unsafe	0.4
			$x_1 \geq 1.0$	safe	0.684
Damped-mass spring [27]	11	3	$x_3 \leq 1 \wedge x_8 \leq 1.5$	safe	1.06
			$x_8 \leq -0.2$	unsafe	1.08
PEEC [9]	480	2	$x_{478} \geq 0.05$	safe	28.84
			$x_{478} \geq 0.01$	unsafe	28.25
MNA-1 [9]	578	2	$x_1 \geq -0.001$	safe	192.7
			$x_1 \geq -0.0015$	unsafe	202.6
MNA-4 [9]	980	3	$x_2 \geq 0.0005$	safe	1858.4
			$x_2 \geq 0.0002$	unsafe	1836.04
Stokes-equation [27]	4880	2	$v_x^c + v_y^c \leq -0.04$	unsafe	3502.3
			$v_x^c \geq 0.2$	safe	3532.3

Second, we analyze the reachable set computation time along with the *width* of the basic matrix of the initial set $V(0)$, i.e., the number of the initial basic vectors. Finally, because the reachable set of the system is constructed from the reachable set of its corresponding ODE subsystem, which is computed using ODE solvers as shown in the reachable set construction algorithm in Algorithm A.2, we investigate the time performance of reachable set computation using different ODE solving schemes. Table 2 presents the verification time, *V-T*, for the Stokes-equation benchmark with different dimensions. The verification time is broken into three components measured in seconds: decoupling time *D-T*, reachable set computation time *RSC-T*, and checking safety time *CS-T*. Table 2 shows the decoupling and reachable set computation times dominate the time for verification process. In addition, these times increase as the system size grows.

Table 2. Verification time of Stokes-equation with different dimensions n.

n	86	321	706	1241	1926	2761
D-T	$0.012s$	$0.63s$	$6.32s$	$40.38s$	$155.32s$	$466.38s$
RSC-T	$0.019s$	$0.37s$	$2.98s$	$19.29s$	$68.15s$	$200.89s$
CS-T	$0.0017s$	$0.0014s$	$0.0015s$	$0.0017s$	$0.0018s$	$0.002s$
V-T	$0.0327s$	$1.0014s$	$9.3015s$	$59.6717s$	$223.4718s$	$667.272s$

Table 3. Reachable set computation time of Stokes-equation of dimensions $n = 321$ with different number of initial basic vectors k.

k	2	4	6	8	10	12	14
RSC-T	$1.9s$	$3.41s$	$5.01s$	$6.71s$	$8.3s$	$9.9s$	$11.44s$

The time for checking safety is almost unchanged and very small. This happens because the size of the feasibility problem $\bar{P}$ defined in the verification/falsification algorithm in Algorithm A.3 is unchanged and usually small when we only check the safety in some specific directions defined by the unsafe matrix G in the algorithm.

Since the reachable set the Stokes-equation benchmark is constructed by simulating its corresponding ODE subsystem with each initial vector of its initial basic matrix, the time for computing the reachable set of the Stokes-equation depends linearly on the number of the initial basic vectors k. Table 3 shows the reachable set computation time, $RSC-T$, for the Stokes-equation of dimension $n = 321$ versus the number of the initial basic vectors k.

Our approach relies on existing ODE solvers. Therefore, it is interesting to consider how the reachable set computation time performs with different existing ODE solving schemes supported by the *scipy* package such as *vode*, *zvode*, *lsoda*, *dopri5* and *dop853*. All solvers are used with the absolute tolerance $atol = 1e\text{-}12$ and the relative tolerance $rtol = 1e\text{-}08$. Figure 1 illustrates the time performance of different schemes and indicates that the *vode*, *dopri5*, and *dop853* are fast schemes that should be used for large DAE systems. In addition, we should avoid using the *lsoda* and *zvode* schemes for large DAE systems due to theirs slow performance.

7 Conclusion and Future Work

We have studied a simulation-based reachability analysis for high-index, linear DAE systems. The experiential results show that our approach can deal with DAE systems with up to thousands of state variables. Therefore, it is useful and applicable to verify or falsify safety-critical CPS involving DAE dynamics.

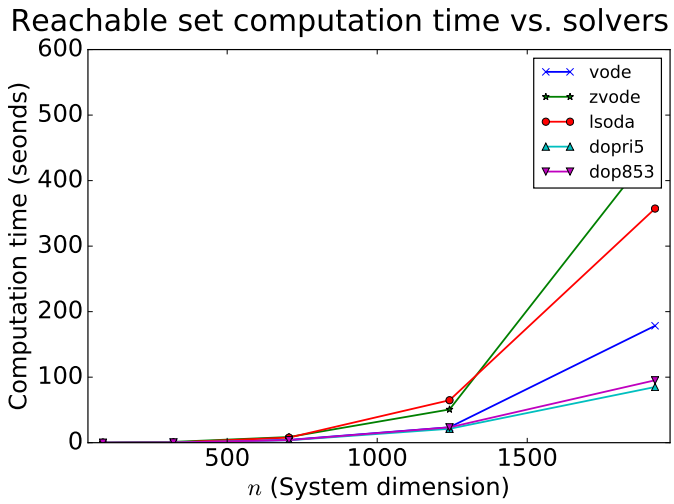


Fig. 1. Reachable set computation time of Stokes-equation using different ode solvers

Additionally, the decoupling and the consistency checking techniques used in our approach can be used as a transformation pass for existing over-approximation techniques [2, 19] to verify the safety of DAE systems with small and medium dimension.

The reachability analysis for DAE systems with millions of dimensions remains challenging, although recent symbolic state-space representations, such as star sets, that allow for analyzing very large ODEs may also prove pivotal for DAEs [6]. The verification time of our approach depends mostly on the decoupling and the reachable set computation times. Therefore, to enhance the time performance and the scalability of our approach to make it work for million-dimensional DAE systems, both decoupling and reachable set computation techniques need to be improved. A promising application that inspires seeking a such scalable approach is verification and falsification of very large circuits, such as those that may arise in analog/mixed signal (AMS) designs, which are described as high-index DAEs. Transformations from standard circuit languages such as Verilog-AMS or VHDL-AMS to representations as hybrid automata may enable such analyses [3, 4].

Acknowledgments

The material presented in this paper is based upon work supported by the National Science Foundation (NSF) under grant numbers CNS 1464311, CNS 1713253, SHF 1527398, and SHF 1736323, the Air Force Office of Scientific Research (AFOSR) through contract numbers FA9550-15-1-0258, FA9550-16-1-0246, and FA9550-18-1-0122. The U.S. government is authorized to reproduce

and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of AFOSR or NSF.

References

1. Althoff, M., Krogh, B.: Reachability analysis of nonlinear differential-algebraic systems. Automatic Control, IEEE Transactions on **59**(2), 371–383 (2014). https://doi.org/10.1109/TAC.2013.2285751
2. Althoff, M.: An introduction to cora 2015. In: Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems (2015)
3. Bak, S., Beg, O.A., Bogomolov, S., Johnson, T.T., Nguyen, L.V., Schilling, C.: Hybrid automata: from verification to implementation. International Journal on Software Tools for Technology Transfer **21**(1), 87–104 (Feb 2019). https://doi.org/10.1007/s10009-017-0458-1
4. Bak, S., Bogomolov, S., Johnson, T.T.: Hyst: a source transformation and translation tool for hybrid automaton models. In: Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control. pp. 128–133. ACM (2015)
5. Bak, S., Duggirala, P.S.: Simulation-equivalent reachability of large linear systems with inputs. In: International Conference on Computer Aided Verification. pp. 401–420. Springer (2017)
6. Bak, S., Tran, H.D., Johnson, T.T.: Numerical verification of affine systems with up to a billion dimensions. In: Proceedings of the 22Nd ACM International Conference on Hybrid Systems: Computation and Control. pp. 23–32. HSCC '19, ACM, New York, NY, USA (2019). https://doi.org/10.1145/3302504.3311792
7. Banagaaya, N., Alì, G., Schilders, W.H.: Index-aware model order reduction methods. Springer (2016)
8. Byrne, G., Ponzi, P.: Differential-algebraic systems, their applications and solutions. Computers & chemical engineering **12**(5), 377–382 (1988)
9. Chahlaoui, Y., Van Dooren, P.: A collection of benchmark examples for model reduction of linear time invariant dynamical systems. (2002)
10. Chen, X., Ábrahám, E., Sankaranarayanan, S.: Flow*: An analyzer for non-linear hybrid systems. In: International Conference on Computer Aided Verification. pp. 258–263. Springer (2013)
11. Cross, E.A., Mitchell, I.M.: Level set methods for computing reachable sets of systems with differential algebraic equation dynamics. In: American Control Conference, 2008. pp. 2260–2265. IEEE (2008)
12. Dai, L.: Singular control systems (lecture notes in control and information sciences) (1989)
13. Dang, T., Donzé, A., Maler, O.: Verification of analog and mixed-signal circuits using hybrid system techniques. In: International Conference on Formal Methods in Computer-Aided Design. pp. 21–36. Springer (2004)
14. Duan, G.R.: Analysis and design of descriptor linear systems, vol. 23. Springer Science & Business Media (2010)
15. Duggirala, P.S., Mitra, S., Viswanathan, M., Potok, M.: C2e2: a verification tool for stateflow models. In: International Conference on Tools and Algorithms for the Construction and Analysis of Systems. pp. 68–82. Springer (2015)

16. Duggirala, P.S., Viswanathan, M.: Parsimonious, simulation based verification of linear systems. In: International Conference on Computer Aided Verification. pp. 477–494. Springer (2016)
17. Eich-Soellner, E., Führer, C.: Numerical methods in multibody dynamics, vol. 45. Springer (1998)
18. Fan, C., Qi, B., Mitra, S., Viswanathan, M., Duggirala, P.S.: Automatic reachability analysis for nonlinear hybrid models with c2e2. In: International Conference on Computer Aided Verification. pp. 531–538. Springer (2016)
19. Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: Spaceex: Scalable verification of hybrid systems. In: Computer Aided Verification. pp. 379–395. Springer (2011)
20. Gerdin, M.: Parameter estimation in linear descriptor systems. Citeseer (2004)
21. Girard, A.: Reachability of uncertain linear systems using zonotopes. In: Hybrid Systems: Computation and Control, pp. 291–305. Springer (2005)
22. Guernic, C.L., Girard, A.: Reachability analysis of linear systems using support functions. Nonlinear Analysis: Hybrid Systems **4**(2), 250–262 (2010). https://doi.org/10.1016/j.nahs.2009.03.002
23. Han, Z., Krogh, B.H.: Reachability analysis of large-scale affine systems using low-dimensional polytopes. In: Hybrid Systems: Computation and Control, pp. 287–301. Springer (2006)
24. Ho, C.W., Ruehli, A., Brennan, P.: The modified nodal approach to network analysis. IEEE Transactions on circuits and systems **22**(6), 504–509 (1975)
25. Kong, S., Gao, S., Chen, W., Clarke, E.: dreach: δ-reachability analysis for hybrid systems pp. 200–205 (2015)
26. März, R.: Canonical projectors for linear differential algebraic equations. Computers & Mathematics with Applications **31**(4-5), 121–135 (1996)
27. Mehrmann, V., Stykel, T.: Balanced truncation model reduction for large-scale systems in descriptor form. In: Dimension Reduction of Large-Scale Systems, pp. 83–115. Springer (2005)
28. Mitchell, I.M., Susuki, Y.: Level set methods for computing reachable sets of hybrid systems with differential algebraic equation dynamics. In: International Workshop on Hybrid Systems: Computation and Control. pp. 630–633. Springer (2008)
29. Musau, P., Lopez, D.M., Tran, H.D., Johnson, T.T.: Linear differential-algebraic equations (benchmark proposal). EPiC Series in Computing **54**, 174–184 (2018)
30. Schon, T., Gerdin, M., Glad, T., Gustafsson, F.: A modeling and filtering framework for linear differential-algebraic equations. In: Decision and Control, 2003. Proceedings. 42nd IEEE Conference on. vol. 1, pp. 892–897. IEEE (2003)
31. Tran, H.D., Bao, T., Johnson, T.T.: Discrete-space analysis of partial differential equations. EPiC Series in Computing **54**, 185–195 (2018)
32. Tran, H.D., Nguyen, L.V., Johnson, T.T.: Large-scale linear systems from order-reduction (benchmark proposal). In: 3rd Applied Verification for Continuous and Hybrid Systems Workshop (ARCH), Vienna, Austria (2016)
33. Tran, H.D., Nguyen, L.V., Xiang, W., Johnson, T.T.: Order-reduction abstractions for safety verification of high-dimensional linear systems. Discrete Event Dynamic Systems **27**(2), 443–461 (2017)
34. Tran, H.D., Xiang, W., Bak, S., Johnson, T.T.: Reachability analysis for one dimensional linear parabolic equations. IFAC-PapersOnLine **51**(16), 133–138 (2018)

A Algorithms

A.1 Admissible Projectors Construction Algorithm

Algorithm A.1 Admissible Projectors Construction

Input: (E, A) % matrices of a DAE system
Output: admissible projectors

procedure INITIALIZATION
  projectors = [ ] % a list of projectors
  $E_0 = E,\ A_0 = A$ and $n =$ *number of state variables*
procedure CONSTRUCTION OF ADMISSIBLE PROJECTORS
  if *rank(E_0)* == n:
    exit() % E is nonsingular, thus, the DAE is equivalent to an ODE.
  else:
    $Q_0 =$ *orthogonal_projector_on_Ker(E_0)*, $P_0 = I_n - Q_0$, $E_1 = E_0 - A_0Q_0$
    if *rank(E_1)* == n:
      projectors $\leftarrow Q_0$ % the DAE has index-1
    else:
      $Q_1 =$ *orthogonal_projector_on_Ker(E_1)*, $P_1 = I_n - Q_1$
      $A_1 = A_0P_0,\ E_2 = E_1 - A_1Q_1$
      if *rank(E_2)* == n:
        $Q_1^* = -Q_1E_2^{-1}A_1$
        projectors $\leftarrow (Q_0,\ Q_1^*)$ % the DAE has index-2
      else:
        $Q_2 =$ *orthogonal_projector_on_Ker(E_2)*, $P_2 = I_n - Q_2$
        $A_2 = A_1P_1,\ E_3 = E_2 - A_2Q_2$
        if *rank(E_3)* == n:
          $Q_2' = Q_2E_3^{-1}A_2,\ \ P_2' = I_n - Q_2',\ \ Q_1' = Q_1P_2'E_3^{-1}A_1$
          $E_2' = E_1 - A_1Q_1',\ P_1' = I_n - Q_1',\ \ A_2' = A_1P_1'$
          $Q_2'' =$ *orthogonal_projector_on_Ker(E_2')*, $P_2'' = I_n - Q_2''$
          $E_3'' = E_2' - A_2'Q_2'',\ Q_2^* = -Q_2''(E_3'')^{-1}A_2'$
          projectors $\leftarrow (Q_0,\ Q_1', Q_2^*)$ % the DAE has index-3
        else:
          exit() % the DAE has index lager than 3
  return projectors

A.2 Reachable Set Construction Algorithm

A.3 Bounded-time Safety Verification/falsification Algorithm

B Verification Results using deSpex

In this section, we shows that our reachability analysis approach for high-index DAEs based on combining the decoupling technique and existing ODE reachability analysis is extensible and generic. We will present the result of using the

Algorithm A.2 Reachable set computation

Inputs: Matrices of an autonomous DAE system (E, A), initial set of states $\Theta(0) = \langle V(0), P\rangle$, time step h, number of steps N.
Output: Reachable set % A list of stars

procedure INITIALIZATION
  $ListOfStars = [\,]$
  Decoupling the system (Section 3)
  Obtain consistent space $Ker(\Gamma)$ (Definition 8)
  If $V(0) \notin Ker(\Gamma)$: exit() % inconsistent initial set of states
  Else: Obtain initial set of states for ODE subsystem:
    $\Theta_1(0) = \langle V_1(0), P\rangle$, $V_1(0) = [v_1^1(0) \ \cdots \ v_k^1(0)]$
procedure REACHABLE SET CONSTRUCTION
  for $j = 0, 1, 2, \cdots, N$:
    for $i = 1, 2, \cdots, k$:
      Compute $v_i^1(jh) = e^{N_1 jh} v_i^1(0)$ % using ODE solvers
    Construct $V_1(jh) = [v_1^1(jh) \ v_2^1(jh) \ \cdots \ v_k^1(jh)]$
    Compute $V(jh)$ from $V_1(jh)$ using Lemma 6
    Construct $\Theta(jh) = \langle V(jh), P\rangle$
    $ListOfStars \leftarrow \Theta(jh)$
  return $ListOfStars$

Algorithm A.3 Bounded-time safety verification/falsification

Inputs: $Reachable\_Set$ % a list of stars; $Unsafe(\Delta) \triangleq Gx \le f$ % the unsafe set
Output: $Safe/Unsafe$ and $Unsafe\_Trace$

procedure INITIALIZATION
  N = number of stars in the reachable set
  $Status = Safe$
  $Unsafe\_Trace = [\,]$
procedure VERIFICATION/FALSIFICATION
  for $j = 1, 2, \cdots, N$:
    $\Theta_j = Reachable\_Set[j] = \langle V_j, P\rangle$, $P \triangleq C\alpha \le d$
    Construct $\bar{P} \triangleq \begin{bmatrix} GV_j \\ C \end{bmatrix} \alpha \le \begin{bmatrix} f \\ d \end{bmatrix}$
    If $\bar{P}$ is feasible:
      $Status = Unsafe$, get $\alpha_{feasible}$, exit()
  If $Status = Unsafe$:
    for $j = 1, 2, \cdots, N$:
      Compute $x_j = V_j \alpha_{feasible}$
      $Unsafe\_Trace \leftarrow x_j$
  return $Status$, $Unsafe\_Trace$

Table 4. Verification results for all benchmarks using deSpex.

Benchmarks	n	Index	Unsafe Set	Result	V-T(s)
RL network [24]	3	2	$x_1 \leq -0.2 \wedge x_2 \leq -0.1$	unsafe	2.002
			$x_1 \geq 0.2$	safe	0.502
RLC circuit [12]	4	1	$x_1 + x_3 \geq 0.2$	unsafe	2.902
			$x_4 \leq -0.3$	safe	3.01
Interconnected rotating mass [30]	4	2	$x_3 \leq -0.9$	safe	0.802
			$x_4 \leq -1.0$	unsafe	1.02
Generator [20]	9	3	$x_9 \geq 0.01$	unsafe	10.02
			$x_1 \geq 1.0$	safe	1.602
Damped-mass spring [27]	11	3	$x_3 \leq 1 \wedge x_8 \leq 1.5$	safe	2.31
			$x_8 \leq -0.2$	unsafe	2.81

combination of our decoupling method and SpaceEx, which we call deSpex, to verify DAE systems. Using SpaceEx for DAE systems verification is non-trivial. To do this, we first decouple a DAE and check the consistency condition of the initial set of states and inputs. Then, we construct an automaton with the decoupled ODE subsystem. Finally, the state of the DAE system is declared as a set of invariants of the automaton using the "reachable set projector" Ψ in Lemma 6.

Table 1 shows the verification results of several benchmarks using deSpex. Compared between Table 1 and Table 4, we can see that deSpex cannot produce verification results for large benchmarks such as PEEC, MNA-1, MNA-4, and Stokes-equation[4], which can be done by Daev using star-set computation. Besides, Daev and deSpex provide the same verification results for other benchmarks.

C Proofs for Section 3

Before going forward, we present some useful properties of the matrix chain defined in Equation (2) and the admissible projectors in Definition 3 that are used in the decoupling process.

[4] SpaceEx cannot parse the large model files of PEEC, MNA-1, MNA-4, and Stokes-equation benchmarks

Proposition 2 (Matrix chain properties). *The matrix chain defined in Equation (2) has the following properties:*

$$\begin{aligned} &E_{j+1}P_j = E_j,\ E_{j+1}Q_j = -A_jQ_j,\ j = 0, 1, \cdots, \mu-1, \\ &A_\mu = A_0 + E_1Q_0 + E_2Q_1 + \cdots + E_\mu Q_{\mu-1} \\ &\quad = A_0 + E_\mu(P_{\mu-1}\cdots P_1Q_0 + P_{\mu-2}\cdots P_2Q_1 + \cdots + Q_{\mu-1}). \end{aligned} \tag{8}$$

Proof. From the definition of the matrix chain, we have: $E_{j+1}P_j = E_jP_j - A_jQ_jP_j = E_j(I_n - Q_j) = E_j$ and $E_{j+1}Q_j = E_iQ_i - A_iQ_i^2 = -A_iQ_i$.

From the definition and the first property, we have $A_{j+1} = A_jP_j = A_j(I_n - Q_j) = A_j + E_{j+1}Q_j$. Therefore, $A_\mu = A_{\mu-1} + E_\mu Q_{\mu-1} = \cdots = A_0 + E_1Q_0 + E_2Q_1 + \cdots + E_\mu Q_{\mu-1}$. Further applying $E_{j+1}P_j = E_j$ completes the proof.

Proposition 3 (Admissible projectors properties). *The admissible projectors defined in Definition 3 have the following properties:*

$$P_jQ_i = Q_i,\ Q_jP_i = Q_j,\ P_iP_jP_i = P_iP_j,\ P_jP_iP_j = P_iP_j,\ \forall j > i. \tag{9}$$

Proof. From the definition of admissible projectors, we have: $P_jQ_i = (I_n - Q_j)Q_i = Q_i$, $Q_jP_i = Q_j(I_n - Q_i) = Q_j$, $P_iP_jP_i = P_iP_j(I_n - Q_i) = P_iP_j - P_iP_jQ_i = P_iP_j - P_iQ_i = P_iP_j$ since $P_iQ_i = 0, P_jQ_i = Q_i$. In addition, $P_jP_iP_j = (I_n - Q_j)P_iP_j = (P_i - Q_jP_i)P_j = (P_i - Q_j)P_j = P_iP_j - Q_jP_j = P_iP_j$ since $Q_jP_i = Q_j$ and $Q_jP_j = 0$.

C.1 Proof for Lemma 1

Proof. Using the matrix chain defined in Equation (2) and Proposition 2, we have: $E_0\dot{x}(t) = A_0x(t) + Bu(t) \to E_1P_0\dot{x}(t) = (A_1 - E_1Q_0)x(t) + Bu(t)$. Since the system is index-1, E_1 is non-singular. Therefore, we have:

$$P_0\dot{x}(t) + Q_0x(t) = E_1^{-1}[A_1x(t) + Bu(t)]. \tag{10}$$

By left multiplying Equation (10) by P_0 and Q_0 and using the fact that $A_1x(t) = A_1(P_0 + Q_0)x(t) = A_0P_0(P_0 + Q_0)x(t) = A_0P_0x(t)$, the index-1 DAE system can be decoupled by:

$$\begin{aligned} \dot{x}_1(t) &= N_1x_1(t) + M_1u(t), \\ x_2(t) &= N_2x_1(t) + M_2u(t), \\ x(t) &= x_1(t) + x_2(t), \end{aligned}$$

where $x_1(t) = P_0x(t)$, $N_1 = P_0E_1^{-1}A_0$, $M_1 = P_0E_1^{-1}B$; and $x_2(t) = Q_0x(t)$, $N_2 = Q_0E_1^{-1}A_0$, $M_2 = Q_0E_1^{-1}B$. This completes the proof.

C.2 Proof for Lemma 2

Proof. Similar to the index-1 DAE case, using the matrix chain and Proposition 2 we have: $E_2P_1P_0\dot{x}(t) = [A_2 - E_2(P_1Q_0 + Q_1)]x(t) + Bu(t)$. Further assume

that Q_0, Q_1 are admissible projectors, then using Proposition 3 and the fact that E_2 is nonsingular we have:

$$P_1P_0\dot{x}(t) + Q_0x(t) + Q_1x(t) = E_2^{-1}A_2x(t) + E_2^{-1}Bu(t). \tag{11}$$

Left multiplying Equation (11) by P_0P_1 leads to:

$$P_0P_1^2P_0\dot{x}(t) + P_0P_1Q_0x(t) + P_0P_1Q_1x(t) = P_0P_1E_2^{-1}[A_2x(t) + Bu(t)].$$

From Proposition 3, we have: $P_0P_1^2P_0 = P_0P_1P_0 = P_0P_1$, $P_0P_1Q_0 = P_0Q_0 = 0$, $P_0P_1Q_1 = 0$. In addition, $A_2x(t) = A_2[P_0P_1 + P_0Q_1 + Q_0]x(t) = A_2P_0P_1x(t)$ because $A_2P_0Q_1 = A_1P_1P_0Q_1 = A_0P_0P_1P_0Q_1 = A_0P_0P_1Q_1 = 0$ and $A_2Q_0 = A_1P_1Q_0 = A_1Q_0 = A_0P_0Q_0 = 0$. By combining these identities, the ODE subsystem can be derived by:

$$\Delta_1: \quad \dot{x}_1(t) = N_1x_1(t) + M_1u(t),$$

where $x_1(t) = P_0P_1x(t)$, $N_1 = P_0P_1E_2^{-1}A_2$ and $M_1 = P_0P_1E_2^{-1}B$.

Left multiplying Equation (11) by P_0Q_1 leads to:

$$P_0Q_1P_1P_0\dot{x}(t) + P_0Q_1Q_0x(t) + P_0Q_1^2x(t) = P_0Q_1E_2^{-1}[A_2x_1(t) + Bu(t)].$$

Due to $P_0Q_1P_1P_0 = 0$, $P_0Q_1Q_0 = 0$ and $P_0Q_1^2 = P_0Q_1$, the first AC subsystem can be derived by:

$$\Delta_2: \quad x_2(t) = N_2x_1(t) + M_2u(t),$$

where $x_2(t) = P_0Q_1x(t)$, $N_2 = P_0Q_1E_2^{-1}A_2$ and $M_2 = P_0Q_1E_2^{-1}B$.

Left multiplying Equation (11) by Q_0P_1 leads to:

$$Q_0P_1^2P_0\dot{x}(t) + Q_0P_1Q_0x(t) + Q_0P_1Q_1x(t) = Q_0P_1E_2^{-1}[A_2x(t) + Bu(t)],$$

Note that $Q_0P_1Q_0 = Q_0^2 = Q_0$, $Q_0P_1Q_1 = 0$ and $Q_0P_1^2P_0\dot{x}(t) = Q_0P_1P_0(P_0P_1 + P_0Q_1 + Q_0)\dot{x}(t) = Q_0P_1P_0Q_1\dot{x}(t) = Q_0[I_n - Q_1]P_0Q_1\dot{x}(t) = -Q_0Q_1P_0Q_1\dot{x}(t) = -Q_0Q_1\dot{x}_2(t)$. Therefore, the second AC subsystem can be derived below:

$$\Delta_3: \quad x_3(t) = N_3x_1(t) + M_3u(t) + L_3\dot{x}_2(t),$$

where $x_3(t) = Q_0x(t)$, $N_3 = Q_0P_1E_2^{-1}A_2$, $M_3 = Q_0P_1E_2^{-1}B$ and $L_3 = Q_0Q_1$.

It is easy to see that $I_n = P_0 + Q_0 = P_0(P_1 + Q_1) + P_0 = P_0P_1 + P_0Q_1 + Q_0$, therefore we have $x(t) = x_1(t) + x_2(t) + x_3(t)$. This completes the proof.

C.3 Proof for Lemma 3

Similar to the index-2 DAE case, using the matrix chain with admissible projectors leads to:

$$E_3P_2P_1P_0\dot{x}(t) = [A_3 - E_3(P_2P_1Q_0 + P_2Q_1 + Q_2)]x(t) + Bu(t),$$

or equivalently,

$$P_2P_1P_0\dot{x}(t) + Q_0x(t) + Q_1x(t) + Q_2x(t) = E_3^{-1}[A_3x(t) + Bu(t)]. \tag{12}$$

By left multiplying Equation (12) by $P_0P_1P_2$ with noticing that $P_0P_1P_2P_2P_1P_0 = P_0P_1P_2P_1P_0 = P_0P_1P_2P_0 = P_0P_1P_2(I_n - Q_0) = P_0P_1P_2$, $P_0P_1P_2Q_0 = P_0P_1Q_0 = P_0Q_0 = 0$, $P_0P_1P_2Q_1 = P_0P_1Q_1 = 0$, $P_0P_1P_2Q_2 = 0$ and $A_3x(t) = A_3(P_0P_1P_2 + Q_0P_1P_2 + Q_1P_2 + Q_2)x(t) = A_3P_0P_1P_2x(t)$, the ODE subsystem of the DAE system can be derived by:

$$\Delta_1 : \quad x_1(t) = N_1x_1(t) + M_1u(t),$$

where $x_1(t) = P_0P_1P_2x(t)$, $N_1 = P_0P_1P_2E_3^{-1}A_3$ and $M_1 = P_0P_1P_2E_3^{-1}B$.

Similarly, by left multiplying Equation (12) by $P_0P_1Q_2$, the first AC subsystem of the DAE system can be derived below:

$$\Delta_2 : \quad x_2(t) = N_2x_1(t) + M_2u(t),$$

where $x_2(t) = P_0P_1Q_2x(t)$, $N_2 = P_0P_1Q_2E_3^{-1}A_3$ and $M_2 = P_0P_1Q_2E_3^{-1}B$.

Left multiplying Equation (12) by $P_0Q_1P_2$ yields:

$$P_0Q_1P_2P_1P_0\dot{x}(t) + P_0Q_1x(t) = P_0Q_1P_2E_3^{-1}[A_3x(t) + Bu(t)],$$

in which: $P_0Q_1P_2P_1P_0\dot{x}(t) = P_0Q_1(I_n - Q_2)P_1P_0\dot{x}(t) = -P_0Q_1Q_2\dot{x}(t) = -P_0Q_1Q_2(P_0P_1P_2 + P_0P_1Q_2)\dot{x}(t) = -P_0Q_1Q_2\dot{x}_2(t)$. Therefore, we have the second AC subsystem as follows.

$$\Delta_3 : \quad x_3(t) = N_3x_1(t) + M_3u(t) + L_3\dot{x}_2(t),$$

where $x_3(t) = P_0Q_1x(t)$, $N_3 = P_0Q_1P_2E_3^{-1}A_3$, $M_3 = P_0Q_1P_2E_3^{-1}B$ and $L_3 = P_0Q_1Q_2$.

Left multiplying Equation (12) by $Q_0P_1P_2$ yields:

$$Q_0P_1P_2^2P_1P_0\dot{x}(t) + Q_0x(t) = Q_0P_1P_2E_3^{-1}[A_3x(t) + Bu(t)],$$

in which: $Q_0P_1P_2^2P_1P_0\dot{x}(t) = Q_0P_1P_2P_0\dot{x}(t) = -(Q_0Q_1 + Q_0P_1Q_2)\dot{x}(t) = -(Q_0Q_1 + Q_0P_1Q_2)(P_0P_1P_2 + P_0P_1Q_2 + P_0Q_1 + Q_0)\dot{x}(t) = -Q_0P_1Q_2\dot{x}_2(t) - Q_0Q_1\dot{x}_3(t)$. Therefore, the last AC subsystem of the DAE system can be derived below:

$$\Delta_4 : \quad x_4(t) = N_4x_1(t) + M_4u(t) + L_4\dot{x}_3(t) + Z_4\dot{x}_2(t),$$

where $x_4(t) = Q_0x(t)$, $N_4 = Q_0P_1P_2E_3^{-1}A_3$, $M_4 = Q_0P_1P_2E_3^{-1}B$, $L_4 = Q_0Q_1$ and $Z_4 = Q_0P_1Q_2$.

It is easy to see that $x(t) = (P_0P_1P_2 + P_0P_1Q_2 + P_0Q_1 + Q_0)x(t) = x_1(t) + x_2(t) + x_3(t) + x_4(t)$. This completes the proof.

C.4 Proof for Proposition 1

Proof. Note that $K = [K_1\ K_2]$ is an unitary matrix, i.e., $KK^T = K^TK = I_n$. Consequently, $K_1^TK_2 = 0$ and $K_2^TK_2 = I_{n-r}$. It is easy to see that $Z = L_1SK_1^T$, so we have $ZQ = 0$. In addition, $Q = Q^T$ and $Q^2 = K_2K_2^TK_2K_2^T = K_2K_2^T = Q$. Therefore, Q is a orthogonal projector on Z. This completes the proof.

C.5 Proof for Lemma 4

Proof. We need to prove that Q_1^* is also a projector on E_1 and $Q_1^*Q_0^* = 0$. We have $Q_1^*Q_1 = -Q_1E_2^{-1}A_1Q_1 = Q_1E_2^{-1}E_2Q_1 = Q_1^2 = Q_1$ since $A_1Q_1 = -E_2Q_1$ (Proposition 2). We also have $Q_1Q_1^* = -Q_1^2E_2^{-1}A_1 = -Q_1E_2^{-1}A_1 = Q_1^*$. Therefore, Q_1^* is also a projector on E_1. In addition, $Q_1^*Q_0^* = -Q_1E_2^{-1}A_0P_0Q_0 = 0$. This completes the proof.

C.6 Proof for Lemma 5

We first need to prove that Q_1^* and Q_2^* are respectively projectors on E_1 and E_2'. Then we prove that Q_0^*, Q_1^* and Q_2^* satisfy admissible conditions. We have $Q_2'Q_2 = Q_2E_3^{-1}E_3Q_2 = Q_2^2 = Q_2$ and $Q_2Q_2' = -Q_2^2E_3^{-1}A_2 = -Q_2E_3^{-1}A_2 = Q_2'$. Thus, Q_2' is a projector on E_2. Consequently, we can check that $P_2'P_2 = (I_n - Q_2')(I_n - Q_2) = P_2'$.

One can see that $Q_2'Q_1 = 0$ due to $A_2Q_1 = A_1P_1Q_1 = 0$, consequently, $P_2'Q_1 = (I_n - Q_2')Q_1 = Q_1$. Therefore, $Q_1'Q_1 = Q_1P_2'E_3^{-1}E_2Q_1 = Q_1P_2'E_3^{-1}E_3P_2Q_1 = Q_1P_2'P_2Q_1$. In addition, we have $P_2'P_2 = P_2'$. Consequently, $Q_1'Q_1 = Q_1^2 = Q_1$. Furthermore, it is easy to see $Q_1Q_1' = Q_1'$. Therefore, Q_1' is a projector on E_1. Similarly, it is easy to check that Q_2^* is also a projector on E_2' since $Q_2^*Q_2'' = Q_2''$ and $Q_2''Q_2^* = Q_2^*$.

Next, we prove that $Q_1^*Q_0^* = 0$, $Q_2^*Q_0^*$ and $Q_2^*Q_1^* = 0$. We have $Q_1^*Q_0^* = -Q_1P_2'E_3^{-1}A_1Q_0 = 0$ due to $A_1Q_0 = A_0P_0Q_0 = 0$; $Q_2^*Q_1^* = 0$ because of $A_2'Q_1' = A_1P_1'Q_1' = 0$; $Q_2^*Q_0^* = 0$ because of $A_2'Q_0 = A_1P_1'Q_0 = A_1Q_0 = A_0P_0Q_0 = 0$ (note that $Q_1'Q_0 = 0 \to P_1'Q_0 = Q_0$). This completes the proof.

D Proof for Section 5

D.1 Proof for Lemma 6

Proof. Let $x_1(t) \in \Theta_1(t)$ is a solution of the ODE subsystem at time t. Then, we have: 1) if the autonomous DAE system is index-1, from Lemma 1, the solution of the DAE system is $x(t) = x_1(t) + x_2(t) = (I_n + N_2)x_2(t)$, consequently, the reachable set of the autonomous DAE system at time t is $\Theta(t) = \langle (I_n + N_2)V_1(t), P\rangle$; 2) if the DAE system is index-2, from Lemma 2, the solution of the DAE system is $x(t) = x_1(t)+x_2(t)+x_3(t) = x_1(t)+N_2x_1(t)+N_3x_1(t)+L_3\dot{x}_2(t) = (I_n + N_2 + N_3 + L_3N_2N_1)x_1(t)$, consequently, the reachable set of the DAE system at time t is $\Theta(t) = \langle (I_n + N_2 + N_3 + L_3N_2N_1)V_1(t), P\rangle$; 3) if the DAE system is index-3, from Lemma 3, the solution of the DAE system is $x(t) = x_1(t) + x_2(t) + x_3(t) + x_4(t) = x_1(t) + N_2x_1(t) + N_3x_1(t) + L_3\dot{x}_2(t) + N_4x_1(t) + L_4\dot{x}_3(t) + Z_4\dot{x}_2(t) = x_1(t) + N_2x_1(t) + N_3x_1(t) + L_3N_2N_1x_1(t) + N_4x_1(t) + L_4[N_3N_1x_1(t) + L_3N_2N_1^2x_1(t)] + Z_4N_2N_1x_1(t) = (I_n + N_2 + N_3 + L_3N_2N_1 + N_4 + L_4N_3N_1 + L_4L_3N_2N_1 + Z_4N_2N_1)x_1(t)$, consequently, the reachable set of the DAE system at time t is: $\Theta(t) = \langle (I_n + N_2 + N_3 + N_4 + L_3N_2N_1 + L_4N_3N_1 + L_4L_3N_2N_1^2 + Z_4N_2N_1)V_1(t), P\rangle$. This completes the proof.

E Safety verification and falsification of the interconnected rotating mass system

Example 2 (Interconnected rotating masses [30]). This is an index-2 DAE system with four state variables $x(t) = [z_1^T(t), z_2^T(t), M_2^T(t), M_3^T(t)]^T$ and two inputs $u(t) = [M_1(t)^T, M_4^T(t)]^T$ where $z_1(t)$ and $z_2(t)$ are the angular velocities of the first and the second masses respectively, and $M_2(t)$ and $M_3(t)$ are the torques on the connection of these two masses. $M_1(t)$ and $M_4(t)$ are the input torques applied to the first and the second masses. The system matrices E, A, and B are described by:

$$E = \begin{bmatrix} J_1 & 0 & 0 & 0 \\ 0 & J_2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 \\ -1 & 1 & 0 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; J_1 = 1, J_2 = 2.$$

We are interested in the angular velocity, $z_1(t)$, and the torque, $M_2(t)$, of the first mass. The unsafe set for the system is defined by: $Unsafe \triangleq M_2(t) \leq -0.9$. The system is controlled by *sine* function inputs defined as follows.

$$\begin{bmatrix} \dot{M}_1(t) \\ \dot{M}_4(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} M_1(t) \\ M_4(t) \end{bmatrix}, u(0) = \begin{bmatrix} M_1(0) \\ M_4(0) \end{bmatrix} \in U.$$

We transform the system with given inputs to an autonomous DAE system as described in Equation (6). A consistent initial set of states $\Theta(0) = \langle V(0), P \rangle$ for the autonomous DAE system is chosen below.

$$V(0) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.513 & 0 \\ -0.513 & 0 \\ -0.616 & 0.447 \\ 0.308 & 0.894 \end{bmatrix}, \; P(\alpha) \triangleq C\alpha \leq d, \; C = \begin{bmatrix} 1 & 0 \\ -1 & 0 \\ 0 & 1 \\ 0 & -1 \end{bmatrix}, \; d = \begin{bmatrix} 0.2 \\ -0.1 \\ 1.2 \\ -1.0 \end{bmatrix}$$

Using Algorithm A.1, we construct admissible projectors Q_0, Q_1 for the autonomous DAE system below.

$$Q_0 = \begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{bmatrix}, \; Q_1 = \begin{bmatrix} \frac{2}{3} & \frac{-2}{3} & 0&0&0&0 \\ \frac{-1}{3} & \frac{1}{3} & 0&0&0&0 \\ \frac{2}{3} & \frac{-1}{3} & 0&0&0&0 \\ \frac{-2}{3} & \frac{2}{3} & 0&0&0&0 \\ 0 & 0 & 0&0&0&0 \\ 0 & 0 & 0&0&0&0 \end{bmatrix}.$$

Using these admissible projectors and Lemma 2, the autonomous DAE system can be decoupled into an equivalent decoupled system with the following matrix coefficients:

$$N_1 = \begin{bmatrix} 0&0&0&0&\frac{1}{3}&\frac{1}{3} \\ 0&0&0&0&\frac{1}{3}&\frac{1}{3} \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&0&-1&0 \end{bmatrix}, \; N_2 = 0, \; N_3 = \begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&\frac{-2}{3}&\frac{1}{3} \\ 0&0&0&0&\frac{2}{3}&\frac{-1}{3} \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{bmatrix}, \; L_3 = \begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ \frac{2}{3}&\frac{-2}{3}&0&0&0&0 \\ \frac{-2}{3}&\frac{2}{3}&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \end{bmatrix}.$$

Using the decoupled system, we verify the safety property of the original DAE system over time up to $T = 10$ seconds using fixed time step $h = 0.01$. In 0.37 second, our approach can show that the system is simulationally unsafe and produces a trace violating the safety property which is depicted in Figure 2(a). Figure 2(b) shows the reachable set of the outputs $z_1(t)$ and $M_2(t)$ of the DAE system.

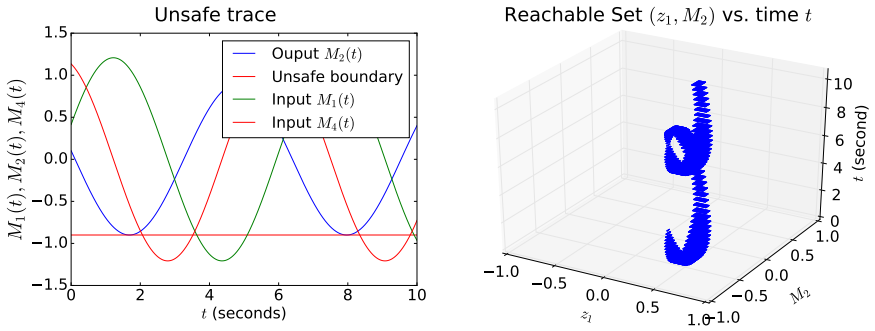
F Mathematical model of the Stokes-equation

The considered Stokes-equation is given as follows.

$$\begin{aligned} &\frac{\partial v}{\partial t} = \Delta v - \nabla \rho + f, \quad \text{in } \Omega \times (0,T), \\ &\nabla v = 0, \quad \text{in } \Omega \times (0,T), \end{aligned} \tag{13}$$

where $v(\zeta,t) \in \mathbb{R}^2$ is the velocity vector, $\rho(\zeta,t) \in \mathbb{E}$ is the pressure, $f(\zeta,t) \in \mathbb{R}^2$ is the vector of external forces, $\Omega = (0,1)^2 \subset \mathbb{R}^2$ is a square domain, T is the endpoint of the time interval, ∇ denotes *the divergence operator* and $\Delta = \nabla^2$.

In this paper, we use Dirichlet boundary condition for the Stokes equation. This condition means that the velocity equals zero on the boundary of the domain. Semi-discretizing the Stokes equation using the well-known MAC scheme



(a) Unsafe trace (b) Reachable set

Fig. 2. Unsafe trace and reachable set of Example 2

[xx] (a scheme leveraging finite element method) leads to an index-2 DAE of the form (1) with the following system matrices:

$$E = \begin{bmatrix} I_{n_v} & 0 \\ 0 & 0 \end{bmatrix}, \; A = \begin{bmatrix} A_{11} & A_{12} \\ A_{12}^T & 0 \end{bmatrix}, \; B = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}, \; x = \begin{bmatrix} v_h \\ \rho_h \end{bmatrix}, \tag{14}$$

where $v_h \in \mathbb{R}^{n_v}$ and $\rho_h \in \mathbb{R}^{n_\rho}$ are the semi-discretized vectors of velocity and pressure, $A_{11} \in \mathbb{R}^{n_v \times n_v}$ is the discrete Laplace operator, $A_{12} \in \mathbb{R}^{n_v \times n_\rho}$ and $A_{12}^T \in \mathbb{R}^{n_\rho \times n_v}$ are the discrete gradient and divergence operators respectively.