

INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

**Generating Invariants for Non-linear Hybrid
Systems**

Rachid Rebiha Arnaldo V. Moura
Nadir Matringe

Technical Report - IC-13-05 - Relatório Técnico

February - 2013 - Fevereiro

The contents of this report are the sole responsibility of the authors.
O conteúdo do presente relatório é de única responsabilidade dos autores.

Generating Invariants for Non-linear Hybrid Systems

Rachid Rebiha* Arnaldo Vieira Moura† Nadir Matringe‡

Abstract

We describe powerful computational techniques, relying on linear algebraic methods, for generating ideals of non-linear invariants of algebraic hybrid systems. We show that the preconditions for discrete transitions and the Lie-derivatives for continuous evolution can be viewed as morphisms, and so can be suitably represented by matrices. We reduce the non-trivial invariant generation problem to the computation of the associated eigenspaces by encoding the new consecution requirements as specific morphisms represented by such matrices. More specifically, our methods are the first to establish very general sufficient conditions that show the existence and allow the computation of invariant ideals. Our methods also embody a strategy to estimate certain degree bounds, leading to the discovery of rich classes of inductive, *i.e.* provable, invariants. By reducing the problem to related linear algebraic manipulations we are able to address various deficiencies of other state-of-the-art invariant generation methods, including the efficient treatment of non-linear hybrid systems. Our approach avoids first-order quantifier elimination, Gröbner basis computation or direct system resolution, thereby circumventing difficulties met by other recent techniques.

1 Introduction

Hybrid systems [1, 2] exhibit both discrete and continuous behaviors, as one often finds when modeling digital system embedded in analog environments. Most safety-critical systems, *e.g.* aircraft, automobiles, chemicals and nuclear power plants and biological systems, operate semantically as non-linear hybrid systems. As such, they can only be adequately modeled by means of non linear arithmetic over the real numbers involving multivariate polynomials and fractional or transcendental functions. The analysis of hybrid systems has been one of the main challenges for the formal verification community for several decades.

An invariant at a location of a system is an assertion true of any reachable state associated to this location. Some verification approaches for treating such models are based on inductive invariant generation methods [3, 4] and also on the Abstract Interpretation framework [5, 6], combined with the reduction of safety-critical properties to invariant properties [7, 8]. We look for invariants that strengthen what we wish to prove, and so allow us

*Instituto de Computação, Universidade Estadual de Campinas, 13081970 Campinas, SP. Pesquisa desenvolvida com suporte financeiro da FAPESP, processo 2011089471

†Instituto de Computação, Universidade Estadual de Campinas, 13081970 Campinas, SP.

‡Université de Poitiers, Laboratoire Mathématiques et Applications and Institut de Mathématiques de Jussieu Université Paris 7-Denis Diderot, France.

to establish the desired properties. Also, they can provide precise over-approximations of the set of reachable states in the continuous state space.

Some more recent approaches to invariant generation have been constraint-based [9, 10, 11, 12, 13]. In these cases, a candidate invariant with a fixed degree and unknown parametric coefficients, *i.e.*, a template form, is proposed as the target invariant to be generated. The conditions for invariance are then encoded, resulting in constraints on the unknown coefficients whose solutions yield invariants. One of the main advantage of such constraint-based approaches is that they are goal-oriented. But, on the other hand, they still require the computation of several Gröbner Bases [14] or require first-order quantifier elimination [15, 16]. And known algorithms for those problems are, at least, of double exponential complexity. Alternatively, SAT Modulo Theory decision procedures and polynomial systems [17, 18, 10] could also, eventually, lead to decision procedures for linear theories and, thus, to decidable systems. evolution modes. Nonetheless, despite significant progress over the years [9, 19, 20, 10, 12, 21, 22, 23, 24, 17, 13, 25], the problem of invariant generation for hybrid systems remains very challenging for both non-linear discrete systems as well as non-linear differential systems with non abstracted local and initial conditions.

In this work we use hybrid automata as computational models for hybrid systems. A hybrid automaton describes the interaction between discrete transitions and continuous dynamics, the latter being governed by local differential equations. We present new methods for the automatic generation of non-linear invariants for non-linear hybrid systems. These methods give rise to more efficient algorithms, with much lower time and space complexities.

First, we extend and generalize our previous work on invariant generation for hybrid systems [26, 27, 28, 29]. To do so, we provide methods to generate non trivial basis of provable invariants for local continuous evolution modes described by non linear differential rules. These invariants can provide precise over-approximations of the set of reachable states in the continuous state space. As a consequence, they can determine which discrete transitions are possible and can also verify if a given property is fulfilled or not. Next, in order to generate invariants for hybrid systems, we complete and extend our previous work on non linear invariant generation for discrete programs [30, 31]. The contribution and novelty in our approaches clearly differ from those in [9] as their constraint-based techniques are based on several Gröbner Basis or Syzygy Basis [32] computations and on solving non linear problems for each location. On the other hand, these works introduce a useful formalism and we start from similar definitions for hybrid systems, inductive invariants and consecution conditions.

We then propose methods to identify suitable morphisms to encode the relaxed consecution requirements. We show that the preconditions for discrete transitions and the Lie-derivatives for continuous evolutions can be viewed as morphisms over a vector space of terms, with polynomially bounded degrees, which can be suitably represented by matrices. The relaxed consecution requirements are also encoded as morphisms represented by matrices. By so doing, we do not need to start with candidate invariants that generate intractable problems. Moreover, our methods are not constraint-based. Rather, we automatically identify the needed degree of a generic multivariate polynomial, or fractional, as a relaxation of the consecution condition. The invariant basis are, then, generated by computing the Eigenspace of another matrix that is constructed. We identify the needed approximations

and the relaxations of the consecution conditions in order to guaranteed sufficient conditions for the existence and computation of invariants. Moreover, the unknown parameters that are introduced are all fixed in such a way that certain specific matrices will have a non null kernel, guaranteeing a basis for non-trivial invariants.

The contribution of this work are summarized thus:

- We demonstrate powerful algorithms [27, 28, 26, 31, 33, 29], relying on linear algebraic methods, capable of computing basis for ideals of non-trivial invariants for non-linear hybrid systems. In other words, looking at complex hybrid systems, we are able to extract automatically the generator basis of a vectorial space where each elements provide us with non-trivial invariants.
- We reduce the non-trivial invariant generation problem to the computation of associated eigenspaces or nullspaces by encoding consecution requirements as specific morphisms represented by matrices.
- Our methods display lower complexities than the mathematical foundations of previous approaches based on fixed point computation, as well as the present constraint-based approaches and other approaches that use Gröbner basis calculations, Syzygy calculations or quantifier elimination.
- We handle non-linear hybrid systems, extended with parameters and variables that are functions of time. We note that the latter conditions are still not treated by other state-of-the-art invariant generation methods.
- We establish general sufficient conditions guaranteeing the existence and allowing the computation of invariant ideals for situations not treated by other modern invariant generation approaches.
- Our algorithm incorporates a strategy for estimating optimal degree bounds for candidate invariants, thus being able to automatically compute basis for ideals of non-trivial non-linear invariants.

In Section 2 we introduce ideals of polynomials, inductive assertions and algebraic hybrid systems. In Section 3 we present new forms of approximating consecution for non-linear differential systems. In Section 5, we discuss morphisms suitable to handle non-linear differential rules and show how to generate invariants for differential rules. In Section 6 we introduce a strategy that can be used to choose the degree of invariants. Section 7 presents some experiments and in Section 8 we show how to handle discrete transition systems. In Section 9, we show how to generate ideals for global invariants by taking into account the ideal basis of local differential invariants, together with those derived from the discrete transition analysis and the initial constraints. We present our conclusions in Section 10.

In this writing, we strive to precede the most important proofs by sketches. Full proofs, more details and examples can be found in an Appendix and also in [26, 33, 31, 30].

2 Algebraic Hybrid Systems and Inductive Assertions

Let $\mathbb{K}[X_1, \dots, X_n]$ be the ring of multivariate polynomials over the set of variables $\{X_1, \dots, X_n\}$. An ideal is any set $I \subseteq \mathbb{K}[X_1, \dots, X_n]$ which contains the null polynomial and is closed under addition and multiplication by any element in $\mathbb{K}[X_1, \dots, X_n]$. Let $E \subseteq \mathbb{K}[X_1, \dots, X_n]$ be a set of polynomials. The ideal generated by E is the set of finite sums $(E) = \{\sum_{i=1}^k P_i Q_i \mid P_i \in \mathbb{K}[X_1, \dots, X_n], Q_i \in E, k \geq 1\}$. A set of polynomials E is said to be a *basis* of an ideal I if $I = (E)$. By the Hilbert basis theorem, we know that all ideals have a *finite basis*.

Notationally, as is standard in static program analysis, a primed symbol x' refers to the next state value of x after a transition is taken. We may also write \dot{x} for the derivative $\frac{dx}{dt}$. We denote by $\mathbb{R}_d[X_1, \dots, X_n]$ the ring of multivariate polynomials over the set of real variables $\{X_1, \dots, X_n\}$ of degree at most d . Also, $Vect(v_1, \dots, v_n)$ is the vector space generated by v_1, \dots, v_n .

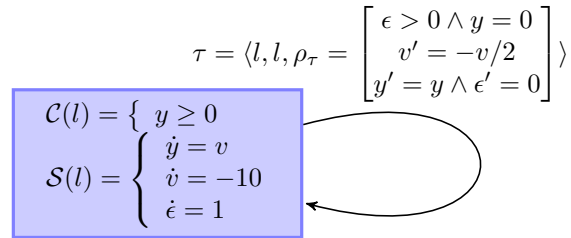
Definition 2.1. A hybrid system is a tuple $\langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{S}, l_0, \Theta \rangle$, where

- $V = \{a_1, \dots, a_m\}$ is a set of parameters,
- $V_t = \{X_1(t), \dots, X_n(t)\}$ where $X_i(t)$ is a function of t ,
- L is a set of locations,
- l_0 is the initial location,
- Θ is the initial condition, given as a first-order assertion over $V \cup V_t$,
- \mathcal{C} maps each location $l \in L$ to a local condition $\mathcal{C}(l)$ denoting an assertion over $V \cup V_t$, and \mathcal{S} associates each location $l \in L$ to a differential rule $\mathcal{S}(l)$ corresponding to an assertion over $V \cup \{dX_i/dt \mid X_i \in V_t\}$.

Finally, a transition $\tau \in \mathcal{T}$ is given by $\langle l_{pre}, l_{post}, \rho_\tau \rangle$, where l_{pre} and l_{post} name the pre- and post- locations of τ , and the transition relation ρ_τ is a first-order assertion over $V \cup V_t \cup V' \cup V'_t$.

A state is a pair (location and variable interpretations) from $L \times \mathbb{R}^{|V|}$. □

Example 2.1. The dynamic system of a bouncing ball ([34]) can be modeled by the following hybrid automaton:



$V = \{y, v, \epsilon\}$, $\Theta = (v = 16 \wedge y = \epsilon = 0)$, $l_0 = l$, $L = \{l\}$ and $\mathcal{T} = \{\tau\}$. □

The evolution of variables and functions in an interval must satisfy the local conditions and the local differential rules.

Definition 2.2. *A run of a hybrid automaton is an infinite sequence*

$$(l_0, \kappa_0) \rightarrow \cdots \rightarrow (l_i, \kappa_i) \rightarrow \cdots$$

of states where l_0 is the initial location and $\kappa_0 \models \Theta$.

For any two consecutive states $(l_i, \kappa_i) \rightarrow (l_{i+1}, \kappa_{i+1})$ in such a run, we have a discrete consecution if there exists a transition $\langle q, p, \rho_i \rangle \in \mathcal{T}$ such that $q = l_i$, $p = l_{i+1}$ and $\langle \kappa_i, \kappa_{i+1} \rangle \models \rho_i$ where the primed symbols refer to κ_{i+1} . Otherwise, it is a continuous consecution condition and we must have $q \in L$, $\varepsilon \in \mathbb{R}$ and a differentiable function $\phi : [0, \varepsilon] \rightarrow \mathbb{R}^{|V \cup V_t|}$ such that the following conditions hold:

- (i) $l_i = l_{i+1} = q$;
- (ii) $\phi(0) = \kappa_i$, $\phi(\varepsilon) = \kappa_{i+1}$;
- (iii) During the time interval $[0, \varepsilon]$, ϕ satisfies the local condition $\mathcal{C}(q)$ and the local differential rule $\mathcal{S}(q)$. That is, for all $t \in [0, \varepsilon]$ we must have $\phi(t) \models \mathcal{C}(q)$ and $\langle \phi(t), d\phi(t)/dt \rangle \models \mathcal{S}(q)$.

A state (ℓ, κ) is reachable if we have $(\ell, \kappa) = (l_i, \kappa_i)$ for some $i \geq 0$. □

Example 2.2. *Returning to Example 2.1, consider the run:*

$$(l, \kappa_0) \xrightarrow{\mu_0} (l, \kappa_1) \xrightarrow{\mu_1} (l, \kappa_2),$$

where $\kappa_0 = (0, 16, 0)$. In a valuation $(a, b, c) \in \mathbb{R}^3$, a is the value of y , b is the value of v and c is the value of ϵ . Clearly, $\kappa_0 \models \Theta$, as required. Now take $\kappa_1 = (0, -16, \varepsilon)$, where $\varepsilon = \frac{16}{5}$, and consider $\phi : [0, \varepsilon] \rightarrow \mathbb{R}^{|V_t|}$ such that $\phi(t) = (y(t), v(t), \epsilon(t)) = (-5t^2 + 16t, -10t + 16, t)$. Then $\phi(0) = (0, 16, 0) = \kappa_0$ and $\phi(\varepsilon) = (y(\varepsilon), v(\varepsilon), \epsilon(\varepsilon)) = \kappa_1$. Further, for all $t \in [0, \varepsilon]$ we get $\phi(t) \models \mathcal{C}(q)$ because $y(t)$ is clearly non-negative for $t \in [0, \varepsilon]$. Also, for all $t \in [0, \varepsilon]$ we have $\langle \phi(t), d\phi(t)/dt \rangle \models \mathcal{S}(q)$ because

$$d\phi(t)/dt = (dy(t)/dt, dv(t)/dt, d\epsilon(t)/dt) = (v, -10, 1).$$

So, by construction, μ_0 is a continuous consecution.

Now, since $\langle (0, -16, \varepsilon), (0, 8, 0) \rangle \models \rho_\tau$, if we let $\kappa_2 = (0, 8, 0)$, then μ_1 is a discrete consecution. □

Definition 2.3. *Let W be a hybrid system. An assertion φ over $V \cup V_t$ is an invariant at $l \in L$ if $\kappa \models \varphi$ whenever (l, κ) is a reachable state of W .* □

Definition 2.4. *Let W be a hybrid system and let \mathbb{D} be an assertion domain. An assertion map for W is a map $\gamma : L \rightarrow \mathbb{D}$. We say that γ is inductive if and only if the following conditions hold:*

1. *Initiation:* $\Theta \models \gamma(l_0)$;

2. *Discrete Consecution:* for all $\langle l_i, l_j, \rho_\tau \rangle \in \mathcal{T}$ we have

$$\gamma(l_i) \wedge \rho_\tau \models \gamma(l_j)';$$

3. *Continuous Consecution:* for all $l \in L$, and two consecutive states (l, κ_i) and (l, κ_{i+1}) in a possible run of W such that κ_{i+1} is obtained from κ_i according to the local differential rule $\mathcal{S}(l)$, if $\kappa_i \models \gamma(l)$ then $\kappa_{i+1} \models \gamma(l)$. \square

In item (3) of the previous definition, let $\gamma(l) \equiv (P_\gamma(X_1(t), \dots, X_n(t)) = 0)$ for all $t \in [0, \varepsilon]$ where P_γ is a multivariate polynomial in $\mathbb{R}[X_1, \dots, X_n]$ such that it has null values on the trajectory $(X_1(t), \dots, X_n(t))$ during the time interval $[0, \varepsilon]$. If P_γ is not the null polynomial, then $\mathcal{C}(l) \wedge (P_\gamma(X_1(t), \dots, X_n(t)) = 0) \models (d(P_\gamma(X_1(t), \dots, X_n(t)))/dt = 0)$ during the local time interval. Hence, if γ is an inductive assertion map then $\gamma(l)$ is an invariant at l for W .

Example 2.3. Consider the hybrid system of Example 2.1. It is easy to verify that the assertion $y = v \times \epsilon + 5 \times \epsilon^2$ is a provable, inductive invariant. We can see that the assertion holds during discrete transitions and the continuous evolution. \square

3 New continuous consecution conditions

Now we show how to encode differential continuous consecution conditions. First, we establish some notation.

Definition 3.1. For a polynomial P in $\mathbb{R}_d[X_1, \dots, X_n]$, we define the polynomial \mathcal{D}_P of $\mathbb{R}_d[Y_1, \dots, Y_n, X_1, \dots, X_n]$ thus:

$$\mathcal{D}_P(Y_1, \dots, Y_n, X_1, \dots, X_n) = \frac{\partial P(X_1, \dots, X_n)}{\partial X_1} Y_1 + \dots + \frac{\partial P(X_1, \dots, X_n)}{\partial X_n} Y_n.$$

\square

Consider a hybrid automaton W . Let $l \in L$ be a location which could, eventually, be in a circuit, and let η be an assertion map such that $\eta(l) \equiv (P_\eta(X_1(t), \dots, X_n(t)) = 0)$, where P_η is a non-null multivariate polynomial in $\mathbb{R}[X_1, \dots, X_n]$ with null values on the local trajectory $(X_1(t), \dots, X_n(t))$ during the local time interval $[0, \varepsilon]$. We have

$$\frac{dP_\eta}{dt} = \frac{\partial P_\eta(X_1, \dots, X_n)}{\partial X_1} \frac{dX_1(t)}{dt} + \dots + \frac{\partial P_\eta(X_1, \dots, X_n)}{\partial X_n} \frac{dX_n(t)}{dt}.$$

and so $\frac{dP_\eta}{dt} = \mathcal{D}_{P_\eta}(\dot{X}_1, \dots, \dot{X}_n, X_1, \dots, X_n)$. Now, let (l, κ_i) and (l, κ_{i+1}) be two consecutive configurations in a run. Then we can express local state continuous consecutions as

$$\mathcal{C}(l) \wedge (P_\eta(X_1(t), \dots, X_n(t)) = 0) \models (dP_\eta/dt = 0)$$

during the local time interval.

Next, we define some notions of continuous consecution.

Definition 3.2. Let W be a hybrid automaton, $l \in L$ a location and let η be an algebraic inductive map with $\eta(l) \equiv (P_\eta(X_1(t), \dots, X_n(t)) = 0)$ for all t in the time interval of mode l (so, P_η has a null value over the local trajectory $(X_1(t), \dots, X_n(t))$). We identify the following notions to encode continuous consecution conditions:

- η satisfies a differential Fractional-scale consecution at l if and only if there exists a multivariate fractional $\frac{T}{Q}$ such that $\mathcal{C}(l) \models (dP_\eta/dt - \frac{T}{Q}P_\eta = 0)$. We say that P_η is a fractional-scale and a $\frac{T}{Q}$ -scale differential invariant.
- η satisfies a differential Polynomial-scale consecution at l if and only if there exist a multivariate polynomial T such that $\mathcal{C}(l) \models dP_\eta/dt - TP_\eta = 0$. We say that P_η is a polynomial-scale and a T -scale differential invariant.
- η satisfies a differential Constant-scale consecution at l if and only if there exists a constant $\lambda \in \mathbb{R} \setminus \{0\}$ such that $\mathcal{C}(l) \models (dP_\eta/dt - \lambda P_\eta = 0)$. We say that P_η is a constant-scale and a λ -scale differential invariant.
- η satisfies a differential Strong-scale consecution at l if and only if $\mathcal{C}(l) \models (dP_\eta/dt = 0)$. If so, P_η is a strong-scale differential invariant. \square

Differential Polynomial-scale consecution encodes the fact that the numerical value of the Lie derivative of the polynomial P_η associated with assertion $\eta(l)$ is given by T times its numerical value throughout the time interval $[0, \varepsilon]$. First, we proposed methods [27, 28] for T -scale invariant generation where T is a constant (constant-scaling) or null (strong-scaling). As can be seen, the consecution conditions are relaxed when going from strong to polynomial scaling. Also, the T polynomials can be understood as *template multiplicative factors*. In other words, they are polynomials with unknown coefficients. In the next section, we consider polynomial-scale consecution and then we could extend the methods of [26, 29] to fractional-scale consecution conditions. In later sections we show how to combine these conditions with others induced by discrete transitions. In [33, 31, 30, 26, 29] one can find more details on how to handle other constraints associated to locations.

Theorem 3.1. (Soundness) Let P be a continuous function and let

$$\mathcal{S} = \begin{bmatrix} \dot{X}_1(t) = P_1(X_1(t), \dots, X_n(t)) \\ \vdots \\ \dot{X}_n(t) = P_n(X_1(t), \dots, X_n(t)) \end{bmatrix}$$

be a differential rule, with initial condition (x_1, \dots, x_n) . Any polynomial which is a P -scale differential invariant for these initial conditions is actually an inductive invariant. \square

Theorem 3.2. (Completeness) There exist a differential rule \mathcal{S} such that its invariants are not Polynomial-scale differential invariants. Such systems are then counter-example for completeness. \square

4 Differential Invariant Generation

Invariant generation for continuous time evolution is one of the main challenging steps in the static analysis and verification of hybrid systems. That is why we first restrict the analysis to differential system which appear in locations. We start with strong-differential invariants generation.

4.1 Morphisms for *strong*-scale differential consecution

First, we consider a differential system of the form:

$$\mathcal{S} = \begin{bmatrix} \dot{X}_1 = P_1(X_1, \dots, X_n) \\ \vdots \\ \dot{X}_n = P_n(X_1, \dots, X_n) \end{bmatrix}. \quad (1)$$

We have the following lemma.

Lemma 4.1. *Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ such that $\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = 0$. Then Q is a strong-scale differential invariant. \square*

If $P \in \mathbb{R}[X_1, \dots, X_n]$ is of degree r and the maximal degree of the P_i 's is d , then the degree of $\mathcal{D}_P(P_1, \dots, P_n, X_1, \dots, X_n)$ is $r + d - 1$. Passing to linear algebra, consider the morphism $D : \mathbb{R}_r[X_1, \dots, X_n] \rightarrow \mathbb{R}_{r+d-1}[X_1, \dots, X_n]$ where $P \mapsto \mathcal{D}_P(P_1, \dots, P_n, X_1, \dots, X_n)$. Let M_D be the matrix of such a morphism D in the canonical basis of $\mathbb{R}_r[X_1, \dots, X_n]$ and $\mathbb{R}_{r+d-1}[X_1, \dots, X_n]$.

Example 4.1. (*M_D for 2 variables, a degree 2 differential rule, and degree 2 invariants*)
Consider the following differential rules:

$$\begin{bmatrix} \dot{x}(t) = x^2(t) + x(t)y(t) + 3y^2(t) + 3x(t) + 4y(t) + 4 \\ \dot{y}(t) = 3x^2(t) + x(t)y(t) + y^2(t) + 4x(t) + y(t) + 3 \end{bmatrix}. \quad (2)$$

In this example we write $P_1(x, y) = x^2 + xy + 3y^2 + 3x + 4y + 4$ and $P_2(x, y) = 3x^2 + xy + y^2 + 4x + y + 3$. Consider the associated morphism D from $\mathbb{R}_2[x, y]$ to $\mathbb{R}_3[x, y]$. Using the basis

$$B_1 = (x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_2[x, y]$ and

$$B_2 = (x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_3[x, y]$, we can obtain M_D . For that, compute $D(P)$ for all elements P in the basis

$$(x^2, xy, y^2, x, y, 1)$$

and express the results in the basis

$$(x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1).$$

$$D(x^2) = 2x^3 + 2x^2y + 6xy^2 + 0y^3 + 6x^2 + 8xy + 0y^2 + 8x + 0y + 0 \times 1$$

$$M_D = \begin{pmatrix} 2 & 3 & 0 & 0 & 0 & 0 \\ 2 & 2 & 6 & 0 & 0 & 0 \\ 6 & 2 & 2 & 0 & 0 & 0 \\ 0 & 3 & 2 & 0 & 0 & 0 \\ 6 & 4 & 0 & 1 & 3 & 0 \\ 8 & 7 & 8 & 1 & 1 & 0 \\ 0 & 4 & 2 & 3 & 1 & 0 \\ 8 & 3 & 0 & 3 & 4 & 0 \\ 0 & 4 & 6 & 4 & 1 & 0 \\ 0 & 0 & 0 & 4 & 3 & 0 \end{pmatrix}.$$

 Figure 4: Computing M_D

For the first column of M_D consider $P(x, y) = x^2$, the first element of B_1 , and we compute

$$D(P) = \mathcal{D}_P(P_1, P_2, x, y)$$

which is expressed in B_2 as shown in Figure 4.1.

As we can see, a differential system \mathcal{S} and a degree r , are the only required informations in order to build M_D . \square

Now let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a strong-scale differential invariant for a given differential system defined by $P_1, \dots, P_n \in \mathbb{R}[X_1, \dots, X_n]$. Then

$$\begin{aligned} (\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = 0) &\Leftrightarrow (D(Q) = 0_{K[X_1, \dots, X_n]}) \\ &\Leftrightarrow (Q \in \text{Ker}(M_D)). \end{aligned}$$

We can see that Q will be a strong-scale differential invariant if and only if it is in the kernel of M_D .

Theorem 4.1. *A polynomial Q of $\mathbb{R}_r[X_1, \dots, X_n]$ is a strong-scale differential invariant for the differential system (1) if and only if it lies in the kernel of M_D .* \square

Now we want to know when one can assert the existence of a non-trivial polynomial invariant of degree r . We denote by $v(r)$ the dimension of $\mathbb{R}_r[X_1, \dots, X_n]$. If we consider initial conditions of the form $(x_1(0) = u_1, \dots, x_n(0) = u_n)$, we are looking for a strong-scale differential invariant in $\mathbb{R}_r[x_1, \dots, x_n]$ that belongs to the hyperplane $P(u_1, \dots, u_n) = 0$, i.e., we are looking for Q in

$$\text{ker}(M_D) \cap \{P \mid P(u_1, \dots, u_n) = 0\}.$$

We deduce the following theorem.

Theorem 4.2. *Let Q be in $\mathbb{R}_r[X_1, \dots, X_n]$. Then Q is an inductive invariant for the differential system with initial values (u_1, \dots, u_n) if and only if Q is in the intersection of $\text{Ker}(M_D)$ and the hyperplane $Q(u_1, \dots, u_n) = 0$. \square*

The intersection of the hyperplane $\{P|P(u_1, \dots, u_n) = 0\}$ with constant polynomials is always reduced to zero, and the intersection of any hyperplane with a subspace of $\mathbb{R}_r[x_1, \dots, x_n]$ has dimension at least 1. From the preceding theorem and the remark that follows it, there always exists non-trivial invariant when M_D has a kernel of dimension at least 2 (i.e. when M_D has rank at most $v(r) - 2$) as it will intersect any initial (semi-)hyperplane. We deduce the following corollary.

Corollary 4.1. *There exists a strong-scale invariant of degree r for the differential system with initial conditions (any initial conditions, actually), if and only if the kernel of M_D is of dimension at least 2. The basis of $\text{Ker}(M_D)$ gives a basis of a non-trivial invariant ideal \square*

So, if Corollary 4.1 holds for a given differential systems, we can compute the basis of $\text{Ker}(M_D)$ to obtain a basis of non-trivial invariant. We will see that such strategies are very effective and practical once the consecution condition is relaxed to constant-scaling and polynomial-scaling. Now consider the following differential system with initial conditions

$$\begin{bmatrix} \dot{x}(t) = x(t) \\ \dot{y}(t) = ny(y) \\ (x(0), y(0)) = (\lambda, \mu) \end{bmatrix}, \quad (3)$$

where n is a parameter in V and $x(t)$, $y(t)$ are function of t in V_t . The solutions of this system are well known: $x(t) = \lambda e^t$ and $y(t) = \mu e^{nt}$. Consider the polynomial $Q(x, y) = x^n/\lambda^n - y/\mu$. It is immediate that the polynomial assertion $x^n/\lambda^n - y/\mu = 0$ is an invariant. It is actually a generator of the ideal of invariants. For if Q' is invariant, it is null on the points $(\lambda u, \mu u^n)$ for $u \in \mathbb{R}$ and so $x^n/\lambda^n - y/\mu$ divides Q' . For this system it is the most significant invariant one can get. Now, $Q(x, y) = x^n/\lambda^n - y/\mu$ is not a strong-scale differential invariant because $\partial_x Q = nx^{n-1}/\lambda^n$ and $\partial_y Q = -1/\mu$, and $\partial_x Q(x, y)x + \partial_y Q(x, y)y = nx^n/\lambda^n - y/\mu \neq 0$. In order to simplify the notation, take $n = 1$. We show that there cannot exist a non-trivial strong-scale differential invariant for the system

$$\begin{bmatrix} \dot{x} = x \\ \dot{y} = y \end{bmatrix}. \quad (4)$$

Suppose such an invariant exists. Write it as $Q(x, y) = \sum_{i,j} a_{i,j} x^i y^j$. The relation $\partial_x Q(x, y)x + \partial_y Q(x, y)y = 0$ implies $\sum_{i,j} i a_{i,j} x^i y^j + \sum_{i,j} j a_{i,j} x^i y^j = 0$, which gives $(i + j)a_{i,j} = 0$. As $i \geq 0$ and $j \geq 0$, this implies that all $a_{i,j} = 0$ but for $a_{0,0}$. Hence, Q is constant. Thus, even in cases where very simple invariants can be found, one will not find *strong-scale* differential invariants which are non-trivial inductive invariants. We will show how to handle such systems in Section 4.2, Example 4.5. Therefore, we can conjecture that strong invariants exist in special cases. In the following we establish characterisation properties and classes of differential systems admitting *strong-scale* differential invariants which are non-trivial inductive invariants. We will use the following lemma.

Lemma 4.2. *Let Q_1, \dots, Q_n be n polynomials in $\mathbb{R}[X_1, \dots, X_n]$. Then there exists a polynomial Q such that $\partial_1 Q = Q_1, \dots, \partial_n Q = Q_n$ if and only if for any $i \neq j$, $1 \leq i, j \leq n$, one has $\partial_i Q_j = \partial_j Q_i$. \square*

Let $\text{Syz}(P_1, \dots, P_n)$ denote the *Syzygy Module* [35] of (P_1, \dots, P_n) .

Definition 4.1. *Let P_1, \dots, P_K be k polynomials in $\mathbb{R}[X_1, \dots, X_n]$. Then $\text{Syz}(P_1, \dots, P_k)$ is the following set:*

$$\{ (Q_1, \dots, Q_k) \in \mathbb{R}[X_1, \dots, X_n] \mid Q_1 P_1 + Q_2 P_2 + \dots + Q_k P_k = 0 \}.$$

\square

We can state the following theorem.

Theorem 4.3. *There exists a strong-scale invariant for a differential system if and only if there exists (Q_1, \dots, Q_n) in $\text{Syz}(P_1, \dots, P_n)$ such that for any i, j with $i \neq j$ and $1 \leq i, j \leq n$, one has $\partial_i Q_j = \partial_j Q_i$. \square*

For example, when $n = 2$, we get the following class of systems for which one can always find a strong invariant:

$$\begin{bmatrix} \dot{x}_1 = P_1(x_1, x_2) \\ \dot{x}_2 = P_2(x_1, x_2) \end{bmatrix}. \quad (5)$$

with $\partial_2 P_2 = -\partial_1 P_1$. Indeed, $(P_2 - P_1)$ always belongs to $\text{Syz}(P_1, P_2)$. In fact, it is actually a basis when P_1 and P_2 are relatively prime.

Example 4.2. *Consider the following differential rules.*

$$\begin{bmatrix} \dot{x} = xy \\ \dot{y} = -y^2/2 \end{bmatrix}. \quad (6)$$

Here, we indeed have $\partial_y P_2 = -\partial_x P_1 = -y$. The corresponding invariant is $Q(x, y) = xy^2/2$. \square

Example 4.3. *Another example of systems admitting strong invariants is a generalization to dimension n of the rotational motion of a rigid body:*

$$\begin{bmatrix} \dot{x}_1 = a_1 x_2 \dots x_n \\ \vdots \\ \dot{x}_n = a_n x_1 \dots x_{n-1} \end{bmatrix}. \quad (7)$$

We treat the case when the a_i 's are non zero parameters, other cases being easier. Indeed, the vector

$$(Q_1 = x_1/a_1, Q_2 = -x_2/(n-1)a_2, \dots, Q_n = -x_n/(n-1)a_n)$$

belongs to $\text{Syz}(P_1, \dots, P_n)$, where $P_i = a_i x_1 \dots x_{i-1} x_{i+1} \dots x_n$ belongs to the set of polynomials defining the differential rule. Now if $i \neq j$, one has $\partial_i Q_j = \partial_j Q_i = 0$, and applying Theorem 4.3 we deduce that the system admits a strong invariant. In order to obtain an invariant, we just have to solve $\partial_1 Q = x_1/a_1; \partial_2 Q = -x_2/(n-1)a_2; \dots; \partial_n Q = -x_n/(n-1)a_n$. A trivial solution is $Q(x_1, \dots, x_n) = x_1^2/2a_1 - x_2^2/2(n-1)a_2 \dots - x_n^2/2(n-1)a_n$. Hence, the system admits as strong invariant the following assertion: $Q(x_1, \dots, x_n) = x_1^2/2a_1 - x_2^2/2(n-1)a_2 \dots - x_n^2/2(n-1)a_n = 0$. \square

4.2 Morphisms for *constant*-scale differential consecution

Consider the differential system S depicted in (1). We state the following lemma.

Lemma 4.3. *Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be such that*

$$\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = \lambda Q(X_1, \dots, X_n).$$

Then Q is a λ -scale invariant. □

If Q has degree r , and the maximal degree of the P_i 's is d , then we know that

$$\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n)$$

has degree $r + d - 1$. Hence we deduce that, in general, constant-scale consecution will work when the polynomials P_i of the differential transition system are of degree one, *i.e.* when the transition system is affine. So, suppose that the P_i 's are of degree one. Now we want to find an invariant Q of degree r . We reduce the problem again to linear algebra. Consider the endomorphism D of $\mathbb{R}_r[X_1, \dots, X_n]$ given by

$$P \mapsto \mathcal{D}_P(P_1, \dots, P_n, X_1, \dots, X_n).$$

Using lemma 4.3, Q will be a λ -invariant for constant-scale consecution of degree at most r if and only if λ is an eigenvalue of D , and Q is an eigenvector for λ . By letting M_D be the matrix of D in the canonical basis of $\mathbb{R}_r[X_1, \dots, X_n]$ we can state the following theorem.

Theorem 4.4. *A polynomial Q of $\mathbb{R}_r[X_1, \dots, X_n]$ is a λ -scale invariant for continuous scale consecution of the differential system if and only if there exists an eigenvalue λ of M_D such that Q belongs to the eigenspace of M_D corresponding to λ .* □

Zero is always an eigenvalue of M_D , since its last column is always null. But this gives a constant eigenvector, which is less interesting. In the following cases we describe the methods in the most general case for 2 variables and the generation of λ -invariant of degree 2

Example 4.4. *(General case for 2 variables and degree 2) Consider the differential system of the following form:*

$$\begin{cases} \dot{x} = a_1x + b_1y + c_1 \\ \dot{y} = a_2x + b_2y + c_2 \end{cases}. \quad (8)$$

The matrix M_D in the basis $(x^2, xy, y^2, x, y, 1)$ is

$$M_D = \begin{pmatrix} 2a_1 & a_2 & 2b_2 & 0 & 0 & 0 \\ 2b_1 & a_1 + b_2 & 2a_2 & 0 & 0 & 0 \\ 0 & b_1 & 0 & 0 & 0 & 0 \\ 2c_1 & c_2 & 0 & a_1 & 0 & 0 \\ 0 & c_1 & 2c_2 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & c_1 & c_2 & 0 \end{pmatrix}.$$

This matrix is block lower triangular, with blocks of size 3×3 . Hence, its characteristic polynomial is the product of two degree 3 polynomials, and roots of such polynomials can be computed by Cardan's method. Thus, one will always be able to find non-null λ -scale invariants in this case. □

We just proved the following proposition and gave a method for finding the corresponding invariants.

Proposition 4.1. *If we are looking at an affine differential transition system with polynomials in two variables, then one is always able to find good scale invariants.* \square

As we did in [30] when dealing with discrete consecution, we can identify large decidable classes, e.g.

- (i) when M_D is block triangular with 4×4 blocks or less; and
- (ii) when the eigenspace associated with eigenvalue 1 is of dimension greater than 1; among others.

Theorem 4.5. *A polynomial Q in $\mathbb{R}_r[X_1, \dots, X_n]$ is a λ -scale invariant for the differential system with initial values (u_1, \dots, u_n) if and only if there exists an eigenvalue λ of M_D such that Q belongs to the intersection of the eigenspaces corresponding to λ and the hyperplane $Q(u_1, \dots, u_n) = 0$.* \square

Corollary 4.2. *There will be a non-null polynomial invariant for any given initial values if and only if there exists an eigenspace of M_D with dimension at least 2.* \square

Example 4.5. *Consider system (3) again, which we could not handle using strong-scale invariant encoding. We recall that the differential system*

$$\begin{bmatrix} \dot{x} = x \\ \dot{y} = ny \\ (x(0), y(0)) = (\lambda, \mu) \end{bmatrix} \quad (9)$$

has an associated endomorphism $D : Q(x, y) \mapsto \partial_x Q(x, y)x + n\partial_y Q(x, y)y$. Writing its matrix in the basis $(x^n, x^{n-1}y, \dots, xy^{n-1}, y^n, \dots, x, y, 1)$ we have:

$$\begin{pmatrix} n & \dots & 0 & 0 \\ 0 & M_D & 0 & 0 \\ 0 & \dots & n & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}.$$

We see that the eigenspace corresponding to n has dimension at least 2, and it contains $\text{Vect}(x^n, y)$ (the vector space generated by x^n and y). Using the theorem on the existence on solutions for any initial conditions, we deduce that for the initial values $(x(0) = \lambda, y(0) = \mu)$ there exists an invariant of the form $ax^n + by$, and which must verify $a\lambda^n + b\mu = 0$. If λ and μ are non zero, which is the interesting case, one can take $a = \lambda^{-n}$ and $b = -\mu^{-1}$, which gives the inductive invariant

$$Q(x, y) = x^n/\lambda^n - y/\mu = 0.$$

\square

5 Handling non-linear differential systems

We consider a *non-linear* differential system of the form:

$$\mathcal{S} = \begin{bmatrix} \dot{X}_1(t) = P_1(X_1(t), \dots, X_n(t)) \\ \vdots \\ \dot{X}_n(t) = P_n(X_1(t), \dots, X_n(t)) \end{bmatrix},$$

with the P_i 's in $\mathbb{R}[X_1, \dots, X_n]$. We know that as soon as one of the P_i 's has degree more than one, we must use polynomial-scale consecution in order to obtain interesting invariants [33]. We have the following lemma.

Lemma 5.1. *Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ such that*

$$\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = TQ$$

with T in $\mathbb{R}[X_1, \dots, X_n]$. Then Q is a T -scale invariant. \square

If $P \in \mathbb{R}[X_1, \dots, X_n]$ is of degree r and the maximal degree of the P_i 's is d , then the degree of $\mathcal{D}_P(P_1, \dots, P_n, X_1, \dots, X_n)$ is $r + d - 1$. Hence, T must be searched in the subspace of $\mathbb{R}[X_1, \dots, X_n]$, which is of degree at most $r + d - 1 - r = d - 1$.

Consider the morphism

$$D : \mathbb{R}_r[X_1, \dots, X_n] \rightarrow \mathbb{R}_{r+d-1}[X_1, \dots, X_n],$$

where

$$P \mapsto \mathcal{D}_P(P_1, \dots, P_n, X_1, \dots, X_n).$$

Let M_D be the corresponding matrix in the canonical basis of $\mathbb{R}_r[X_1, \dots, X_n]$ and $\mathbb{R}_{r+d-1}[X_1, \dots, X_n]$. Here, we construct matrices M_D in a same manner as we did and described in Section 4.1, Example 4.1.


Choosing a generic T in $\mathbb{R}_{d-1}[X_1, \dots, X_n]$, we define the associated morphism

$$\bar{T} : \mathbb{R}_r[x_1, \dots, x_n] \rightarrow \mathbb{R}_{r+d-1}[x_1, \dots, x_n],$$

where

$$P \mapsto TP.$$

Denote by L_T its matrix in the canonical basis, obtained as in the computation of M_D . Matrices L_T corresponding to multiplication by polynomials T of $\mathbb{R}_{d-1}[x_1, \dots, x_n]$ have a very precise form, dependent on the coefficients of T . Thus, for fixed n , r and d , they can be easily identified. We will denote by $M(pol)$ the set of such matrices. It is, in fact, a (vector) subspace of matrices corresponding to morphisms from $\mathbb{R}_r[x_1, \dots, x_n]$ to $\mathbb{R}_{r+d-1}[x_1, \dots, x_n]$. To be even more precise, if T is a *generic template* in $\mathbb{R}_{d-1}[X_1, \dots, X_n]$, let $t_1, \dots, t_{v(d-1)}$ be its coefficients where $v(d-1)$ is the dimension of $\mathbb{R}_{d-1}[X_1, \dots, X_n]$. Then the coefficients of L_T are in $\{t_1, \dots, t_{v(d-1)}\}$ and it has a natural block decomposition. In order to fix ideas, we show what happens for two variables P_i of maximal degree 3. Thus, we are looking for an invariant in $\mathbb{R}_2[x, y]$. Hence, T lies in $\mathbb{R}_2[x, y]$.

$$\bar{T}(x^2) = \begin{matrix} t_1 x^4 + t_2 x^3 y + t_3 x^2 y^2 + 0 xy^3 + 0 y^4 + t_4 x^3 + t_5 x^2 y + 0 xy^2 + 0 y^3 + t_6 x^2 + \\ 0 xy + 0 y^2 + 0 x + 0 y + 0 \end{matrix} \times 1$$


$$\begin{pmatrix} t_1 & 0 & 0 & 0 & 0 \\ t_2 & 0 & 0 & 0 & 0 \\ t_3 & t_1 & 0 & 0 & 0 \\ 0 & t_2 & 0 & 0 & 0 \\ 0 & t_3 & 0 & 0 & 0 \\ t_4 & 0 & t_1 & 0 & 0 \\ t_5 & 0 & t_2 & t_1 & 0 \\ 0 & t_4 & t_3 & t_2 & 0 \\ 0 & t_5 & 0 & t_3 & 0 \\ t_6 & 0 & t_4 & 0 & t_1 \\ 0 & 0 & t_5 & t_4 & t_2 \\ 0 & t_6 & 0 & t_5 & t_3 \\ 0 & 0 & t_6 & 0 & t_4 \\ 0 & 0 & 0 & t_6 & t_5 \\ 0 & 0 & 0 & 0 & t_6 \end{pmatrix}.$$

 Figure 5: The matrix of \bar{T} in basis B_4

Example 5.1. A generic T is of the form

$$T(x, y) = t_1 x^2 + t_2 xy + t_3 y^2 + t_4 x + t_5 y + t_6.$$

Using the basis

$$B_2 = (x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_2[x, y]$ and the basis

$$B_4 = (x^4, x^3 y, x^2 y^2, xy^3, y^4, x^3, x^2 y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_4[x, y]$, we obtain the matrices L_T . To do so, we compute $\bar{T}(P)$ for all elements P in the basis B_2 and we express the results in the basis B_4 . In other words, to get the first column of L_T we first consider $P(x, y) = x^2$ the first element of B_2 , and we compute $\bar{T}(P) = TP$ which is expressed in B_4 as in Figure 5. This determines $M(pol)$. \square

Now let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a T -scale invariant for a given differential system defined by $P_1, \dots, P_n \in \mathbb{R}[X_1, \dots, X_n]$. Then

$$\begin{aligned} (\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = TQ) &\Leftrightarrow D(Q) = \bar{T}(Q) \\ &\Leftrightarrow ((D - \bar{T})(Q) = 0_{\mathbb{R}[X_1, \dots, X_n]}) \\ &\Leftrightarrow (Q \in Ker(M_D - L_T)). \end{aligned}$$

So, a T -scale invariant is nothing else than a vector in the kernel of $M_D - L_T$.

Theorem 5.1. *There is a polynomial-scale invariant for the differential system if and only if there exists a matrix L_T in $M(\text{pol})$, corresponding to a polynomial T of $\mathbb{R}_{d-1}[x_1, \dots, X_n]$, such that $\text{Ker}(M_D - L_T)$ is not reduced to zero. And, any vector in the kernel of $M_D - L_T$ will give a T -scale differential invariant. \square*

Notice that $M_D - L_T$ with a non trivial kernel is equivalent to it having rank strictly less than the dimension $v(r)$ of $\mathbb{R}_r[x_1, \dots, x_n]$. By a classical theorem [36], this is equivalent to the fact that each $v(r) \times v(r)$ sub-determinant of $M_D - L_T$ is equal to zero. Those determinants are polynomials in $(t_1, \dots, t_{v(d-1)})$, which we denote by $E_1(t_1, \dots, t_{v(d-1)}), \dots, E_s(t_1, \dots, t_{v(d-1)})$.

Theorem 5.2. *There is a non trivial T -scale invariant if and only if the polynomials (E_1, \dots, E_s) admit a common root, other than the trivial one $(0, \dots, 0)$. \square*

This theorem provides us with important existence results. But we can provide a more practical way to get invariant ideals without computing common roots. Consider initial values given by unknown parameters $x_1(0) = u_1, \dots, x_n(0) = u_n$. The initial step defines a linear form on $\mathbb{R}_r[x_1, \dots, x_n]$, namely $I_u : P \mapsto P(u_1, \dots, u_n)$. Hence, initial values correspond to a hyperplane of $\mathbb{R}_r[X_1, \dots, X_n]$ given by the kernel I_u , which is

$$\{Q \in \mathbb{R}_r[X_1, \dots, X_n] \mid Q(u_1, \dots, u_n) = 0\}.$$

Theorem 5.3. *Let Q be in $\mathbb{R}_r[X_1, \dots, X_n]$. Then Q is an inductive invariant for the differential system with initial values (u_1, \dots, u_n) if and only if there exists a matrix $L_T \neq 0$ in $M(\text{pol})$, corresponding to T in $\mathbb{R}_{d-1}[X_1, \dots, X_n]$, such that Q is in the intersection of $\text{Ker}(M_D - L_T)$ and the hyperplane $Q(u_1, \dots, u_n) = 0$. \square*

Now, if $\text{Dim}(\text{Ker}(M_D - L_T)) \geq 2$ then $\text{Ker}(M_D - L_T)$ would intersect any initial hyperplane.

Corollary 5.1. *There are non-trivial invariants for any given initial values if and only if there exists a matrix L_T in $M(\text{pol})$ such that $\text{Ker}(M_D - L_T)$ has dimension at least 2. \square*

Also, we have that $\text{Dim}(\text{Ker}(M_D - L_T)) \geq 2$ if and only if we also have $\text{Rank}(M_D - L_T) \leq \text{Dim}(\mathbb{R}_r[X_1, \dots, X_n]) - 2$. Further, we also show how to assign values to the coefficients of T in order to guarantee the existence and generation of invariants.

Example 5.2. *(Running example) Consider the following differential rules with $P_1 = x^2 + 2xy + x$ and $P_2 = xy + 2y^2 + y$:*

$$\begin{cases} \dot{x}(t) = x^2(t) + 2x(t)y(t) + x(t) \\ \dot{y}(t) = x(t)y(t) + 2y^2(t) + y(t) \end{cases}. \quad (10)$$

- **Step 1:** *We build the matrix $M_D - L_T$. The maximal degree of the systems is $d = 2$ and the T -scale invariant will be of degree $r = 2$. Then, T is of degree $d - 1 = 1$ and we write t_1, t_2, t_3 for its unknown coefficients, i.e. the canonical form is $T(x, y) = t_1x + t_2y + t_3$. Using the basis $(x^2, xy, y^2, x, y, 1)$ of*

$\mathbb{R}_2[x, y]$ and the basis $(x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$ of $\mathbb{R}_3[x, y]$, the matrix $M_D - L_T$ is:

$$M_D - L_T = \begin{pmatrix} 2 - t_0 & 0 & 0 & 0 & 0 & 0 \\ 4 - t_1 & 2 - t_0 & 0 & 0 & 0 & 0 \\ -t_2 & 4 - t_1 & 2 - t_0 & 0 & 0 & 0 \\ 0 & 0 & 4 - t_1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 - t_0 & 0 & 0 \\ 0 & 2 - t_2 & 0 & 2 - t_1 & 1 - t_0 & 0 \\ 0 & 0 & 2 - t_2 & 0 & 2 - t_1 & 0 \\ 0 & 0 & 0 & 1 - t_2 & 0 & -t_0 \\ 0 & 0 & 0 & 0 & 1 - t_2 & -t_1 \\ 0 & 0 & 0 & 0 & 0 & -t_2 \end{pmatrix}.$$

- **Step 2:** Now all unknown t_i is given a value so as to guarantee the existence of invariants. Our algorithm fixes $t_1 = 2$, $t_2 = 4$ and $t_3 = 2$ to get $T(x, y) = 2x + 4y + 2$. Matrix $M_D - L_T$ has its second and third columns equal to zero. So, the rank of $M_D - L_T$ is less than 4 and its kernel has dimension at least 2. Any vector in this kernel will be a T -scale differential invariant.
- **Step 3** Now, Corollary 5.1 applies to $M_D - L_T$. So, there will always be invariants, whatever the initial values. We compute and output the basis of $\text{Ker}(M_D - L_T)$. Using our prototype `Ideal_Inv_Gen`, to be presented shortly, we get

```
Polynomial scaling continuous evolution
T(x,y) = 2 x + 4 y + 2
Module of degree 6 and rank 2 and Kernel of dimension 4
{{0, 1, 0, 0, 0, 0}, {0, 0, 1, 0, 0, 0}}
```

Vectors of the basis are interpreted in the canonical basis of $\mathbb{R}_2[x, y]$. We get as output:

```
Basis of invariant Ideal
{x y, y^2}
```

We have an ideal for non trivial inductive invariants and we search for one of the form $axy + by^2$. If the system has initial conditions $x(0) = \lambda$ and $y(0) = \mu$, then $a\lambda\mu + b\mu^2 = 0$, and $\mu xy - \lambda y^2 = 0$ is an invariant for all μ and λ . \square

6 Obtaining optimal degree bounds

In order to guarantee the existence of non-trivial invariants of degree r , we need a polynomial T such that $\text{Ker}(M_D - L_T) \neq 0$. First, define T as a polynomial with parametrized coefficients. We can then create a decision procedure to assign values to the coefficients of T in such a way that $\text{Ker}(M_D - L_T) \neq 0$. Algorithm 1 illustrates this strategy. Its contribution relies on very general sufficient conditions for the existence and the computation of invariants. From the differential rules, we obtain matrix M_D (see line 5) with real entries. We can then define degree bounds for matrices L_T that can be used to approximate the consecution requirements (see line 6). As we recall from Section 5, $\text{Ker}(M_D - L_T) \neq 0$ is equivalent to having $M_D - L_T$ with rank strictly less than the dimension $v(r)$ of $\mathbb{R}_r[x_1, \dots, x_n]$. We then

Algorithm 1: Ideal_Inv_Gen($r, P_1, \dots, P_n, X_1, \dots, X_n$)

Data: r is the degree for the set of invariants we are looking for, P_1, \dots, P_n are the n polynomials given by differential rules, and $X_1, \dots, X_n \in V_t$ are functions of time.

Result: B_{Inv} , a basis of ideal of invariants.

begin

```

1   int  $d$ ; Template  $T$ ; Matrix  $M_D, L_T$ ;
2    $d \leftarrow$  Max_degree( $\{P_1, \dots, P_n\}$ ); /* $d$  is the maximal degree of  $P_i$ 's*/;
3   if  $d \geq 2$  then
4        $T \leftarrow$  Template_Canonical_Form( $d - 1$ );
5        $M_D \leftarrow$  Matrix_D( $r, r + d - 1, P_1, \dots, P_n$ );
6        $L_T \leftarrow$  Matrix_L( $r, r + d - 1, T$ );
7        $\overline{M} \leftarrow$  Reduce_Rank_Assigning_Values( $M_D - L_T$ );
8       if Rank( $\overline{M}$ )  $\geq$  Dim( $R_r[X_1, \dots, X_n]$ ) then
9           /*Increase the degree  $r$  of candidate invariants.*/;
9           return Ideal_Inv_Gen( $r + 1, P_1, \dots, P_n, X_1, \dots, X_n$ );
10          else
11              /*There is an ideal that we can compute*/;
11              return Nullspace_Basis( $\overline{M}$ );
12          else
12              ... /*See our previous work for strong and constant scaling.*/;

```

reduce the rank of $M_D - L_T$ by assigning values of terms in M_D to parameters in L_T (see line 7).

Next, we determine whether matrix \overline{M} has a trivial kernel by first computing its rank and then checking if $(\text{Rank}(\overline{M}) < \text{Dim}(R_r[X_1, \dots, X_n]))$ holds (see line 8). By so doing, we can increase the degree r of invariants until Theorem 5.1 (or Corollary 5.1) applies or until stronger hypotheses occur, *e.g.* if all $v(r) \times v(r)$ sub-determinants are null. Then, we compute and output the basis of the nullspace of matrix \overline{M} in order to construct an ideal basis for non trivial invariants (see **Nullspace_Basis**, line 10). We can directly see that if there is no ideal for non-trivial invariants for a value r_i then we conclude that there is no ideal of non-trivial invariants for all degrees $k \leq r_i$. This could guide other constraint-based techniques, since checking for invariance with a template of degree less or equal to r_i will not be necessary. In case there is no ideal for invariants of degree r (see line 8), we first increment the value of r by 1 before the recursive call to **Ideal_Inv_Gen**.

We thus showed how to reduce the invariant generation problem to the problem of computing a kernel basis for polynomial mappings. For the latter, we use well-known state-of-the-art algorithms, *e.g.* that the software Mathematica provides. These algorithms calculate the eigenvalues and associated eigenspaces of \overline{M} when it is a square matrix. When \overline{M} is a rectangular matrix, we can use its *singular value decomposition* (SVD). A SVD of \overline{M} provides an explicit representation of its rank and kernel by computing unitary matrices U and V and a regular diagonal matrix S such that $\overline{M} = USV$. We compute the SVD of a $v(r + d - 1) \times v(r)$ matrix \overline{M} by a two step procedure. First, reduce it to a bi-diagonal matrix, with a cost of $O(v(r)^2 v(r + d - 1))$ flops. The second step relies on an iterative

method, as is also the case for other eigenvalue algorithms. In practice, however, it suffices to compute the SVD up to a certain precision, *i.e.* up to a machine epsilon. In this case, the second step takes $O(v(r))$ iterations, each using $O(v(r))$ flops. So, the overall cost is $O(v(r)^2v(r + d - 1))$ flops. For an implementation of the algorithm we could rewrite Corollary 5.1 as follow.

Corollary 6.1. *Let $\overline{M} = U \cdot S \cdot V$ be the singular value decomposition of matrix \overline{M} described just above. There will be a non trivial T -invariant for any given initial condition if and only if the number of non-zero elements in matrix S is less than $v(r) - 2$, where $v(r)$ is the dimension of $\mathbb{R}_r[x_1, \dots, x_n]$. Moreover, the orthonormal basis for the nullspace obtained from the decomposition directly gives an ideal for non-linear invariants. \square*

It is important to emphasize that eigenvectors of \overline{M} are computed after the parameters of L_T have been assigned. When the differential system has several variables and none or few parameters, \overline{M} will be over the reals and there will be no need to use the symbolic version of these algorithms.

7 Examples and Experimental Results

By reducing the problem to linear algebra, we obtain new optimization techniques, as illustrated in the following examples. Depending on the form of the monomials present in the system, we may be able to find T and a vector X such that $X \in \text{Ker}(M_D - L_T)$ without defining T as a template, *i.e.* without using a polynomial with unknown coefficients for scaling consecution. The idea is to directly obtain a suitable T by *factorization*. The following are examples of large classes of systems where the methods apply.

Example 7.1. *Let $s \in \mathbb{N}$ be positive and consider the differential rules:*

$$\begin{bmatrix} \dot{x}_1(t) = \sum_{k=0}^s a_k x_1(t)^{k+1} x_2(t)^k \dots x_n(t)^k \\ \vdots \\ \dot{x}_n(t) = \sum_{k=0}^s a_k x_1(t)^k \dots x_{n-1}(t)^k x_n(t)^{k+1} \end{bmatrix}. \quad (11)$$

This differential system contains parameters and variables that are time functions. We denote the polynomials thus

$$P_1 = \sum_{k=0}^s a_k x_1^{k+1} x_2^k \dots x_n^k; \dots; P_n = \sum_{k=0}^s a_k x_1^k \dots x_{n-1}^k x_n^{k+1}$$

Let D be the morphism associated with (11) and let M_D be its matrix in the canonical basis. Then, it is immediate that $\mathcal{D}_P(x_i) = P_i$. Now, for this particular class of P_i 's, we see that $\mathcal{D}_P(x_i) = x_i T$, where $T = \sum_{k=0}^s a_k x_1^k x_2^k \dots x_{n-1}^k x_n^k$. This means that if \overline{T} is the morphism associated to multiplication by T , we have $\mathcal{D}_P(x_i) = \overline{T}(x_i)$ for each i . Let L_T be its matrix in the canonical basis. We deduce that $\text{Vect}(x_1, \dots, x_n) \subset \text{Ker}(M_D - L_T)$. Hence, for $n \geq 2$, the space $\text{Ker}(M_D - L_T)$ has dimension greater than 2, and we can apply our existence theorem for invariants, given any initial values. We can then search for an invariant of

the form $a_1x_1 + \dots + a_nx_n$. Given the initial conditions $x_1(0) = \lambda_1, \dots, x_n(0) = \lambda_n$, a vector $(a_1, \dots, a_n)^\top$ is such that the polynomial $a_1x_1 + \dots + a_nx_n$ is an invariant for (11) whenever it belongs to the kernel of the linear form with matrix $(\lambda_1, \dots, \lambda_n)$. Summarizing, with polynomial scaling, any polynomial $Q = a_1x_1 + \dots + a_nx_n$ with $(a_1, \dots, a_n)^\top$ in the kernel of $(\lambda_1, \dots, \lambda_n)$ is an invariant for (11). \square

Example 7.2. In order to handle air traffic management systems [25, 37] automatically, we consider the given differential system:

$$\begin{cases} \dot{x}_1 = a_1 \cos(\omega t + c) \\ \dot{x}_2 = a_2 \sin(\omega t + c) \end{cases}. \quad (12)$$

This models the system satisfied by one of the two airplanes. We introduce the new variables d_1 and d_2 to handle the transcendental functions, axiomatizing them by differential equations, so that d_1 and d_2 satisfy

$$\begin{cases} \dot{d}_1 = -a_1/a_2\omega d_2 \\ \dot{d}_2 = a_2/a_1\omega d_1. \end{cases} \quad (13)$$

If D is the morphism associated to this system, it is immediate that $D(a_2^2d_1^2) = -2a_1a_2\omega d_1d_2$ whereas $D(a_1^2d_2^2) = 2a_1a_2\omega d_1d_2$. From [27, 28], this implies that $\text{Vect}(a_2^2d_1^2 + a_1^2d_2^2) \subset \text{Ker}(D)$ and so $a_2^2d_1^2 + a_1^2d_2^2$ is a strong-scale invariant (i.e. a T -scale invariant where T is null) for the system. But $\dot{x}_1 = \dot{d}_1 = [a_1/(a_2\omega)]\dot{d}_2$ and $\dot{x}_2 = \dot{d}_2 = [-a_2/(a_1\omega)]\dot{d}_1$. Therefore, there exist constants c_1 and c_2 , determined by the initial values, such that $x_1 = a_1/a_2\omega d_2 + c_1$ and $x_2 = d_2 = -a_2/a_1\omega d_1 + c_2$.

This implies that $(a_2x_1 - k_1)^2 + (a_1x_2 - k_2)^2 = 0$, with $k_1 = a_2c_1$ and $k_2 = a_1c_2$, is an invariant of the first system. Hence the two airplanes, at least for some lapse of time, follow an elliptical path. \square

In the following two examples we have shown again how to deal with differential systems with parameters and several variables.

Example 7.3. Consider the following differential rules:

$$\begin{cases} \dot{x} = ax^2(t) + bx(t)y(t) + cx(t) \\ \dot{y} = ax(t)y(t) + by^2(t) + cy(t) \end{cases}. \quad (14)$$

We have two polynomials of degree 2, variables $x(t)$ and $y(t)$ in V_t and parameters a, b, c , in V with $P_1 = ax^2 + bxy + cx$ and $P_2 = axy + by^2 + cy$. With basis $(x^2, xy, y^2, x, y, 1)$ of $\mathbb{R}_2[x, y]$ and $(x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$ of $\mathbb{R}_3[x, y]$, the matrix M_D is at the left below

$$M_D = \begin{pmatrix} 2a & 0 & 0 & 0 & 0 & 0 \\ 2b & 2a & 0 & 0 & 0 & 0 \\ 0 & 2b & 2a & 0 & 0 & 0 \\ 0 & 0 & 2b & 0 & 0 & 0 \\ 2c & 0 & 0 & a & 0 & 0 \\ 0 & 2c & 0 & b & a & 0 \\ 0 & 0 & 2c & 0 & b & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$L_T = \begin{pmatrix} t_1 & 0 & 0 & 0 & 0 & 0 \\ t_2 & t_1 & 0 & 0 & 0 & 0 \\ t_3 & t_2 & t_1 & 0 & 0 & 0 \\ 0 & 0 & t_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & t_1 & 0 & 0 \\ 0 & t_3 & 0 & t_2 & t_1 & 0 \\ 0 & 0 & t_3 & 0 & t_2 & 0 \\ 0 & 0 & 0 & t_3 & 0 & t_1 \\ 0 & 0 & 0 & 0 & t_3 & t_2 \\ 0 & 0 & 0 & 0 & 0 & t_3 \end{pmatrix}$$

Here the polynomial T we use for scaling must be of degree 1. Hence $T(x, y) = t_1x + t_2y + t_3z$ where t_1, t_2, t_3 are unknown parameters that will be assigned values in order to guarantee the existence and generation of invariants. The associated matrix L_T of the T -multiplication morphism has the form depicted at the right above. Then taking $T(x, y) = 2ax + 2by + 2c$, i.e. $t_1 = 2a, t_2 = 2b$ and $t_3 = 2c$ one verifies that the matrix $M_D - L_T$ has its second and third columns equal to zero. Hence, the rank of $M_D - L_T$ is less than 4, and our existence theorem for any given initial values applies. \square

Example 7.4. Consider the following differential rules:

$$\begin{bmatrix} \dot{x}(t) = x^2(t) + x(t)y(t) - x(t)z(t) \\ \dot{y}(t) = 2x(t)y(t) + y^2(t) \\ \dot{z}(t) = z(t)y(t) - 2z^2(t) \end{bmatrix}. \quad (15)$$

The method gives $x^2(t) - y(t)z(t) - x_0 = 0$ as an inductive invariant with polynomial scaling $T = 2(x + y - z)$, and with $x_0 = x(0)$ as an initial parameter. \square

Table 1 summarizes the type of linear algebraic problems associated with each consecution approximation. The last column gives some existential results that could be reused by any constraint-based approach or reachability analysis.

In Table 2 we list some experimental results. More recent approaches have been constraint-based [9, 10, 11, 12, 13]. In these approaches, the local differential systems are seen as varieties and their algebraic assertions and their induced ideal J . First, the Gröbner bases of J is computed. Then, a candidate invariant Q is considered. Next, Q is taken with a fixed degree and unknown parametric coefficients, i.e., it is a template form that can be understood as the target invariant to be generated. Then, the normal form reduction $NF_G(Q)$ of G over Q is obtained in order to generate a system ($NF_G(Q) = 0$) of equations encoding the conditions for invariance, resulting in constraints on the unknown coefficients whose solutions yield invariants. Each single computation step, i.e., computations of Gröbner bases, normal form reductions of the template and the resolution of the constraints, require a high numbers of operations, and are of double exponential complexity. Moreover the set of constraints they generate remains non-linear when the local continuous rules are non-linear differential systems. Even for linear local continuous rules, the constraints generated could form a very complex non-linear differential system which makes their resolution intractable. In terms of performance and efficiency, our techniques have few computational

Table 1: Linear algebraic problems and consecution approximations

Aprox.Consec.	Lin. Alg. Prob.	Existence Conditions
Strong	nullspaces	$\text{Ker}(M_D) \neq \emptyset$ or (see [27]) $\exists(Q_1, \dots, Q_n) \in \text{Syz}(P_1, \dots, P_n)$, s.t. $\partial_i Q_j = \partial_j Q_i$
Lambda	eigenspaces	$\text{Ker}(M_D) \geq 2$ for any init. cond., and $\text{Ker}(M_D) \neq \emptyset$ otherwise.
Polynomial	nullspaces	$\text{Ker}(M_D - L_T) \geq 2$ for any init. cond., and $\text{Ker}(M_D - L_T) \neq \emptyset$ otherwise.

steps of polynomial complexity: we compute first some specific matrices and we then compute their nullspaces. Further, our approaches do not generate an invariant at a time. Instead we generate the basis of a vector space providing us with an ideal of invariants (an infinite structure). Moreover, as one of the main results, we provide very general sufficient conditions allowing for the existence and computation of invariant ideals. Note that these conditions could be directly used by any invariant generation method.

8 Handling algebraic discrete transition systems

In this section we treat discrete transitions by extending and adapting our previous work on loop invariant generation for discrete programs [31, 30]. We also consider discrete transitions that are part of connected components and circuits, thus generalizing the case for simple propagation. We recall that V_k denotes the subspace of $\mathbb{R}[X_1, \dots, X_n]$ of degree at most k .

Definition 8.1. *Let $\tau = \langle l_i, l_j, \rho_\tau \rangle$ be a transition in \mathcal{T} and let η be an algebraic inductive map with $\eta(l_i) \equiv (P_\eta(X_1, \dots, X_n) = 0)$ and $\eta(l_j) \equiv (P'_\eta(X_1, \dots, X_n) = 0)$.*

- *Then η satisfies a Fractional-scale consecution for τ if and only if there exists a multivariate fractional $\frac{T}{Q}$ such that $\rho_\tau \models (P_\eta(X'_1, \dots, X'_n) - \frac{T}{Q}P_\eta(X_1, \dots, X_n) = 0)$. We also say that P_η is a $\frac{T}{Q}$ -scale discrete invariant.*
- *Then η satisfies a Polynomial-scale consecution for τ if and only if there exists a multivariate polynomial T such that $\rho_\tau \models (P_\eta(X'_1, \dots, X'_n) - TP_\eta(X_1, \dots, X_n) = 0)$. We also say that P_η is a polynomial-scale and a T -scale discrete invariant.*

8.1 Discrete transition with polynomial systems

Consider an algebraic transition system:

$$\rho_\tau \equiv [X'_1 = P_1(X_1, \dots, X_n), \dots, X'_n = P_n(X_1, \dots, X_n)],$$

where the P_i 's are in $\mathbb{R}[X_1, \dots, X_n]$. We have the following T -scale discrete invariant characterization.

Table 2: Experimental results: Basis of invariant ideals obtained automatically by our prototype. All examples are treated in Section 4.1, Section 4.2, Section 5 and Section 7

Differential Systems.	Scaling	CPU/s
See Section 7, system 14.	<i>Polynomial</i>	1.12
See Section 7, system 13.	<i>Polynomial</i>	2.04
See Section 7, system 15.	<i>Polynomial</i>	0.34
See Section 7, systems 11.	<i>Polynomial</i>	98.49
See Section 5, system 10.	<i>Polynomial</i>	0.43
See Section 4.2, system 9.	<i>Lambda</i>	2.48
See Section 4.1, system 6.	<i>Strong</i>	0.02
See Section 7, systems 12.	<i>Strong</i>	1.29
See Section 4.1, system 4.	<i>Lambda</i>	0.03
See Section 4.1, system 7	<i>Strong</i>	15.90
See Section 4.2, system 8	<i>Lambda</i>	1.04
From [33] Ex.6.	<i>Polynomial</i>	2.4
From [28] Ex.1.	<i>Polynomial</i>	0.35
From [26]	<i>Polynomial</i>	10.1
From [26] Ex.2.	<i>Polynomial</i>	0.45
From [27] Ex.2.	<i>Lambda</i>	2.5
From [33]	<i>Strong</i>	0.2
From [26]. Ex.4.	<i>Strong</i>	1.3
From [33]. Ex.4.	<i>Lambda</i>	0.05
From [33].	<i>Lambda</i>	1.06
From [27].	<i>Strong</i>	6.80

Theorem 8.1. *A polynomial Q in $\mathbb{R}[X_1, \dots, X_n]$ is a T -scale discrete invariant for polynomial-scale consecution with parametric polynomial $T \in \mathbb{R}[X_1, \dots, X_n]$ for τ if and only if*

$$Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = T(X_1, \dots, X_n)Q(X_1, \dots, X_n).$$

If $Q \in \mathbb{R}[X_1, \dots, X_n]$ is of degree r and the maximal degree of the P_i 's is d , then we are looking for a T of degree $e = dr - r$. Write its ordered coefficients as $\lambda_0, \dots, \lambda_s$, with $s + 1$ being the number of monomials of degree inferior to e . Let M be the matrix, in the canonical basis of V_r and V_{dr} , of the morphism \mathcal{M} from V_r to V_{dr} given by $Q(X_1, \dots, X_n) \mapsto Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n))$. Let L be the matrix, in the canonical basis of V_r and V_{dr} , of the morphism \mathcal{L} from V_r to V_{dr} given by $P \mapsto TP$. Matrix L will have a very simple form: its non zero coefficients are the λ_i 's, and it has a natural block decomposition. Now let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a T -scale discrete invariant for a transition relation defined by the P_i 's. Then

$$\begin{aligned} Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) &= T(X_1, \dots, X_n)Q(X_1, \dots, X_n) \\ \Leftrightarrow \mathcal{M}(Q) &= \mathcal{L}(Q) \\ \Leftrightarrow (\mathcal{M} - \mathcal{L})(Q) &= 0_{\mathbb{R}[X_1, \dots, X_n]} \\ \Leftrightarrow Q &\in \text{Ker}(M - L). \end{aligned}$$

A T -scale discrete invariant is nothing else than a vector in the kernel of $M - L$. Our problem is equivalent to finding a L such that $M - L$ has a non trivial kernel.

Theorem 8.2. *Consider M as described above. Then, (i) there will be a T -scale discrete invariant if and only if there exists a matrix L (corresponding to $P \mapsto TP$) such that $M - L$ has a nontrivial kernel. Further, any vector in the kernel of $M - L$ will give a T -scale invariant polynomial; (ii) there will be a non trivial inductive invariant if and only if there exists a matrix L such that the intersection of the kernel of $M - L$ and the hyperplane given by the initial values is not zero. The invariants correspond to vectors in the intersection; and (iii) if $\dim(\text{Ker}(M - L)) \geq 2$, then the basis of $\text{Ker}(M - L)$ is a basis for non trivial inductive invariants, whatever the initial conditions.*

Example 8.1. (Running example) *Let's consider the following transition:*

$$\tau = \langle l_i, l_j, \rho_\tau \equiv [x' = xy + x ; y' = y^2] \rangle.$$

Step 1: *We build matrix $M - L$. The maximal degree of the system ρ_τ is $d = 2$ and the T -scale invariant will be of degree $r = 2$. Then, T is of degree $e = dr - r = 2$ and we write $\lambda_0, \dots, \lambda_5$ as its ordered coefficients i.e. its canonical form is $T = \lambda_0 x^2 + \lambda_1 xy + \lambda_2 y^2 + \lambda_3 x + \lambda_4 y + \lambda_5$. Consider the associated morphisms \mathcal{M} and \mathcal{L} from $\mathbb{R}_2[x, y]$ to $\mathbb{R}_4[x, y]$. Using the basis*

$$C_1 = (x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_2[x, y]$ and the basis

$$C_2 = (x^4, yx^3, y^2x^2, y^3x, y^4, x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$$

of $\mathbb{R}_4[x, y]$, our algorithm compute the matrix $M - L$ as

$$M - L = \begin{pmatrix} -\lambda_0 & 0 & 0 & 0 & 0 & 0 \\ -\lambda_1 & -\lambda_0 & 0 & 0 & 0 & 0 \\ 1 - \lambda_2 & -\lambda_1 & -\lambda_0 & 0 & 0 & 0 \\ 0 & 1 - \lambda_2 & -\lambda_1 & 0 & 0 & 0 \\ 0 & 0 & 1 - \lambda_2 & 0 & 0 & 0 \\ -\lambda_3 & 0 & 0 & -\lambda_0 & 0 & 0 \\ 2 - \lambda_4 & -\lambda_3 & 0 & -\lambda_1 & -\lambda_0 & 0 \\ 0 & 1 - \lambda_4 & -\lambda_3 & -\lambda_2 & -\lambda_1 & 0 \\ 0 & 0 & -\lambda_4 & 0 & -\lambda_2 & 0 \\ 1 - \lambda_5 & 0 & 0 & -\lambda_3 & 0 & -\lambda_0 \\ 0 & -\lambda_5 & 0 & 1 - \lambda_4 & -\lambda_3 & -\lambda_1 \\ 0 & 0 & -\lambda_5 & 0 & 1 - \lambda_4 & -\lambda_2 \\ 0 & 0 & 0 & 1 - \lambda_5 & 0 & -\lambda_3 \\ 0 & 0 & 0 & 0 & -\lambda_5 & -\lambda_4 \\ 0 & 0 & 0 & 0 & 0 & 1 - \lambda_5 \end{pmatrix}.$$

Step 2: *We then reduce the rank of $M - L$ by assigning values to the λ_i 's. Our procedure fixes $\lambda_0 = \lambda_1 = \lambda_3 = 0$, $\lambda_2 = \lambda_5 = 1$ and $\lambda_4 = 2$, so that $T(x, y) = y^2 + 2y + 1$. The first column of $M - L$ becomes zero and the second column is equal to the fourth. Hence, the rank of $M - L$ is less than 4 and its kernel has dimension at least 2. Any vector in this kernel will be a T -invariant.*

Step 3: *Now matrix $M - L$ satisfies the hypotheses of Theorem 8.2(iii). So, there will always be invariants, whatever the initial values. We compute the basis of $\text{Ker}(M - L)$. Our prototype `Ideal_Inv_Gen` outputs:*

Polynomial scaling discrete step

$$T(x,y) = y^2 + 2y + 1$$

Module of degree 6 and rank 3 and Kernel of dimension 3

$$\{\{1, 0, 0, 0, 0, 0\}, \{0, 1, 0, -1, 0, 0\}, \{0, 0, 1, 0, -2, 1\}\}$$

The vectors of the basis are interpreted in the canonical basis C_1 of $\mathbb{R}_2[x, y]$:

Basis of invariant Ideal

$$\{x^2, xy - x, y^2 - 2y + 1\}$$

We thus obtained an ideal of non trivial inductive invariants. In other words, for all $G_1, G_2, G_3 \in \mathbb{R}[x, y]$, $(G_1(x, y)(x^2) + G_2(x, y)(xy - x) + G_3(x, y)(y^2 - 2y + 1) = 0)$ is an inductive invariant. For instance, consider the initial step $(y = y_0, x = 1)$. An invariant is $y_0(1 - y_0)x^2 + xy - x + y^2 - 2y + 1 = 0$. \square

8.2 Discrete transition with fractional systems

We now want to deal with transition systems ρ_τ of the following type:

$$[X'_1 = P_1(X_1, \dots, X_n)/Q_1(X_1, \dots, X_n), \dots, X'_n = P_n(X_1, \dots, X_n)/Q_n(X_1, \dots, X_n)],$$

where the P_i 's and Q_i 's belong to $\mathbb{R}[X_1, \dots, X_n]$ and P_i is relatively prime to Q_i . One need to relax the consecution conditions to fractional-scale as soon as fractions appear in the transition relation.

Theorem 8.3. (*F-scale inv. charac.*) *A polynomial Q in $\mathbb{R}[X_1, \dots, X_n]$ is a F-scale invariant for fractional discrete scale consecution with a parametric fractional $F \in \mathbb{R}(X_1, \dots, X_n)$ for τ if and only if $Q\left(\frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n}\right) = FQ$.*

Let d be the maximal degree of the P_i 's and Q_i 's, and let Π be the least common multiple (lcm) of the Q_i 's. Further, suppose that we are looking for a F -invariant Q of degree r . Let \mathcal{M} be the morphism of vector spaces

$$Q \mapsto \Pi^r Q(P_1/Q_1, \dots, P_n/Q_n)$$

from V_r to V_{nrd} , and let M be its matrix in a canonical basis. Let T be a polynomial in V_{nrd-r} , let \mathcal{L} denote the morphism of vector spaces

$$Q \mapsto TQ$$

from V_r to V_{nrd} , with L its matrix in a canonical basis. As we show in the following theorem, our problem is equivalent to finding a L such that $M - L$ has a non trivial kernel.

Theorem 8.4. *Consider M and L as described above. Then,*

(i) *there exists F-scale invariants (with F is of the form T/Π^r) if and only if there exists a matrix L such that*

$$Ker(M - L) \neq \emptyset.$$

In this situation, any vector in the kernel of $M - L$ will give a F-scale discrete invariant;
 (ii) *we have a non trivial invariant if and only if there exists a matrix L such that the*

intersection of the kernel of $M - L$ and the hyperplane given by the initial values is not zero, the invariants will correspond to vectors in the intersection; and
 (iii) we will have a non-trivial invariant for any non-trivial initial value if there exists a matrix L such that

$$\dim(\text{Ker}(M - L)) \geq 2.$$

Example 8.2. Consider the system

$$\rho_\tau \equiv [x'_1 = x_2/(x_1 + x_2) ; x'_2 = x_1/(x_1 + 2x_2)].$$

We are looking for a F -scale invariant polynomial of degree two. The lcm of $(x_1 + x_2)$ and $(x_1 + 2x_2)$ is their product, so that \mathcal{M} is given by: $[Q \in V_2 \mapsto [(x_1 + x_2)(x_1 + 2x_2)]^2 Q(x_1/(x_1 + x_2), x_2/(x_1 + 2x_2))]$. As both $x_2/(x_1 + x_2)$ and $x_1/(x_1 + 2x_2)$ have “degree” zero, $[(x_1 + x_2)(x_1 + 2x_2)]^2 Q(x_2/(x_1 + x_2), x_1/(x_1 + 2x_2))$ will be a linear combination of degree four, if it is non null. Hence, \mathcal{M} has values in $\text{Vect}(x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4)$. For T and Q in V_2 to verify $[(x_1 + x_2)(x_1 + 2x_2)]^2 Q(x_2/(x_1 + x_2), x_1/(x_1 + 2x_2)) = TQ$, as the left member is in $\text{Vect}(x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4)$, T must be of the form $\lambda_0x_1^2 + \lambda_1x_1x_2 + \lambda_2x_2^2$ and Q of the form $a_0x_1^2 + a_1x_1x_2 + a_3x_2^2$. We see that we can take Q in $\text{Vect}(x_1^2, x_1x_2, x_2^2)$, and similarly for T . Then both $\mathcal{M}, \mathcal{L} : (Q \mapsto TQ)$ will be morphisms from $\text{Vect}(x_1^2, x_1x_2, x_2^2)$ in $\text{Vect}(x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2^4)$. In the corresponding canonical basis, the matrix $M - L$ is

$$M - L = \begin{pmatrix} -\lambda_0 & 0 & 1 \\ -\lambda_1 & 1 - \lambda_0 & 2 \\ 1 - \lambda_2 & 3 - \lambda_1 & 1 - \lambda_0 \\ 4 & 2 - \lambda_2 & -\lambda_1 \\ 4 & 0 & -\lambda_2 \end{pmatrix}.$$

Taking $\lambda_0 = 1, \lambda_1 = 3$ and $\lambda_2 = 2$ cancels the second column. Hence, the kernel equals $\text{Vect}(0, 1, 0)$. Now, Theorem 8.4(iii) applies to $M - L$. We get from our prototype:

```
Fractional scaling discrete step
T(x,y) / Q(x,y) = 1 / ((x + y) (x + 2 y))^2
Module of degree 3 and rank 1 and Kernel of dimension 2
{0, 1, 0}
Basis of invariant Ideal
{ x y }
```

It was clear from the beginning that the corresponding polynomial x_1x_2 is $1/[(x_1 + x_2)(x_1 + 2x_2)]^2$ -scale invariant. For instance, it is an invariant for the initial values $(0, 1)$. Moreover, it clearly never cancels $x_1 + x_2$ and $x_1 + 2x_2$, because they are of the form $(a, 0)$ or $(0, b)$ with a and b strictly positive. \square

9 Putting it all together: Global invariants

In the previous sections and in Section 8 we have shown how to handle continuous and discrete consecution conditions and how to generate ideals of invariants for each location. To be more precise, we thus generated a basis of a vector space which describes invariants for each location, transitions and initial conditions. A global invariant would be any invariant which is in the intersection of these three vector spaces. In this way, we avoid the definition

of a single isomorphism for the whole hybrid system. Instead, we generate the basis for each separate consecution condition. To compute the basis of global invariants, we could use Theorem 9.1. It proposes to *multiply* all the elements of each computed basis. By so doing, we also avoid the heavy computation of ideal intersections. This approach is a sound, but not complete, way of computing ideals for global hybrid invariants, and it has a low computational complexity.

Theorem 9.1. *Let W be a hybrid system and let l be one of its locations. Let $I = \{I_1, \dots, I_k\}$ a set of ideals in $\mathbb{R}[X_1, \dots, X_n]$ such that $I_j = (f_{n_1}^{(j)}, \dots, f_{n_j}^{(j)})$ where $j \in [1, k]$. Let $\otimes(I_1, \dots, I_k) = \{\delta_1, \dots, \delta_{n_1 n_2 \dots n_k}\}$ be such that all elements δ_i in $\otimes(I_1, \dots, I_k)$ are formed by the product of one element from each ideal in I . Assume that the I_j 's are collections of invariant ideals associated to $\mathcal{S}(l)$, its differential rule $\mathcal{C}(l)$, its local conditions, and all invariant ideals generated considering incoming transitions at l . Then $\otimes(I_1, \dots, I_k)$ is a non-trivial invariant ideal for location l . \square*

Corollary 9.1. *Let l be a state and let $\mathcal{C}(l) \equiv (P_i(x_1, \dots, x_n) < 0)$ be its semi-algebraic local conditions and Q be an inductive invariant for its differential rule $\mathcal{D}(l)$, and all ideals of invariants generated considering all incoming transitions at l . Then $(P_i(x_1, \dots, x_n) - Q(x_1, \dots, x_n) < 0)$ is an inductive invariant. \square*

Semi-algebraic local state conditions, as well as initiation and transition guards are assertions of the form $(P_i(x_1, \dots, x_n) < 0)$ with $P_i \in K[x_1, \dots, x_n]$. Then, we obtain an operator, similar to the one introduced in Theorem 9.1, to generate ideals of non-trivial invariants at a state l with semi-algebraic local conditions. We can then generate ideals of non-trivial semi-algebraic invariants.

10 Conclusions

It is presently established in industry and academia that reasoning about non-linear differential systems is a critical bottleneck for automated verification and static analysis of hybrid systems. In this article, we introduced new symbolic techniques with fast numerical computations. In terms of performance and efficiency, we succeeded in reducing the invariant generation problem for non-linear hybrid systems to linear algebraic problems, *i.e.* to the computation of eigenspaces of specific morphisms. We proposed a method of lower complexity than previous modern approaches based on fixed point computation and constraint-based approaches. Each computational step required by our techniques remains of polynomial complexity. We compute first specific matrices and then we compute their nullspaces.

We can also handle non-linear hybrid systems, extended with parameters and variables that are functions of time. We note that these type of hybrid system are still not treated by other state-of-the-art invariant generation methods. Instead of generating an invariant at a time, our approaches are capable of computing an ideal of invariants which is an enormous, *i.e.* infinite, structure. Our algorithm embodies a strategy to guess the degree bounds which allow the non-triviality of the computed invariants.

It is also important to emphasize that the very general sufficient conditions allowing for the existence and computation of invariant ideals provided in this work could also be directly used by any constraint-based invariant generation method [10, 9, 13, 12], or by any analysis methods based on over-approximations and reachability [38, 25, 39].

The examples discussed are beyond other current state-of-the-art approaches, and illustrate the strength of our methods.

References

- [1] T. Henzinger, The theory of hybrid automata, in: Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science (LICS '96), New Brunswick, New Jersey, 1996, pp. 278–292.
- [2] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P. h. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, The algorithmic analysis of hybrid systems, *Theoretical Computer Science* 138 (1995) 3–34.
- [3] Z. Manna, *Mathematical Theory of Computation*, McGraw-Hill, 1974.
- [4] A. Tiwari, H. Rueß, H. Saïdi, N. Shankar, A technique for invariant generation, in: TACAS: Proc. of the 7th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems, 2001.
- [5] P. Cousot, R. Cousot, Abstract interpretation and application to logic programs, *Journal of Logic Programming* 13 (2–3) (1992) 103–179.
- [6] P. Cousot, R. Cousot, Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints, in: Conf. Record of the 4th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, ACM Press, NY, Los Angeles, California, 1977, pp. 238–252.
- [7] T. A. Henzinger, P.-H. Ho, Hytech: The cornell hybrid technology tool, in: *Hybrid Systems*, 1994, pp. 265–293.
- [8] J. Bengtsson, K. G. Larsen, F. Larsson, P. Pettersson, W. Yi, Uppaal - a tool suite for automatic verification of real-time systems, in: *Hybrid Systems*, 1995, pp. 232–243.
- [9] S. Sankaranarayanan, H. Sipma, Z. Manna, Constructing invariants for hybrid system, in: *Hybrid Systems: Computation and Control HSCC*, Vol. 2993 of LNCS, Springer, 2004, pp. 539–554.
- [10] S. Gulwani, A. Tiwari, Constraint-based approach for analysis of hybrid systems, in: Proc. of the 14th Int. Conf. on Computer Aided Verification CAV, 2008.
- [11] S. Prajna, A. Jadbabaie, Safety verification of hybrid systems using barrier certificates (2004).

- [12] A. Tiwari, Generating box invariants, in: Proc. of the 11th Int. Conf. on Hybrid Systems: Computation and Control HSCC, 2008.
- [13] S. Sankaranarayanan, T. Dang, F. Ivancic, Symbolic model checking of hybrid systems using template polyhedra, in: 14th Int. Conf. Tools and Algorithms for the Construction and Analysis of Systems TACAS, 2008.
- [14] B. Buchberger, Symbolic computation: Computer algebra and logic, in: Frontiers of Combining Systems: Proceedings of the 1st Int. Workshop, Munich (Germany), 1996, pp. 193–220.
- [15] V. Weispfenning, Quantifier elimination for real algebra - the quadratic case and beyond, *Applicable Algebra in Engineering, Communication and Computing* 8 (2) (1997) 85–101.
- [16] G. E. Collins, *Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition*, LNCS, 1975.
- [17] C. Borralleras, S. Lucas, R. Navarro-Marset, E. Rodriguez-Carbonell, A. Rubio, Solving non-linear polynomial arithmetic via sat modulo linear arithmetic, *CADE (2009)* 294–305.
- [18] M. Fränzle, C. Herde, T. Teige, S. Ratschan, T. Schubert, Efficient solving of large non-linear arithmetic constraint systems with complex boolean structure., *JSAT* 1 (3-4) (2007) 209–236.
- [19] A. Tiwari, G. Khanna, Nonlinear systems: Approximating reach sets, in: *Hybrid Systems: Computation and Control HSCC*, Vol. 2993 of LNCS, Springer, 2004, pp. 600–614.
- [20] E. Rodriguez-Carbonell, A. Tiwari, Generating polynomial invariants for hybrid systems, in: *Hybrid Systems: Computation and Control, HSCC 2005*, Vol. 3414 of LNCS, 2005, pp. 590–605.
- [21] T. A. Henzinger, P. -H. Ho, Algorithmic analysis of nonlinear hybrid systems, in: *Proc. of the 7th Inter. Conf. On Computer Aided Verification*, Vol. 939, 1995, pp. 225–238.
- [22] A. Bauer, M. Pister, M. Tautschnig, Tool-support for the analysis of hybrid systems and models, in: *DATE '07: Proceedings of the conference on Design, automation and test in Europe*, EDA Consortium, San Jose, CA, USA, 2007, pp. 924–929.
- [23] M. Fränzle, C. Herde, Hysat: An efficient proof engine for bounded model checking of hybrid systems, *Form. Methods Syst. Des.* 30 (3) (2007) 179–198.
- [24] B. Akbarpour, L. C. Paulson, Applications of metitarski in the verification of control and hybrid systems, in: *HSCC '09: Proc. of the 12th Inter. Conf. on Hybrid Systems: Computation and Control*, Springer-Verlag, Berlin, Heidelberg, 2009, pp. 1–15.

- [25] A. Platzer, E. M. Clarke, Computing differential invariants of hybrid systems as fixed-points, in: *Computer-Aided Verification, CAV 2008*, Princeton, USA, Proceedings, LNCS, Springer, 2008.
- [26] N. Matringe, A. V. Moura, R. Rebiha, Generating invariants for non-linear hybrid systems by linear algebraic methods, in: *17th Int. Static Analysis Symposium, SAS2010*, LNCS, 2010.
- [27] N. Matringe, A. V. Moura, R. Rebiha, Morphisms for non-trivial non-linear invariant generation for algebraic hybrid systems, in: *12th Int. Conf. Hybrid Systems: Computation and Control (HSCC2009)*, LNCS, 2009.
- [28] N. Matringe, A. V. Moura, R. Rebiha, Morphisms for analysis of hybrid systems, in: *ACM/IEEE Cyber-Physical Systems CPSWeek'09, Second International Workshop on Numerical Software Verification.(NSV2009) Verification of Cyber-Physical Software Systems*, San Francisco, CA, USA, 2009.
- [29] R. Rebiha, A. V. Moura, N. Matringe, Transcendental inductive invariants generation for non-linear differential and hybrid systems, in: *15th International ACM Conference in Hybrid Systems: Computation and Control (HSCC2012) and ACM/IEEE Cyber-Physical Systems CPSWeek'12*, ACM/IEEE, Beijing/Pequim, China, 2012.
- [30] N. Matringe, A. V. Moura, R. Rebiha, Endomorphisms for non-trivial non-linear loop invariant generation, in: *5th Int. Conf. Theoretical Aspects of Computing*, LNCS, 2008, pp. 425–439.
- [31] N. Matringe, A. V. Moura, R. Rebiha, Endomorphism for non-trivial semi-algebraic loop invariant generation, Tech. Rep. TR-IC-08-31, Institute of Computing, University of Campinas (November 2008).
- [32] S. Sankaranarayanan, Automatic invariant generation for hybrid systems using ideal fixed points, in: *HSCC '10: Proc. of the 13th ACM Int. Conf. on Hybrid systems: computation and control*, ACM, 2010, pp. 221–230.
- [33] N. Matringe, A. V. Moura, R. Rebiha, Morphisms for non-trivial non-linear invariant generation for algebraic hybrid systems, Tech. Rep. TR-IC-08-32, Institute of Computing, University of Campinas (November 2008).
- [34] S. Sankaranarayanan, H. B. Sipma, Z. Manna, Constructing invariants for hybrid systems, *Form. Methods Syst. Des.* 32 (1) (2008) 25–55.
- [35] A. Kreuzer, L. Robbiano, *Computational commutative algebra*, Springer Verlag, 2005.
- [36] S. Lang, *Algebra*, Springer, 2002.
- [37] C. Tomlin, G. J. Pappas, S. Sastry, Conflict resolution for air traffic management: a study in multiagent hybrid systems, *Automatic Control, IEEE Transactions on* 43 (4) (1998) 509–521.

- [38] C. Piazza, M. Antoniotti, V. Mysore, A. Policriti, F. Winkler, B. Mishra, Algorithmic Algebraic Model Checking I: Challenges from Systems Biology, Vol. 3576, 2005.
- [39] N. Ramdani, N. Meslem, Y. Candau, Reachability of uncertain nonlinear systems using a nonlinear hybridization, in: Hybrid Systems: Computation and Control, HSCC'08, Vol. 4981, LNCS, 2008, pp. 415–428.

A Proofs for Section 3

Proof of Theorem 3.1

Suppose that $Q \in \mathbb{R}[X_1, \dots, X_n]$ is such an invariant. Then if $(X_1(t), \dots, X_n(t))$ is a solution of (S) then, by the definition of P -scale invariant, one would have $D_Q(P_1, \dots, P_n, X_1, \dots, X_n) = PQ(X_1, \dots, X_n)$. Denote by $f(t)$ the function $Q(X_1(t), \dots, X_n(t))$. Then we get $\dot{f}(t) = P(X_1(t), \dots, X_n(t))f(t)$. Call $R(t)$ an anti-derivative of $P(X_1(t), \dots, X_n(t))$. Then f must be of the form $t \mapsto \lambda e^{R(t)}$ for some scalar λ . Now taking into account the initial conditions, if $Q(x_0, \dots, x_n) = 0 \Leftrightarrow f(0) = 0$, then λ must be zero. Hence, $f(t) = Q(X_1(t), \dots, X_n(t))$ is the zero function, and Q is an invariant of (S) .

Proof of Theorem 3.2

Consider polynomial-scale consecution. The system $\{\dot{x} = ax(t); \dot{y} = ay(t) + bx(t)y(t)\}$ could be cited as counter-example for completeness as its invariants are not P -scale differential invariants.

B Proofs for Section 4

Proof of Lemma 4.1

Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a polynomial such that

$$D_Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n), X_1, \dots, X_n) = 0.$$

then $dQ/dt = 0$ and Q is a strong invariant as $\frac{dX_i(t)}{dt} = P_i(X_1, \dots, X_n)$ for all i in $[1, n]$ and by construction of D_Q .

Proof of Theorem 4.1

Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a polynomial. Then

$$\begin{aligned} (\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = 0) &\Leftrightarrow (D(Q) = 0_{K[X_1, \dots, X_n]}) \\ &\Leftrightarrow (Q \in \text{Ker}(M_D)). \end{aligned}$$

Using the definition of an invariant and Lemma 4.1, we can see that Q will be a strong-scale invariant if and only if it is in the kernel of M_D .

Proof of Theorem 4.2

We first consider Theorem 4.1. The initiation step defines on $\mathbb{R}_r[x_1, \dots, x_n]$ a linear form on

this space, namely, $I_u : P \mapsto P(u_1, \dots, u_n)$. Hence, initial values correspond to a hyperplane of $\mathbb{R}_r[X_1, \dots, X_n]$ given by the kernel I_u , which is $\{Q \in \mathbb{R}_r[X_1, \dots, X_n] \mid Q(u_1, \dots, u_n) = 0\}$. If we add initial conditions of the form $(x_1(0) = u_1, \dots, x_n(0) = u_n)$, we are looking for a *strong-scale* differential invariant in $\mathbb{R}_r[x_1, \dots, x_n]$ that belongs to the hyperplane $P(u_1, \dots, u_n) = 0$, *i.e.*, we are looking for Q in $\ker(M_D) \cap \{P \mid P(u_1, \dots, u_n) = 0\}$.

Proof of Corollary 4.1

(\Rightarrow) If there is a non-trivial strong-scale invariant for any initial value, then the corresponding kernel has dimension at least 2. Indeed, if the space was of dimension only 1 (which is at least necessary to have strong-invariants), taking any non-zero vector Q in the kernel (*i.e.* a strong-invariant), Q should lie in any hyperplane of initial values, *i.e.* for every n -tuple (u_1, \dots, u_n) , one would have $Q(u_1, \dots, u_n) = 0$, *i.e.* $Q = 0$, which is absurd.

(\Leftarrow) A kernel of M_D with dimension at least 2 will intersect any space, or semi-hyperplane, given by any initial constraints.

Proof of Lemma 4.2

We treat the case of two variables, the case of n variables being a straight generalization. Suppose that $\partial_i Q_j = \partial_j Q_i$ for each pair (i, j) . We choose a polynomial Q^1 , an anti-derivative of Q_1 with respect to x_1 . Now $\partial_1(\partial_2 Q^1) = \partial_2(\partial_1 Q^1) = \partial_2 Q_1 = \partial_1 Q_2$. Hence $\partial_1(\partial_2 Q^1 - Q_2) = 0$, and so $\partial_2 Q^1 = Q_2 + b(x_2, \dots, x_n)$ for some function b of (x_2, \dots, x_n) which is actually a polynomial. Choosing an anti-derivative $B(x_2, \dots, x_n)$ of $b(x_2, \dots, x_n)$ with respect to x_2 , one verifies that $Q_{1,2} = Q^1 - B(x_2, \dots, x_n)$ is such that $\partial_1 Q_{1,2} = Q_1$ and $\partial_2 Q_{1,2} = Q_2$. Now, $\partial_1 \partial_3 Q_{1,2} = \partial_3 \partial_1 Q_{1,2} = \partial_3 Q_1 = \partial_1 Q_3$, and $\partial_2 \partial_3 Q_{1,2} = \partial_2 Q_3$ as well. Hence, $\partial_3 Q_{1,2} - Q_3 = c(x_3, \dots, x_n)$ for a polynomial c . Taking C as an anti-derivative of c with respect to x_3 , one deduces that $Q_{1,2,3} = Q_{1,2} - C$ is such that $\partial_i Q_{1,2,3} = Q_i$ for $i = 1, 2, 3$. Repeating the process, we construct $Q_{1,\dots,n}$ such that $\partial_i Q_{1,\dots,n} = Q_i$, for $i = 1, 2, 3$.

Proof of Theorem 4.3

Immediate, using Lemma 4.2.

Proof of Lemma 4.3

Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a polynomial such that

$$D_Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n), X_1, \dots, X_n) = \lambda Q(X_1, \dots, X_n).$$

As $\frac{dX_i(t)}{dt} = P_i(X_1, \dots, X_n)$ for all i in $[1, n]$ and by construction of D_Q we obtain $\frac{dQ}{dt} = \lambda Q$. So, $\frac{dQ}{dt} - \lambda Q = 0$ and Q is a λ -scale invariant.

Proof of Theorem 4.4

$$\begin{aligned}
 (\mathcal{D}_Q(P_1, \dots, P_n, X_1, \dots, X_n) = \lambda Q(X_1, \dots, X_n)) &\Leftrightarrow \\
 (D(Q) = \lambda Id(Q)) &\Leftrightarrow \\
 ((D - \lambda Id)(Q) = 0_{\mathbb{R}[X_1, \dots, X_n]}) &\Leftrightarrow \\
 (Q \in Ker(D - \lambda Id)) &\Leftrightarrow \\
 (Q \in Ker(M_D - \lambda I)). &
 \end{aligned}$$

Using the definition of an invariant and Lemma 4.3, we can see that Q will be a strong-scale invariant if and only if it is in the kernel of M_D .

Proof of Theorem 4.5

It follows by a similar reasoning as the proof of Theorem 4.2. Thus we would looking at $ker(M_D - \lambda I) \cap \{P \mid P(u_1, \dots, u_n) = 0\}$.

Proof of Corollary 4.2

(\Rightarrow) If there is a λ -scale invariant for any initial value, then the corresponding eigenspace has dimension at least 2. Indeed, if the space was of dimension only 1 (which is at least necessary to have λ -invariants), taking any non-zero vector Q in the eigenspace (*i.e.* a λ -invariant), Q should lie in any hyperplane of initial values, *i.e.* for every n -tuple (u_1, \dots, u_n) , one would have $Q(u_1, \dots, u_n) = 0$, *i.e.* $Q = 0$, which is absurd.

(\Leftarrow) An eigenspace of M_D with dimension at least 2 will intersect any space, or semi-hyperplane, given by any initial constraints.

C Proofs for Section 5

Proof of Lemma 5.1

Let $Q \in \mathbb{R}[X_1, \dots, X_n]$ be a polynomial such that

$$D_Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n), X_1, \dots, X_n) = TQ(X_1, \dots, X_n).$$

As $\frac{dX_i(t)}{dt} = P_i(X_1, \dots, X_n)$ for all i in $[1, n]$ and by construction of D_Q we obtain $\frac{dQ}{dt} = TQ$. So, $\frac{dQ}{dt} - TQ = 0$ and Q is a T -scale invariant.

Proof of Theorem 5.1

The sketch of the proof is induced by the constructed linear algebraic reduction. Assume that there is an invariant Q in $\mathbb{R}_r[x_1, \dots, x_n]$ for differential polynomial-scale consecution corresponding to the differential system. And, there exists a polynomial T such that $Q(x_1, \dots, x_n) = T(x_1, \dots, x_n)Q(x_1, \dots, x_n)$. By definition, we have $D_Q(P_1, \dots, P_n, x_1, \dots, x_n) = TQ$ and then $D(Q) = \bar{T}(Q)$. In other words $(D - T)(Q) = 0$, *i.e.* $Q \in Ker(M_D - L_T)$ which means that $Ker(M_D - L_T) \neq \emptyset$. On the other hand if $Ker(M_D - L_T) \neq \emptyset$ then there exists a polynomial P such that $M_D(P) = L_T(P)$. By definition, $D(P) = \bar{T}(P)$ and $D_P(P_1, \dots, P_n, x_1, \dots, x_n) = TP$. In other words, $P(x_1, \dots, x_n) = T(x_1, \dots, x_n)P(x_1, \dots, x_n)$

and P is a T invariant in $\mathbb{R}_r[x_1, \dots, x_n]$ for differential polynomial-scale consecution corresponding to the differential system.

Proof of Theorem 5.2

From linear algebra, we know that $M_D - L_T$ with a non trivial kernel is equivalent to it having rank strictly less than the dimension $v(r)$ of $\mathbb{R}_r[x_1, \dots, x_n]$. This is equivalent to the fact that each $v(r) \times v(r)$ sub-determinant of $M_D - L_T$ is equal to zero. Those determinants are polynomials with variables $(t_1, \dots, t_{v(d-1)})$, which we will denote by $E_1(t_1, \dots, t_{v(d-1)}), \dots, E_s(t_1, \dots, t_{v(d-1)})$. From the form of L_T , this is zero when $(t_1, \dots, t_{v(d-1)}) = (0, \dots, 0)$. Hence, in this case, $M_D - L_T$ has its last column equal to zero, giving a common root for these polynomials, corresponding to the constant invariants.

Proof of Theorem 5.3

We first consider Theorem 5.1. The initiation step defines on $\mathbb{R}_r[x_1, \dots, x_n]$ a linear form on this space, namely, $I_u : P \mapsto P(u_1, \dots, u_n)$. Hence, initial values correspond to a hyperplane of $\mathbb{R}_r[X_1, \dots, X_n]$ given by the kernel I_u , which is $\{Q \in \mathbb{R}_r[X_1, \dots, X_n] \mid Q(u_1, \dots, u_n) = 0\}$. If we add initial conditions of the form $(x_1(0) = u_1, \dots, x_n(0) = u_n)$, we are looking for a T -scale differential invariant in $\mathbb{R}_r[x_1, \dots, x_n]$ that belongs to the hyperplane $P(u_1, \dots, u_n) = 0$, *i.e.*, we are looking for Q in $\ker(M_D - L_T) \cap \{P \mid P(u_1, \dots, u_n) = 0\}$.

Proof of Corollary 5.1

Considering T -scale invariant for any initial value and the kernel of $M_D - L_T$, it follows by a similar reasoning as the proof of Corollary 4.2.

D Proofs for Section 6

Proof of Corollary 6.1

The right singular vectors corresponding to vanishing singular values of \overline{M} span the null space of \overline{M} . The left singular vectors corresponding to the non-zero singular values of \overline{M} span the range of \overline{M} . As a consequence, the rank of \overline{M} equals the number of non-zero singular values which is the same as the number of non-zero elements in the matrix S .

E Proofs for Section 8

Proof of Theorem 8.1

If $Q(X'_1, \dots, X'_n) - TQ(X_1, \dots, X_n)$ belongs to the ideal I generated by the family $(X'_1 - P_1, \dots, X'_n - P_n)$, then there exists a family (A_1, \dots, A_n) of polynomials in $\mathbb{R}[X'_1, \dots, X'_n, X_1, \dots, X_n]$ such that $Q(X'_1, \dots, X'_n) - \lambda Q(X_1, \dots, X_n) = (X'_1 - P_1)A_1 + \dots + (X'_n - P_n)A_n$. Letting $X'_i = P_i$, we obtain that $Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = TQ(X_1, \dots, X_n)$.

Conversely let $Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = TQ(X_1, \dots, X_n)$. Then as $Q(X'_1, \dots, X'_n)$ is equal to $Q(P_1, \dots, P_n)$ modulo the ideal I , we get that $Q(X'_1, \dots, X'_n) = \lambda Q(X_1, \dots, X_n)$ modulo I .

Proof of Theorem 8.2

Claim (i): Let Q be a polynomial in $\mathbb{R}[X_1, \dots, X_n]$. In fact, a polynomial Q is T -invariant if and only if

$$Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = T(X_1, \dots, X_n)Q(X_1, \dots, X_n),$$

i.e. if and only if $\mathcal{M}(Q) = \mathcal{L}(Q) \Leftrightarrow (\mathcal{M} - \mathcal{L})(Q) = 0_{\mathbb{R}[X_1, \dots, X_n]}$. Using matrices we have $((M - L)Q = 0) \Leftrightarrow (Q \in \text{Ker}(M - L))$, and we are done.

Claim (ii): Consider Claim (i). It follows by a similar reasoning as the proof of Theorem 4.5.

Claim (iii): Considering T -scale discrete invariant for any initial value and the kernel of $M - L$, it follows by a similar reasoning as the proof of Corollary 4.2.

Proof of Theorem 8.3

If $Q(X'_1, \dots, X'_n) - FQ(X_1, \dots, X_n)$ belongs to the fractional ideal J generated by the family $(X'_1 - P_1/Q_1, \dots, X'_n - P_n/Q_n)$, then there exists a family (A_1, \dots, A_n) of fractional functions in $\mathbb{R}(X'_1, \dots, X'_n, X_1, \dots, X_n)$ such that $Q(X'_1, \dots, X'_n) - FQ(X_1, \dots, X_n) = (X'_1 - P_1/Q_1)A_1 + \dots + (X'_n - P_n/Q_n)A_n$. Letting $X'_i = \frac{P_i}{Q_i}$, we obtain that $Q(\frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n}) = \lambda Q(X_1, \dots, X_n)$. Conversely suppose $Q(\frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n}) = FQ(X_1, \dots, X_n)$, then as $Q(X'_1, \dots, X'_n)$ is equal to $Q(\frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n})$ modulo the ideal J , we get that $Q(X'_1, \dots, X'_n) = FQ(X_1, \dots, X_n)$ modulo J .

Proof of Theorem 8.4

Claim (i): Let Q be a polynomial in $\mathbb{R}[X_1, \dots, X_n]$. In fact, a polynomial Q is T/Π^r -invariant if and only if $Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = T/\Pi^r(X_1, \dots, X_n)Q(X_1, \dots, X_n)$, which is equivalent to

$$\Pi^r Q(P_1(X_1, \dots, X_n), \dots, P_n(X_1, \dots, X_n)) = T(X_1, \dots, X_n)Q(X_1, \dots, X_n),$$

i.e. if and only if $(\mathcal{M}(Q) = \mathcal{L}(Q)) \Leftrightarrow ((\mathcal{M} - \mathcal{L})(Q) = 0_{\mathbb{R}[X_1, \dots, X_n]})$. Writing this in equivalent terms of matrices: $((M - L)Q = 0) \Leftrightarrow (Q \in \text{Ker}(M - L))$, we get the statement of the theorem.

Claim (ii): Consider Claim (i). It follows by a similar reasoning as the proof of Theorem 4.5.

Claim (iii) : Considering F -scale discrete invariant for any initial value and the kernel of $M - L$, it follows by a similar reasoning as the proof of Corollary 4.2.

F Proofs for Section 9

Proof of Theorem 9.1

Let $f_1^{(j)}, \dots, f_{n_j}^{(j)}$ in $K[X_1, \dots, X_n]$ such that $I_j = (f_1^{(j)}, \dots, f_{n_j}^{(j)})$, for all j in $[1, k]$. Let $\beta \in (\otimes(I_1, \dots, I_k))$, then there exists $e_1, \dots, e_{n_1 n_2 \dots n_k}$ in $K[X_1, \dots, X_n]$ such that $\beta = e_1 \delta_1 + \dots + e_{n_1 n_2 \dots n_k} \delta_{n_1 n_2 \dots n_k}$. Also, by the construction of $\otimes(I_1, \dots, I_k)$ we know that for all $r \in [1, \dots, n_1 n_2 \dots n_k]$, $\delta_r \in \otimes(I_1, \dots, I_k)$, there is $(\alpha_1^{(r)}, \dots, \alpha_k^{(r)}) \in I_1 \times I_2 \times \dots \times I_k$ such that

$\delta_r = \prod_{i=0}^k \alpha_i^{(r)}$. Then we have $\beta = \sum_{j=1}^{n_1 n_2 \dots n_k} [\lambda_j \prod_{i=1}^k \alpha_i^{(j)}]$. Now, for all m in $[1, k]$, if I_m correspond to a pre-computed inductive ideal of invariants associated to one of the transition τ_m at the location l , then for all $j \in [1, n_1 n_2 \dots n_k]$, $\alpha_m^{(j)}(X_1, \dots, X_n) = 0$. And so for all $j \in [1, n_1 n_2 \dots n_k]$, $\prod_{i=1}^k \alpha_i^{(j)} = 0$. Finally we have $\beta(X_1, \dots, X_n) = 0$ for all m in $[1, n_1 n_2 \dots n_k]$. That is, $(\beta(X_1, \dots, X_n) = 0)$ is an algebraic assertion true at any step of the iteration of the loop for any transition τ_m that could possibility be taken. Then $(\beta(X_1, \dots, X_n) = 0)$ is an inductive invariant and we can conclude that $(\otimes(I_1, \dots, I_k))$ is an ideal of inductive invariant.

Proof of Corollary 9.1

This is immediate from the fact that $(P_i(x_1, \dots, x_n) - Q(x_1, \dots, x_n) < 0)$ will be an invariant as soon as $Q(x_1, \dots, x_n) = 0$ is an inductive invariant at l . We get the result using Theorem 9.1.