INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Morphisms for Non-trivial Non-Linear Invariant Generation for Semi-Algebraic Hybrid Systems

Nadir Matringe *Arnaldo Vieira Moura*
Rachid Rebiha

Technical Report - IC-08-08-32 - Relatório Técnico

November - 2008 - Novembro

Morphisms for Non-trivial Non-Linear Invariant Generation for Semi-Algebraic Hybrid Systems

Nadir Matringe[2], Arnaldo Vieira Moura[3] ⋆, and Rachid Rebiha[1,3] ⋆⋆

[1] Faculty of Informatics, University of Lugano, Switzerland.
rachid.rebiha@lu.unisi.ch or rachid@ic.unicamp.br
[2] Institue de Mathematiques de Jussieu (UMR 7586) Université Paris 7-Denis Diderot, France.
matringe@math.jussieu.fr
[3] Institute of Computing, University of Campinas, SP.Brasil.
arnaldo@ic.unicamp.br

Abstract. We present a new method that addresses the various deficiencies of the state-of-the-art non-linear invariant generation methods for hybrid systems. Present approaches for non-linear invariant generation are limited to linear systems, or they relay on non scalable methods which have high complexity. Moreover, for hybrid systems with discrete transitions, differential rules, and local conditions that are described by multivariate polynomial or fractional systems, no applicable method is known that lends itself to *non-trivial* non-linear invariants generation. We demonstrate a powerful computational *complete* method to solve this problem. By identifying suitable endomorphisms for each consecution condition, we reduce the problem to the intersection between specific eigenspaces and initial semi-affine/algebraic constraints. Our approach avoids first-order quantifier elimination, Grobner bases computation or direct resolution of the systems, hereby circumventing difficulties met by other recent techniques.

1 Introduction

Consider a hybrid system [1], and its computational model. An invariant at a location is an assertion true of any reachable system states associated to this location. In this paper, we present mathematical methods and design efficient algorithms for the automatic generation of non-linear (non-trivial) invariants for non-linear hybrid systems. As it is for static analysis and verification of programs, it is well-known that formal verification of hybrid systems strongly depends on the ease with which invariants can be automatically generated [2, 3], e.g. safety properties over hybrid system [4, 5] can be reduced to invariant properties.

In order to automate the generation of *non-trivial* multivariate polynomial invariants, one needs to handle *initiation* and *discrete consecution* conditions. For the latter, we need to discover inductive algebraic assertions that hold at the initialization, and we must also find algebraic assertions induced by the structure of the discrete transitions at each state. Moreover, one needs to handle *continuous consecution* conditions: *differential consecution* and *local* conditions. This requires inductive algebraic assertions that hold at each state satisfying the local state conditions and obeying the local differential rules.

Invariant generation for hybrid systems have seen tremendous progress [6, 7, 8, 9, 10, 11, 12, 13] in recent years. But they are often limited to linear discrete systems, linear or

⋆ Research supported in part by CNPq — Conselho Nacional de Desenvolvimento Científico e Tecnológico, grant #472504/2007-0

⋆⋆ List of Authors in Alphabetic Order. Research supported in part by CNPq — Conselho Nacional de Desenvolvimento Científico e Tecnológico, grant #142170/2007-0

constant differential systems and they omit the *local* and *initial* conditions, or they relay on methods based on high complexity computations. Moreover, for hybrid systems with discrete states, differential rules, initiation and local state conditions that describe multivariate polynomials or multivariate fractional systems, no applicable method is known that lends itself to *non-trivial* non-linear invariants generation. In [6, 9, 14, 10, 12, 13], the invariant generation problem is reduced to a numerical constraint solving problem over indeterminate polynomial coefficients. The main initial idea (see [6, 9]) is to fix the degree of a candidate invariant with unknown coefficients and then generate invariant conditions that these coefficients need to satisfy. In addition, they require computations with a (doubly) exponential complexity: Grobner Bases computations [15], first-order quantifier elimination [16, 17] or coarse abstraction. In [7, 8] similar forward propagation techniques use an abstract interpretation [18] framework and Grobner bases construction to compute invariants as fixed points of operations on ideals. The main challenge for these techniques is that abstract interpretation introduces imprecision (*widening*, operator not automatically found) to assure termination. This is the main reason why these approaches could often produce trivial invariants or relay on constant and linear systems due to a too coarse abstraction. On the other hand, for *non-linear* invariants, the difficulty of automatic generation arises from the lack of *completeness* of *scalable decision procedures* when based on *existence* and *decidability* results. Here, we demonstrate a powerful computational method to solve these problems. First we extend our previous work on non-linear non-trivial invariant generation for programs with nested loops and conditional statements that describe multivariate polynomial or fractional systems [19]. We identify suitable endomorphisms for each consecution condition of non-linear systems. The non-trivial non-linear invariant generation problem is then reduced to linear algebraic problems associated to the identified endomorphisms.

We can summarize our contribution as follows: (i) In contrast with other approaches and as our first key contribution, our methods do not require (doubly) exponential computation from the use of Grobner bases, quantifier elimination, cylindrical algebraic decomposition or direct resolution of algebraic systems, and also do not require any abstraction operator; (ii) considering a hybrid system, we succeeded in reducing the non-linear invariant generation problem to the intersection between specific eigenspaces and initial semi-affine/algebraic forms; (iii) given an algebraic hybrid system we provide automatically suitable complete encoding techniques for their invariance consecution conditions and identify the suitable endomorphisms; (iv) due to our reduction to linear algebraic problems, we generate *eigenspaces of non-trivial non-linear invariants* in *polynomial steps*. With the same complexity, we handle semi-algebraic local, initiation conditions and transition guards and we generate semi-algebraic invariants and box invariants; (v) moreover, we present the first necessary and sufficient conditions for the existence of *non-trivial* non-linear differential invariants for each type of non linear differential system using precise notions from computational and commutative algebras; (vi) In contrast to what have been claimed, we prove that invariant generation methods using any type of scaling-consecution encoding are linear algebraic problems, and not non-linear algebraic problems as it was supposed in the literature; (vii) we present undecidable and large decidable classes for the problem of invariant generation for non-linear hybrid systems. We also focus on generic class as examples. To the best of our knowledge, we propose the first invariant generation method for hybrid systems with discrete transitions, differential rules, and local conditions that are described by *multivariate fractional systems*; Also, the important result on the existence of non-trivial non-linear differential invariants can complete, and be directly used by, any constraint-based invariant generation method [9, 6, 12, 10] and is applicable to any over-approximation and reachability analysis [20, 13, 21]

In Section 2 we introduce ideals of polynomials and their possible interaction with algebraic inductive assertions for hybrid systems. By extending our previous work on non-linear invariant generation [19] we show in Section 3 how we can handle invariance conditions for the discrete transition structure of hybrid systems using specific endomorphisms. In Section 4 we present new sound and complete continuous consecution conditions for non-linear differential systems. In Section 5, we present our invariant generation methods by identifying endomorphisms for *strong* encoding of differential invariance conditions. We present important theorems for the existence of non-trivial invariants and expose large decidable classes. In Section 6 we extend our method and analysis to deal with constant scale-consecution conditions. Then, in Section 7, we generalise our methods and analysis to handle polynomial scale-consecution conditions. In Section 8, we show how we deal with semi-algebraic assertions describing local conditions, initiation, guards transitions.

2 Ideals of Polynomials, Inductive Assertions and Hybrid Systems

Let $A_n = K[X_1, .., X_n]$ be the ring of multivariate polynomials over the set of variables $\{X_1, .., X_n\} \subset K$. An ideal $I \in A_n$ is closed under addition, it includes 0 and it is closed by multiplication with each element in A_n. Let $E \subseteq A_n$ a set of polynomials, the *ideal generated* by E is the following set of *finite* sums: $(E) = \{\sum_{i=1}^{k} P_i Q_i \mid P_i \in K[X_1, \dots, X_n], Q_i \in E, k \geq 1\}$. 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.* We use transition systems as representations of hybrid systems and hybrid automata as their computational models.

Definition 1 *A* hybrid system *is given by $\langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta \rangle$, where V is a set of variables, $V_t = \{X_1, \dots, X_n\}$ where the X_i's are functions $X_i(t)$ of t, L is a set of locations and l_0 is the initial location. A state is given by an interpretation of the variables in $V \cup V_t$. A transition $\tau \in \mathcal{T}$ is given by a tuple $\langle l_{pre}, l_{post}, \rho_\tau \rangle$, where l_{pre} and l_{post} name the pre- and post- locations of τ. The transition relation ρ_τ is a first-order assertion over $V \cup V_t \cup V' \cup V_t'$, where V and V_t correspond to current-state variables and functions, while V' and V_t' correspond to the next-state variables and functions. Θ is the initial condition, given as a first-order assertion over $V \cup V_t$. Also, $\mathcal{C}$ associates each location $l \in L$ to a* local condition *$\mathcal{C}(l)$ denoting an assertion over $V \cup V_t$. Finally, $\mathcal{D}$ associates each location $l \in L$ to a* differential rule *$\mathcal{D}(l)$ corresponding to an assertion over $V \cup \{dX_i/dt | X_i \in V_t\}$. This differential rule describes the local evolution of variables and functions in V_t during a local time interval.*

Definition 2 *A run of a hybrid automaton is an infinite sequence $\langle l_0, \kappa_0 \rangle \xrightarrow{\mu_0} \cdots \xrightarrow{\mu_{i-1}} \langle l_i, \kappa_i \rangle \xrightarrow{\mu_i} \cdots$ of states $\langle l_i, \kappa_i \rangle \in L \times \mathbb{R}^{|V \cup V_t|}$ and where l_0 is the* initial *location and $\kappa_0 \models \Theta$.*

Considering two consecutive states $\langle l_i, \kappa_i \rangle$ and $\langle l_{i+1}, \kappa_{i+1} \rangle$, each condition μ_i describes 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 $\langle \kappa_i, \kappa_{i+1} \rangle \models \rho_i$. Otherwise μ_i is a* continuous consecution *condition and there exists $q \in L$, $\varepsilon \in \mathbb{R}$ and a differentiable and continuous function $\phi : [0, \varepsilon] \to \mathbb{R}^{|V \cup V_t|}$ such that:*

- $l_i = l_{i+1} = q$

- $\phi(0) = \kappa_i$, $\phi(\varepsilon) = \kappa_{i+1}$
- *During the time interval* $[0, \varepsilon]$, ϕ *satisfies the local condition* $\mathcal{C}(q)$ *(i.e.* $\forall t \in [0, \varepsilon]$, $\phi(t) \models \mathcal{C}(q)$*) according to the local differential rule* $\mathcal{D}(q)$ *(in other words* $\forall t \in [0, \varepsilon]$, $\langle \phi(t), d\phi(t)/dt \rangle \models \mathcal{D}(q)$*).*

Definition 3 *Consider a hybrid system* $W = \langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta \rangle$. *An* invariant φ *at location* $l \in L$ *is defined by an assertion over* $V \cup V_t$ *which holds on all states that reach location* l*. Formally, if* $\langle l, \kappa \rangle$ *is a reachable state in a possible run of* W *then* $\kappa \models \varphi$*.*

Definition 4 *Let* $W = \langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta \rangle$ *be a hybrid system and let a domain for assertion* D *be given. An assertion map for* W *is a map* $\gamma : L \to D$*. We say that* γ *is* inductive *if and only if the* Initiation *and* Consecution *conditions hold:*

- $\Theta \models \gamma(l_0)$ *(Initiation)*
- *for all* $\tau \in \mathcal{T}$ *s.t* $\tau = \langle l_i, l_j, \rho_\tau \rangle$ *we have* $\gamma(l_i) \wedge \rho_\tau \models \gamma(l_j)'$ *(Discrete Consecution)*
- *for all* $l \in L$*, and two consecutive reachable states* $\langle l, \kappa_i \rangle$ *and* $\langle l, \kappa_{i+1} \rangle$ *in a possible run of* W *such that* κ_{i+1} *is obtained from* κ_i *according to the local differential rule* $\mathcal{D}(l)$*, if* $\kappa_i \models \gamma(l)$ *then* $\kappa_{i+1} \models \gamma(l)$*. If* $\gamma(l) \equiv (Q(X_1, .., X_n) = 0)$ *where* Q *is a multivariate polynomial in* $K[X_1, .., X_n]$ *then* $\mathcal{C}(l) \wedge (Q(X_1, .., X_n) = 0) \models (d(Q(X_1, .., X_n)/dt = 0)$ *(Continuous Consecution).*

By analogy with the relation between invariants and inductive assertions of programs established by Floyd and Hoare [22], we see that if γ is an inductive assertion map then $\gamma(l)$ is an invariant at l for W.

3 Endomorphisms for discrete consecution conditions

Here we extend our previous work on non-linear non-trivial invariant generation for non-linear discrete structures to the discrete transition structures of hybrid systems [19]. The invariant generation problem required first a precise analysis of consecution induced in strongly connected component or circuit. That is why we assume that the discrete transitions mentioned in this section are part of connected component. To encode discrete consecution conditions, we use the following notions.

Definition 5 *Let* $W = \langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta \rangle$ *a hybrid automaton,* η *be an algebraic inductive map and let* $\tau = \langle l_i, l_j, \rho_\tau \rangle$ *be a transition in* $\mathcal{T}$*. We identify the following* complete *notion of discrete consecution conditions:*

1. η *satisfies a* Fractional-*scale consecution for* τ *if and only if there exists a multivariate fractional* $\frac{T}{Q}$ *such that* $\rho_\tau \models (\eta(l_j)' - \frac{T}{Q}\eta(l_j) = 0)$
2. η *satisfies a* Polynomial-*scale consecution for* τ *if and only if there exist a multivariate polynomial* T *such that* $\rho_\tau \models (\eta(l_j)' - T\eta(l_j) = 0)$
3. η *satisfies a* Constant-*scale consecution for* τ *if and only if there exists a constant* $\lambda \in K$ *such that* $\rho_\tau \models (\eta(l_j)' - \lambda\eta(l_j) = 0)$

Constant-scale consecution encodes the fact that the numerical value of the assertion after the transition τ is given by λ times its numerical value prior the the transition. *Polynomial-scale* consecution encodes the fact that the numerical value of the assertion after the transition τ has been multiplied by a multivariate polynomial T. *Fractional-scale* consecution encodes the fact that the numerical value of the assertion after the transition τ is a T/Q multivariate fractional multiple of its numerical value prior to the transition. We are able to handle the most general case (transitions describing a multivariate fractional system) with the *fractional-scale* consecution notion. Constant and polynomial scale consecution were introduced in [6] as sound encoding for invariance conditions. But, as we have shown in [19], present constraint-based approaches associated to these scale consecutions are limited to a restricted class of linear transition systems. Moreover, they require Grobner bases computation and direct resolution of non-linear system. In the following, we show how we solve this problem in polynomial steps.

3.1 Endomorphisms for algebraic discrete transitions systems

All proofs and examples of this section are completely described in our previous work [19] and our associated technical report associated to this section [23]. Let $\tau = \langle l_i, l_i, \rho_\tau \rangle$ be a discrete transition in (T), with: $\rho_\tau \equiv [X_1' = R_1(X_1,..,X_n) \wedge \cdots \wedge X_n' = R_n(X_1,..,X_n)]$. In this section we consider the case where the R_i's are multivariate polynomials in $K[X_1,..,X_n]$. First, we show how to express the discrete invariant consecution conditions in terms of the ideal membership problem.

Definition 6 *Let Q be a polynomial in $K[X_1,...,X_n]$. Modulo the ideal of $K[X_1',..,X_n',X_1,..,X_n]$ corresponding to the transition τ, generated by the basis $(X_1' - R_1(X_1,..,X_n),..,X_n' - R_n(X_1,..,X_n))$, the polynomial Q is said to be a T-*invariant for polynomial-scale consecution *for τ if and only if there exists a polynomial $T \in K[X_1,..,X_n]$, verifying $Q(X_1',..,X_n') = T(X_1,..,X_n)Q(X_1,..,X_n)$.*

Theorem 1 ***(T-invariant characterization)*** *Let $Q \in K[X_1,..,X_n]$ be a multivariate polynomial with indeterminate coefficients (a template). Let $T \in \mathbb{K}[X_1,..,X_n]$ be a multivariate polynomial. Then Q is a T-invariant if and only if $Q(R_1(X_1,..,X_n),..,R_n(X_1,..,X_n)) = T(X_1,..,X_n)Q(X_1,..,X_n)$.*

Proof. See, [19] and our associated technical report associated to this section [23].

We are looking for a T-invariant of degree r for an algebraic transition τ, that is, a polynomial Q of degree r such that there exists a polynomial T, verifying equation depicted in theorem 1. Using linear algebra, we write the T-invariant candidate's ordered coefficients $a_0,...,a_t$ ($t+1$ being the number of monomials of degree inferior to r). Let d be the maximal degree of the R_i's. We are thus going to look for a T of degree $e = dr - r$. Let's write its ordered coefficients as $\lambda_0,...,\lambda_s$ ($s+1$ being the number of monomials of degree inferior to e). We recall that V_m denotes the subspace of $K[X_1,\ldots,X_n]$ of degree inferior to or equal to m. Let M be the matrix, in the canonical basis of V_r and V_{dr}, of the morphism from V_r to V_{dr} given by $P(X_1,\ldots,X_n) \mapsto P\big(R_1(X_1,\ldots,X_n),\ldots,R_n(X_1,\ldots,X_n)\big)$. The coefficients of M will be polynomials in the coefficients of the R_i's. Let L be the matrix in the canonical basis of V_r and V_e of the morphism from V_r to V_{dr} given by: $P \mapsto TP$. Then matrix L has a very simple form. Right now we just claim that its non zero coefficients are the λ_i's, and that it has a natural block decomposition. Let u be the number of terms of degree less than dr (*i.e.* the dimension of V_{rd}). Our problem is equivalent to finding a matrix L such that

$M - L$ has a non trivial kernel. In other words, such that $M - L$ is of rank less than u. We know that a matrix is of rank less than $k \in \mathbb{N}$ exists if and only if it has an *invertible* $k * k$ sub-matrix of $\mathcal{M}$. Now, notice that $M - L$ having a non trivial kernel is equivalent to it having rank strictly less than the dimension $d(r)$ of V_r. By a classical theorem [24], this is equivalent to the fact that each $d(r) \times d(r)$ sub-determinant of $M - L$ is equal to zero. Those determinants are polynomials with variables $(\lambda_0, \lambda_1, .., \lambda_s)$.

Theorem 2 ***(Existence of non trivial invariants using polynomial scaling)*** *We will have a non trivial invariant if and only if there exists a matrix L (corresponding to $P \mapsto TP$ in the canonical basis with the non null coefficients of T being $\lambda_0, ..., \lambda_s$), 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.*

Proof. See, [19] and our associated technical report associated to this section [23].

We deal with the most practical case using the following theorem that holds whatever are the type of the initial conditions.

Theorem 3 ***(Existence of non trivial invariant for any type of initial conditions)*** *If one can find T (*i.e. *L) such that $dim(Ker(M - L)) \geq 2$, for* any initial conditions*, then there will always be non trivial invariants.*

Proof. See, [19] and our associated technical report associated to this section [23].

3.2 Endomorphisms for fractional discrete scale consecution

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

$$\rho_\tau \equiv [\ x'_1 = P_1(x_1, \ldots, x_n)/Q_1(x_1, \ldots, x_n) \ldots x'_n = P_n(x_1, .., x_n)/Q_n(x_1, .., x_n)] \qquad (1)$$

where the P_i's and Q_i's belong to $K[X_1, ..., X_n]$, and P_i is relatively prime to Q_i.

Definition 7 *Let Q be a polynomial in $K[X_1, .., X_n]$. Modulo the ideal of $K[X'_1, .., X'_n, X_1, .., X_n]$ corresponding to the transition τ, generated by the basis $(X'_1 - R_1(X_1, .., X_n), .., X'_n - R_n(X_1, .., X_n))$, Q is said to be a F-*invariant for polynomial-scale consecution *for τ if and only if there exists a multivariate fractional $F \in K(X_1, .., X_n)$, verifying $Q(X'_1, .., X'_n) = F(X_1, .., X_n)Q(X_1, .., X_n)$.*

Theorem 4 ***(F-invariant characterization)*** *Let $Q \in K[X_1, \ldots, X_n]$ be a multivariate polynomial with indeterminate coefficients (a template). Q is a F-invariant for fractional scale consecution with a* parametric fractional *$F \in K(X_1, .., X_n)$ for τ if and only if $Q\left(\frac{P_1(X_1,..,X_n)}{Q_1(X_1,..,X_n)}, .., \frac{P_n(X_1,..,X_n)}{Q_n(X_1,..,X_n)}\right) = F(X_1, .., X_n)Q(X_1, .., X_n)$.*

Proof. See, [19] and our associated technical report associated to this section [23].

Let d be the maximal degree of the P_i's and Q_i's, and let Π be the lcm of the Q_i's. Further, suppose that we are looking for an invariant Q of degree r. Let m be the morphism of vector spaces $Q \mapsto \Pi^r Q(P_1/Q_1, \ldots, P_n/Q_n)$ 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 l denote the morphism of vector spaces $Q \mapsto TQ$ from V_r to V_{nrd}, with L its matrix in a canonical basis. Combining theorem 3 and the preceding discussion, we have the following theorem:

Theorem 5 *Let M be as described above. There will exist a F-invariant polynomial if and only if there exists a matrix L (corresponding to $Q \mapsto TQ$) such that $M-L$ has a nontrivial kernel. In this situation, any vector in the kernel of $M-L$ will give a F-invariant polynomial.*

Proof. See, [19] and our associated technical report associated to this section [23].

Theorem 6 ***(Existence of non trivial invariants using fractional scaling)*** *We will have a non trivial invariant if and only if there exists a matrix L (corresponding to $Q \mapsto TQ$ in the canonical basis, with the coefficients of T being $\lambda_0, ..., \lambda_s$), such that the intersection of the kernel of $M-L$ and the hyperplane given by the initial values is not zero, the invariants corresponding to vectors in the intersection.*

Proof. See, [19] and our associated technical report associated to this section [23].

Theorem 7 ***(Existence of non trivial invariants using fractional scaling for any initial value)*** *We will have a non trivial invariant for any non-trivial initial value if there exists a matrix L such that the kernel of $M-L$ is of dimension greater or equal than 2.*

Proof. See, [19] and our associated technical report associated to this section [23].

4 New continuous consecution conditions for non-linear differential systems

Here we present another method that allows us to encode differential continuous consecution conditions. Consider W as the hybrid automaton introduced just above. Here again, we are interested in the case where states are in strongly conected component, with possible ietartion in a run. Let $l \in L$ and $\eta(l)$ be a polynomial with unknown coefficients (a template, a candidate invariant) of the form $\eta(l) = P(X_1, .., X_n)$ where the X_i's are functions $X_i(t)$ of t. Hence we have

$$d\eta(l)/dt = \frac{\partial P(X_1, \ldots, X_n)}{\partial X_1}\frac{dX_1(t)}{dt} + \cdots + \frac{\partial P(X_1, \ldots, X_n)}{\partial X_n}\frac{dX_n(t)}{dt}.$$

Definition 8 *For a polynomial $P(X_1, .., X_n) \in \mathbb{R}[X_1, .., X_n]$, we define the polynomial D_P:*

$$D_P(Y_1, \ldots, Y_n, X_1, \ldots, X_n) = \frac{\partial P(X_1, \ldots, X_n)}{\partial X_1}Y_1 + \cdots + \frac{\partial P(X_1, \ldots, X_n)}{\partial X_n}Y_n$$

of $\mathbb{R}[Y_1, \ldots, Y_n, X_1, \ldots, X_n]$. If $P(X_1, \ldots, X_n)$ is in $\mathbb{R}_d[X_1, \ldots, X_n]$, the polynomials of degree at most d, then $D_P(Y_1, \ldots, Y_n, X_1, \ldots, X_n)$ is in $\mathbb{R}_d[Y_1, \ldots, Y_n, X_1, \ldots, X_n]$.

Hence we have that $d\eta(l)/dt = D_P(\dot{X_1},..,\dot{X_n},X_1,..,X_n)$. In the sequel we will use the notation $\dot{F} = dF/dt$. Consider two consecutive configurations $\langle l, \kappa_i\rangle$ and $\langle l, \kappa_{i+1}\rangle$ in a possible run of the hybrid system. Using definition 2, we can express local state continuous consecutions as $\mathcal{C}(l) \wedge (\eta(l) = 0) \models (\dot{\eta}(l) = 0)$. Next, we define the following notion of scaling-consecution for non-linear local state assertions.

Definition 9 *Let $W = \langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta\rangle$ a hybrid automaton and let η be an algebraic inductive map. We identify the following* complete *notion to encode* continuous consecution conditions *(see definition 2):*

1. *η satisfies a* Fractional-*scale local consecution at l if and only if there exists a multivariate fractional $\frac{T}{Q}$ such that $\mathcal{C}(l) \models (d\eta(l)/dt - \frac{T}{Q}\eta(l) = 0)$*
2. *η satisfies a* Polynomial-*scale local consecution at l if and only if there exist a multivariate polynomial T such that $\mathcal{C}(l) \models d\eta(l)/dt - T\eta(l) = 0$*
3. *η satisfies a* Constant-*scale local consecution at l if and only if there exists a constant $\lambda \in K$ such that $\mathcal{C}(l) \models (d\eta(l)/dt - \lambda\eta(l_j) = 0)$.*
4. *η satisfies a* Strong-*scale local consecution at l if and only if $\mathcal{C}(l) \models (d\eta(l)/dt = 0)$.*

Theorem 8 ***(Soundness)*** *Let P be a continuous function and*

$$(S) = \Big\{[\dot{X_1}(t) = P_1(X_1(t),..,X_n(t)),..,\dot{X_n}(t) = P_n(X_1(t),..,X_n(t))]\Big\}$$

be a differential rule, with initial condition $(x_0,\ldots,x_n)$. Any polynomial which is a P-scale invariant for these initial conditions is actually an inductive (true) invariant.

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

5 Endomorphism for non-trivial non-linear *strong* invariant generation

We first consider a non linear differential system without initial conditions of the form:

$$\begin{bmatrix} \dot{X_1} = P_1(X_1,\ldots,X_n) \\ \vdots \\ \dot{X_n} = P_n(X_1,\ldots,X_n) \end{bmatrix}. \tag{2}$$

We can state the following theorem.

Theorem 9 *A polynomial $Q \in K[X_1,..,X_n]$ is a* strong differential invariant *for the preceding differential system if and only if $D_Q(P_1(X_1,..,X_n),..,P_n(X_1,..,X_n),X_1,..,X_n) = 0$.*

Proof. Straight forward from theorem 8.

If Q has degree r, and d is the maximal degree of the P_i's, then $D_Q(P_1..P_n, X_1..X_n)$ has degree at most $r+d-1$. Now, we want to find an invariant Q of degree r.
We reduce the problem by considering the endomorphism D from $\mathbb{R}_r[X_1, .., X_n]$ to $\mathbb{R}_{r+d-1}[X_1, .., X_n]$ given by

$$P(X_1, .., X_n) \mapsto D_P(P_1(X_1, .., X_n), .., P_n(X_1, ..X_n), X_1, .., X_n)$$

and we denote by M_D its matrix in the canonical basis of $\mathbb{R}_r[X_1, \dots, X_n]$ and $\mathbb{R}_{r+d-1}[X_1, \dots, X_n]$. Using the definition of an invariant, Q will be an invariant for the differential system 2 if and only if it is in the kernel of M_D.

Theorem 10 *A polynomial Q of $\mathbb{R}_r[X_1, .., X_n]$ is a strong differential invariant for the differential system 2 if and only if it lies in the kernel of M_D.*

Proof. Obtain from our reduction to the endomorphism D, discussed just above.

Zero is always an eigenvalue of M_D (because M_D's last column is always null), but this gives a constant eigenvector, i.e. a strong but uninteresting invariant. Now we want to know when one can assert the existence of a non trivial invariant polynomial of degree r. We denote by $v(r)$ the dimension of $\mathbb{R}_r[X_1, .., X_n]$. From the preceding theorem and the remark that follows it, there exists a non trivial invariant only when M_D has a kernel of dimension at least two, *i.e.* when M_D has rank at most $v(r)-2$. In order to better understand what is the form of the matrix M_D, we first look at an example.

Example 1. ***(M_D for 2 variables, a degree 2 differential rule, and degree 2 invariants)*** *In this example for the differential system 2, we have two polynomials of degree 2, with two variables. The polynomial P_1 is of the form $P_1(x,y) = a_1x^2+a_2xy+a_3y^2+a_4x+a_5y+a_6$, and P_2 is of the form $P_2(x,y) = a_7x^2+a_8xy+a_9y^2+a_{10}x+a_{11}y+a_{12}$. 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 becomes:*

$$\begin{pmatrix}
2a_1 & a_7 & 0 & 0 & 0 & 0 \\
2a_2 & a_1+a_8 & 2a_7 & 0 & 0 & 0 \\
2a_3 & a_2+a_9 & 2a_8 & 0 & 0 & 0 \\
0 & a_3 & 2a_9 & 0 & 0 & 0 \\
2a_4 & a_{10} & 0 & a_1 & a_7 & 0 \\
2a_5 & a_4+a_{11} & 2a_{10} & a_2 & a_8 & 0 \\
0 & a_5 & 2a_{11} & a_3 & a_9 & 0 \\
2a_6 & a_{12} & 0 & a_4 & a_{10} & 0 \\
0 & a_6 & 2a_{12} & a_5 & a_{11} & 0 \\
0 & 0 & 0 & a_6 & a_{12} & 0
\end{pmatrix}.$$

Denote by $(a_{1,i}, .., a_{v(r),i})$ the coefficients of the polynomial P_i. Then, the coefficients of the matrix M_D will be linear functions of the $a_{i,j}$'s. If we add initial conditions of the form $(x_1(0) = u_1, \dots, x_n(0) = u_n)$, we are looking for an 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 $ker(M_D) \cap \{P/P(u_1, \dots, u_n) = 0\}$. As the intersection of the hyperplane $\{P|P(u_1, \dots, u_n) = 0\}$ with constant polynomials is always reduced to zero, and as the intersection of any hyperplane with a subspace of $\mathbb{R}_r[x_1, \dots, x_n]$ has dimension at least one, we deduce the following theorem.

Theorem 11 *There exists a strong differential invariant of degree r for the transition system t with initial conditions (any initial conditions, actually), if and only if the kernel of M_D is of dimension at least two.*

Proof. Obtain from theorem 10 and the constructive agumentation (which introduce the sketch of this proof) preceding the theorem.

Now consider the following differential system with initial conditions

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

The solutions of this system are well known: $x(t) = \lambda e^t$ and $y(t) = \mu e^{nt}$. Hence, it is immediate that the polynomial $Q(x, y) = x^n/\lambda^n - y/\mu$ 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 $u \in \mathbb{R}$; hence $x^n/\lambda^n - y/\mu$ divides Q'). For this system it is the most significative invariant one can get. Now, $Q(x, y) = x^n/\lambda^n - y/\mu$ is not a strong invariant because $\partial_1 Q = nx^{n-1}/\lambda^n$ and $\partial_2 Q = -1/\mu$, and $\partial_1 Q(x, y)x + \partial_2 Q(x, y)y = nx^n/\lambda^n - y/\mu \neq 0$.

Take $k = 1$ (to simplify the notation). We show that there cannot exist a non-trivial strong invariant for the system

$$\begin{bmatrix} \dot{x} = x \\ \dot{y} = y \end{bmatrix}. \tag{4}$$

Suppose such an invariant exists. Write it as $Q(x, y) = \sum_{i,j} a_{i,j} x^i y^j$. The relation $\partial_1 Q(x, y)x + \partial_2 Q(x, y)y = 0$ would imply $\sum_{i,j} i a_{i,j} x^i y^j + \sum_{i,j} j a_{i,j} x^i y^j = 0$, 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 won't be able to find strong invariants which are non-trivial inductive invariants. Therefore, we can conjecture that strong invariants exist only in very special cases. We will use the following lemma.

Lemma 1 *Let $Q_1, \ldots, Q_n$ be n polynomials in $\mathbb{R}[x_1, \ldots, x_n]$. Then there exists a polynomial Q such that $\partial_1 Q = Q_1, \ldots, \partial_n Q = Q_n$ if and only if for any $i \neq j$, $1 \leq i, j \leq n$, one has $\partial_i Q_j = \partial_j Q_i$.*

Proof. 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 $\partial_2 Q^1 = Q_2 + b(x_2, \ldots, x_n)$ for some function b of $(x_2, \ldots, x_n)$ which is actually a polynomial. Choosing an anti-derivative $B(x_2, \ldots, x_n)$ of $b(x_2, \ldots, x_n)$ with respect to x_2, one verifies that $Q_{1,2} = Q^1 - B(x_2, \ldots, x_n)$ 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, $\partial_3 Q_{1,2} - Q_3 = c(x_3, \ldots, x_n)$ 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 $Q_{1,\ldots,n}$ such that $\partial_i Q_{1,\ldots,n} = Q_i$, for $i = 1, 2, 3$.

As it is commonly done in computational algebra, we denote by $Syz(P_1, \ldots, P_n)$ the Syzygy bases [25] of $(P_1, \ldots, P_n)$. Hence, we get the following theorem.

Theorem 12 *There exists a strong invariant for a differential system if and only if there exists $(Q_1, .., Q_n)$ in $Syz(P_1, .., P_n)$, such that for any i, j with $i \neq j$ and $1 \leq i, j, \leq n$, one has $\partial_i Q_j = \partial_j Q_i$.*

Proof. Obtain using lemma 1.

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

$$\begin{bmatrix} \dot{x_1} = P_1(x_1, x_2) \\ \dot{x_2} = P_1(x_1, x_2) \end{bmatrix}. \tag{5}$$

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

Example 2. Let the following differential rules.

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

Here, we indeed have $\partial_2 P_2 = -\partial_1 P_1 = -y$. The corresponding invariant is $Q(x, y) = xy^2/2$.

Example 3. Another example of systems admitting strong invariants is a generalization to dimension n of the *rotational motion of a rigid body*:

$$\begin{bmatrix} \dot{x_1} = a_1 x_2 \dots x_n \\ \vdots \\ \dot{x_n} = a_n x_1 \dots x_{n-1} \end{bmatrix}. \tag{7}$$

We treat the case when the a_i's are non zero, 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 $Syz(P_1, \dots, P_n)$, 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 12 we deduce that the system admits a strong invariant. In order to obtain an invariant, we just have to solve $\partial_1 Q = x_1/a_1; Q_2 = -x_2/(n-1)a_2; \dots; Q_n = -x_n/(n-1)a_n$. 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 $Q(x_1, \dots, x_n) = x_1^2/2a_1 - x_2^2/2(n-1)a_2 \dots - x_n^2/2(n-1)a_n$ as strong invariant.

6 Endomorphisms for constant-scale differential consecution

We consider differential systems of the form described in 2. A polynomial $Q \in K[X_1, ..., X_n]$ is said to be a *λ-invariant for constant-scale continuous consecution* for the differential systems 2 if $\dot{Q(X_1, \dots, X_n)} = \lambda Q(X_1, .., X_n)$, that is,

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

If Q has degree r, and the maximal degree of the P_i's is d, then $D_Q(P_1, ..., P_n, X_1, ..., X_n)$ has degree $r+d-1$. Hence we deduce that, in general, constant scale consecution will work only 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. Consider the endomorphism D of $\mathbb{R}_r[X_1, \dots, X_n]$ given by

$$P(X_1, .., X_n) \mapsto D_P(P_1, .., P_n, X_1, .., X_n).$$

By the definition of invariant for constant-scale consecution, 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 $\mathbb{R}_r[X_1, .., X_n]$ we can state the following theorem.

Theorem 13 *A polynomial Q of $\mathbb{R}_r[X_1, \dots, X_n]$ is a λ-invariant for differential scale consecution corresponding to the transition system 2 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.*

Proof. We stated this theorem by proposing the sketch of its proof in the paragraph just above.

Zero is always an eigenvalue of M_D (because M_D's last column is always null). But this gives a constant eigenvector, which is not interesting.

*Example 4. (General case for 2 variables and degree 2)*Consider the transition system of the form depicted below on the left and the matrix M_D in the basis $(x^2, xy, y^2, x, y, 1)$ is given on the right:

$$\begin{bmatrix} \dot{x} = a_1x + b_1y + c_1 \\ \dot{y} = a_2x + b_2y + c_2 \end{bmatrix}. \qquad (8) \qquad M_D = \begin{pmatrix} 2a_1 & a_2 & 2b_2 & 0 & 0 & 0 \\ 2b_1 & a_1+b_2 & 2a_2 & 0 & 0 & 0 \\ 0 & b_1 & 0 & 0 & 0 & 0 \\ 2c_1 & c_2 & 0 & a_1 & 0 & 0 \\ 0 & c_1 & 2c_2 & b_1 & b_2 & 0 \\ 0 & 0 & 0 & c_1 & c_2 & 0 \end{pmatrix}.$$

This matrix is block upper 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 calculated by Cardan's method. Thus, one will always be able to find good λ invariants in this case.

We just proved and gave a method for the following proposition:

Proposition 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.*

In the general case, matrix M_D will always be block triangular, but with blocks $r \times r$ with $r \geq 5$ as soon as we have more than two variables. Hence, by Galois theory, one cannot always find λ-invariants, except in cases where the P_i's are such that the matrix M_D has a "good" form.

Theorem 14 ***(Undecidability/Decidability of scale consecution)*** *Let M_D the matrix introduced in this section and ϕ_λ its characteristic polynomial. Finding a non trivial λ invariant is equivalent to finding a root of ϕ_λ other than zero. If the degree of ϕ_λ is greater than or equal to six, then $\phi_\lambda/(\lambda)$ has degree greater than or equal to five, and roots of such polynomials are usually incalculable. But, as we did in [19] dealing with discrete consecution, we identify large decidable class. E.g. (i) M_D is block triangular (with 4×4 blocks or less); (ii) Eigenspace associated with eigenvalue 1 is of dimension greater than 1.*

Proof. Using classical Galois theory results on resolvability of polynomial equations.

Now let's go back to the example 5 that could we not handle using strong invariant encoding (an alternative proof using λ-scaling). We recall that the system $[\ \dot{x} = x \wedge \dot{y} = ny \wedge (x(0), y(0)) = (\lambda, \mu)\ ]$ has associated endomorphism $L : Q(x, y) \mapsto \partial_x Q(x, y)x + n\partial_y Q(x, y)y$. Writing its matrix in the basis $(x^n, x^{n-1}y, \dots, xy^{n-1}, y^n, \dots\dots, x, y, 1)$ gives:

$$\begin{pmatrix} n \dots & 0 & 0 \\ 0 \ \ M & 0 & 0 \\ 0 \dots & n & 0 \\ 0 \dots & 0 & 0 \end{pmatrix}$$

.

We see that the eigenspace corresponding to n has at least dimension 2, and it contains $Vect(x^n, y)$. Using the theorem on the existence on solutions for any initial conditions, we deduce that for 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 invariant

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

7 Generalization to Polynomial-scale Consecution Conditions of Algebraic Differential Systems

We just saw that as soon as one of the P_i's has degree more than one, one must use polynomial-scale consecution in order to obtain interesting invariants. A polynomial Q in $\mathbb{R}[x_1, \dots, x_n]$ is a T-invariant for some polynomial T in $\mathbb{R}[x_1, \dots, x_n]$, if it verifies

$$D_Q(P_1, \dots, P_n, x_1, \dots, x_n) = TQ.$$

We recall that in general, if $P \in \mathbb{R}[x_1, \dots, x_n]$ is of degree r, and the maximal degree of the P_i's is equal to d, then the degree of $D_P(P_1, \dots, P_n, x_1, \dots, x_n)$ is equal to $r + d - 1$. Hence, T must be searched in the subspace of $\mathbb{R}[x_1, \dots, x_n]$, which is of degree at most $r + d - 1 - r = d - 1$.

Transposing the situation to linear algebra we have, as before, a morphism D from $\mathbb{R}_r[x_1, \dots, x_n]$ to $\mathbb{R}_{r+d-1}[x_1, \dots, x_n]$ given by

$$P \mapsto D_P(P_1, \dots, P_n, x_1, \dots, x_n)$$

, and we still denote by M_D its matrix in the canonical basis of $\mathbb{R}_r[x_1, \dots, x_n]$ and $\mathbb{R}_{r+d-1}[x_1, \dots, x_n]$.

Choosing a generic T in $\mathbb{R}_{d-1}[x_1, \dots, x_n]$, we define the associated morphism $\overline{T}$ from $\mathbb{R}_r[x_1, \dots, x_n]$ to $\mathbb{R}_{r+d-1}[x_1, \dots, x_n]$ given by $P \mapsto TP$, and we denote by L_T its matrix in the canonical basis. Matrices L_T corresponding to multiplication by polynomials T of $\mathbb{R}_{d-1}[x_1, \ldots, x_n]$ have a very precise form (depending on the coefficients of T). Thus, for a fixed n, r and d, they can easily be identified. We will call $M(pol)$ the set of such matrices. It is, in fact, a (vector-)subspace of matrices corresponding to morphisms from $\mathbb{R}_r[x_1, \ldots, x_n]$ to $\mathbb{R}_{r+d-1}[x_1, \ldots, x_n]$. To be even more precise, if T is a generic template in $\mathbb{R}_{d-1}[x_1, \ldots, x_n]$, call $t_0, \ldots, t_{v(d-1)}$ its coefficients (where $v(d-1)$ is the dimension of $\mathbb{R}_{d-1}[x_1, \ldots, x_n]$). Then the coefficients of L_T are in $\left\{t_1, \ldots, t_{v(d-1)}\right\}$.

In order to fix ideas, we show what happens for two variables, P_i's of maximal degree 3, and we are looking for an invariant in $\mathbb{R}_2[x, y]$. Hence, T lies in $\mathbb{R}_2[x, y]$.

Example 5. A generic T is of the form $T(x, y) = t_1x^2+t_2xy+t_3y^2+t_4x+t_5y+t_6$. Here, using the basis $(x^2, xy, y^2, x, y, 1)$ of $\mathbb{R}_2[x, y]$ and the basis $(x^4, x^3y, x^2y^2, xy^3, y^4, x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1)$ of $\mathbb{R}_4[x, y]$, we get for L_T:

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

This determines $M(pol)$.

A T-invariant polynomial Q in $\mathbb{R}_r[x_1, \ldots, x_n]$ is nothing else than a vector in the kernel of $D - \overline{T}$. Hence we have reduced the problem thus:

Theorem 15 *There exists an invariant Q in $\mathbb{R}_r[x_1, \ldots, x_n]$ for differential polynomial-scale consecution corresponding to the transition system 2, if and only if there exists a matrix L_T in $M(pol)$, corresponding to a polynomial T of $\mathbb{R}_{d-1}[x_1, \ldots, x_n]$, such that $Ker(M_D - L_T)$ is not reduced to zero. And, in that case, one can choose Q in $Ker(M_D - L_T)$.*

Proof. The sketch of the proof is the algebraic reduction constructed just above.

Now 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 $\mathbb{R}_r[x_1, \ldots, x_n]$. 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 $(t_1, .., t_{v(d-1)})$, which we will denote by $D_1(t_1, ..., t_{v(d-1)}), ..., D_s(t_1, ..., t_{v(d-1)})$. From the form of L_T, this is zero when $(t_1, ..., t_{v(d-1)}) = (0, ..., 0)$. 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.

Theorem 16 *There will be a non trivial T-invariant if and only if the polynomials $(D_1, .., D_s)$ described just above admit a common root, other than the trivial one $(0, ..., 0)$.*

Proof. The sketch of the proof is given in the paragraph introducing the theorem.

7.1 Initiation steps for constant and polynomial scaling

Up to now, initiation has not been taken into account. Let's consider the differential system 2, with initial values given by $(x_1(0) = u_1, \ldots, x_n(0) = u_n)$, and an invariant candidate Q of degree r for scale or polynomial consecution. The initiation step defines on

$\mathbb{R}_r[x_1, \ldots, x_n]$ a linear form on this space, namely, $I_u : P \mapsto P(u_1, ..., u_n)$. Hence, initial values correspond to a hyperplane of $\mathbb{R}_r[X_1, .., X_n]$ given by the kernel I_u, which is $\{Q \in \mathbb{R}_r[X_1, .., X_n] | Q(u_1, \ldots, u_n) = 0\}$. Hence we have, for constant-scale consecution with initial values:

Theorem 17 ***(Existence of non linear differential invariants using constant scaling).*** *A polynomial Q in $\mathbb{R}_r[X_1, .., X_n]$ is an λ-invariant for system 2 with initial values $(u_1, \ldots, u_n)$ 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 $Q(u_1, \ldots, u_n) = 0$.*

Proof. The sketch of the proof is given by the paragraph introducing the theorem and by using theorem 15.

Corollary 1. ***(Existence of non-null invariants using constant scaling for any initial values)*** *There will be a non-null invariant polynomial for any given initial values if and only if there exists an eigenspace of M with dimension at least 2.*

Proof. Using theorem 17 and the fact that the intersection between an eigenspace of M with dimension at least 2 will intersect any hyperplan, space given by initial constraints.

We can obtain similar results for polynomial-scale consecution with initial values.

Theorem 18 ***(Existence of invariants using polynomial scaling)*** *A polynomial Q in $\mathbb{R}_r[x_1, \ldots, x_n]$ is a T-invariant for system 2 with initial values $(u_1, \ldots, u_n)$ if and only if there exists a matrix L_T in $M(pol)$, corresponding to T in $\mathbb{R}_{d-1}[x_1, \ldots, x_n]$, such that Q belongs to the intersection of $Ker(M_D - L_T)$ and the hyperplane $Q(u_1, \ldots, u_n) = 0$.*

Proof. Similar to the proof of theorems 17.

Corollary 2. ***(Existence of non-null invariants using polynomial scaling for any initial values)*** *There will be a non-null invariant polynomial for any given initial values if and only if there exists a matrix L_T in $M(pol)$ such that $Ker(M - L_T)$ has dimension at least 2.*

Proof. Using 18 and the fact that the intersection between a kernel $Ker(M - L_T)$ with dimension at least 2 will intersect any hyperplan, space given by initial constraints.

Example 6. ***(Decidable Class with polynomial scaling for 2 variables, degree 2 differential system, degree 2 invariants)*** In this example for the differential system 2, we have two polynomials of degree 2, with two variables. Polynomial $P_1(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$, and $P_2(x, y) = a_7x^2 + a_8xy + a_9y^2 + a_{10}x + a_{11}y + a_{12}$. 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 is depicted on the left just below. Here the polynomial T we will use for scaling must be of degree 1. Hence $T(x, y) = dx + ey + f$, and the associated matrix L_T of the T-multiplication morphism has the form depicted on the right just below:

$$M_D = \begin{pmatrix} 2a_1 & a_7 & 0 & 0 & 0 & 0 \\ 2a_2 & a_1 + a_8 & 2a_7 & 0 & 0 & 0 \\ 2a_3 & a_2 + a_9 & 2a_8 & 0 & 0 & 0 \\ 0 & a_3 & 2a_9 & 0 & 0 & 0 \\ 2a_4 & a_{10} & 0 & a_1 & a_7 & 0 \\ 2a_5 & a_4 + a_{11} & 2a_{10} & a_2 & a_8 & 0 \\ 0 & a_5 & 2a_{11} & a_3 & a_9 & 0 \\ 2a_6 & a_{12} & 0 & a_4 & a_{10} & 0 \\ 0 & a_6 & 2a_{12} & a_5 & a_{11} & 0 \\ 0 & 0 & 0 & a_6 & a_{12} & 0 \end{pmatrix}. \qquad L_T = \begin{pmatrix} d & 0 & 0 & 0 & 0 & 0 \\ e & d & 0 & 0 & 0 & 0 \\ f & e & d & 0 & 0 & 0 \\ 0 & 0 & e & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 \\ 0 & f & 0 & e & d & 0 \\ 0 & 0 & f & 0 & e & 0 \\ 0 & 0 & 0 & f & 0 & d \\ 0 & 0 & 0 & 0 & f & e \\ 0 & 0 & 0 & 0 & 0 & f \end{pmatrix}.$$

Suppose $a_3 = a_5 = a_6 = a_7 = a_{10} = a_{12} = 0$, $a_1 = a_8 = a$, $a_2 = a_9 = b$ and $a_4 = a_11 = c$, *i.e.*, $P_1 = ax^2 + bxy + cx$ *and* $P_2 = axy + by^2 + cy$. Then taking $T(x, y) = 2ax + 2by + 2c$, one verifies that the matrix $M_D - L_T$ has its second and third column equal to zero. Hence the rank of $M_D - L_T$ is less than $n - 2 = 5 - 2 = 3$, and our existence theorem for any given initial values applies.

Let us treat the following concrete example with $P_1 = x^2 + 2xy + x$ and $P_2 = xy + 2y^2 + y$:

$$\begin{bmatrix} \dot{x}(t) = x^2(t) + 2x(t)y(t) + x(t) \\ \dot{y}(t) = x(t)y(t) + 2y^2(t) + y(t) \end{bmatrix}. \tag{9}$$

From what we just saw, the good scaling polynomial is $T(x, y) = 2x + 4y + 2$. Here $Vect(xy, y^2) \subset Ker(M_D - L_T)$, so we search for an invariant of the form $axy + by^2$. Thus if the system has initial conditions $x(0) = \lambda$ and $y(0) = \mu$, then $a\lambda\mu + b\mu^2 = 0$, the polynomial $Q = \mu xy - \lambda y^2$ is an invariant of the system.

Constant scale consecution would give trivial invariant in such a case.

Example 7. Let r be a positive integer. We consider the differential system given by the polynomials $[P_1 = \sum_{k=0}^{r} a_k x_1^{k+1} x_2^k \dots x_n^k; \dots ; P_n = \sum_{k=0}^{r} a_k x_1^k \dots x_{n-1}^k x_n^{k+1}]$. Consider the morphism D_P associated with the system. Then it is immediate that $D_P(x_i) = P_i$. Now for this particular class of P_i's, we see that the matrix $D_P(x_i) = x_i T$ where $T = \sum_{k=0}^{r} a_k x_1^k x_2^k \dots x_{n-1}^k x_n^k$. This means that if L_T is the morphism associated to multiplication by T, we have $D_P(x_i) = L_T(x_i)$ for each i. We deduce that each x_i, hence $Vect(x_1, \dots, x_n) \subset Ker(D_P - L_T)$. Hence for $n \geq 2$, the space $Ker(D_P - L_T)$ has dimenion greater than two, and our existence theorem for invariants given any initial values applies, and we can search for an invariant of the form $a_1 x_1 + \dots + a_n x_n$. Given initial conditions $(x_1(0) = \lambda_1, \dots, x_n(0) = \lambda_n)$, a vector $(a_1 \cdots a_n)^{Tr}$ is such that the polynomial $a_1 x_1 + \cdots + a_n x_n$ is an invaraiant for the system $[P_1 = \sum_{k=0}^{r} a_k x_1^{k+1} x_2^k \dots x_n^k; \dots ; P_n = \sum_{k=0}^{r} a_k x_1^k \dots x_{n-1}^k x_n^{k+1}]$ whenever it belongs to the kernel of the linear form with matrix $(\lambda_1, \dots, \lambda_n)$. Summarizing, we get the following result. Let (S) be the system:

$$\begin{bmatrix} \dot{x}_1(t) = \sum_{k=0}^{r} a_k x_1(t)^{k+1} x_2(t)^k \cdots x_n(t)^k \\ \vdots \\ \dot{x}_n(t) = \sum_{k=0}^{r} a_k x_1(t)^k \cdots x_{n-1}(t)^k x_n(t)^{k+1} \end{bmatrix}. \tag{10}$$

Polynomial scaling shows that any polynomial $Q = a_1x_1 + \cdots + a_nx_n$ with $(a_1 \cdots a_n)^{Tr}$ in the kernel of $(\lambda_1, \ldots, \lambda_n)$ is an invariant of (S).

Consider the following system with initial conditions (simple ones as the more generale case is treaten in Section 8) $(x(0) = 1, y(0) = 1, z(0) = 1)$

$$\begin{bmatrix} \dot{x}(t) = x(t)^3y(t)^2z(t)^2 + 2x(t) \\ \dot{y}(t) = x(t)^2y(t)^3z(t)^2 + 2y(t) \\ \dot{z}(t) = x(t)^2y(t)^2z(t)^3 + 2z(t) \end{bmatrix}. \tag{11}$$

It admits $x + y - 2z$ as an invariant.

8 Semi-affine/algebraic initial and local conditions

All invariant generation methods we proposed generate automatically ideals of non-trivial invariants where the bases is the one associated with the generated eigenspaces. In the following section we show how we handle initial and local conditions describing semi-affine/algebraic assertions. We use the following theorem to generate invariants for state inside a strongly connected component (w.r.t the induction from possible iteration).

Theorem 19 *Let W be a hybrid system and let l be one of its states. Let $I = \{I_1, ..., I_k\}$ a finte set of ideals in $K[X_1, ..., X_n]$. Let $\nabla(I_1, ..., I_k) = \{\delta_1, ..., \delta_{n_1n_2...n_k}\}$ be such that all elements δ_i in $\nabla(I_1, ..., I_k)$ are formed by the product of one element from each ideal in I. Assume that the I_js are collections of ideals of invariants associated to $\mathcal{D}(l)$ (its differential rule), $\mathcal{C}(l)$ (its local conditions) and all ideals of invariants generated considering all incoming transitions of l. Then $(\nabla(I_1, ..., I_k))$ is an ideal of non-trivial non-linear invariants for the state l.*

Proof. Let $f_1^{(j)}, ..., f_{n_j}^{(j)}$ in $K[X_1, .., X_n]$ such that $I_j = ({f^{(j)}}_1, ..., f_{n_j}^{(j)})$, forall j in $[1, k]$.Let $\beta \in (\nabla(I_1, ..., I_k))$,then there exists $e_1, .., e_{n_1n_2..n_k}$ in $K[X_1, .., X_n]$ such that $\beta = e_1\delta_1 + .. + e_{n_1n_2..n_k}\delta_{n_1n_2..n_k}$. Also, by construction of $\nabla(I_1, ..., I_k)$ we know that: $\forall r \in [1, .., n_1n_2..n_k]$, $\delta_r \in \nabla(I_1, ..., I_k)$. $\exists(\alpha_1^{(r)}, .., \alpha_k^{(r)}) \in I_1 \times I_2 \times .. \times I_k$ such that $\delta_r = \prod_{i=o}^{k} \alpha_i^{(r)}$. Then we have $\beta = \sum_{j=1}^{n_1n_2..n_k} [\lambda_j \prod_{i=1}^{k} \alpha_i^{(j)}]$. Now, for all m in $[1, k]$, if I_m correspond to a pre-computer inductive ideal of invariant associated to one of the transition τ_m at the location l, then $\forall j \in [1, n_1n_2..n_k]$, $\alpha_m^{(j)}(X_1, .., X_n) = 0$. And so $\forall j \in [1, n_1n_2..n_k]$, $\prod_{i=1}^{k} \alpha_i^{(j)} = 0$. Finally we obtain $\beta(X_1, .., X_n) = 0$ for all m in $[1, n_1n_2..n_k]$. In other words, $(\beta(X_1, .., X_n) = 0)$ is an algebraic assertion true at any step of the iteration of the loop for any transition τ_m that could possibliy taken. Then $(\beta(X_1, .., X_n) = 0)$ is an inductive invariant and we can conclude that $(\nabla(I_1, ..., I_k))$ is an ideal of inductive invariant.

Semi-algebraic local state conditions, initiation and transition guards are assertions of the form $(P_i(x_1, .., x_n) < 0)$ with $P_i \in K[x_1, .., x_n]$.

Corollary 3. *Let a state l and $\mathcal{C}(l) \equiv (P_i(x_1, .., x_n) < 0)$ its semi-algebraic local conditions and Q an inductive invariant for $\mathcal{D}(l)$ (its differential rule) and all ideals of invariants generated considering all incoming transitions of l. Then $(P_i(x_1, .., x_n) - Q(x_1, .., x_n) < 0)$ is an inductive invariant.*

Proof. This is straight forward from the fact that $(P_i(x_1,..,x_n) - Q(x_1,..,x_n) < 0)$ will be an invariant as soon as $Q(x_1,..,x_n) = 0$ is an inductive invariant at l. We conclude using theorem 19.

Then, we obtain an operator (similar to the one introduced in theorem 19) to generate ideal of non-trivial invariant at a state l with semi-algebraic local conditions. Our prototype can then generates ideals of non-trivial semi-algebraic invariant or Box-invariant (see state l_0 in following the example).

Example 8. Here we considere the example depicted in figure 1 For each state of the semi-algebraic hybrid systems describe below, our prototype generates in polynomial steps ideals of non-trivial invariants. By taking into account inequality, it generates *semi-algebraic* or *box invariants* when the local state conditions is not abstracted to true. We present below, on the right, the out put of our prototype in order to summarize the nature of the computation needed. In the initial state l_0 we deal with non-linear differential rules Also the local condition is describer by the semi-algebraic assertion $0 < -(u/u_0)^{2N} + 3\omega(u/u_0)^N + u_0(u/u_0)^{4N} - 1/\omega_0(\omega_0^3 - \omega)$ and the initial conditions $((u(0), \omega(0)) = (u_0, \omega_0)) \wedge (-1/4 < \omega_0) \wedge (0 < u_0)$. Our approaches generate automatically in polynomial time the non-trivial generators of invariants `[Diff-Invariant][`$(U^N/u_0) + (W/w_0)$`]`, the *semi-algebraic invariant* `[Ineq-Invariant] [`$0 < (U/u_0)^2 * N - (U/u_0)^N - w_0$`]`(taking into account semi-algebraic local and initial condition) and *box-invariant* `[Box-Invariants] [`$u_0 * (2^N/(1-4*w_0)^{N/2}) < U < 2^N * u_0$`]`. Also, we use the state l_2 to illustrate the theorem 19 to deal with the two transitions ρ_{τ_2} and ρ_{τ_2}. For $\mathcal{D}(l_2)$ we have `[Invariant][`$(k_0 * K * V - v_0 * V^2) * (A * B) * (s_0 * (1 - s_0) * R^2 + R * S + S^2 - R - 2 * S + 1)$`]`.

On the other hand, our prototype combines new optimisation techniques like the one we proposed to deal with air traffic management systems [13, 26] in polynomial time and automatically.

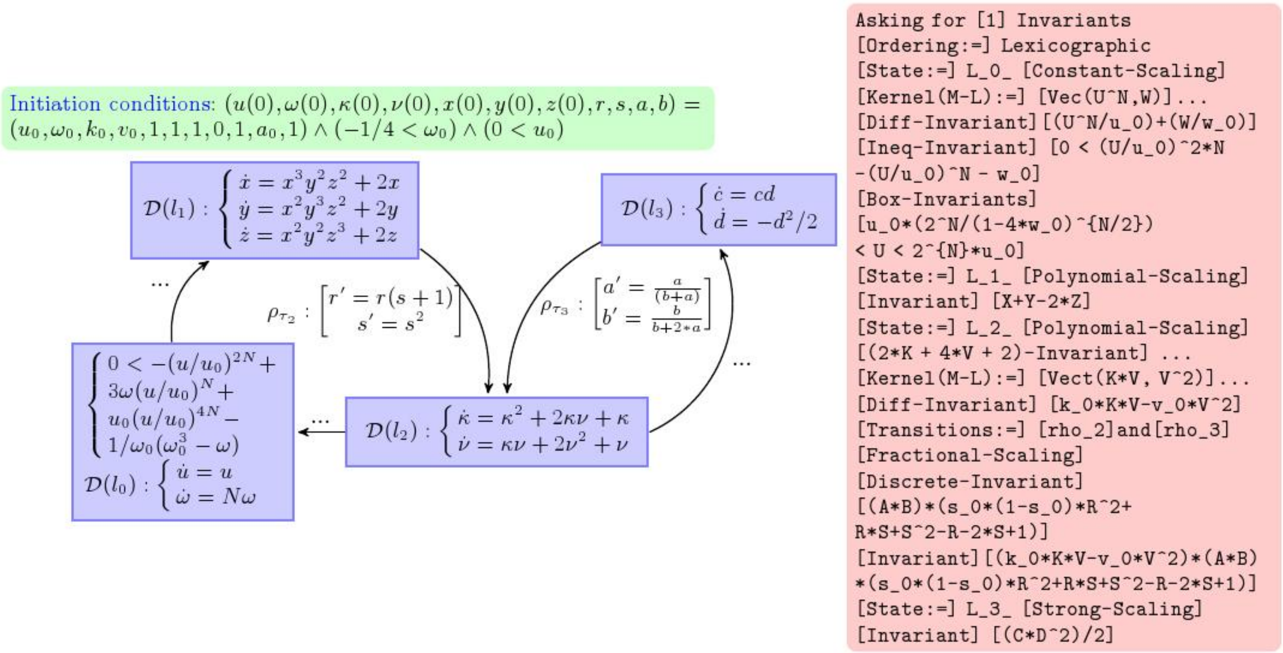
Example 9. We consider the differential system

$$\begin{bmatrix} \dot{x_1} = a_1 cos(\omega t + c) \\ \dot{x_2} = a_2 sin(\omega t + c) \end{bmatrix}. \tag{12}$$

It is the system satisfied by one of the two air plains (or planets). We introduce the new variables d_1 and d_2 to handle the transcendental functions, which axiomatizing them by differential equations, so that d_1 and d_2 verify:

$$\begin{bmatrix} \dot{d_1} = -a_1/a_2 \omega d_2 \\ \dot{d_2} = a_2/a_1 \omega d_1 \end{bmatrix}. \tag{13}$$

If L is the endomorphism associated to this system, it is immediate that $L(a_2^2 d_1^2) = -2a_1 a_2 \omega d_1 d_2$ whereas $L(a_1^2 d_2^2) = 2a_1 a_2 \omega d_1 d_2$, which implies that $Vect(a_2^2 d_1^2 + a_1^2 d_2^2) \subset Ker(L)$ and $a_2^2 d_1^2 + a_1^2 d_2^2$ is a strong invariant of the system. Now we want to catch back our first indeterminate x_1 and x_2. But $\dot{x_1} = d_1 = a_1/a_2 \omega \dot{d_2}$ and $\dot{x_2} = d_2 = -a_2/a_1 \omega \dot{d_1}$. Therefore there will exist constants c_1 and c_2 determined by 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 $(a_2 x_1 - k_1)^2 + (a_1 x_2 - k_2)^2$ for $k_1 = a_2 c_1$ and $k_2 = a_1 c_2$, is an invariant of


Initiation conditions: $(u(0),\omega(0),\kappa(0),\nu(0),x(0),y(0),z(0),r,s,a,b) = (u_0,\omega_0,k_0,v_0,1,1,1,0,1,a_0,1) \wedge (-1/4 < \omega_0) \wedge (0 < u_0)$
$\mathcal{D}(l_1) : \begin{cases} \dot{x} = x^3y^2z^2 + 2x \\ \dot{y} = x^2y^3z^2 + 2y \\ \dot{z} = x^2y^2z^3 + 2z \end{cases}$
$\mathcal{D}(l_3) : \begin{cases} \dot{c} = cd \\ \dot{d} = -d^2/2 \end{cases}$
$\rho_{\tau_2} : \begin{bmatrix} r' = r(s+1) \\ s' = s^2 \end{bmatrix}$
$\rho_{\tau_3} : \begin{bmatrix} a' = \frac{a}{(b+a)} \\ b' = \frac{b}{b+2*a} \end{bmatrix}$
...
...
...
$\begin{cases} 0 < -(u/u_0)^{2N} + \\ 3\omega(u/u_0)^N + \\ u_0(u/u_0)^{4N} - \\ 1/\omega_0(\omega_0^3 - \omega) \end{cases}$
$\mathcal{D}(l_0) : \begin{cases} \dot{u} = u \\ \dot{\omega} = N\omega \end{cases}$
$\mathcal{D}(l_2) : \begin{cases} \dot{\kappa} = \kappa^2 + 2\kappa\nu + \kappa \\ \dot{\nu} = \kappa\nu + 2\nu^2 + \nu \end{cases}$

```
Asking for [1] Invariants
[Ordering:=] Lexicographic
[State:=] L_0_ [Constant-Scaling]
[Kernel(M-L):=] [Vec(U^N,W)]...
[Diff-Invariant][(U^N/u_0)+(W/w_0)]
[Ineq-Invariant] [0 < (U/u_0)^2*N
-(U/u_0)^N - w_0]
[Box-Invariants]
[u_0*(2^N/(1-4*w_0)^{N/2})
< U < 2^{N}*u_0]
[State:=] L_1_ [Polynomial-Scaling]
[Invariant] [X+Y-2*Z]
[State:=] L_2_ [Polynomial-Scaling]
[(2*K + 4*V + 2)-Invariant] ...
[Kernel(M-L):=] [Vect(K*V, V^2)]...
[Diff-Invariant] [k_0*K*V-v_0*V^2]
[Transitions:=] [rho_2]and[rho_3]
[Fractional-Scaling]
[Discrete-Invariant]
[(A*B)*(s_0*(1-s_0)*R^2+
R*S+S^2-R-2*S+1)]
[Invariant][(k_0*K*V-v_0*V^2)*(A*B)
*(s_0*(1-s_0)*R^2+R*S+S^2-R-2*S+1)]
[State:=] L_3_ [Strong-Scaling]
[Invariant] [(C*D^2)/2]
```

Fig. 1. An example which is beyond the limit of state-of-the-art approaches. The semi-algebraic hybrid system is depectied on the left and the result given by our methods is on the right.

the first system. Hence the two air plains (or planets) at least for some lapse of time, follow an elliptical path.

9 Conclusions

Our methods do not require (doubly) exponential computations from the use of Grobner bases, quantifier eliminations, cylindrical algebraic decompositions or direct resolution of non-linear systems, as well as they do not depend on any abstraction operators. Considering algebraic hybrid system, we succeeded in reducing the non-linear invariant generation problem to the intersection between specific eigenspaces and initial semi-affine/algebraic forms. Our non-trivial non-linear invariant generation method is sound and complete as we provide a complete encoding to handle multivariate fractional differential and discrete systems (algebraic system with multivariate rational functions). By reductions to linear algebraic problems, we generate *eigenspaces of non-trivial non-linear invariants* in *polynomial steps*. To the best of our knowledge, this is the first invariant generation method for hybrid systems with discrete transitions, differential rules, and local conditions that are described by *multivariate fractional systems*. Moreover, we presented the first necessary and sufficient conditions for the existence of *non-trivial* non-linear invariants for each type of non-linear differential rules using precise notions from computational and commutative algebras. We also identified large decidable classes for the non-linear non-trivial invariant generation problem. These important results can be used directly by any constraint-based invariant generation methods [9, 6, 12, 10] and any over-approximation and reachability analysis [20, 13, 21]. Finally, we believe that our methods could complete and reinforce the framework proposed in [6, 9].

References

[1] Henzinger, T.: 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) 278–292

[2] Tiwari, A., Rueß, H., Saïdi, H., Shankar, N.: 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)

[3] Manna, Z.: Mathematical Theory of Computation. McGrw-Hill (1974)

[4] Henzinger, T.A., Ho, P.H.: Hytech: The cornell hybrid technology tool. In: Hybrid Systems. (1994) 265–293

[5] Bengtsson, J., Larsen, K.G., Larsson, F., Pettersson, P., Yi, W.: Uppaal - a tool suite for automatic verification of real-time systems. In: Hybrid Systems. (1995) 232–243

[6] Sankaranarayanan, S., Sipma, H., Manna, Z.: Constructing invariants for hybrid system. In: Hybrid Systems: Computation and Control HSCC. Volume 2993 of LNCS., Springer (March 2004) 539–554

[7] Tiwari, A., Khanna, G.: Nonlinear systems: Approximating reach sets. In: Hybrid Systems: Computation and Control HSCC. Volume 2993 of LNCS., Springer (March 2004) 600–614

[8] Rodriguez-Carbonell, E., Tiwari, A.: Generating polynomial invariants for hybrid systems. In: Hybrid Systems: Computation and Control, HSCC 2005. Volume 3414 of LNCS. (March 2005) 590–605

[9] 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)

[10] A. Tiwari: Generating box invariants. In: Proc. of the 11th Int. Conf. on Hybrid Systems: Computation and Control HSCC. (2008)

[11] T. A. Henzinger, P. -H. Ho: Algorithmic analysis of nonlinear hybrid systems. In: Proceedings of the 7th International Conference On Computer Aided Verification. Volume 939. (1995) 225–238

[12] 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)

[13] Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Computer-Aided Verification, CAV 2008, Princeton, USA, Proceedings. LNCS, Springer (2008)

[14] Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates (2004)

[15] Buchberger, B.: Symbolic computation: Computer algebra and logic. In: Frontiers of Combining Systems: Proceedings of the 1st Int. Workshop, Munich (Germany). (1996) 193–220

[16] Weispfenning, V.: Quantifier elimination for real algebra - the quadratic case and beyond. Applicable Algebra in Engineering, Communication and Computing **8**(2) (1997) 85–101

[17] Collins, G.E.: Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition. LNCS (1975)

[18] Cousot, P., Cousot, R.: Abstract interpretation and application to logic programs. Journal of Logic Programming **13**(2–3) (1992) 103–179

[19] Rebiha, R., Matringe, N., Moura, A.V.: Endomorphisms for non-trivial non-linear loop invariant generation. In: 5th Int. Conf. Theoretical Aspects of Computing, LNCS (2008) 425–439

[20] Piazza, C., Antoniotti, M., Mysore, V., Policriti, A., Winkler, F., Mishra, B.: Algorithmic Algebraic Model Checking I: Challenges from Systems Biology. Volume 3576. (July 2005)

[21] Ramdani, N., Meslem, N., Candau, Y.: Reachability of uncertain nonlinear systems using a nonlinear hybridization. In: Hybrid Systems: Computation and Control, HSCC'08. Volume 4981., LNCS (2008) 415–428

[22] Floyd, R.W.: Assigning meanings to programs. In: Proc. 19th Symp.Applied Mathematics. (1967) 19–37

[23] Matringe, N., Vieira-Moura, A., Rebiha, R.: Endomorphism for non-trivial semi-algebraic loop invariant generation. Technical Report TR-IC-08-31, Institute of Computing, University of Campinas (November 2008)

[24] Lang, S.: Algebra. Springer (January 2002)

[25] Kreuzed, A., Robbiano, L.: Computational commutative algebra. Springer Verlag (2005)

[26] Tomlin, C., Pappas, G.J., Sastry, S.: Conflict resolution for air traffic management: a study in multiagent hybrid systems. Automatic Control, IEEE Transactions on **43**(4) (1998) 509–521