INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Multivariate Formal Power Series Invariants Generation for Non Linear Hybrid Systems

Nadir Matringe *Arnaldo Vieira Moura*
Rachid Rebiha

Technical Report - IC-09-09-48 - Relatório Técnico

December - 2009 - Dezembro

Multivariate Formal Power Series Invariants Generation for Non Linear 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 the first automatic verification methods that automatically generate invariants which are assertions expressed by *multivariate formal power series*. We also discuss their convergence analysis over hybrid systems that exhibit highly non linear models. As far as we know, this is the first approach that can deal with this type of systems or that can automatically generate this type of invariants. We show that the preconditions for discrete transitions, the Lie-derivatives for continuous evolution and the newly introduced relaxed consecution requirements can be viewed as morphisms and thus can be suitably represented by matrices. By doing so, we reduce the invariant generation problem to linear algebraic matrix systems, from which one can provide very effective methods for solving the original problem. Such methods have much lower time complexities than other approaches based on Grobner basis computations, quantifier eliminations, cylindrical algebraic decompositions, directly solving non-linear systems or abstract operators, or even the more recent constraint-based approaches. We illustrate the efficiency of our computational methods by dealing with highly non linear and complex hybrid systems.

1 Introduction

An invariant at a location of a system is an assertion that holds true for every reachable state associated to this location. Hybrid systems [1, 2] exhibit both discrete and continuous behaviors, as one often finds when modeling digital system embedded in analog environments. Moreover, most safety-critical systems, *e.g.* aircraft, automobiles, chemicals plants and biological systems, operate semantically as non-linear hybrid systems and can only be adequately modeled by means of non-linear arithmetic over the real numbers involving multivariate polynomial, fractional or transcendental functions. In this work, we use hybrid automata as a computational model for such hybrid systems. A hybrid automaton describes the interaction between discrete transitions and continuous dynamics, the latter being governed by local differential equations.

The analysis of hybrid systems has been one of the main challenges for the formal verification community for over a decade. Known verification approaches are based on inductive invariant generation methods [3, 4], combined with the reduction of safety-critical

⋆ 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

properties to invariant properties [5, 6]. More recent approaches have been constraint-based [7, 8, 9, 10, 11]. In these cases, a candidate invariant with 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 over the unknown coefficients, and whose solutions yield the desired invariants. One of the main advantage of such constraint-based approaches is that they do not dependent on widening operators that could lead to a too coarse abstraction when used together with fixed-point based techniques and, further, they are goal-oriented. But, on the other hand, they still require the computation of Grobner Bases [12], first-order quantifier elimination [13, 14] or abstraction operators, and known algorithms for those problems are, at least, of double exponential time complexity.

Despite tremendous progress over the past years [7, 15, 16, 8, 10, 17, 11, 18, 19, 20], the problem of invariant generation for hybrid systems remains very challenging for non-linear discrete systems, as well as for non-linear differential systems with non abstracted local and initial conditions. SAT Modulo Theory decision procedures could eventually be used to solve linear and decidable systems, but it is known that it is not adequate for treating non-linear theories. In fact, in the latter context it faces an intractable, undecidable problem [21, 22, 23].

Here, we present new methods for the automatic generation of invariants in the form of assertions where continuous functions are expressed by multivariate formal power series. These methods can then be applied to systems that exhibit continuous evolution modes described by multivariate polynomials or fractional differential rules. As far as we know, there are no methods that could deal with this type of systems or that could automatically generate this type of invariants. Also, these methods give rise to more efficient algorithms, with much lower complexity in space and time. The contribution is significant as it proposes the first automatic verification methods capable of generating such precise provable invariants, while dealing with highly non linear models present today in many critical hybrid embedded systems.

We develop the new methods by first extending our previous work on non-linear non-trivial invariant generation for discrete programs with nested loops and conditional statements that describe multivariate polynomial or fractional systems [24, 25, 26]. Then, we extend and generalize our previous work on non-linear invariant generation for hybrid systems [27, 28, 29, 30].

We can summarize our contributions as follows:

- As far as it is our knowledge we present the first methods which generates *Formal Power Series Invariant* for hybrid systems with highly non linear models. We reach a new level of precision that could be used for static analysis, reachability analysis, and safety verification of hybrid systems. We do not need to start with candidate invariants that generate intractable solving problems. Instead, we show that the preconditions for discrete transitions and the Lie-derivatives for continuous evolution can be viewed as morphisms and suitably represented by matrices. In this way, we reduce the invariant generation problem to linear algebraic matrix manipulations. We present an in-depth analysis of these automatically computed matrices and provide automated resolution

techniques and convergence analysis in order to reach precise provable multivariate formal power series invariants.
- We provide a computational method of lower complexity than the previous approaches that depend on Grobner basis computations, quantifier eliminations, cylindrical algebraic decompositions, direct resolution of algebraic systems or abstract operators.
- We bring in some new insights and necessary and sufficient conditions that allow for nice existence and completeness proofs of formal power series invariants. Our existence results and our methods could be reused to reduce the complexity of other fixed-point computations or constraint based approaches, *i.e.*, to reduce the number of Grobner basis computations and quantifier eliminations.
- We handle highly non-linear hybrid systems, extended with parameters and variables that are functions of time, that exhibit multivariate fractional or polynomial differential rules and discrete transitions relations.
- We introduce a more general approximation of consecution, for assertions expressed by multivariate formal power series.

In Section 2 we introduce algebraic hybrid systems and inductive assertions. In Section 3 we introduce our notations and representations for multivariate formal series and differential systems rules. In Section 4 we present new forms of approximating consecution with multivariate formal power series. In Section 5 we reduce the problem to triangular linear algebraic matrix systems. In Section 6 we provide necessary and sufficient conditions for existence proofs, and we show how to automatically compute invariants. In Section 7 we present convergence analysis. Before presenting our conclusions in Section 9, we illustrate the efficiency of our methods in Section 8 by generating invariants for some Volterra systems. The latter being well-known for their intractability when taken in their complete form by other state-of-the-art formal methods and static analysis approaches.

2 Algebraic Hybrid Systems and Inductive Assertions

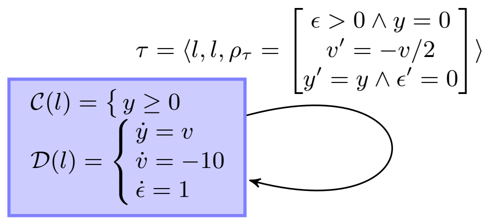
Let $K[X_1, .., X_n]$ be the ring of multivariate polynomials over the set of variables $\{X_1, .., X_n\}$. An ideal is any set $I \subseteq K[X_1, .., X_n]$ which contains the null polynomial and is closed under addition and under multiplication by any element in $K[X_1, .., X_n]$. Let $E \subseteq K[X_1, .., X_n]$ be a set of polynomials, the ideal generated by E is the set of finite sums $(E) = \{\sum_{i=1}^{k} P_i Q_i \mid P_i \in K[X_1, \ldots, X_n], Q_i \in E, k \geq 1\}$. 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*. Also, in the following we will write $\dot{F}$ for $\frac{dF}{dt}$ and we will use the standard notation $\frac{\partial F}{\partial x_j}$ for partial derivatives.

We use the notion of a hybrid automaton as the computational models for hybrid systems.

Definition 1 *A* hybrid system *is a tuple $\langle V, V_t, L, \mathcal{T}, \mathcal{C}, \mathcal{D}, l_0, \Theta \rangle$, where $V = \{X_1, .., X_n\}$ is a set of variables, $V_t = \{X_1(t), .., X_n(t)\}$ where $X_i(t)$ is a function of t, L is a set of locations and l_0 is the initial location. 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 $V \cup V_t \cup V' \cup V_t'$, 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. Also, Θ is the initial condition, given as a first-order assertion over $V \cup V_t$, and $\mathcal{C}$ 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 $V \cup \{dX_i/dt | X_i \in V_t\}$.*

A state is any pair from $L \times \mathbb{R}^{|V|}$. □

Example 1. The dynamic system of a bouncing ball ([31]) is modeled by the following hybrid automaton:



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

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

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 where l_0 is the* initial location *and we require $\kappa_0 \models \Theta$. For any two consecutive states $\langle l_i, \kappa_i \rangle$ and $\langle l_{i+1}, \kappa_{i+1} \rangle$ in such a run, the 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 $\langle \kappa_i, \kappa_{i+1} \rangle \models \rho_i$ where the primed state variables refer to κ_{i+1}. Otherwise, μ_i is a* continuous consecution *condition and we must have $q \in L$, $\varepsilon \in \mathbb{R}$ and a differentiable function $\phi : [0, \varepsilon] \to \mathbb{R}^{|V \cup V_t|}$ such that the following three conditions hold:*

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

A state $\langle \ell, \kappa \rangle$ is reachable if there is a run and some $i \geq 0$ such that $\langle \ell, \kappa \rangle = \langle \ell_i, \kappa_i \rangle$. □

Example 2. Return to Example 1 and consider a possible run: $\langle l, \kappa_0 \rangle \xrightarrow{\mu_0} \langle l, \kappa_1 \rangle \xrightarrow{\mu_1} \langle l, \kappa_2 \rangle$, where $\kappa_0 = (0, 16, 0)$. Note that in a valuation $(a, b, c) \in \mathbb{R}^3$, a is the value of the variable 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 $\phi : [0, \varepsilon] \to \mathbb{R}^{|V_t|}$ 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 $\langle \phi(t), d\phi(t)/dt \rangle \models \mathcal{D}(q)$ because $d\phi(t)/dt = (dy(t)/dt, dv(t)/dt, d\epsilon(t)/dt) = (v, -10, 1)$. So, by construction, μ_0 illustrates a possible continuous consecution.

Now, since $\langle (0, -16, \varepsilon), (0, 8, 0) \rangle \models \rho_\tau$, if we let $\kappa_2 = (0, 8, 0)$, then we can see that μ_2 is a discrete consecution. □

Definition 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 $\langle l, \kappa \rangle$ is a reachable state of W.* □

An invariant at l holds on all states that reach location l. Next, we need the notion of inductive assertions.

Definition 4 *Let W be a hybrid system and let D be an assertion domain. 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:*

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 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 $\kappa_{i+1} \models \gamma(l)$.* □

In other words, an inductive assertion holds in the initial state and at every possible state reachable by a combination of discrete transitions and continuous flow.

Example 3. Consider the hybrid system of Example 1. It is easy to verify that the assertion $y = v \times \epsilon + 5 \times \epsilon^2$ is a provable, inductive invariant. To do so, we just need to compute its derivative to see that the assertion holds during the continuous evolution. By direct observation of the transition relations, we can see that the assertion holds during discrete transitions too. □

3 Multivariate Formal Power Series and Differential Systems

Let W be a hybrid system, and let $\gamma(l)$ be an inductive assertion, as in Definition 4. Recall that an inductive assertion holds at the initial state and at every other possible states in a run. So, if $\gamma(l) \equiv (f(x_1, .., x_n) = 0)$ where f is a smooth function then $\mathcal{C}(l) \wedge (f(x_1, .., x_n) = 0) \models (d(f(x_1, .., x_n)/dt = 0)$. Hence, if γ is an inductive assertion map then $\gamma(l)$ is an invariant at l for W.

Let us describe the continuous evolution rules by a polynomial differential system S of the form:

$$S = \begin{cases} \dot{x}_1(t) = P_1(x_1(t), ..., x_n(t)) \\ \dot{x}_2(t) = P_2(x_1(t), ..., x_n(t)) \\ \vdots \\ \dot{x}_n(t) = P_n(x_1(t), ..., x_n(t)). \end{cases} \tag{1}$$

By a formal power series, we mean the following:

Definition 5 *A formal power series in the indeterminates $x_1, \ldots, x_n$ is an expression of the following type:*
$\sum_{(i_1,..,1_n) \in \mathbb{N}^n} f_{i_1,...,i_n} x^{i_1} ... x^{i_n}$*, where the coefficients $f_{i_1,...,i_n}$ belong to $\mathbb{R}$.* □

Whenever $i = (i_1, ..., i_n) \in \mathbb{N}^n$, we denote the sum $i_1 + \cdots + i_n$ by $|i|$.

Definition 6 *We say that an order $<$ is a lexicographical total ordering in $\mathbb{N}^n$ if for any two elements $i = (i_1, ..., i_n) \in \mathbb{N}^n$ and $j = (j_1, ..., j_n) \in \mathbb{N}^n$ we have that $(j_1, ..., j_n) < (i_1, ..., i_n)$ holds if and only if one of the following condition holds:*

- $|j| < |i|$, *or*
- $|j| = |i|$, *and the first non zero component of $i - j$ is positive.* □

Hence, the monomials $x_1^{i_1}...x_n^{i_n}$ with $|i| = k$, where $i = (i_1, ..., i_n)$, form an ordered basis for the vector space of homogeneous polynomials of total degree k. This means that any homogeneous polynomial of total degree k can be written in the following ordered form:

$$\sum_{|i|=k} f_{i_1,...,i_n} x_1^{i_1} \dots x_n^{i_n}.$$

As a consequence, as a formal power series $F(x_1, .., x_n)$ is the direct sum of its homogeneous components, and it can be written in the following ordered form:

$$F(x_1, .., x_n) = \sum k \geq 1 \sum_{|i|=k} f_{i_1,...,i_n} x_1^{i_1} \dots x_n^{i_n}.$$

We will use the following useful notation from [32]: the coefficients of homogeneous polynomials of degree k will be denote by

$$F_k = \begin{bmatrix} f_{k,0,0,...,0} \\ f_{k-1,1,0,...,0} \\ f_{k-1,0,1,...,0} \\ \vdots \\ f_{0,0,0,...,k} \end{bmatrix}$$

and a monomial of degree k will be denoted by the following vector:

$$X^k = \begin{bmatrix} {x_1}^k \\ {x_1}^{k-1} x_2 \\ {x_1}^{k-1} x_3 \\ \vdots \\ {x_n}^k \end{bmatrix}.$$

where the coordinates are ordered with the lexicographical total ordering as in Definition 6.

With this notation, the formal power series $F(x_1, .., x_n)$ can be written as

$$\sum_{k \geq 1} F_k \cdot X^k = F_1 \cdot X^1 + ... + F_k \cdot X^k + ...,$$

where $F_k \cdot X^k$ denotes the scalar product $\langle F_k, X^k \rangle$.

The polynomial $P_i(x_1, \dots, x_n)$ can thus be written in the form:

$$P_i(x_1, \dots, x_n) = P_1^i \cdot X^1 + ... + P_m^i \cdot X^m,$$

where m is the maximal degree among all the polynomials P_i, and P_j^i is the coefficient vector of P_i. Denote by $x(t)$ the vector $(x_1(t), ..., x_n(t))T$. Then system S can be written as

$$\dot{x} = A_1 \cdot X^1(t) + ... + A_m \cdot X^m(t),$$

where

$$A_j = \begin{bmatrix} P_j^1 \\ \vdots \\ P_j^n \end{bmatrix}.$$

In particular, A_1 is the $n \times n$ matrix which is actually equal to the Jacobian matrix of the polynomial system given by the P_i's at zero.

4 New continuous consecution conditions

Now we show how to encode differential continuous consecution conditions. Let S be a polynomial differential system as described by Eq. (1).

Definition 7 *A function F from $\mathbb{R}^n$ to $\mathbb{R}$ is said to be a λ-invariant for system S if, for any solution $x(t) = (x_1(t), ..., x_n(t))$ of S, we have*

$$d/dtF(x_1(t), ..., x_n(t)) = \lambda F(x_1(t), ..., x_n(t)). \tag{2}$$

□

Eq. (2) encodes the fact that the numerical value of the Lie derivative of F is given by λ times its numerical value throughout out the time interval $[0, \varepsilon]$. Without loss of generality we will assume that λ is a constant. It is worth noticing, however, that our methods will also work when λ is a multivariate fractional or multivariate polynomial, as we proposed for the case of multivariate polynomial invariants generation.

Now, we want to establish sufficient conditions over system S for it to admit λ-invariants which are formal power series. Note that a formal power series $F(x) = F_1 \cdot X^1 + ... + F_k \cdot X^k + ...$ is a λ-invariant if the following conditions holds:

$$\sum_{i=0}^{n} \frac{\partial F(x)}{\partial x_j} P_i(x) = \lambda F(x). \tag{3}$$

Using our notation, we obtain:

$$\sum_{i=0}^{n} \frac{\partial (F_1 \cdot X^1 + ... + F_k \cdot X^k + ...)}{\partial x_j} (P_1^i \cdot X^1 + ... + P_m^i \cdot X^m)$$
$$= \lambda (F_1 \cdot X^1 + ... + F_k \cdot X^k + ...). \tag{4}$$

5 Reduction to linear algebra

Starting from Eq. (4), we get

$$\sum_{i=0}^{n} \frac{\partial(F_1 \cdot X^1 + ... + F_k \cdot X^k + ...)}{\partial x_j}(P_1^i \cdot X^1 + ... + P_m^i \cdot X^m)$$
$$-\lambda(F_1 \cdot X^1 + ... + F_k \cdot X^k + ...) = 0.$$

By directly expanding the left side and collecting terms corresponding to increasing degrees, we have:

$$\begin{array}{ll}
(1): & \sum_{j=1}^{n} \frac{\partial(F_1X^1)}{\partial x^j} P_1^j X^1 - \lambda F_1 X^1 = 0 \\
(2): & \sum_{j=1}^{n} [\frac{\partial(F_1X^1)}{\partial x^j} P_2^j X^2 + \frac{\partial(F_2X^2))}{\partial x^j} P_1^j X^1] - \lambda F_2 X^2 = 0 \\
(3): & \sum_{j=1}^{n} [\frac{\partial(F_1X^1)}{\partial x^j} P_3^j X^3 + \frac{\partial(F_2X^2))}{\partial x^j} P_2^j X^2 + \frac{\partial(F_1X^1))}{\partial x^j} P_3^j X^3] - \lambda F_3 X^3 = 0 \\
\vdots & \vdots \\
(m): & \sum_{j=1}^{n} [\frac{\partial(F_1X^1)}{\partial x^j} P_m^j X^m + \frac{\partial(F_2X^2))}{\partial x^j} P_{m-1}^j X^{m-1} + \\
 & + \cdots + \frac{\partial(F_mX^m))}{\partial x^j} P_1^j X^1] - \lambda F_m X^m = 0 \\
(m+1): & \sum_{j=1}^{n} [\frac{\partial(F_2X^2)}{\partial x^j} P_m^j X^m + \frac{\partial(F_3X^3))}{\partial x^j} P_{m-1}^j X^{m-1} + \\
 & + \cdots + \frac{\partial(F_{m+1}X^{m)+1})}{\partial x^j} P_1^j X^1] - \lambda F_{m+1} X^{m+1} = 0 \\
\vdots & \vdots
\end{array}$$

The equation corresponding to degree k is:

$$\sum_{j=1}^{n} [\frac{\partial(F_{k-min(k,m)+1}X^{k-min(k,m)+1})}{\partial x^j} P_m^j X^m + \frac{\partial(F_{k-min(k,m)+2}X^{k-min(k,m)+1})}{\partial x^j} P_{m-1}^j X^{m-1} +$$
$$+ \cdots + \frac{\partial(F_kX^k)}{\partial x_j} P_1^j X^1] - \lambda F_k X^k = 0$$

Now, consider the linear morphism $D_{p-k,p}$ from $R_{p-k}[x_1, \dots, x_n]$ to $R_p[x_1, \dots, x_n]$, given by

$$D_{p-k,p} : \begin{cases} \mathbb{R}_{p-k}[x_1, \dots, x_n] \to \mathbb{R}_p[x_1, \dots, x_n] \\ P(X = x_1, \dots, x_n) \mapsto \sum_{j=1,\dots,n} (\partial_j P(X)) P_{k+1}^j . X^{k+1} \end{cases}$$

which can be represented by the matrix $M_{p-k,p}$, in the ordered canonical basis of $R_{p-k}[x_1, \dots, x_n]$ and $R_p[x_1, \dots, x_n]$, respectively. Its l-th column is the decomposition of the polynomial

$$\sum_{j=1,\dots,n} (\partial_j P(X)) P_{k+1}^j . X^{k+1},$$

where $P(X)$ is the l-th monomial in the ordered basis

$$\left\{x_1^p, x_1^{p-1}x_2, x_1^{p-1}x_3, \dots, x_n^p\right\}.$$

Then we can reduce the infinite equation systems, described just above, to the following linear algebraic system:

$$\begin{cases} (M_{1,1} - \lambda I_2)F_1 = 0 \\ M_{1,2}F_1 + (M_{2,2} - \lambda I_2)F_2 = 0 \\ M_{1,3}F_1 + M_{2,3}F_2 + (M_{3,3} - \lambda I_4)F_3 = 0 \\ \vdots \\ M_{k-min(k,m)+1,k}F_{k-min(k,m)+1} \\ +M_{k-min(k,m)+2,k}F_{k-min(k,m)+2} \\ + \cdots + (M_{k,k} - \lambda I_{k+1})F_k = 0 \\ \vdots \end{cases} \tag{5}$$

By definition of the linear morphisms $D_{p-k,p}$, we can precisely and symbolically compute all the matrices $M_{m,n}$. By so doing, we obtain matrices similar to those that appeared in the determinant analysis of integrability of differential systems in [32]. We will, thus, use our following characterization.

Lemma 1 *Assume that matrix $A = M_{1,1}$ is trigonal, i.e.*

$$A = \begin{bmatrix} \lambda_1 & & & & \\ \star & \lambda_2 & & & \\ \star & \star & \ddots & & \\ \star & \star & \star & \lambda_{n-1} & \\ \star & \star & \star & \star & \lambda_n \end{bmatrix}.$$

Then $M_{p,p}$ is also trigonal with diagonal terms $i_1\lambda_1 + \cdots + i_n\lambda_n$, where $i_1 + \cdots + i_n = p$. $\square$

Proof. In this case,

$$P_1^j.X^1 = \lambda_j x_j + a_{j,j+1}x_{j+1} + \cdots + a_{j,n}x_n.$$

Now consider the monomial basis $P(X) = x_1^{i_1} \dots x_n^{i_n}$, where $i_1 + \cdots + i_n = p$. One has

$$\begin{aligned} D_{p,p}(X) &= i_1 x_1^{i_1-1} \dots x_n^{i_n}(\lambda_1 x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n) \\ &\quad + i_2 x_1^{i_1} x_2^{i_2-1} \dots x_n^{i_n}(\lambda_2 x_2 + a_{2,3}x_3 + \cdots + a_{2,n}x_n) \\ &\quad + \cdots + i_n x_1^{i_1} \dots x_n^{i_n-1}(\lambda_n x_n) \\ &= (i_1\lambda_1 + \cdots + i_n\lambda_n)x_1^{i_1} \dots x_n^{i_n} + \Omega, \end{aligned}$$

where Ω indicates a sum of monomials that come after $x_1^{i_1} \dots x_n^{i_n}$ in the ordered basis of $R_p[x_1, \dots, x_n]$, that is, they are higher terms.

Then, the matrix $M_{p,p}$ corresponding to $D_{p,p}$, in the canonical ordered basis of $R_p[x_1,\dots,x_n]$, is:

$$\begin{bmatrix} p\lambda_1 & & & & & & \\ \star & (p-1)\lambda_1+\lambda_2 & & & & & \\ \star & \star & \ddots & & & & \\ \star & \star & \star & \sum_{k=1}^{n} i_k\lambda_k & & & \\ \star & \star & \star & \star & \ddots & & \\ \star & \star & \star & \star & \star & \lambda_{n-1}+(p-1)\lambda_n & \\ \star & \star & \star & \star & \star & \star & p\lambda_n \end{bmatrix}$$

Thus, it is also trigonal with diagonal terms $i_1\lambda_1+\cdots+i_n\lambda_n$, where $i_1+\cdots+i_n=p$. □

6 Existence proofs and invariants generation

First, let us examine necessary and sufficient existence conditions for the computation of λ-invariants.

6.1 Existence conditions and the computation of λ-invariants

We obtain the following main results on existence of formal power series invariants for system described as system S, in Eq. (1).

Theorem 1 *Let A be the Jacobian matrix at zero of the polynomial $P=(P_1,...,P_n)$ defining the system S, whose expression is: $(\partial_i P_j(0,...,0)i,j\in[1,n]^2)$. Assume $P_k(0,..,0)=0$. If A is trigonalizable with eigenvalues $\lambda_1\le...\le\lambda_n$ then there exists a formal power series λ-invariant for S when all eigenvalues are positive, or are all negative, with $\lambda=\lambda_1$.* □

Proof. Up to a linear change of variables, we can assume that matrix A is triangular with diagonal terms $\lambda_1\le...\le\lambda_n$. We know that matrix $M_{k,k}$ has the form described in Lemma 1. As A is triangular, so is $M_{k,k}$, and its diagonal terms are the real numbers $i_1\lambda_1+\cdots+i_n\lambda_n$, where $i_1+\cdots+i_n=k$. Hence, the diagonal terms of $M_{k,k}-\lambda I_{k+1}$ are $0\le\lambda_2-\lambda...\le\lambda_n-\lambda$ when $k=1$. Also, it has a nonzero kernel, and so we can chose a nonzero F_1, such that $(M_{1,1}-\lambda I_2)F_1=0$.

For $k\ge 2$ and $i_1+\cdots+i_n=k$, the diagonal terms $i_1\lambda_1+\cdots+i_n\lambda_n-\lambda$ of the triangular matrix $M_{k,k}-\lambda I_{k+1}$ are greater than $i_1\lambda_1+\cdots+i_n\lambda_n-\lambda=k\lambda-\lambda>\lambda>0$. So, $M_{k,k}-\lambda I_{k+1}$ is invertible.

Hence we can choose:

- $F_2=-(M_{2,2}-\lambda I_3)^{-1}M_{1,2}F_1$, and then
- $F_3=-(M_{3,3}-\lambda I_4)^{-1}(M_{1,3}F_1+M_{2,3}F_2)$, and recursively,
- $F_k=-(M_{k,k}-\lambda I_{k+1})^{-1}(M_{k-min(k,m)+1,k}F_{k-min(k,m)+1}+\cdots+M_{k-1,k}F_{k-1})$.

This gives $(F_1,F_2,\dots)$ as a nonzero solution of the system, and the corresponding formal power series $\sum_i F_iX^i$ is a formal λ-invariant. □

In the proof of the preceding important theorem, we also provide the methods for the resolution of the triangular matrix system. Clearly, we are then able to generates nonzero formal power series $\sum_i F_i X^i$ which are λ-invariants associated to the nonzero solution $(F_1, F_2, \dots)$. We note that we used Maple to compute the matrix products to obtain F_k in its symbolic form.

Remark 1. The trigonizable matrices of $M_n(\mathbb{R})$ form a dense open subset of total measure of $M_n(\mathbb{R})$.

Next, we treat inductive invariants.

6.2 Inductive invariants for any initial conditions

We have the following basic result.

Theorem 2 *Let A be the Jacobian matrix at zero of the polynomial $P = (P_1, ..., P_n)$ defining a system S, as in Eq. (1), and whose expression is $(\partial_i P_j(0, ..., 0),\ i, j \in [1, n]^2)$. Assume, further, that $P_k(0, .., 0) = 0$.*
Suppose that A is trigonalizable with eigenvalues $\lambda_1 \leq ... \leq \lambda_n$. We will also denote λ_1 by λ and will assume also that the eigenspace associated with λ is of dimension at least 2.
Then the (proof of the) preceding theorem asserts the existence of at least 2 independent λ-invariants F_1 and F_2. If there is an open subset U of $\mathbb{R}^n$, over which F_1 and F_2 define two normally convergent power series, then for any initial value $(x_{1,0}, \dots, x_{n,0})$, the power series

$$F_2(x_{1,0}, \dots, x_0^n)F_1 - F_1(x_0^1, \dots, x_0^n)F_2$$

defines an inductive invariant on U for the solution of S with initial conditions $x_1(0) = x_{1,0}, \dots, x_n(0) = x_{n,0}$. □

Proof. We know that F_1 and F_2 are convergent for a solution $(x_1(t), \dots, x_n(t))$ with initial values $(x_{1,0}, \dots, x_{n,0})$ in U. Hence, it must stay in U for small t. Moreover, since F_1 and F_2 are independent,

$$F = F_2(x_{1,0}, \dots, x_{n,0})F_1 - F_1(x_{1,0}, \dots, x_{n,0})F_2$$

is a nonzero λ-invariant which vanishes at $(x_{1,0}, \dots, x_{n,0})$. As the power series converges normally on U, so does any of their derivatives. Thus,

$$\begin{aligned} \dot{F}(x_1(t), \dots, x_n(t)) &= \textstyle\sum_{i=1}^n \partial_i F(x_1(t), \dots, x_n(t))\dot{x}_i(t) \\ &= \lambda F(x_1(t), \dots, x_n(t)) \end{aligned}$$

because of the λ-invariant property. Hence, $F(x_1(t), \dots, x_n(t))$ must be equal to $t \mapsto k e^{\lambda t}$ for some constant k. But now, as $F(x_{1,0}, \dots, x_{n,0})$ equals zero, this implies that k is zero, and so is $F(x_1(t), \dots, x_n(t))$ for any t such that $(x_1(t), \dots, x_n(t))$ is in U. □

All the invariant generation methods presented so far, automatically generate basis for non trivial multivariate formal power series invariants for each differential rule associated to locations in the hybrid automaton. In previous works [27, 28, 29, 30], we have shown that the preconditions for discrete transitions can be viewed as morphisms over a vector space of degree bounded by polynomials which can, thus, be suitably represented by matrices. For the discrete transitions consecution conditions we only used one morphism per circuit or loop in the transition relations. We also introduced more general forms of approximating discrete transition consecution, called fraction and polynomial consecutions. The new relaxed consecution requirements are also encoded as morphisms represented by matrices with terms that are linear in the unknown coefficients used to approximate the consecution conditions. See [27, 28, 29, 30] for more details on how we put it all together, *i.e.* how we integrate all type of invariants and initial conditions in order to generates a global one.

7 Diagonal dominant trigonalisable degree 2 systems of 2 variables

In this section we show how our method applies to the general system:

$$\begin{cases} \dot{x}(t) = ax(t) + by(t) + a_{1,1}x^2(t) + a_{1,2}x(t)y(t) + a_{2,2}y^2(t) \\ \dot{y}(t) = cy(t) + b_{1,1}x^2(t) + b_{1,2}x(t)y(t) + b_{2,2}y^2(t) \end{cases}$$

where $a, b, c, a_{1,1}, a_{1,2}, a_{2,2}, b_{1,1}, b_{1,2}, b_{2,2}$ are parameters in V and x, y are in V_t.

The Jacobian matrix at zero of the polynomials defining the system is $\begin{pmatrix} a & \\ b & c \end{pmatrix}$. Hence, from Theorem 1, we already know that we can find a formal power F series which is a a-invariant. Looking more closely at the coefficients of such a series we will show that it must converge in some appropriate neighborhood of 0. Moreover, as the multiplicity of a as an eigenvalue is 2, we will be able to apply Theorem 2.

7.1 The matrices $M_{p-k,p}$

Using our notation, the coefficient vectors P_i are zero, for all $i \geq 2$. Then $M_{p-k,p}$ is the matrix whose l-th column is the vector corresponding to the decomposition of the polynomial

$$\begin{aligned} &\partial_1[(0,\ldots,0,\underbrace{1}_{l-th\ place},0,\ldots,0)X^{p-k}]P^1_{k+1}X^{k+1} \\ &+\partial_2[(0,\ldots,0,\underbrace{1}_{l-th\ place},0,\ldots,0)X^{p-k}]P^2_{k+1}X^{k+1} \end{aligned}$$

in the ordered canonical basis of $\mathbb{R}_p[x,y]$. Here, the polynomial $(0,\ldots,0,\underbrace{1}_{l-th\ place},0,\ldots,0)X^{p-k}$ is the l-th monomial of the canonical basis of $\mathbb{R}_{p-k}[x,y]$.

Therefore, the matrices $M_{p-k,p}$ are zero unless $k = 0$ or $k = 1$. When $k = 0$, the general form of $M_{p,p}$ is given in Section 5 and, in our particular case, it is

$$\begin{pmatrix} pa & & & & & \\ p.b & (p-1)a+c & & & & \\ & (p-1)b & (p-2)a+2c & & & \\ & & \ddots & \ddots & & \\ & & & 2b & a+(p-1)c & \\ & & & & b & pc \end{pmatrix}.$$

Note that $p+1$ is actually the dimension of $\mathbb{R}_p[x,y]$.

Matrix $M_{p-1,p}$ is rectangular with $p+1$ rows, and p columns. Here, the l-th monomial in the basis of $\mathbb{R}_{p-1}[x,y]$ is $x^{p-l-1}y^l$. Also, the polynomial $P_2^1X^2$ is $a_{1,1}x^2+a_{1,2}xy+a_{2,2}y^2$ and the polynomial $P_2^2X^2$ is $b_{1,1}x^2+b_{1,2}xy+b_{2,2}y^2$. Hence, matrix $M_{p-1,p}$ can be written as:

$$\begin{pmatrix}
(p-1)a_{1,1} & b_{1,1} & & & & \\
(p-1)a_{1,2} & (p-2)a_{1,1}+b_{1,2} & 2b_{1,1} & & & \\
(p-1)a_{2,2} & (p-2)a_{1,2}+b_{2,2} & (p-3)a_{1,1}+2b_{1,2} & 3b_{1,1} & & \\
 & \ddots & \ddots & \ddots & \ddots & \\
 & & 3a_{2,2} & 2a_{1,2}+(p-3)b_{1,2} & a_{1,1}+(p-2)b_{1,2} & (p-1)b_{1,1} \\
 & & & 2a_{2,2} & a_{1,2}+(p-2)b_{2,2} & (p-1)b_{1,2} \\
 & & & & a_{2,2} & (p-1)b_{2,2}
\end{pmatrix}.$$

7.2 Resolution of the infinite triangular system

Since we are looking for λ-scale invariants, we already know that we can choose $\lambda = min(a,c)$. Then, the system to solve is given by

$$\begin{cases}
(M_{1,1}-\lambda I_2)F_1 = 0 \\
M_{1,2}F_1 + (M_{2,2}-\lambda I_3)F_2 = 0 \\
M_{2,3}F_2 + (M_{3,3}-\lambda I_4)F_3 = 0 \\
\vdots \\
M_{k-1,k}F_{k-1} + (M_{k,k}-\lambda I_{k+1})F_k = 0 \\
\vdots
\end{cases}$$

It can be written as:

$$\begin{cases}
(M_{1,1}-\lambda I_2)F_1 = 0 \\
F_2 = -(M_{2,2}-\lambda I_3)^{-1}M_{1,2}F_1 \\
F_3 = -(M_{3,3}-\lambda I_4)^{-1}M_{2,3}F_2 \\
\vdots \\
F_k = -(M_{k,k}-\lambda I_{k+1})^{-1}M_{k-1,k}F_{k-1} \\
\vdots
\end{cases}$$

So, one can choose thus

- any F_1, and then
- F_k as $(-1)^{k+1}U_k(F_1)$, where U_k is the matrix with $k+1$ rows and 2 columns given by the product

$$\begin{aligned}
&[(M_{k,k}-\lambda I_{k+1})^{-1}M_{k-1,k}]\cdot[(M_{k-1,k-1}-\lambda I_k)^{-1}M_{k-2,k-1}] \\
&\qquad \ldots [(M_{2,2}-\lambda I_3)^{-1}M_{2,3}]\cdot[(M_{2,2}-\lambda I_3)^{-1}M_{1,2}].
\end{aligned}$$

$M_{k,k} - \lambda I_{k+1}$ is

$$\begin{pmatrix} ka-\lambda & & & & & \\ k.b & (k-1)a+c-\lambda & & & & \\ & (k-1)b & (k-2)a+2c-\lambda & & & \\ & & \ddots & \ddots & & \\ & & & 2b & a+(k-1)c-\lambda & \\ & & & & b & kc-\lambda \end{pmatrix},$$

which can be decomposed as the product

$$DT = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & d_3 & & & \\ & & & \ddots & & \\ & & & & d_k & \\ & & & & & d_{k+1} \end{pmatrix} \begin{pmatrix} 1 & & & & & \\ t_2 & 1 & & & & \\ & t_3 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & t_k & 1 & \\ & & & & t_{k+1} & 1 \end{pmatrix},$$

where $d_i = (k+1-i)a + (i-1)c$ and $t_j = (k+2-j)b/d_j$.

So, matrix $(M_{k,k} - \lambda I_{k+1})^{-1}$ is equal to $T^{-1}D^{-1}$, where D^{-1} has the obvious form and T^{-1} is

$$\begin{pmatrix} 1 & & & & & \\ -t_2 & 1 & & & & \\ t_2t_3 & -t_3 & 1 & & & \\ -t_2t_3t_4 & t_3t_4 & -t_4 & 1 & & \\ \star & \star & \star & \star & \star & \\ (-1)^k t_2 \dots t_{k+1} & (-1)^{k-1} t_3 \dots t_{k+1} & \dots & t_k t_{k+1} & -t_{k+1} & 1 \end{pmatrix}.$$

7.3 Convergence of the λ-invariant

We want to show that if $\lambda > 2b$, the coefficients of the F_i vectors decrease quickly enough so that the invariant F converges in a neighborhood of zero. But first, we recall basic properties of norms in finite dimension real vector spaces, as well as the associated matrix norms.

If v, with coordinates v_i, belongs to $\mathbb{R}^n$, we denote by $|v|_\infty$ the value $\max_{i=1,\dots,n} |v_i|$. Now, if A is a matrix with m rows and n columns, representing a morphism from $(\mathbb{R}^n, |.|_\infty)$ to $(\mathbb{R}^m, |.|_\infty)$ in the canonical basis, it is well-known and easily proved that associated with the norm $|.|_\infty$ is the matricial norm $||.||$ on $M_{m,n}(\mathbb{R})$, where

$$||A|| = \max_{i=1,\dots,m} (\sum_{j=1}^{n} |A_{i,j}|).$$

Moreover, using this norm, if $v \in \mathbb{R}^n$ then one has that $|Av|_\infty \leq ||A||.|v|_\infty$. This implies that if A and B are two matrices belonging, respectively, to $M_{m,n}(\mathbb{R})$ and $M_{n,p}(\mathbb{R})$, then one has that

$$||AB|| \leq ||A|| \cdot ||B||.$$

In particular, the norm $||U_k||$ is less than or equal to the product

$$||M_{k,k} - \lambda I_{k+1}| \cdot |||M_{k-1,k}|| \dots ||M_{2,2} - aI_3|| \cdot ||M_{1,2}||.$$

But, from the expressions for matrices $M_{k-1,k}$, we have that $||M_{k-1,k}|| \leq f(k-1)$, where $f = 4 \cdot \max(|a_{i,j}|, |b_{i',j'}|)$. From the preceding paragraph again, we deduce that

$$||(M_{k,k} - \lambda I_{k+1})^{-1}|| \leq ||D^{-1}|| \cdot ||T^{-1}||.$$

But $||D^{-1}|| = \max_i(d_i^{-1}) = [(k-1)\lambda]^{-1}$, because $\lambda = \min(a, c)$, and so

$$||T^{-1}|| = \max_i (1 + t_i + t_{i-1}t_i + \cdots + t_2 t_3 \ldots t_{i-1} t_i),$$

but as each t_j is less than $(k+2-j)b/d_j \leq kb/[(k-1)\lambda] \leq 2b/\lambda$. Suppose now that $\lambda > 2b$. Then

$$||T^{-1}|| \leq 1 + 2b/\lambda + \cdots + (2b/\lambda)^k \leq 1/(1 - 2b/\lambda).$$

By letting e be the constant $1/(1 - 2b/\lambda)$, we can write

$$||(M_{k,k} - \lambda I_{k+1})^{-1}|| \leq e/(k-1)\lambda.$$

Finally, $||U_k||$ is less than $(ef/\lambda)^{k-2} = r^{k-2}$. Hence, eventually we have

$$|F_k|_\infty = |U_k(F_1)|_\infty \leq ||U_k||.|F_1|_\infty \leq r^{k-2}|F_1|_\infty.$$

Let t be $\max(|x|, |y|)$. Then

$$\begin{aligned} |F(x,y)| &\leq \\ |F_1 X^1| + |F_2 X^2| \cdots + |F_k X^k| + \cdots &\leq \\ 2|F_1|_\infty t + 3|F_2|_\infty t^2 + \cdots + (k+1)|F_k|_\infty t^k + \ldots \end{aligned}$$

The right part of the inequality is itself inferior to

$$1/r^2 |F_1|_\infty [2(rt) + 3(rt)^2 + \cdots + (k+1)(rt)^k + \ldots],$$

which, from the classical theory of one variable power series, is convergent in the open disk centered at zero and of radius $1/r$.

Hence we have proved the following.

Proposition 1 *Consider the system*

$$\begin{cases} \dot{x}(t) = ax(t) + by(t) + a_{1,1}x(t)^2 + a_{1,2}x(t)y(t) + a_{2,2}y(t)^2 \\ \dot{y}(t) = cy(t) + b_{1,1}x(t)^2 + b_{1,2}x(t)y(t) + b_{2,2}y(t)^2 \end{cases}$$

with a and c positive and strictly greater than $2b$. Let λ be the minimum between a and c. Then there exists a λ-invariant, obtained as in Theorem 2, and which always converges in a neighborhood of zero. □

7.4 The case of eigenspaces with dimension 2

Now, suppose that the eigenspace corresponding to λ has multiplicity 2, *i.e.* $a = c = \lambda > 0$ and $b = 0$. We know, from the previous subsection, that any λ-invariant will converge in a ball of radius $1/r$ and centered at zero. Moreover, according to Theorem 2, this will actually give an inductive invariant for the system, for any initial solutions within this ball.

More precisely, by letting $F_1^1 = \begin{pmatrix}1\\0\end{pmatrix}$ and $F_1^2 = \begin{pmatrix}0\\1\end{pmatrix}$, we get a basis $F^1(x,y)$ and $F^2(x,y)$ of λ-invariants that converge in the open $|.|_\infty$-disk of radius $1/r$ and centered at zero. Note that the monomial of degree one in F^1's Taylor series is x, and it is y in F^2's Taylor series. In other words, if we take the first coefficient of F as $\begin{pmatrix}1\\0\end{pmatrix}$, we obtain a λ-invariant $F = F^1(x,y)$ and, similarly, if we take the second coefficient of F as $\begin{pmatrix}0\\1\end{pmatrix}$, we obtain another λ-invariant $F = F^2(x,y)$ Moreover, these two invariants form a basis for invariants that converge in the open $|.|_\infty$-disk and of radius $1/r$ and centered at zero.

Assume now that we are given initial values, $x(0) = x_0$ and $y(0) = y_0$, for solutions in this open disk. Then, there will always exist two real numbers, λ and μ, such that

$$\lambda(x_0,y_0)F^1(x_0,y_0) + \mu(x_0,y_0)F^2(x_0,y_0) = 0,$$

where $\lambda(x_0,y_0) = F^2(x_0,y_0)$ and $\mu(x_0,y_0) = -F^1(x_0,y_0)$. Then,

$$\lambda(x_0,y_0)F^1 + \mu(x_0,y_0)F^2$$

is an invariant for the solution corresponding to the initial condition (x_0,y_0). Clearly, given (x_0,y_0) in the $|.|_\infty$-disk of radius $1/r$ and centered at zero, the invariant depends smoothly on the initial condition.

8 Example: Volterra systems

In this section, we show how our method applies to the so called Lotka-Volterra systems [33], which are given by:

$$\begin{cases} \dot{x}(t) = ax(t) + bx(t)y(t) \\ \dot{y}(t) = cy(t) + dx(t)y(t). \end{cases}$$

Also known as the *predator-prey equations*, these non linear differential equations are frequently used to describe the dynamics of biological systems in which two species interact, one a predator and the other its prey. Variable x, which is a function of time, gives the number of preys, and y corresponds to the number of predators. Their derivatives, $\dot{x}$ and $\dot{y}$, model the growth of the two population as time passes. Here, a, b, c and d are parameters modeling the interaction between predators and preys. The first equation expresses the fact that the change in the number of preys is given by its own growth minus the rate at which it is preyed upon. The second equation can be interpreted as the change in the number of predators fueled by the food supply, minus natural death.

The Jacobian matrix at zero for the polynomials defining the system is $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Hence, from Theorem 1, we already know that we can find a formal power series F which is an a-invariant. Looking more closely at the coefficients of such a series, we will show that it must converge in some appropriate neighborhood of 0. Moreover, since the multiplicity of a as an eigenvalue is 2, we will be able to apply Theorem 2 also.

8.1 The matrices $M_{p-k,p}$

The coefficient vectors P_i are zero, for $i \geq 2$. So, $M_{p-k,p}$ is the matrix whose l-th column is the vector corresponding to the decomposition of the polynomial

$$\begin{aligned} &\partial_1[(0,\dots,0,\underbrace{1}_{l-th\ place},0,\dots,0)X^{p-k}]P^1_{k+1}X^{k+1} \\ &+\partial_2[(0,\dots,0,\underbrace{1}_{l-th\ place},0,\dots,0)X^{p-k}]P^2_{k+1}X^{k+1} \end{aligned}$$

in the ordered canonical basis of $\mathbb{R}_p[x,y]$. Hence, in the Volterra case, the matrices $M_{p-k,p}$ are zero unless $k=0$ or $k=1$. When $k=0$, the general form of $M_{p,p}$ in our particular case is, as given in Section 5, equal to paI_{p+1}. Note that $p+1$ is actually the dimension of $\mathbb{R}_p[x,y]$. The matrix $M_{p-1,p}$ is rectangular with $p+1$ rows, and p columns. In this case, the l-th monomial of the basis of $\mathbb{R}_{p-1}[x,y]$ is $x^{p-l-1}y^l$, the polynomial $P^1_2X^2$ is bxy and the polynomial $P^2_2X^2$ is dxy.

Hence

$$\begin{aligned} &\partial_1[(0,\dots,0,\underbrace{1}_{l-th\ place},0,\dots,0)X^{p-1}]P^1_2X^2 \\ &+\partial_2[(0,\dots,0,\underbrace{1}_{l-th\ place},0,\dots,0)X^{p-1}]P^2_2X^2 \end{aligned}$$

reduces to $b(p-l-1)x^{p-l-1}y^{l+1}+dlx^{p-l}y^l$. Eventually, the matrix can be written as:

$$M_{p-1,p} = \begin{pmatrix} 0 & & & & & \\ (p-1)b & d & & & & \\ & (p-2)b & 2d & & & \\ & & \ddots & \ddots & & \\ & & & 2b & (p-2)d & \\ & & & & b & (p-1)d \\ & & & & & 0 \end{pmatrix}.$$

8.2 Resolution of the infinite triangular system

In our case, looking for λ-scale invariants, we already know that we must choose $\lambda = a$. Then the system to solve is the following:

$$\begin{cases} (M_{1,1} - aI_2)F_1 = 0 \\ M_{1,2}F_1 + (M_{2,2} - aI_2)F_2 = 0 \\ M_{2,3}F_2 + (M_{3,3} - aI_3)F_3 = 0 \\ \vdots \\ M_{k-1,k}F_{k-1} + (M_{k,k} - aI_k)F_k = 0 \\ \vdots \end{cases}$$

As the matrix $M_{k,k}$ is equal to kaI_{k+1}, the system becomes:

$$\begin{cases} 0.F_1 = 0 \\ F_2 = -a^{-1}M_{1,2}F_1 \\ F_3 = -(2a)^{-1}M_{2,3}F_2 \\ \vdots \\ F_k = -[(k-1)a]^{-1}M_{k-1,k}F_{k-1} \\ \vdots \end{cases}$$

This means that one can choose

- any F_1, and then
- F_k as $(-1)^{k+1}a^{-k+1}U_k(F_1)$, where U_k is the matrix with $k+1$ rows and 2 columns given by the product

$$[1/(k-1)M_{k-1,k}] \cdot [1/(k-2)M_{k-2,k-1}] \dots [1/2M_{2,3}]M_{1,2}.$$

8.3 Convergence of the a-invariant

We are going to show that the coefficients of the F_i vectors decrease quickly enough for the invariant F to converge in a neighborhood of zero. In particular, the norm $||U_k||$ is less than or equal to the product

$$\frac{1}{(k-1)!}||M_{k-1,k}|| \dots ||M_{1,2}||.$$

From the expression of $M_{k-1,k}$, we have that $||M_{k-1,k}|| \leq ck$, where $c = \max(|b|, |d|)$. Hence, we can conclude that one $||U_k|| \leq ck!/(k-1)! = ck$. Eventually, we will have

$$|F_k|_\infty = a^{-k+1}|U_k(F_1)|_\infty \leq a^{-k+1}||U_k||.|F_1|_\infty \leq \frac{ck}{a^{k-1}}|F_1|_\infty.$$

Let t be $\max(|x|, |y|)$. Then

$$\begin{aligned} &|F(x,y)| \leq \\ &|F_1X^1| + |F_2X^2| \dots + |F_kX^k| + \dots \\ &\leq 2|F_1|_\infty t + 3|F_2|_\infty t^2 + \dots + (k+1)|F_k|_\infty t^k + \dots \end{aligned}$$

The right member of the inequality is inferior to

$$ac|F_1|_\infty[2(\frac{t}{a}) + 3.2(\frac{t}{a})^2 + \dots + (k+1)k(\frac{t}{a})^k + \dots].$$

From the classical theory of one variable power series, it converges in the open disk of radius a and centered at zero. More precisely, taking F_1 respectively equal to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, we get a basis $F^1(x,y)$ and $F^2(x,y)$ for a-invariants of the system, and which converge in the opened $|.|_\infty$-disk of radius a centered at zero. Assume now that we are given initial values $x(0) = x_0$ and $y(0) = y_0$ for solutions of the system within this open disk. Then, there will always exist two real numbers λ and μ, such that

$$\lambda(x_0, y_0)F^1(x_0, y_0) + \mu(x_0, y_0)F^2(x_0, y_0) = 0,$$

where $\lambda(x_0, y_0) = F^2(x_0, y_0)$ and $\mu(x_0, y_0) = -F^1(x_0, y_0)$. Then, the expression

$$\lambda(x_0, y_0)F^1 + \mu(x_0, y_0)F^2$$

is an invariant for solutions corresponding to the initial condition (x_0, y_0). It is also clear that, for (x_0, y_0) in the $|.|_\infty$-disk of radius a and center at zero, that it depends smoothly on the initial condition.

9 Conclusions

As far as it is our knowledge, we present the first methods which generate *multivariate formal power series invariants* for hybrid systems with highly non linear behavior.

We also reach a new level of precision, but still an over-approximation, for the static analysis and verification of hybrid systems,

We generate bases for invariants that are expressed as formal power series. We also provide convergence analysis and existence results and note that, as such, they could be reused by other fixed-point computation methods or other constraint based approaches.

We illustrate the efficiency of our methods by generating such invariants for Volterra-like systems. The latter are well-known for being intractable by other state-of-the-art formal methods for invariant generation or static analysis.

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] Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T.A., h. Ho, P., Nicollin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. Theoretical Computer Science **138** (1995) 3–34

[3] 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)

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

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

[6] 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

[7] 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

[8] 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)
[9] Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates (2004)
[10] A. Tiwari: Generating box invariants. In: Proc. of the 11th Int. Conf. on Hybrid Systems: Computation and Control HSCC. (2008)
[11] 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)
[12] Buchberger, B.: Symbolic computation: Computer algebra and logic. In: Frontiers of Combining Systems: Proceedings of the 1st Int. Workshop, Munich (Germany). (1996) 193–220
[13] Weispfenning, V.: Quantifier elimination for real algebra - the quadratic case and beyond. Applicable Algebra in Engineering, Communication and Computing **8**(2) (1997) 85–101
[14] Collins, G.E.: Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition. LNCS (1975)
[15] 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
[16] 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
[17] 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
[18] Ramdani, N., Meslem, N., Candau, Y.: Reachability of uncertain nonlinear systems using a nonlinear hybridization. In: HSCC '08: Proceedings of the 11th international workshop on Hybrid Systems, Berlin, Heidelberg, Springer-Verlag (2008) 415–428
[19] Akbarpour, B., Paulson, L.C.: Applications of metitarski in the verification of control and hybrid systems. In: HSCC '09: Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control, Berlin, Heidelberg, Springer-Verlag (2009) 1–15
[20] 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)
[21] Bauer, A., Pister, M., Tautschnig, M.: Tool-support for the analysis of hybrid systems and models. In: DATE '07: Proceedings of the conference on Design, automation and test in Europe, San Jose, CA, USA, EDA Consortium (2007) 924–929
[22] Fränzle, M., Herde, C., Teige, T., Ratschan, S., Schubert, T.: Efficient solving of large non-linear arithmetic constraint systems with complex boolean structure. JSAT **1**(3-4) (2007) 209–236
[23] Fränzle, M., Herde, C.: Hysat: An efficient proof engine for bounded model checking of hybrid systems. Form. Methods Syst. Des. **30**(3) (2007) 179–198
[24] Matringe, N., Moura, A.V., Rebiha, R.: Endomorphisms for non-trivial non-linear loop invariant generation. In: 5th Int. Conf. Theoretical Aspects of Computing, LNCS (2008) 425–439
[25] 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)
[26] Nadir Matringe, Arnaldo V. Moura, R.R.: Morphism for non-linear loop invariant generation. Invited submission to the Journal of Symbolic Computation. Special issue on Loop Invariant and Automated Reasoning
[27] Matringe, N., Moura, A.V., Rebiha, R.: 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] Matringe, N., Moura, A.V., Rebiha, R.: 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] Nadir Matringe, Arnaldo V. Moura, R.R.: Generating invariants for non-linear hybrid systems by linear algebraic methods. Invited submission to the Journal of ACM Transactions in Embedded Computing Systems (TECS). Special issue of NSV2009.
[30] Matringe, N., Vieira-Moura, A., Rebiha, R.: Morphisms for non-trivial non-linear invariant generation for algebraic hybrid systems. Technical Report TR-IC-08-32, Institute of Computing, University of Campinas (November 2008)

[31] Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. Form. Methods Syst. Des. **32**(1) (2008) 25–55

[32] Boularas, D., Chouikrat, A.: Equations d'amorçage d'intégrales premières formelles. In: Linear and Multilinear Algebra. Volume 54. (2006) 219–233

[33] Bernard, O., Gouze, J.L.: Global qualitative description of a class of nonlinear dynamical systems. Artificial Intelligence **136**(1) (2002) 29–59