Theoretical Computer Science 594 (2015) 180–200

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Generating invariants for non-linear hybrid systems

Rachid Rebiha [a,*,1], Arnaldo V. Moura [a,1], Nadir Matringe [b,1]

[a] Institute of Computing, University of Campinas, São Paulo, Brazil
[b] Laboratoire de Mathématiques et Applications, University of Poitiers, France

ARTICLE INFO

Article history:
Received 26 November 2012
Received in revised form 16 April 2015
Accepted 5 June 2015
Available online 12 June 2015
Communicated by N. Shankar

Keywords:
Formal methods
Inductive invariant generation
Hybrid systems
Linear algebra

ABSTRACT

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

1. Introduction

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

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

More recent approaches for invariants generation are constraint-based [8–12]. In these cases, a candidate invariant with a fixed degree and unknown parametric coefficients, *i.e.*, a template form, is proposed as the target invariant to be generated.

* Principal corresponding author.
E-mail addresses: rachid@ic.unicamp.br (R. Rebiha), arnaldo@ic.unicamp.br (A.V. Moura), matringe@math.univ-poitiers.fr (N. Matringe).

[1] FAPESP grant number 2011/08947-1 and FAPESP/BEPE grant number 2013/04734-9.

http://dx.doi.org/10.1016/j.tcs.2015.06.018
0304-3975/

The conditions for invariance are then encoded, resulting in constraints on the unknown coefficients whose solutions yield invariants. One of the main advantages of such constraint-based approaches is that they are goal-oriented. But, on the other hand, they still require the computation of several Gröbner Bases [13] or require first-order quantifier elimination [14,15], and known algorithms for those problems are, at least, of double exponential complexity. Alternatively, SAT Modulo Theory decision procedures and polynomial systems [16,17,9,18,19] could also, eventually, lead to decision procedures for invariant generation. Nonetheless, despite significant progress over the years in static analysis and formal methods for algorithms and programs verification [8,20,21,9,11,22–25,16,12,26], 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.

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

We provide a unified presentation and a generalization of our previous work on invariant generation for hybrid systems [27–30]. Specifically, we provide methods to generate non-trivial bases of provable invariants for local continuous evolution modes described by non-linear differential rules. As a consequence, they can determine which discrete transitions are possible and they can also verify if a given property is fulfilled or not. In order to generate invariants for hybrid systems, we complete and adapt our previous work on non-linear invariant generation for discrete programs [31,32]. The contribution and novelty in our approaches clearly differ from those in [8] as their constraint-based techniques depend on several Gröbner Bases or Syzygy Bases [33] computations, and also on solving non-linear problems for each location. On the other hand, these works introduce a useful formalism, and so we chose to start from similar definitions for hybrid systems, inductive invariants and consecution conditions.

We then propose methods to identify suitable morphisms to encode the relaxed consecution requirements. We show that the preconditions for discrete transitions and the Lie-derivatives for continuous evolutions can be viewed as morphisms over a vector space of terms, with polynomially bounded degrees, which can be suitably represented by matrices. The relaxed consecution requirements are also encoded as morphisms represented by matrices. By doing so, we do not need to start with candidate invariants that generate intractable problems. Moreover, our methods are not constraint-based. Rather, we identify the needed degree of a generic multivariate polynomial, or fractional, as a relaxation of the consecution condition. The invariant bases are, then, generated by computing the eigenspace or nullspace of a specific matrix (related to the encoding of the loop instructions and the consecution condition) that is constructed. We identify the needed approximations and the relaxations of the consecution conditions in order to guarantee sufficient conditions for the existence and computation of invariants. Moreover, the unknown parameters that are introduced are all fixed in such a way that certain specific matrices will have a non-null kernel, guaranteeing bases for non-trivial invariants.

The contribution of this work are summarized thus:

- We demonstrate powerful algorithms [28,29,27,32,34,30], relying on linear algebraic methods, capable of computing bases for ideals of non-trivial invariants for non-linear hybrid systems. In other words, looking at complex hybrid systems, we are able to extract the generator basis of a vector space where each element provides us with non-trivial invariants.
- We reduce the non-trivial invariant generation problem to the computation of associated eigenspaces, or null spaces, by encoding consecution requirements as specific morphisms represented by matrices.
- Our methods display lower complexities than the mathematical foundations of previous approaches based on fixed point computation, as well as the present constraint-based approaches, or any other approach that uses Gröbner bases calculations, Syzygy calculations or quantifier eliminations.
- We handle non-linear hybrid systems, extended with parameters and variables that are functions of time. We note that the latter conditions are still not treated by other state-of-the-art invariant generation methods.
- We establish general sufficient conditions guaranteeing the existence and allowing the computation of invariant ideals for situations not treated by other modern invariant generation approaches. Our algorithm incorporates a strategy for estimating optimal degree bounds for candidate invariants.

In Section 2 we introduce ideals of polynomials, inductive assertions and algebraic hybrid systems. In Section 3 we present new forms of approximating consecution for non-linear differential systems. We consider consecution conditions, and the associated techniques to generate ideals of inductive invariants, in Section 4. In particular, morphisms suitable for handling non-linear differential rules, and techniques to generate invariants for such differential rules, appear in Section 4.3. In Section 5 we introduce a strategy that can be used to find the degree of invariants. In Section 6 we show how to handle discrete transition systems. In Section 7 we show how to generate ideals for global invariants by taking into account the ideal basis of local differential invariants, together with those derived from the discrete transition analysis and the initial constraints. Section 8 provides a discussion of related works and also compares our methods with other closely related works. In this section, we also give some insight about how our invariant generation methods and the general sufficiency conditions can be used in other verification or theorem proving approaches. Section 9 presents some experiments. We present our conclusions in Section 10.