Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations

Khalil Ghorbal, Andrew Sogokon, André Platzer

Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations*

Khalil Ghorbal[1], Andrew Sogokon[2], and André Platzer[1]

[1] Carnegie Mellon University, Computer Science Department, Pittsburgh, PA, USA,
{kghorbal|aplatzer}@cs.cmu.edu
[2] University of Edinburgh, LFCS, School of Informatics, Edinburgh, Scotland, UK,
a.sogokon@sms.ed.ac.uk

Abstract In this paper we seek to provide greater automation for formal deductive verification tools for continuous and hybrid dynamical systems which involve reasoning about invariance of conjunctive equational assertions. We present an efficient procedure to check invariance of conjunctions of polynomial equalities under the flow of polynomial ordinary differential equations. The procedure is based on a necessary and sufficient condition that characterizes the invariance of a conjunction of polynomial equalities. We contrast this approach to an alternative one which combines fast and sufficient (but not necessary) conditions using a special cut rule for soundly restricting the system evolution domain.

1 Introduction

The problem of reasoning about invariant sets of dynamical systems is of fundamental importance to verification and modern control design. A set is an invariant of a dynamical system if no trajectory can escape from it. Of particular interest are safety assertions which describe states of the system which are deemed safe; it is clearly important to ensure that these sets are indeed invariant.

Hybrid dynamical systems combine discrete and continuous behavior and have found application in modelling a vast quantity of industrially relevant designs, many of which are safety-critical. In order to verify safety properties in hybrid models, one often requires the means of reasoning about safety in continuous systems. This paper focuses on developing and improving the automation of reasoning principles for a particular class of invariant assertions for continuous systems – conjunctions of polynomial equalities; these can be used, e.g. to assert the property that certain values (temperature, pressure, water level, etc.) in the system are maintained at a constant level as the system evolves.

In practice, it is also highly desirable to have the means of deciding whether a given set is invariant in a particular dynamical system. It is equally important that such methods be efficient enough to be of practical utility. This paper will address both of these issues in the case when the invariant set is given by a conjunction of equations.

Contributions. The contributions of this paper are twofold:

* This material is based upon work supported by the National Science Foundation by NSF CAREER Award CNS-1054246, NSF EXPEDITION CNS-0926181, CNS-0931985, DARPA FA8750-12-2-0291 and EPSRC EP/I010335/1.

- It gives a differential radical characterization of invariance for algebraic sets (conjunctions of polynomial equalities) under the flow of algebraic differential equations. A new related proof rule is introduced together with an optimized decision procedure.
- It explores an alternative approach which, while deductively less powerful, allows one to exploit knowledge about the system to yield efficient proofs and is furthermore able to work with non-polynomial systems.

The two approaches to proving invariance of conjunctive equational assertions explored in this paper are complementary and aim at improving proof automation—deductive power and efficiency—in deductive formal verification tools.

Content. In Section 2, we recall some basic definitions and concepts that we will use through the paper. Section 3 will introduce a new proof rule to check invariance of a conjunction of polynomials. We discuss its complexity and present an optimization of the original algorithm (Section 3.2). Its average performance is assessed using a set of 31 benchmarks (Section 6). The remainder of the paper presents another novel approach to check invariance of a conjunction; it leverages efficient existing proof rules together with *differential cuts* and *differential weakening* (Section 4). Section 5 presents an automated proof strategy that can be used to combine proof rules.

2 Preliminaries

We consider autonomous[3] polynomial vector fields (see Def. 1 below).

Let $\boldsymbol{x} = (x_1, \ldots, x_n) : \mathbb{R}^n$, and $\boldsymbol{x}(t) = (x_1(t), \ldots, x_n(t))$, where $x_i : \mathbb{R} \to \mathbb{R}$, $t \mapsto x_i(t)$. The ring of polynomials over the reals will be denoted by $\mathbb{R}[x_1, \ldots, x_n]$.

Definition 1 (Polynomial Vector Field). *Let p_i, $1 \leq i \leq n$, be multivariate polynomials in the polynomial ring $\mathbb{R}[\boldsymbol{x}]$. A* polynomial vector field*, $\boldsymbol{p}$, is an explicit system ordinary differential equations with polynomial right-hand side:*

$$\frac{dx_i}{dt} = \dot{x}_i = p_i(\boldsymbol{x}), \quad 1 \leq i \leq n \ . \tag{1}$$

One important problem is that of determining whether a set of states satisfying a polynomial equation $h = 0$ remains invariant under the flow of the vector field. That is, whether the following formula of differential dynamic logic [24] is valid, i.e. true in all states

$$(h = 0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0) \tag{2}$$

where $[\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0)$ is true in a state $\boldsymbol{x}_\iota$ if postcondition $h = 0$ is true in all states reachable from $\boldsymbol{x}_\iota$ by following the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$ for any amount of time. The implication in the formula Eq. (2) expresses that $h = 0$ stays true forever from all initial states $\boldsymbol{x}_\iota$ that satisfy $h = 0$. Note that h is a polynomial in $\boldsymbol{x}$, but we write $h = 0$ for $h(\boldsymbol{x}) = 0$ in this paper for simplicity.

[3] Autonomous means that the rate of change of the system over time depends only on the system's state, not on time. Non-autonomous systems with time dependence can be made autonomous by adding a new state variable to account for the progress of time.

In this work we investigate a generalization of Eq. (2) to a conjunction of polynomial equations; that is, instead of $h = 0$, we ask whether a conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, where h_i are polynomials, holds true in all reachable states if it is initially true.

$$(h_1 = 0 \wedge \cdots \wedge h_r = 0) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](h_1 = 0 \wedge \cdots \wedge h_r = 0) \tag{3}$$

Since polynomial functions are smooth (C^∞, i.e. they have derivatives of any order), they are locally Lipschitz-continuous. By Cauchy-Lipschitz theorem (a.k.a. Picard-Lindelöf theorem) [17], there exists a unique maximal solution to the initial value problem ($\dot{\boldsymbol{x}} = \boldsymbol{p}$, $\boldsymbol{x}(0) = \boldsymbol{x}_\iota$) defined for t in some non-empty open interval $U_{\boldsymbol{x}_\iota} \subseteq \mathbb{R}$.

Geometrically, Eq. (3) is represented by the set of real roots of the system $h_1 = 0, \ldots, h_r = 0$. Such a set is called an algebraic set or a *variety* and will be henceforth denoted by $V_{\mathbb{R}}(h_1, \ldots, h_r)$. Therefore, the fact that the variety $V_{\mathbb{R}}(h_1, \ldots, h_r)$ is an invariant region of the vector field $\boldsymbol{p}$ is equivalent to the invariance of the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, that is, if $h_1(\boldsymbol{x}_\iota) = 0 \wedge \cdots \wedge h_r(\boldsymbol{x}_\iota) = 0$, then, $h_1(\boldsymbol{x}(t)) = 0 \wedge \cdots \wedge h_r(\boldsymbol{x}(t))$ for all $t \in U_{\boldsymbol{x}_\iota}$, where $\boldsymbol{x}(t)$ denotes the solution of the initial value problem ($\dot{\boldsymbol{x}} = \boldsymbol{p}, \boldsymbol{x}(0) = \boldsymbol{x}_\iota$). While varieties are not the only invariants of interest [28,27], they are still intimately related to all other algebraic invariants, such as semi-algebraic invariants. We thus believe the comparison and the empirical performance study we initiate in this paper to be an important step towards understanding the invariance problem in polynomial vector fields, and hence also in hybrid systems with polynomial continuous dynamics.

Ideals are sets of polynomials with interesting algebraic properties: they are closed under addition and external multiplication. That is, if I is an ideal, then for all $h_1, h_2 \in I$, the sum $h_1 + h_2 \in I$; and if $h \in I$, then, $qh \in I$, for all $q \in \mathbb{R}[x_1 \ldots, x_n]$.

We recall the notion of Lie derivation. We will use ∇h, to denote the gradient of a polynomial h, that is the vector of its partial derivatives $\left(\frac{\partial h}{\partial x_1}, \ldots, \frac{\partial h}{\partial x_n}\right)$. The *Lie derivative* of a polynomial h along a vector field $\boldsymbol{p}$ is defined as follows ($\cdot$ denotes the scalar product).

$$\mathfrak{L}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} \nabla h \cdot \boldsymbol{p} = \sum_{i=1}^{n} \frac{\partial h}{\partial x_i} p_i \ . \tag{4}$$

Higher-order Lie derivatives are defined recursively: $\mathfrak{L}_{\boldsymbol{p}}^{(k+1)}(h) = \mathfrak{L}_{\boldsymbol{p}}(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h))$, where $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) = h$.

3 Invariance of Conjunctions of Polynomial Equations

In this section we give an exact characterization of invariance for conjunctions of polynomial equalities under the flow of algebraic differential equations. When the evolution domain is constrained, we only consider the trajectory of a solution as long as is satisfies the constraints. The characterization, as well as the proof rule, generalize our previous work which handles purely equational invariants of the form $h = 0$ without considering evolution domains.

The differential radical invariants proof rule DRI [12, Theorem 2] has been shown to be a necessary and sufficient criterion for invariance of equations of the form $h = 0$.

We reproduce the proof rule for convenience:

$$(\mathrm{DRI})\frac{h = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0)} \ . \tag{5}$$

The *order* $N \geq 1$ denotes the length of the chain of ideals $\langle h \rangle \subseteq \langle h, \mathfrak{L}_{\boldsymbol{p}}(h) \rangle \subseteq \cdots$ which reaches a fixed point after finitely many steps by the ascending chain property of Noetherian rings. Therefore, the order N is always finite and computable—using e.g. Göbner Bases [4]—for polynomials with rational coefficients. The premise of the proof rule DRI is a real quantifier elimination problem and can be also solved algorithmically [5].

A naïve approach to prove invariance of a conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$, without evolution domain constraints, is to use the proof rule DRI together with the following sum-of-squares equivalence from real arithmetic:

$$h_1 = 0 \wedge \cdots \wedge h_r = 0 \ \equiv_{\mathbb{R}} \ \sum_{i=1}^{r} h_i^2 = 0 \ . \tag{6}$$

The use of sum-of-squares comes at a cost as the degree of the newly-defined candidate h at least doubles, increasing the complexity of the problem (Section 3.2 will discuss in more detail the link between the complexity of DRI-based proof rules and the degree of the polynomials involved).

Instead, we present in the sequel an extention of the proof rule DRI that exploits the underlying algebraic structure of the conjunction. For an equational conjunction, $h_1 = 0 \wedge \cdots \wedge h_r = 0$, the order N—defined earlier for one atom—is generalized to the length of the chain of ideals formed by *all* the involved polynomials and their subsequent Lie derivatives:

$$I = \langle h_1, \ldots, h_r \rangle \subseteq \langle h_1, \ldots, h_r, \mathfrak{L}_{\boldsymbol{p}}(h_1), \ldots, \mathfrak{L}_{\boldsymbol{p}}(h_r) \rangle \subseteq \cdots \ . \tag{7}$$

Theorem 2 (Differential Radical Characterization). *Let $h_1, \ldots, h_r \in \mathbb{R}[\boldsymbol{x}]$ with the order N for the vector field $\boldsymbol{p}$. Let H denote some evolution domain constraint. Then, the conjunction $h_1 = 0 \wedge \cdots \wedge h_r = 0$ is invariant under the flow of the vector field $\boldsymbol{p}$, subject to the evolution constraint H, if and only if*

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0 \ . \tag{8}$$

Proof. See proof of [13, Theorem 2].

When the evolution domain constraints are dropped (H =True) and $r = 1$ (one equation), one recovers exactly the statement of [12, Theorem 2] which characterizes the purely equational case.

Intuitively, Theorem 2 says that on the invariant algebraic set, all higher-order Lie derivatives of each polynomial h_i must vanish. It adds however a crucial detail: checking finitely many—exactly N—higher-order Lie derivatives is both necessary and sufficient. Observe that the theorem does not check for invariance of each conjunct taken

separately, rather it handles the conjunction in its entirety. The order N itself is defined as a property of the ideal chain formed by all the polynomials and their Lie derivatives taken together. If N_i denotes the order of each atom h_i taken separately, then one can readily see that

$$N \leq \max_i N_i \ . \tag{9}$$

The equality does not hold in general: consider for instance $h_1 = x$, $h_2 = y$ and $\boldsymbol{p} = (y, x)$. Since $\mathfrak{L}^{(2)}_{\boldsymbol{p}}(h_i) = h_i$, for $i = 1, 2$, we have $N_1 = N_2 = 2$. However,

$$\langle x, y\rangle = \langle h_1, h_2\rangle \subseteq \langle h_1, h_2, \mathfrak{L}_{\boldsymbol{p}}(h_1), \mathfrak{L}_{\boldsymbol{p}}(h_2)\rangle = \langle x, y, y, x\rangle,$$

which means that $N = 1$. This example reflects one of the main differences between this work and the characterization given in [19], where the criterion is given by

$$H \vdash \bigwedge_{j=1}^{r} h_j = 0 \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N_j - 1} \mathfrak{L}^{(i)}_{\boldsymbol{p}}(h_j) = 0 \ . \tag{10}$$

As a consequence, the criterion of Theorem 2 requires to discharge N (versus $\sum_{j=1}^{r} N_j$ in [19]) ideal membership problems and $\sum_{N_j \leq N}(N_j - 1) + \sum_{N_j > N}(N - 1)$ (versus $\sum_{j=1}^{r} N_j - 1$ in [19]) purely universal quantifier elimination problems. Therefore, using Eq. (9), and if k denotes $\operatorname{argmax}_i N_i$, Theorem 2 saves at least—when $N = N_k$—$\sum_{j=1, j\neq k}^{r} N_j$ ideal membership problems and $\sum$

The proof rule DRI [12] generalizes to conjunctions with evolution domain constraints as follows:

$$(\mathrm{DRI}_\wedge)\frac{H \vdash \big(\bigwedge_{j=1}^{r} h_j = 0\big) \rightarrow \bigwedge_{j=1}^{r} \bigwedge_{i=1}^{N-1} \mathfrak{L}^{(i)}_{\boldsymbol{p}}(h_j) = 0}{\big(\bigwedge_{j=1}^{r} h_j = 0\big) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\big(\bigwedge_{j=1}^{r} h_j = 0\big)} \ . \tag{11}$$

In what follows, we implement the proof rule $\mathrm{DRI}_\wedge$ and discuss its theoretical complexity.

3.1 Decision Procedure

To check the validity of the premise in the proof rule $\mathrm{DRI}_\wedge$, one needs to compute the order N and to decide a purely universally quantified sentence in the theory of real arithmetic. These two tasks do not need to be performed in that precise order, and in fact we present an algorithm that computes N on the fly while breaking down the quantifier elimination problem into smaller, more tractable problems.

Algorithm 1 terminates as the variable $\check{N}$ strictly increases at each iteration of the outermost **while** loop, while being bounded by the finite order N, $\check{N} \leq N$. The algorithm returns True if and only if the candidate is an invariant. It is therefore a decision procedure for the invariance problem with conjunctive equational candidates.

The algorithm does not know N a priori. The variable $\check{N}$ converges, from below, in finite steps toward N; at each iteration of the **while** loop it checks whether $\check{N} = N$. Toward this, it computes a Gröbner Basis (GB) of the ideal I, containing the polynomials h_i as well as their respective higher-order Lie derivatives up to the derivation order

Algorithm 1: Checking the invariance of a conjunction of polynomial equations.

Data: H (evolution domain constraints), $\boldsymbol{p}$ (vector field), $\boldsymbol{x}$ (state variables)
Data: $h_1, \ldots, h_r$ (conjunction candidate)
Result: True if and only if the conjunction candidate is an invariant

```
1  Ň ← 1
2  I ← {h_1, ..., h_r}
3  L ← {h_1, ..., h_r}
4  symbs ← Variables[p, h_1, ..., h_r]
5  while True do
6      GB ← GröbnerBasis[I, x]
7      LD ← {}
8      foreach ℓ in L do
9          LieD ← LieDerivative[ℓ, p, x]
10         Rem ← PolynomialRemainder[LieD, GB, x]
11         if Rem ≠ 0 then
12             LD ← LD ∪ LieD
13     if LD = {} then
14         return True
15     else
16         foreach ℓ in LD do
17             if QE[∀ symbs, H ∧ h_1 = 0 ∧ ··· ∧ h_r = 0 → ℓ = 0] ≠ True then
18                 return False
19         I ← GB ∪ LD
20         Ň ← Ň + 1
21         L ← LD
```

$\check{N} - 1$. Then enters a **for** loop (line 8), where it computes the $\check{N}$th order Lie derivatives and their respective reductions (or remainders) (`LieD`) by the Gröbner Basis `GB`. All non-null remainders are stored in the list `LD` (line 12). If the list is empty, then we just proved that $\check{N} = N$. Otherwise, the outermost **while** loop (line 5) needs to be executed one more time after increasing $\check{N}$ (line 20). Before re-executing the **while** loop, however, we make sure that the premise of the proof rule $\mathrm{DRI}_\wedge$ holds up to $\check{N}$. Since in this case, we know that $\check{N} < N$, if the quantifier elimination fails to discharge the premise of the proof rule $\mathrm{DRI}_\wedge$ up to $\check{N}$, then we do not need to go any further as the invariance property is falsified. The main purpose of the **for** loop in line 16 is to decompose the quantifier elimination problem

$$H \to \big(\bigwedge_{j=1}^{r} h_j = 0\big) \to \bigwedge_{j=1}^{r} \mathfrak{L}_{\boldsymbol{p}}^{(\check{N})}(h_j) = 0,$$

into at most r smaller problems:

$$H \to \big(\bigwedge_{j=1}^{r} h_j = 0\big) \to \mathfrak{L}_{\boldsymbol{p}}^{(\check{N})}(h_j) = 0,$$

exploiting the logical equivalence

$$a \to (b \wedge c) \equiv (a \to b) \wedge (a \to c),$$

for any boolean variables a, b, and c. Observe that the quantifier elimination problem in line 17 performs a universal closure for all involved symbols—state variables and parameters— denoted by `symbs` and determined once at the beginning of the algorithm using the procedure `Variables` (line 4). Besides, by eliminating the states variables in line 17, the algorithm can be readily adapted to explicitly return extra conditions on the parameters to ensure invariance of the given conjunction. When the algorithm returns False, any counterexample to the quantifier elimination problem of line 17 can be used as an initial condition for a concrete counterexample that falsifies the invariant.

3.2 Complexity

Algorithm 1 relies on two expensive procedures: deciding purely universally quantified sentences in the theory of real arithmetic (line 17) and ideal membership of multivariate polynomial using Gröbner bases (line 6). We discuss in this section their respective theoretical complexity.

Quantifier elimination over the reals is decidable [30]. The purely existential fragment of the theory real arithmetic has been shown to exhibit singly exponential time complexity in the number of variables [1]. Theoretically, the best bound on the complexity of deciding a sentence in the existential theory of $\mathbb{R}$ is given by $(sd)^{O(n)}$, where s is the number of polynomials in the formula, d their maximum degree and n the number of variables [1]. However, in practice this has not yet led to an efficient decision procedure, so typically it is much more efficient to use cylindrical algebraic decomposition (CAD) due to Collins [5,6], which has running time complexity doubly-exponential in the number of variables.

The ideal membership of multivariate polynomial with rational coefficients is an `EXPSPACE`-complete problem [21]. Gröbner bases [4] allow to perform membership checks in ideals generated by multivariate polynomials. Significant advances have been made in algorithms for computing Gröbner bases [10,11] which in practice can be expected to perform very well. The degree of the polynomials involved in a Gröbner basis computation can be very large. Theoretically, a Gröbner basis may contain polynomials with degree 2^{2^d} [22]. The degrees of all involved polynomials is bounded by $O(d^{2^n})$ [9]. Gröbner bases algorithms are highly sensitive to the monomial order, that is the particular order one chooses to arrange the different monomials of a multivariate polynomial[4]. It is known [2] that the Degree Reverse Lexicographic (`degrevlex`) order gives on average Gröbner bases with the smallest total degree, although there exist known examples (cf. Mora's example in [15]), for which, even for the `degrevlex` monomial ordering, the (reduced) Gröbner basis contains a polynomial of total degree $O(d^2)$. Finally, the involved rational coefficients of Gröbner bases elements may get complicated (compared to the rational coefficients of the original polynomials of the ideal) which may increase the computational complexity and the required storage space.

[4] See for instance [7, Chapter 2] for the formal definitions.

3.3 Optimization

The theoretical complexity of both the quantifier elimination and Gröbner Bases algorithms suggest several optimization for Algorithm 1.

To reduce the complexity of the quantifier elimination problem (line 17) we attempt to keep a low maximal degree of all involved polynomials. We consider the maximal degree of the polynomials involved in H fixed. In general, considering the conjunction with the polynomials h_i instead of an equivalent representation—typically Gröbner basis' elements— performs better in view of the discussion above about the degree and coefficients of Gröbner basis' elements. However, the degree of the right-hand-side of the implication can be reduced: by choosing a total degree monomial ordering (e.g. `degrevlex`), the remainder `Rem` has at most the same total degree of `LieD` and permits hence on average to reduce the quantifier elimination complexity. Lem. 3 proves that the substitution of `LieD` by its remainder `Rem` in line 17 is equivalent.

Lemma 3. *Let q be the remainder of the reduction of the polynomial s by the Gröbner basis of the ideal generated by the polynomials $h_1, \ldots, h_r$. Then,*

$$h_1 = 0 \land \cdots \land h_r = 0 \to s = 0 \text{ if and only if } h_1 = 0 \land \cdots \land h_r = 0 \to q = 0 \ .$$

Proof. By construction, we have $s = \sum_{i=1}^{r} \alpha_i h_i + q$ for some polynomials α_i. Therefore, the conjunction $h_1 = 0 \land \cdots \land h_r = 0$ implies that $s - q = 0$, or equivalently $s = q$, and the lemma follows. □

To reduce the complexity of Gröbner bases computation, we also attempt to keep a low maximal degree of all involved polynomials of the ideal `I`. Since the degree of `LieD` tends to increase rapidly, we substitute by its remainder `Rem`, which in the worst case will have the same total degree than `LieD`. Lem. 4 shows that the substitution is equivalent: the ideal `I` remains the same whether we construct the list `LD` using `LieD` or `Rem`.

Lemma 4. *Let q be the remainder of the reduction of the polynomial s by the Gröbner basis of the ideal generated by the polynomials $h_1, \ldots, h_r$. Then,*

$$\langle h_1, \ldots, h_r, s \rangle = \langle h_1, \ldots, h_r, q \rangle \ .$$

Proof. By construction, we have $s = \sum_{i=1}^{r} \alpha_i h_i + q$ for some polynomials α_i. Therefore, $s \in \langle h_1, \ldots, h_r, q \rangle$ and $q \in \langle h_1, \ldots, h_r, s \rangle$, which respectively leads to
$\langle h_1, \ldots, h_r, s \rangle \subseteq \langle h_1, \ldots, h_r, q \rangle$ and $\langle h_1, \ldots, h_r, s \rangle \supseteq \langle h_1, \ldots, h_r, q \rangle$. □

For the presented optimization, one should keep in mind that with this equivalent substitution, although it attempts to keep a low total degree of the elements, the coefficients of the remainder q may get substantially more complicated than the coefficients of the original polynomial s. In Section 6 we give an empirical comparison of the optimized—as detailed in this section—versus the non-optimized version of Algorithm 1.

The next section discusses an alternative approach to proving invariance of conjunctive assertions that leverages sufficient (but not necessary) proof rules together with additional proof rules to discharge such candidates. The technique exploits the hierarchy

that some conjunctions exhibit to reduce the complexity of the checking problem by checking the invariance of isolated atoms instead of considering the global conjunction at once.

4 Sufficient Conditions for Invariance

The previous section dealt with a method for proving invariance which is both necessary and sufficient for conjunctions of polynomial equalities. When one has a proof rule like $\mathrm{DRI}_\wedge$, it is natural to ask whether previously proposed *sufficient* proof rules are still relevant. After all, theoretically, $\mathrm{DRI}_\wedge$ is all that is required for producing proofs of invariance in this class of problems. This is a perfectly legitimate question; however, given the complexity of the underlying decision procedures needed for $\mathrm{DRI}_\wedge$ it is perhaps not surprising that one will eventually face scalability issues. This, in turn, motivates a different question - can one use proof rules (which are perhaps deductively weaker than $\mathrm{DRI}_\wedge$) in such a way as to attain more computationally efficient proofs of invariance?

Before addressing this question, this section will review existing sufficient proof rules which allow reasoning about invariance of atomic equational assertions. In Fig. 1, $\mathrm{DI}_=$ shows the equational differential invariant [25] proof rule. The condition is sufficient (but not necessary) and characterizes polynomial invariant functions [25,27]. The premise of the Polynomial-consecution rule [20], P-c in Fig. 1, requires $\mathfrak{L}_{\boldsymbol{p}}(h)$ to be in the ideal generated by h. This condition is also only sufficient. The Lie proof rule gives Lie's criterion [16,23,27] for the invariance of $h = 0$ and characterizes *smooth* invariant manifolds. The rule DW is called *differential weakening* [26] and covers the trivial case when the evolution constraint implies the invariant candidate; in contrast to all other rules in the table, DW can work with arbitrary invariant assertions.

$$(\mathrm{DI}_=)\frac{H \vdash \mathfrak{L}_{\boldsymbol{p}}(h) = 0}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)} \qquad (\text{P-c})\frac{H \vdash \mathfrak{L}_{\boldsymbol{p}}(h) \in \langle h \rangle}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)}$$

$$(\mathrm{Lie})\frac{H \vdash h = 0 \to (\mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \nabla h \neq \boldsymbol{0})}{(h=0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H](h=0)} \qquad (\mathrm{DW})\frac{H \vdash F}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&H\ ]F}$$

Figure 1: Proof rules for checking the invariance of $h = 0$ w.r.t. the vector field $\boldsymbol{p}$: $\mathrm{DI}_=$ [27, Theorem 3], P-c [20, Theorem 1], Lie [23, Theorem 2.8], DW [26, Lemma 3.6]

Let us once again stress that unlike the necessary and sufficient condition for invariance of atomic equational assertions provided by the rule DRI (see Section 3), all the other proof rules in Figure 1 only impose sufficient conditions and may thus fail at a proof even in cases when the candidate is indeed an invariant.

The purpose of all the rules shown in Figure 1, save perhaps DW, is to show invariance of atomic equational assertions. However, in general, one faces the problem $F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ H]C$, where F is a formula defining a set of states where the system is

initialized, and C is the post-condition where the system always enters after following the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$ as long as the domain constraint H is satisfied.

One way to prove such a statement is to find an invariant I which is true initially (i.e. $F \to I$), is indeed an invariant for the system ($I \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \;\&\; H]I$), and implies the post-condition ($I \to C$). These conditions can be formalized in the proof rule [28]

$$(inv)\frac{F \to I \qquad I \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]I \qquad I \to C}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}.$$

In this paper we will be dealing with the special case when the invariant is the same as the post-condition, so in the interest of saving space we can drop the last clause and the rule becomes

$$(inv)\frac{F \to C \qquad C \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]C}.$$

In the following sections, we will be working in a proof calculus, rather than considering a single proof rule, and will call upon this definition in the proofs we construct.

5 Differential Cuts and Lie's Rule

When considering a conjunctive invariant candidate $h_1 = 0 \land h_2 = 0 \land \cdots \land h_r = 0$, it may be the case that each conjunct considered separately is an invariant for the system. Then, one could simply invoke the following basic result about invariant sets to prove invariance of each atomic formula individually.

Proposition 5. *Let $S_1, S_2 \subseteq \mathbb{R}^n$ be invariant sets for the differential equation $\dot{\boldsymbol{x}} = \boldsymbol{p}$, then the set $S_1 \cap S_2$ is also an invariant.*

Corollary 6. *The proof rule*

$$(\wedge_{\mathrm{inv}})\frac{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]h_1 = 0 \qquad h_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,]h_2 = 0}{h_1 = 0 \land h_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p} \,\&H\,](h_1 = 0 \land h_2 = 0)} \quad (12)$$

is sound and may be generalized to accommodate arbitrarily many conjuncts.

Of course, one still needs to choose an appropriate proof rule from Figure 1 (or DRI) in order to prove invariance of atomic equational formulas. For purely polynomial problems it would be natural to attempt a proof using DRI first, but in the presence of transcendental functions, one may need to resort to other rules. In general however, even if the conjunction defines an invariant set, the individual conjuncts need *not* themselves be invariants. If such is the case, one cannot simply break down the conjunctive assertion using the rule $\wedge_{\mathrm{inv}}$ and prove invariance of each conjunct individually. In this section, we explore using a proof rule called *differential cut* (DC) to address this issue.

Differential cuts were introduced as a fundamental proof principle for differential equations [25] which can be used to (soundly) strengthen assumptions about the system evolution.

Proposition 7 (Differential Cut [25]). *The proof rule*

$$(\mathrm{DC})\frac{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]C \qquad F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\,C]F}{F \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]F},$$

where C and F denote quantifier-free first-order formulas, is sound.

One may appreciate the geometric intuition behind this rule if one realizes that the left branch requires one to show that the set of states satisfying C is an invariant for the system initialized in any state satisfying F. Thus, the system does not admit any trajectories starting in F that leave C and hence by adding C to the evolution constraint, one does not restrict the behavior of the original system.

Differential cuts may be applied repeatedly to the effect of refining the evolution constraint with more invariant sets. It may be profitable to think of successive differential cuts as showing an *embedding of invariants* in a system.

There is in fact an interesting connection between differential cuts and embeddings of invariant sub-manifolds, when used with the proof rule Lie. To develop this idea, let us remark that if one succeeds at proving invariance of some $h_1 = 0$ using the rule Lie in a system with no evolution constraint, one shows that $h_1 = 0$ is a smooth invariant sub-manifold of $\mathbb{R}^n$. If one now considers the system evolving inside that invariant manifold and finds some $h_2 = 0$ which can be proved to be invariant using Lie with $h_1 = 0$ acting as an evolution constraint, then inside the manifold $h_1 = 0$, $h_2 = 0$ defines an invariant sub-manifold. One can proceed using Lie in this fashion to look for further embedded invariant sub-manifolds. We will illustrate this idea using a basic example.

Example 8 (Differential cut with Lie*).* Let the system dynamics be $\dot{\boldsymbol{x}} = \boldsymbol{p} \equiv (x_1, -x_2)$. This system has an equilibrium at the origin, i.e. $\boldsymbol{p}(\mathbf{0}) = \mathbf{0}$. Consider an invariant candidate $x_1 = 0 \wedge x_1 - x_2 = 0$. One cannot use Lie directly to prove the goal

$$x_1 = 0 \wedge x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\,(x_1 = 0 \wedge x_1 - x_2 = 0).$$

Instead, DC can be used to cut by $x_1 = 0$, which is an invariant for this system provable using Lie. For the left branch of DC, it is required to show

$$x_1 = 0 \wedge x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\,x_1 = 0,$$

which can be proved using

$$\mathrm{inv}\,\frac{\mathbb{R}\,\frac{*}{x_1 = 0 \wedge x_1 - x_2 = 0 \to x_1 = 0} \qquad \mathrm{Lie}\,\frac{\mathbb{R}\,\frac{*}{x_1 = 0 \to x_1 = 0 \wedge (1 \neq 0)}}{x_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\,x_1 = 0}}{x_1 = 0 \wedge x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\,x_1 = 0]\,x_1 = 0}$$

One can also prove that $x_1 = x_2$ is a invariant under the evolution constraint $x_1 = 0$:

$$\wedge_{\mathrm{inv}}\,\frac{\mathrm{DW}\,\frac{*}{x_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\,x_1 = 0]\,x_1 = 0} \qquad \mathrm{Lie}\,\frac{\mathbb{R}\,\frac{*}{x_1 = 0 \vdash x_1 - x_2 = 0 \to x_1 + x_2 = 0 \wedge (1 \neq 0 \vee -1 \neq 0)}}{x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\,x_1 = 0]\,x_1 - x_2 = 0}}{x_1 = 0 \wedge x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\,x_1 = 0]\,(x_1 = 0 \wedge x_1 - x_2 = 0)}$$

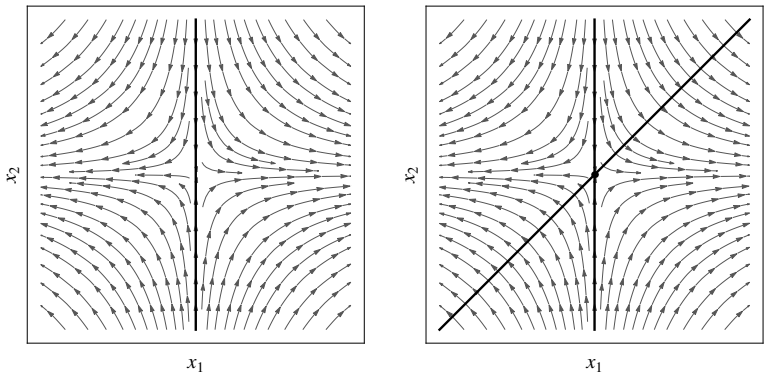

Figure 2: System invariant $x_1 = 0$ (**left**) used in a differential cut to show that the intersection at the origin (**right**) is an invariant.

Using these two sub-proofs to close the appropriate branches, the rule DC proves

$$x_1 = 0 \land x_1 - x_2 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,]\,(x_1 = 0 \land x_1 - x_2 = 0).$$

While this example is very simplistic, it provides a good illustration of the method behind differential cuts. We used DC to restrict system evolution to an invariant manifold $x_1 = 0$ using Lie and then used Lie again to show that $x_1 - x_2 = 0$ defines an invariant sub-manifold inside $x_1 = 0$. This is illustrated in Fig. 2.

It is also worth noting that the choice of conjunct for use in the differential cut was crucial. Had we initially picked $x_1 - x_2 = 0$ to act as C in DC, the proof attempt would have failed, since this does not define an invariant sub-manifold of $\mathbb{R}^2$ (see Fig. 2).

Let us now remark that by employing DC, we proved invariance of a conjunction which could not be described by an atomic equational assertion which is provable using the rule Lie, or by using Lie to prove invariance of each conjunct after breaking down the conjunction with the rule $\wedge_{\text{inv}}$. It has previously been shown that differential cuts increase the deductive power of the system when used in concert with differential invariants [25,28]. We prove that the same is true for differential cuts with Lie. Indeed, differential cuts serve to address some of the limitations inherent in both $\text{DI}_=$ and Lie.

Theorem 9. *The deductive power of* Lie *together with* DC *is strictly greater than that of* Lie *considered separately. We write this as* $\text{DC} + \text{Lie} \succ \text{Lie}$.

Proof. In Example 8 we demonstrate the use of Lie together with DC to prove invariance of a conjunction of polynomial equalities which is *not* provable using Lie alone. To see this, suppose that for the system in Example 8 there exists some real-valued differentiable function $g(\boldsymbol{x})$ whose zero level set is precisely the origin, i.e. $(g(\boldsymbol{x}) = 0) \equiv (\boldsymbol{x} = \boldsymbol{0})$. Then, for all $\boldsymbol{x} \in \mathbb{R}^2 \setminus \{\boldsymbol{0}\}$ this function evaluates to $g(\boldsymbol{x}) > 0$ or $g(\boldsymbol{x}) < 0$ (by continuity of $g(\boldsymbol{x})$) and $\boldsymbol{0}$ is thus the global minimum or global maximum, respectively. In either case, $g(\boldsymbol{x}) = 0 \implies \nabla g(\boldsymbol{x}) = \boldsymbol{0}$ is valid, which cannot satisfy the premise of Lie. □

The use of differential cuts with differential invariants has been explored in [25,27,28] and was shown to increase the deductive power of $\mathrm{DI}_=$ [27]. Below we briefly explore an intriguing connection between the use of differential cuts together with $\mathrm{DI}_=$ and *higher integrals* of dynamical systems.

The premise of the rule $\mathrm{DI}_=$ establishes that $h(\boldsymbol{x})$ is a *first integral* (i.e. a constant of motion) for the system in order to conclude that $h = 0$ is an invariant. More general notions of invariance have been introduced to study integrability of dynamical systems. For instance, $h(\boldsymbol{x})$ is a *second integral* if $\mathfrak{L}_{\boldsymbol{p}}(h) = \alpha h$, where α is some function; this is also sufficient to conclude that $h = 0$ is an invariant. Let us remark that in a purely polynomial setting, such an $h \in \mathbb{R}[\boldsymbol{x}]$ is known as a *Darboux polynomial* [14,8] and the condition corresponds to ideal membership in the premise of P-c). Going further, a *third integral* is a function $h(\boldsymbol{x})$ that remains constant on some level set of a first integral $g(\boldsymbol{x})$ [14, Section 2.6], i.e. $\mathfrak{L}_{\boldsymbol{p}}(h) = \alpha g$ where g is a first integral and α is some function. These ideas generalize to higher integrals (see [14, Section 2.7]).

Example 10 (Deconstructed aircraft [27] - differential cut with $\mathrm{DI}_=$). Consider the system $\dot{\boldsymbol{x}} = \boldsymbol{p} = (-x_2, x_3, -x_2)$ and consider the invariant candidate $x_1^2 + x_2^2 = 1 \wedge x_3 = x_1$. One cannot use $\mathrm{DI}_=$ directly to prove the goal

$$x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, (x_1^2 + x_2^2 = 1 \wedge x_3 = x_1)\,.$$

We can apply DC to cut by $x_1 = x_3$, which is a first integral for the system and is thus provable using $\mathrm{DI}_=$. The left branch requires us to prove

$$x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, x_3 = x_1,$$

which can be proved as follows:

$$\mathrm{inv}\ \frac{\mathbb{R}\ \dfrac{*}{x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \rightarrow x_3 = x_1} \qquad \mathrm{DI}_=\ \dfrac{\mathbb{R}\ \dfrac{*}{-x_2 = -x_2}}{x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, x_3 = x_1}}{x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, x_3 = x_1}$$

For the right branch of DC we need to show that $x_1^2 + x_2^2 = 1$ is an invariant under the evolution constraint $x_3 = x_1$. This is again provable using $\mathrm{DI}_=$.

$$\wedge_{\mathrm{inv}}\ \frac{\mathrm{DW}\ \dfrac{*}{x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ x_3 = x_1]\, x_3 = x_1} \qquad \mathrm{DI}_=\ \dfrac{\mathbb{R}\ \dfrac{*}{x_3 = x_1 \vdash -2x_1x_2 + 2x_2x_3 = 0}}{x_1^2 + x_2^2 = 1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ x_3 = x_1]\, x_1^2 + x_2^2 = 1}}{x_1^2 + x_2^2 = 1 \wedge x_3 = x_1 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}\ \&\ x_3 = x_1]\, (x_1^2 + x_2^2 = 1 \wedge x_3 = x_1)}$$

We can now construct a proof of invariance for the conjunction using DC.

Note that in this example, we have only ever had to resort to the rule $\mathrm{DI}_=$ for showing invariance of an equational candidate. We first showed that $x_3 - x_1$ is an invariant function (first integral) for the system. After restricting the evolution domain to the zero set of the first integral, $x_3 - x_1 = 0$, we proved that the polynomial $x_1^2 + x_2^2 - 1$ is conserved in the constrained system. In this example we have $\mathfrak{L}_{\boldsymbol{p}}(x_1^2 + x_2^2 - 1) = -2x_1x_2 + 2x_2x_3 = 2x_2(x_3 - x_1)$, where $(x_3 - x_1)$ is a first integral of the system. Thus, $x_1^2 + x_2^2 - 1$ is in fact a (polynomial) third integral.

5.1 Proof Strategies using Differential Cuts

Differential cuts can be used to search for a proof of invariance of conjunctive equational assertions. This involves selecting some conjunct $h_i = 0$ to cut by (that is use it as C in DC). If the conjunct is indeed an invariant, it will be possible to strengthen the evolution domain constraint and proceed in a similar fashion by selecting a new C from the remaining conjuncts until a proof is attained. A formal proof of invariance using differential cuts can be quite long and will repeatedly resort to proof rules such as $(\wedge_{\text{inv}})$ (Eq. (12)) and DW (Fig. 1), which is used to prune away conjuncts that have already been added to the evolution domain constraint.

Algorithm 2 presents a simple proof strategy for iteratively selecting a conjunct with which to attempt a differential cut. Before the recursive function `DCSearch` is called, the conjuncts are put into ascending order with respect to the number of variables appearing in the conjunct. For purely polynomial problems, the ordering should additionally be ascending with respect to the maximum degree of the polynomials. The aim of this pre-processing step is to ensure that conjuncts which are potentially less expensive to check for invariance are processed first (see Section 3.2). There is in general no easy way of selecting the "right" proof rule for showing invariance (`Inv`); a possible, albeit not very efficient, solution would be to iterate through all the available proof rules. This would combine their deductive power, but could also lead do diminished performance. In practice, selecting a good proof rule for atomic invariants is very much a problem-specific matter. The overall proof strategy, if successful, would lead to a proof tree resembling that shown below. The proof steps labelled with ? mark choices in selecting the rule for atomic invariants from Figure 1.

$$\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\bigwedge_{i=1}^{r} h_i = 0 \to h_1 = 0}\quad ?\,\dfrac{*}{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h_1 = 0}}{\text{inv}\;\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h_1 = 0}\quad \dfrac{\text{DW}\,\dfrac{*}{h_1 = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, h_1 = 0}\quad \text{DC}\,\dfrac{\dfrac{?\,\dfrac{*}{h_r = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, \bigwedge_{i=1}^{r-1} h_i = 0]\, h_r = 0}}{\text{DC}\,\dfrac{\vdots}{\bigwedge_{i=2}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, \bigwedge_{i=2}^{r} h_i = 0}}}{\wedge_{\text{inv}}\;\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}\,\&\, h_1 = 0]\, \bigwedge_{i=1}^{r} h_i = 0}}{\text{DC}\;\bigwedge_{i=1}^{r} h_i = 0 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, \bigwedge_{i=1}^{r} h_i = 0}$$

5.2 Performance and Limitations

In this section we will identify an example which defeats the current implementation of $\mathrm{DRI}_{\wedge}$ and which is easily provable using differential cuts (see Ex. 11 in Appendix A).

Though this is very much an artificial example, it demonstrates that knowledge of the system can sometimes be exploited to yield efficient proofs using differential cuts. This is especially useful for large systems with many variables where the structure of the problem is well-understood. Additionally, we see that a combination of proof rules ($\mathrm{DI}_{=}, \mathrm{Lie}, \mathrm{DC}$) can be both helpful and efficient.

Knowledge about the system is crucial for differential cuts to be effective. In particular, in this example our knowledge about the system structure informed our decision to "cut by" $x_{13} = 0$ (and use the rule Lie in the left branch of DC), which in the absence of this knowledge may look like an arbitrary choice. The strategy $\mathrm{DCSearch}$ also finds a proof easily in this example.

Algorithm 2: `DCSearch`. Differential cut proof search

Data: $\{h_1, \ldots, h_r\}$, $\boldsymbol{p}$, H
Result: True, False.

```
if r = 0 then
    return True
else
    i ← 1
    while i ≤ r do
        if Inv(h_i, H) then
            if DCSearch({h_1 ..., h_r} \ {h_i}, p, H ∧ h_i = 0) then
                return True
        else
            i ← i + 1
    return False
```

We should note that while differential cuts can serve to increase the deductive power of sufficient proof rules, there are invariant conjunctions of equalities for which applying DC on the conjuncts given in the problem will altogether fail to be fruitful. This is due to DCSearch relying on the fact that at least some of the conjuncts considered individually are invariants for the system, which may not be the case even if the conjunction is invariant [28].

6 Experiments

In this section, we empirically compare the performance of three families of proof rules for checking the invariance of conjunctions: (1) DRI-related proof rules including SoSDRI (DRI plus sum-of-squares rewriting), $\mathrm{DRI}_\wedge$ as well as their optimized versions as detailed in Section 3.3, (2) Differential cut proof search presented in Algorithm 2, and (3) Lie et al. procedure [18] properly adapted to handle a disjunction of equalities—we do not encode the equality $h = 0$ as $h \leq 0 \wedge -h \leq 0$, rather use it as is.

For simplicity, we do not consider any evolution domain constraints, i.e. $H = \text{True}$. The running time for each proof rule as well as the dimension, the different degrees of the candidates and the vector fields, of the used set of benchmarks can be found here [13].

In Fig. 3, the pair (k, l) in the plot of a proof rule P reads: the proof rule P solved k problems each in less than 10^l seconds. The set of benchmarks contains 32 entries composed of equilibria (16), singularities (8), higher integrals (4) and abstract examples (4). The examples we used in our benchmarks originate from a number of sources - many of them come from textbooks on Dynamical Systems; others have been hand-crafted to exploit sweetspots of certain proof rules. For instance, we constructed Hamiltonian systems, systems with equilibria and systems with smooth invariants of various polynomial degrees. The most involved example has 12 state variables, a vector field with a maximum total degree of 291 and an invariant candidate with total degree of 146.

One can clearly see that the $\mathrm{DRI}_\wedge$ is much more efficient on average compared to SoSDRI as it solves 31—out of 32—in less than 0.1s each. The optimization discussed in Section 3.3 yields a slight improvement in the performance of both SoSDRI and $\mathrm{DRI}_\wedge$. In most examples, both $\mathrm{DRI}_\wedge$ and $\mathrm{DRI}_\wedge$-OPT are very efficient. However, the optimized version was able to falsify, in 1.2s, an invariant—higher integral of Goryachev and Chaplygin top [14]—whereas the non-optimized version, as well as all the other proof rules, timed out after 60s. We also noticed for another example—extended Motzkin polynomial—that SoSDRI-OPT timed out whereas SoSDRI was able to check the invariance in 15s. When we investigated this example, it turned out that the rational coefficients of the remainder gets complicated compared to the original polynomial before reduction. For this particular example, the optimized version was able to prove the invariance in 300s which is 20 times slower than the non-optimized version. (cf. [13, Section 6] for more details about both examples).

All DRI-related proof rules fail to prove invariance in one example (discussed in Ex. 11) in less than 60s.

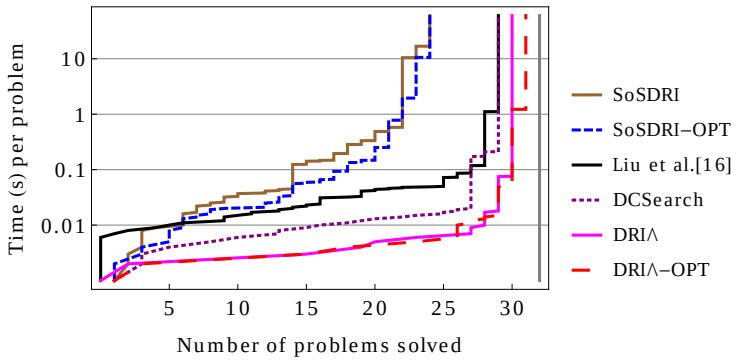

Figure 3: Empirical performance comparison of different proof rules and strategies. The total number of problems solved each in at most ts (log scale) is given in the x-axis for each method.

7 Related Work

In this paper we focus on *checking* invariance of algebraic sets under the flow of polynomial vector fields. For similar techniques used to automatically *generate* invariant algebraic sets we refer the reader to the discussion in [12].

Nagumo's Theorem [31,3], proved by Mitio Nagumo in 1942, characterizes invariant closed sets—a superset of algebraic sets—of locally Lipschitz-continuous vector field—a superset of polynomial vector field. The geometric criterion of the theorem is however intractable. The analyticity of solutions of analytic vector fields—a superset of polynomial vector fields—also gives a powerful, yet intractable, criterion to reason about invariant sets. In [29], the authors attempted to define several special cases exploiting either Nagumo's theorem or the analyticity of the solution, to give proof rules

for checking invariance of (closed) semi-algebraic sets under the flow of polynomial vector fields. Liu et al. in [18] also used analyticity of solutions to polynomial ordinary differential equations and extended [29] using the ascending chain condition in Noetherian rings to ensure termination of their procedure; they gave a necessary and sufficient condition for invariance of arbitrary semi-algebraic sets under the flow of polynomial vector fields and proved the resulting conditions to be decidable.

The approach developed in this paper is phrased in a purely algebraic framework where the ascending chain condition is also used without resorting to Taylor series expansions. As in [18], we also require finitely many higher-order Lie derivatives to vanish; what is different, however, is the definition of the finite number each characterization requires: in [18], one is required to compute all orders N_i of each atom h_i and to prove that all higher-order Lie derivatives of h_i, up to order $N_i - 1$, vanish. We only require that all higher-order Lie derivatives of all h_i, up to order $(N - 1)$ (which is the same for all i) vanish.

Zerz and Walcher [32] have previously considered the problem of deciding invariance of algebraic sets in polynomial vector fields; they gave a sufficient condition for checking invariance of algebraic sets which can be seen as one iteration of Algorithm 1. Therefore, Section 3 generalizes their work by providing a complete characterization of invariant algebraic sets in polynomial vector fields.

8 Conclusion

In this paper, we introduce an efficient decision procedure ($\mathrm{DRI}_\wedge$) for deciding invariance of conjunctive equational assertions for polynomial dynamical systems. We have explored the use of differential cut rule with existing sufficient conditions for invariance of equational assertions both as a means of increasing the deductive power of existing sufficient proof rules and also as a way of attaining more computationally efficient proofs.

The empirical performance we observe in the optimized implementations of DRI and $\mathrm{DRI}_\wedge$ is very encouraging and we are confident that a proof strategy in a deductive formal verification system should give precedence to these methods. However, certain problems fall out of scope of these rules (for instance when the problems involve transcendental functions), or might take unreasonably long to prove, while progress can sometimes be made by employing sufficient proof rules such as $\mathrm{DI}_=$, Lie, etc. in concert with differential cuts.

References

1. Basu, S., Pollack, R., Roy, M.F.: On the combinatorial and algebraic complexity of quantifier elimination. J. ACM 43(6), 1002–1045 (1996)
2. Bayer, D., Stillman, M.E.: A criterion for detecting m-regularity. Inventiones Mathematicae 87, 1 (1987)
3. Blanchini, F.: Set invariance in control. Automatica 35(11), 1747–1767 (1999)
4. Buchberger, B.: Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory. Reidel Publishing Company, Dodrecht - Boston - Lancaster (1985)

5. Collins, G.E.: Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Barkhage, H. (ed.) Automata Theory and Formal Languages. LNCS, vol. 33, pp. 134–183. Springer (1975)
6. Collins, G.E., Hong, H.: Partial cylindrical algebraic decomposition for quantifier elimination. J. Symb. Comput. 12(3), 299–328 (1991)
7. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms - an introduction to computational algebraic geometry and commutative algebra (2. ed.). Springer (1997)
8. Darboux, J.G.: Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. Bulletin des Sciences Mathématiques et Astronomiques 2(1), 151–200 (1878), http://eudml.org/doc/84988
9. Dubé, T.: The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. 19(4), 750–773 (1990)
10. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4) . Journal of Pure and Applied Algebra 139(13), 61 – 88 (1999)
11. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. pp. 75–83. ISSAC '02, ACM, New York, NY, USA (2002)
12. Ghorbal, K., Platzer, A.: Characterizing algebraic invariants by differential radical invariants. In: Ábrahám, E., Havelund, K. (eds.) TACAS. Lecture Notes in Computer Science, vol. 8413, pp. 279–294. Springer (2014)
13. Ghorbal, K., Sogokon, A., Platzer, A.: Invariance of conjunctions of polynomial equalities for algebraic differential equations. Tech. Rep. CMU-CS-14-122, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA (6 2014), http://reports-archive.adm.cs.cmu.edu/anon/2014/abstracts/14-122.html
14. Goriely, A.: Integrability and Nonintegrability of Dynamical Systems. Advanced series in nonlinear dynamics, World Scientific (2001)
15. Lazard, D.: Gröbner-bases, Gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (ed.) EUROCAL. LNCS, vol. 162, pp. 146–156. Springer (1983)
16. Lie, S.: Vorlesungen über continuierliche Gruppen mit Geometrischen und anderen Anwendungen. Teubner, Leipzig (1893)
17. Lindelöf, E.: Sur l'application de la méthode des approximations successives aux équations différentielles ordinaires du premier ordre. Comptes rendus hebdomadaires des séances de l'Académie des sciences 116, 454–458 (1894)
18. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (eds.) EMSOFT. pp. 97–106. ACM (2011)
19. Liu, J., Zhan, N., Zhao, H.: Automatically discovering relaxed Lyapunov functions for polynomial dynamical systems. Mathematics in Computer Science 6(4), 395–408 (2012)
20. Matringe, N., Moura, A.V., Rebiha, R.: Generating invariants for non-linear hybrid systems by linear algebraic methods. In: Cousot, R., Martel, M. (eds.) SAS. LNCS, vol. 6337, pp. 373–389. Springer (2010)
21. Mayr, E.W.: Membership in polynomial ideals over Q is exponential space complete. In: Monien, B., Cori, R. (eds.) STACS. LNCS, vol. 349, pp. 400–406. Springer (1989)
22. Mayr, E.W., Meyer, A.R.: The complexity of the word problems for commutative semigroups and polynomial ideals. Advances in Mathematics 46(3), 305 – 329 (1982)
23. Olver, P.J.: Applications of Lie Groups to Differential Equations. Springer (2000)
24. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reasoning 41(2), 143–189 (2008)

25. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. 20(1), 309–352 (2010)
26. Platzer, A.: Logical Analysis of Hybrid Systems - Proving Theorems for Complex Dynamics. Springer (2010)
27. Platzer, A.: A differential operator approach to equational differential invariants - (invited paper). In: Beringer, L., Felty, A.P. (eds.) ITP. LNCS, vol. 7406, pp. 28–48. Springer (2012)
28. Platzer, A.: The structure of differential invariants and differential cut elimination. Logical Methods in Computer Science 8(4), 1–38 (2012)
29. Taly, A., Tiwari, A.: Deductive verification of continuous dynamical systems. In: Kannan, R., Kumar, K.N. (eds.) FSTTCS. LIPIcs, vol. 4, pp. 383–394. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2009)
30. Tarski, A.: A decision method for elementary algebra and geometry. Bulletin of the American Mathematical Society 59 (1951)
31. Walter, W.: Ordinary Differential Equations. Graduate Texts in Mathematics, Springer New York (1998)
32. Zerz, E., Walcher, S.: Controlled invariant hypersurfaces of polynomial control systems. Qualitative Theory of Dynamical Systems 11(1), 145–158 (2012)

Appendix A

Example 11. Consider the system

$$
\begin{aligned}
\dot{x}_1 &= -292x_7(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_2 &= -292x_8(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_3 &= -42(2x_{10}+2x_{10}^3+2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_4 &= -42(12x_{10}+4x_{10}^3+2x_9+6x_{10}^2x_9)(-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{41},\\
\dot{x}_5 &= -2x_{13}(-1+x_{13}+x_{11}x_{13}),\\
\dot{x}_6 &= -2x_{12}(-1+x_{12}+x_{11}x_{12}),\\
\dot{x}_7 &= 26(-6x_1x_2^2+4x_1^3x_2^2+2x_1x_2^4)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_8 &= 26(-6x_1^2x_2+2x_1^4x_2+4x_1^2x_2^3)(1-3x_1^2x_2^2+x_1^4x_2^2+x_1^2x_2^4)^{25},\\
\dot{x}_9 &= 14(4x_3^3x_4^2+2x_3x_4^4-6x_3x_4^2x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{10} &= 14(2x_3^4x_4+4x_3^2x_4^3-6x_3^2x_4x_5^2)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{11} &= 14(-6x_3^2x_4^2x_5+6x_5^5)(x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^{13},\\
\dot{x}_{12} &= 292x_6(-1+x_6^2+x_7^2+x_8^2)^{145},\\
\dot{x}_{13} &= -x_{13}.
\end{aligned}
$$

Suppose the invariant candidate is given by the following conjunction:

$$
\begin{aligned}
x_{13}=0 \quad \wedge \quad ((x_1^4x_2^2+x_1^2x_2^4-3x_1^2x_2^2+1)^{13})^2 \quad &+\\
((x_3^4x_4^2+x_3^2x_4^4-3x_3^2x_4^2x_5^2+x_5^6)^7)^2 \quad &+\\
((-1+x_6^2+x_7^2+x_8^2)^{73})^2 \quad &+\\
((-3+6x_{10}^2+x_{10}^4+2x_{10}x_9+2x_{10}^3x_9+x_9^2)^{21})^2 \quad &+\\
(x_{12}+x_{11}x_{12}-1)^2=0.&
\end{aligned}
$$

By using a differential cut to restrict the evolution domain to the invariant smooth manifold $x_{13}=0$ (using the rule Lie), one obtains a system for which the sum-of-squares conjunct is a Hamiltonian and thus a first integral; this can be easily proved to be a system invariant using the rule $\mathrm{DI}_{=}$. Naïvely attempting to use $\mathrm{DRI}_{\wedge}$ takes an unreasonable amount of time due to the high degrees involved, while the proof involving DC takes under a second for both branches, provided the right rules are selected to prove invariance of atoms.