A Differential Operator Approach to Equational Differential Invariants[⋆]
(Invited Paper)

André Platzer

Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
aplatzer@cs.cmu.edu

Abstract. Hybrid systems, i.e., dynamical systems combining discrete and continuous dynamics, have a complete axiomatization in differential dynamic logic relative to differential equations. Differential invariants are a natural induction principle for proving properties of the remaining differential equations. We study the equational case of differential invariants using a differential operator view. We relate differential invariants to Lie's seminal work and explain important structural properties resulting from this view. Finally, we study the connection of differential invariants with partial differential equations in the context of the inverse characteristic method for computing differential invariants.

1 Introduction

Hybrid systems [1,11] are dynamical systems that combine discrete and continuous dynamics. They are important for modeling embedded systems and cyber-physical systems. Reachability in hybrid systems is neither semidecidable nor co-semidecidable [11]. Nevertheless, hybrid systems have a complete axiomatization relative to elementary properties of differential equations in differential dynamic logic $\mathsf{d}\mathcal{L}$ [18,21]. Using the proof calculus of $\mathsf{d}\mathcal{L}$, the problem of proving properties of hybrid systems reduces to proving properties of continuous systems.

It is provably the case that the only challenge in hybrid systems verification is the need to find invariants and variants [18,21]; the handling of real arithmetic is challenging in practice [27], even if it is decidable in theory [2], but this is not the focus of this paper. According to our completeness results [18,21], we can equivalently focus on either only the discrete or on only the continuous dynamics, because both are equivalently and constructively interreducible, proof-theoretically. Thus, we can equivalently consider the need to prove properties of differential equations as the only challenge in hybrid systems verification. Since the solutions of most differential equations fall outside the usual decidable classes of arithmetic, or do not exist in closed form, the primary means

[⋆] This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246, NSF EXPEDITION CNS-0926181, and under Grant No. CNS-0931985.

L. Beringer and A. Felty (Eds.): ITP 2012, LNCS 7406, pp. 28–48, 2012.

for proving properties of differential equations is induction [19]. In retrospect, this is not surprising, because our constructive proof-theoretical alignment [21] shows that every proof technique for discrete systems lifts to continuous systems (and vice versa). Since most verification principles for discrete systems are based on some form of induction, this means that induction is possible for differential equations. *Differential invariants* are such an induction principle. We have introduced differential invariants in 2008 [19], and later refined them to a procedure that computes differential invariants in a fixed-point loop [24,25]. Differential invariants are also related to barrier certificates [29], equational templates [30], and a constraint-based template approach [8]. The structure and theory of general differential invariants has been studied in previous work in detail [23].

In this paper, we focus on the equational case of differential invariants. We show that the equational case of differential invariants and similar approaches is already subsumed by Lie's seminal work [14,15,16,17] in the case of open domains. On open (semialgebraic) domains, Lie's approach gives an equivalence characterization of (smooth) invariant functions. This almost solves the differential invariance generation problem for the equational case completely. It turns out, however, that differential invariants and differential cuts may still prove properties indirectly that the equivalence characterization misses. We carefully illustrate why that is the case. We investigate structural properties of invariant functions and invariant equations. We prove that invariant functions form an algebra and that, in the presence of differential cuts provable invariant equations and valid invariant equations form a chain of differential ideals, whose varieties are generated by a single polynomial, which is the most informative invariant.

Furthermore, we study the connection of differential invariants with partial differential equations. We explain the *inverse characteristic method*, which is the inverse of the usual characteristic method for studying partial differential equations in terms of solutions of corresponding characteristic ordinary differential equations. The inverse characteristic method, instead, uses partial differential equations to study solutions of ordinary differential equations. What may, at first, appear to idiosyncratically reduce the easier problem of ordinary differential equations to the more complicated one of partial differential equations, turns out to be very useful, because it relates the differential invariance problem to mathematically very well-understood partial differential equations.

Even though our results generalize to arbitrary smooth functions, we focus on the polynomial case in this paper, because the resulting arithmetic is decidable.

For background on logic for hybrid systems, we refer to previous work [18,20,22].

2 Differential Dynamic Logic (Excerpt)

Continuous dynamics described by differential equations are a crucial part of hybrid system models. An important subproblem in hybrid system verification is the question whether a system following a (vectorial) differential equation $x' = \theta$ that is restricted to an *evolution domain constraint* region H will always stay in the region F. We represent this by the modal formula $[x' = \theta \,\&\, H]F$. It is true at a state ν if, indeed, a system following $x' = \theta$ from ν will always stay in F at all times (at least as long as the system stays in H). It is false at ν if the system can follow $x' = \theta$ from ν and leave F at some point in time, without having left H at any time. Here, F and H are (quantifier-free) formulas of real arithmetic and $x' = \theta$ is a (vectorial) differential equation, i.e., $x = (x_1, \ldots, x_n)$ is a vector of variables and $\theta = (\theta_1, \ldots, \theta_n)$ a vector of polynomial terms; for extensions to rational functions, see [19]. In particular, H describes a region that the continuous system cannot leave (e.g., because of physical restrictions of the system or because the controller otherwise switches to another mode of the hybrid system). In contrast, F describes a region which we want to prove that the continuous system $x' = \theta \,\&\, H$ will never leave.

This modal logical principle extends to a full dynamic logic for hybrid systems, called *differential dynamic logic* $\mathsf{d}\mathcal{L}$ [18,20,21]. Here we only need first-order logic and modalities for differential equations. For our purposes, it is sufficient to consider the $\mathsf{d}\mathcal{L}$ fragment with the following grammar (where x is a vector of variables, θ a vector of terms of the same dimension, and F, H are formulas of (quantifier-free) first-order real arithmetic over the variables x):

$$\phi, \psi \ ::= \ F \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \phi \leftrightarrow \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [x' = \theta \,\&\, H]F$$

A state is a function $\nu : V \to \mathbb{R}$ that assigns real numbers to all variables in the set $V = \{x_1, \ldots, x_n\}$. We denote the value of term θ in state ν by $\nu[\![\theta]\!]$. The semantics is that of first-order real arithmetic with the following addition:
$\nu \models [x' = \theta \,\&\, H]F$ iff for each function $\varphi : [0, r] \to (V \to \mathbb{R})$ of some duration r we have $\varphi(r) \models F$ under the following two conditions:

1. the differential equation holds, i.e., for each variable x_i and each $\zeta \in [0, r]$:
$$\frac{\mathsf{d}\, \varphi(t)[\![x_i]\!]}{\mathsf{d}t}(\zeta) = \varphi(\zeta)[\![\theta_i]\!]$$
2. and the evolution domain is respected, i.e., $\varphi(\zeta) \models H$ for each $\zeta \in [0, r]$.

The following simple $\mathsf{d}\mathcal{L}$ formula is valid (i.e., true in all states):

$$x > 5 \rightarrow [x' = \frac{1}{2}x]x > 0$$

It expresses that x will always be positive if x starts with $x > 5$ and follows $x' = \frac{1}{2}x$ for any period of time.

3 Differential Equations and Differential Operators

In this section, we study differential equations and their associated differential operators. Only properties of very simple differential equations can be proved by working with their solutions, e.g., linear differential equations with constant coefficients that form a nilpotent matrix [18].

Differential Operators. More complicated differential equations need a different approach, because their solutions may not fall into decidable classes of arithmetic, are not computable, or may not even exist in closed form. As a proof technique for advanced differential equations, we have introduced *differential invariants* [19]. Differential invariants turn the following intuition into a formally sound proof procedure. If the vector field of the differential equation always points into a direction where the differential invariant F, which is a logical formula, is becoming "more true" (see Fig. 1), then the system will always stay safe if it initially starts safe. This principle can be understood in a simple but formally sound way in the logic d$\mathcal{L}$ [19,20]. Differential invariants have been introduced in [19] and later refined to a procedure that computes differential invariants in a fixed-point loop [24]. Instead of our original presentation, which was based on differential algebra, total derivatives, and differential substitution, we take a differential operator approach here. Both views are fruitful and closely related.

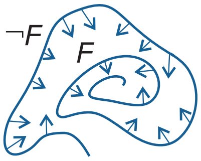

Fig. 1. Differential invariant F

Definition 1 (Lie differential operator). *Let $x' = \theta$ be the differential equation system $x'_1 = \theta_1, \ldots, x'_n = \theta_n$ in vectorial notation. The (Lie)* differential operator *belonging to $x' = \theta$ is the operator $\theta \cdot \nabla$ defined as*

$$\theta \cdot \nabla \overset{def}{=} \sum_{i=1}^{n} \theta_i \frac{\partial}{\partial x_i} = \theta_1 \frac{\partial}{\partial x_1} + \cdots + \theta_n \frac{\partial}{\partial x_n} \tag{1}$$

The $\{\frac{\partial}{\partial x_1}, \cdots, \frac{\partial}{\partial x_n}\}$ are partial derivative operators, but can be considered as a basis of the tangent space at x of the manifold on which $x' = \theta$ is defined. The result of applying the differential operator $\theta \cdot \nabla$ to a differentiable function f is

$$(\theta \cdot \nabla) f = \sum_{i=1}^{n} \theta_i \frac{\partial f}{\partial x_i} = \theta_1 \frac{\partial f}{\partial x_1} + \cdots + \theta_n \frac{\partial f}{\partial x_n}$$

The differential operator lifts *conjunctively* to logical formulas F:

$$(\theta \cdot \nabla) F \overset{\text{def}}{=} \bigwedge_{(b \sim c) \text{ in } F} \big((\theta \cdot \nabla) b \sim (\theta \cdot \nabla) c\big)$$

This conjunction is over all atomic subformulas $b \sim c$ of F for any operator $\sim \in \{=, \geq, >, \leq, <\}$. In this definition, we assume that formulas use dualities like $\neg(a \geq b) \equiv a < b$ to avoid negations and the operator $\neq$ is handled in a special way; see previous work for a discussion [19,22]. The functions and terms in f and F need to be sufficiently smooth for the partial derivatives to be defined and enjoy useful properties like commutativity of $\frac{\partial}{\partial x}$ and $\frac{\partial}{\partial y}$. This is the case for polynomials, which are arbitrarily smooth (C^∞).

Since the differential operator $\theta \cdot \nabla$ is a combination of the total derivative and differential substitution, we have elsewhere [19,22] denoted the result $(\theta \cdot \nabla)F$ of applying $\theta \cdot \nabla$ to a logical formula F by $F'^{\theta}_{x'}$. The latter notation is also appropriate, because $(\theta \cdot \nabla)F \equiv F'^{\theta}_{x'}$ can, indeed, be formed by taking the total derivative F' and then substituting in the right-hand side θ of the differential equation to replace its left-hand side x', the result of which is denoted

${F'}^{\theta}_{x'}$. It is insightful [19] to give a semantics to F', because that is the key to proving advanced differential transformations [19], but beyond the scope of this paper. We refrain from using this alternative notation in this paper, because we want to emphasize the differential operator nature of the combined derivative and differential substitution. In this notation, our differential induction proof rule [19] is:

$$\text{(DI)}\ \frac{H \rightarrow (\theta \cdot \nabla)F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

This *differential induction* rule is a natural induction principle for differential equations. The difference compared to ordinary induction for discrete loops is that the evolution domain constraint H is assumed in the premise (because the continuous evolution is not allowed to leave its evolution domain constraint) and that the induction step uses the differential formula $(\theta \cdot \nabla)F$ corresponding to formula F and the differential operator $\theta \cdot \nabla$ belonging to the differential equation $x' = \theta$ instead of a statement that the loop body preserves the invariant. Intuitively, the *differential formula* $(\theta \cdot \nabla)F$ captures the infinitesimal change of formula F over time along $x' = \theta$, and expresses the fact that F is only getting more true when following the differential equation $x' = \theta$. The semantics of differential equations is defined in a mathematically precise but computationally intractable way using analytic differentiation and limit processes at infinitely many points in time. The key point about differential invariants is that they replace this precise but computationally intractable semantics with a computationally effective use of a differential operator. The valuation of the resulting computable formula $(\theta \cdot \nabla)F$ along differential equations coincides with analytic differentiation [19]. The term $(\theta \cdot \nabla)p$ characterizes how p changes with time along a solution of $x' = \theta$.

Lemma 2 (Derivation lemma). *Let $x' = \theta \,\&\, H$ be a differential equation with evolution domain constraint H and let $\varphi : [0, r] \rightarrow (V \rightarrow \mathbb{R})$ be a corresponding solution of duration $r > 0$. Then for all terms p and all $\zeta \in [0, r]$:*

$$\frac{\mathsf{d}\,\varphi(t)[\![p]\!]}{\mathsf{d}t}(\zeta) = \varphi(\zeta)[\![(\theta \cdot \nabla)p]\!] \ .$$

Proof. This lemma can either be shown directly or by combining the derivation lemma [19, Lemma 1] with differential substitution [19, Lemma 2]. □

The rule DI for differential invariance is computationally very attractive, because it replaces the need to reason about complicated solutions of differential equations with simple symbolic computation and arithmetic on terms that are formed by differentiation, and, hence, have lower degree. The primary challenge, however, is to find a suitable F for a proof.

Equational Differential Invariants. General formulas with propositional combinations of equations and inequalities can be used as differential invariants. For the purposes of this paper, we focus on the equational case in more detail, which is the following special case of DI:

$$(DI_{=})\ \frac{H \to (\theta \cdot \nabla)p = 0}{p = 0 \to [x' = \theta \,\&\, H]p = 0}$$

This equational case of differential invariants turns out to be a special case of Lie's seminal work on what are now called Lie groups [15,16]. Since θ and p are (sufficiently) smooth, we can capture Lie's theorem [17, Proposition 2.6] as a d$\mathcal{L}$ proof rule to make the connection to $DI_{=}$ more apparent.

Theorem 3 (Lie [15,16]). *Let $x' = \theta$ be a differential equation system and H a* domain*, i.e., a first-order formula of real arithmetic characterizing an open set. The following proof rule is a sound global equivalence rule, i.e., the conclusion is valid if and only if the premise is.*

$$(DI_c)\ \frac{H \to (\theta \cdot \nabla)p = 0}{\forall c \left(p = c \to [x' = \theta \,\&\, H]p = c\right)}$$

That is, the following d$\mathcal{L}$ *axiom is sound, i.e., all of its instances valid*

$$\forall x\, \forall c \left(p = c \to [x' = \theta \,\&\, H]p = c\right) \leftrightarrow \forall x\, (H \to (\theta \cdot \nabla)p = 0)$$

Proof (Sketch). We only sketch a proof for the soundness direction of DI_c and refer to [15,16,17,19] for a full proof. Suppose there was a ζ with $\varphi(\zeta)[\![p]\!] \neq \varphi(0)[\![p]\!]$, then, by mean-value theorem, there is a $\xi < \zeta$ such that, when using Lemma 2:

$$0 \neq \varphi(\zeta)[\![p]\!] - \varphi(0)[\![p]\!] = (\zeta - 0)\frac{\mathsf{d}\varphi(t)[\![p]\!]}{\mathsf{d}t}(\xi) = \zeta\varphi(\xi)[\![(\theta \cdot \nabla)p]\!]$$

Thus, $\varphi(\xi)[\![(\theta \cdot \nabla)p]\!] \neq 0$, which contradicts the premise (when $H \equiv \mathit{true}$). □

Note that domains are usually assumed to be connected. We can reason separately about each connected component of H, which are only finitely many, because our domains are first-order definable in real-closed fields [31]. Observe that the conclusion of DI_c implies that of $DI_{=}$ by instantiating c with 0.

Corollary 4 (Decidability of invariant polynomials). *It is decidable, whether a polynomial p with real algebraic coefficients is an invariant function for a given $x' = \theta$ on a (first-order definable) domain H (i.e., the conclusion of DI_c holds). In particular, the set of polynomials with real algebraic coefficients that are invariant for $x' = \theta$ is recursively enumerable.*

This corollary depends on the fact that real algebraic coefficients are countable. A significantly more efficient version of the recursive enumerability is obtained when using symbolic parameters as coefficients in a polynomial p of increasing degree and using the fact that the equivalence in Theorem 3 is valid for each choice of p. In particular, when p is a polynomial with a vector a of symbolic parameters, then, by Theorem 3, the following d$\mathcal{L}$ formula is valid

$$\exists a\, \forall x\, \forall c \left(p = c \to [x' = \theta \,\&\, H]p = c\right) \leftrightarrow \exists a\, \forall x\, (H \to (\theta \cdot \nabla)p = 0) \qquad (2)$$

The right-hand side is decidable in the first-order theory of real-closed fields [31]. Hence, so is the left-hand side, but the approach needs to be refined to be useful.

This includes a logical reformulation of the so-called *direct method*, where the user guesses an *Ansatz* p, e.g., as a polynomial with symbolic parameters a instead of concrete numbers as coefficients, and these parameters are instantiated as needed during the attempt to prove invariance of p. In $\mathsf{d}\mathcal{L}$, we do not need to instantiate parameters a, because it is sufficient to prove existence, for which there are corresponding $\mathsf{d}\mathcal{L}$ proof principles [18]. Other constraints on p need to be considered, however, e.g., that $p = 0$ holds in the initial state and $p = 0$ implies the desired postcondition. Otherwise, the instantiation of a that yields the zero polynomial would be a solution for (2), just not a very insightful one. For example, let $\mathsf{d}\mathcal{L}$ formula A characterize the initial state and $\mathsf{d}\mathcal{L}$ formula B be the postcondition for a continuous system $x' = \theta \,\&\, H$. Then validity of the following (arithmetic) formula

$$\exists a\,\forall x\,((H\rightarrow(\theta\cdot\nabla)p = 0) \land (A \rightarrow p = 0) \land (H \land p = 0 \rightarrow B) \tag{3}$$

implies validity of the $\mathsf{d}\mathcal{L}$ formula

$$A \rightarrow [x' = \theta \,\&\, H]B$$

Formula (3) is decidable if A and B are first-order real arithmetic formulas. Otherwise, the full $\mathsf{d}\mathcal{L}$ calculus is needed to prove (3). Existential quantifiers for parameters can be added in more general ways to $\mathsf{d}\mathcal{L}$ formulas with full hybrid systems dynamics to obtain an approach for generating invariants for proving more general properties of hybrid systems [24,25]. The *Ansatz* p can also be varied automatically by enumerating one polynomial with symbolic coefficients for each (multivariate) degree. This direct method can be very effective, and is related to similar approaches for deciding universal real-closed field arithmetic [27], but, because of the computational cost of real arithmetic [7,4], stops to be efficient for complicated high-dimensional problems. In this paper, we analyze the invariance problem further to develop a deeper understanding of its challenges and ways of solving it.

Since DI_c is an equivalence, Theorem 3 and its corollary may appear to solve the invariance problem (for equations) completely. Theorem 3 is a very powerful result, but there are still many remaining challenges in solving the invariance problem as we illustrate in the following.

Counterexample 5 (Deconstructed aircraft). The following $\mathsf{d}\mathcal{L}$ formula is valid. It is a much simplified version of a formula proving collision freedom for an air traffic control maneuver [19,26]. We have transformed the differential equations to a physically less interesting case that is notationally simpler and still exhibits similar technical phenomena as those that occur in air traffic control verification.

$$x^2 + y^2 = 1 \land e = x\rightarrow[x' = -y, y' = e, e' = -y](x^2 + y^2 = 1 \land e = x) \tag{4}$$

This $\mathsf{d}\mathcal{L}$ formula expresses that an aircraft with position (x, y) will always be safely separated from the origin $(0, 0)$, here, by exactly distance 1 to make things easier. Formula (4) also expresses that the aircraft always is in a compatible y-direction e compared to its position (x, y). In the full aircraft scenario, there is more than one aircraft, each aircraft has more than one direction variable, the relation of the directions to the positions is more complex, and the distance of the aircraft to each other is not fixed at 1, it can be any distance bigger than a protected zone, etc. Yet the basic mathematical phenomena when analyzing (4) are similar to those for full aircraft [19,26], which is why we focus on (4) for notational simplicity. Unfortunately, when we try to prove the valid $\mathsf{d}\mathcal{L}$ formula (4) by a Lie-type differential invariance argument, the proof fails

$$\begin{array}{l}
\text{not valid} \\
\hline
-2xy + 2ey = 0 \\
\hline
(-y)2x + e2y = 0 \land -y = -y \\
\hline
-y\frac{\partial(x^2+y^2)}{\partial x} + e\frac{\partial(x^2+y^2)}{\partial y} = 0 \land -y\frac{\partial e}{\partial e} = -y\frac{\partial x}{\partial x} \\
\hline
\end{array}$$
$${}^{\text{DI}}x^2 + y^2 = 1 \land e = x \rightarrow [x' = -y, y' = e, e' = -y](x^2 + y^2 = 1 \land e = x)$$

This is, at first, surprising, since Theorem 3 is an equivalence, but the conclusion (4) is valid and, yet, the proof does not close. On second thought, the postcondition is a propositional combination of equations instead of the single equation assumed in DI_c and $DI_=$. This discrepancy might have caused Theorem 3 to fail. That is not the issue, however, because we have shown that the deductive power of equational differential invariants equals the deductive power of propositional combinations of equations [19, Proposition 1][23, Proposition 5.1]. That is, every formula that is provable using propositional combinations of equations as differential invariants is provable with single equational differential invariants.

Proposition 6 (Equational deductive power [19,23]). *The deductive power of differential induction with atomic equations is identical to the deductive power of differential induction with propositional combinations of polynomial equations: That is, each formula is provable with propositional combinations of equations as differential invariants iff it is provable with only atomic equations as differential invariants.*

Using the construction of the proof of Proposition 6 on the situation in Counterexample 5, we obtain the following counterexample.

Counterexample 7 (Deconstructed aircraft atomic). The construction in the (constructive) proof of Proposition 6 uses an equivalence, here, the following:

$$x^2 + y^2 = 1 \land e = x \equiv (x^2 + y^2 - 1)^2 + (e - x)^2 = 0$$

The right-hand side of the equivalence is a valid invariant and now a single polynomial as assumed in Theorem 3, but DI_c and $DI_=$ still do not prove it, even though the desired conclusion is valid (because it follows from (4) by axiom K and Gödel's generalization [21]):

$$\begin{array}{r}
\text{not valid}\\ \hline
2(x^2+y^2-1)(-2yx+2ey)=0\\ \hline
2(x^2+y^2-1)(-y2x+e2y)+2(e-x)(-y-(-y))=0\\ \hline
(-y\frac{\partial}{\partial x}+e\frac{\partial}{\partial y}-y\frac{\partial}{\partial e})\big((x^2+y^2-1)^2+(e-x)^2\big)=0\\ \hline
{}^{\text{DI}}(x^2+y^2-1)^2+(e-x)^2=0\rightarrow[x'=-y,y'=e,e'=-y](x^2+y^2-1)^2+(e-x)^2=0
\end{array}$$

How can that happen? And what can we do about it? The key to understanding this is the observation that we *could* close the above proof if only we knew that $e=x$, which is part of the invariant we are trying to prove in this proof attempt. Note that the relation of the variables in the air traffic control maneuver is more involved than mere identity. In that case, a similar relation of the state variables still exists, involving the angular velocity, positions, and multidimensional directions of the aircraft. This relation is crucial for a corresponding proof; see previous work [19,26].

We could close the proof attempt in Counterexample 7 if only we could assume in the premise the invariant F that we are trying to prove. A common mistake is to suspect that F (or the boundary of F) could, indeed, be assumed in the premise when proving invariance of F along differential equations. That would generally be unsound even though it has been suggested [28,8].

Counterexample 8 (No recursive assumptions). The following counterexample shows that it is generally unsound to assume invariants like $F\equiv x^2-6x+9=0$ in the antecedent of the induction step for equational differential invariants

$$\begin{array}{l}
\text{unsound}\\ \hline
x^2-6x+9=0\rightarrow y2x-6y=0\\ \hline
x^2-6x+9=0\rightarrow y\frac{\partial(x^2-6x+9)}{\partial x}-x\frac{\partial(x^2-6x+9)}{\partial y}=0\\ \hline
x^2-6x+9=0\rightarrow[x'=y,y'=-x]x^2-6x+9=0
\end{array}$$

We have previously identified [19] conditions under which F can still be assumed soundly in the differential induction step. Those conditions include the case where F is open or where the differential induction step can be strengthen to an open condition with strict inequalities. Unfortunately, these cases do not apply to equations, which are closed and rarely satisfy strict inequalities in the differential induction step. In particular, we cannot use those to close the proof in Counterexample 7.

Differential Cuts. As an alternative, we have introduced differential cuts [19]. *Differential cuts* [19] are a fundamental proof principle for differential equations. They can be used to strengthen assumptions in a sound way:

$$\text{(DC)}\ \frac{F\rightarrow[x'=\theta\,\&\,H]C \qquad F\rightarrow[x'=\theta\,\&\,(H\wedge C)]F}{F\rightarrow[x'=\theta\,\&\,H]F}$$

The differential cut rule works like a cut, but for differential equations. In the right premise, rule DC restricts the system evolution to the subdomain $H \wedge C$ of H, which restricts the system dynamics to a subdomain but this change is a pseudo-restriction, because the left premise proves that the extra restriction C on the system evolution is an invariant anyhow (e.g. using rule DI). Note that rule DC is special in that it changes the dynamics of the system (it adds a constraint to the system evolution domain region that the resulting system is never allowed to leave), but it is still sound, because this change does not reduce the reachable set. The benefit of rule DC is that C will (soundly) be available as an extra assumption for all subsequent DI uses on the right premise of DC. In particular, the differential cut rule DC can be used to strengthen the right premise with more and more auxiliary differential invariants C that cut down the state space and will be available as extra assumptions to prove the right premise, once they have been proven to be differential invariants in the left premise.

Using differential cuts repeatedly in a process called *differential saturation* has turned out to be extremely useful in practice and even simplifies the invariant search, because it leads to several simpler invariants to find and prove instead of a single complex property [24,25,20]. Differential cuts helped us find proofs for collision avoidance protocols for aircraft [19,26]. Following the same principle in the simplified case of deconstructed aircraft, we finally prove the separation property (4) by a differential cut. The differential cut elimination hypothesis, i.e., whether differential cuts are necessary, has been studied in previous work [23] and will be discussed briefly later.

Example 9 (Differential cuts help separate aircraft). With the help of a differential cut by $e = x$, we can now prove the valid $\mathsf{d}\mathcal{L}$ formula (4), which is a deconstructed variant of how safe separation of aircraft can be proved. For layout reasons, we first show the left premise resulting from DC

$$\text{DC}\;\dfrac{\text{DI}\;\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{-y = -y}}{-y\frac{\partial e}{\partial e} = -y\frac{\partial x}{\partial x}}}{e = x \rightarrow [x' = -y, y' = e, e' = -y]e = x} \qquad \triangleright}{x^2 + y^2 = 1 \wedge e = x \rightarrow [x' = -y, y' = e, e' = -y](x^2 + y^2 = 1 \wedge e = x)}$$

and then show the proof of the right premise of DC resulting from the hidden branch (indicated by $\triangleright$ above):

$$\text{DI}\;\dfrac{\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{e = x \rightarrow -2yx + 2xy = 0}}{e = x \rightarrow (-y)2x + e2y = 0}}{e = x \rightarrow -y\frac{\partial(x^2+y^2)}{\partial x} + e\frac{\partial(x^2+y^2)}{\partial y} = 0}}{x^2 + y^2 = 1 \wedge e = x \rightarrow [x' = -y, y' = e, e' = -y \,\&\, e = x](x^2 + y^2 = 1 \wedge e = x)}$$

Finally, we have a proof of (4) even if it took more than Theorem 3 to prove it.

Another challenge in invariance properties of differential equations the following. Theorem 3 is sufficient, i.e., the premise of DI_c implies the conclusion even if H is not a domain. But the converse direction of necessity may stop to hold, because the conclusion might hold only because all evolutions immediately leave the evolution domain H.

Counterexample 10 (Equivalence requires domain). The following counterexample shows that the equivalence of DI_c requires H to be a domain

$$\dfrac{\dfrac{\dfrac{\text{not valid}}{y=0\to 2=0}}{y=0\to\left(2\frac{\partial}{\partial x}+3\frac{\partial}{\partial y}\right)x=0}}{\forall c\,\big(x=c\to[x'=2,y'=3\,\&\,y=0]x=c\big)}$$

Here, the (closed) restriction $y=0$ has an empty interior and $y'=3$ leaves it immediately. The fact that the evolution leaves $y=0$ immediately is the only reason why $x=c$ is an invariant, which would otherwise not be true, because $x'=2$ leaves $x=c$ when evolving for any positive duration. That is why the above premise is not valid even if the conclusion is. Consequently, DI_c can miss some invariants if H is not a domain. Similar phenomena occur when H has a non-empty interior but is not open.

In the proof of Example 9, after the differential cut (DC) with $e=x$, the refined evolution domain constraint is not a domain anymore, which may appear to cause difficulties in the reasoning according to Counterexample 10. Whether evolution domain restrictions introduced by differential cuts are domains, however, is irrelevant, because the left premise of DC just proved that the differential equation (without the extra constraint C) never leaves C, which turns C into a manifold on which differentiation is well-defined and Lie's theorem applies.

Example 11 (Indirect single proof proof of aircraft separation). We had originally conjectured in 2008 [19] that the differential cuts as used in Example 9 and for other aircraft dynamics are necessary to prove these separation properties. We recently found out, however, that this is not actually the case [23]. The following proof of (4) uses a single differential induction step and no differential cuts:

$$\text{DI}\;\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{-y2e+e2y=0\land -y=-y}}{-y\frac{\partial(e^2+y^2)}{\partial e}+e\frac{\partial(e^2+y^2)}{\partial y}=0\land -y\frac{\partial e}{\partial e}=-y\frac{\partial x}{\partial x}}}{e^2+y^2=1\land e=x\to[x'=-y,y'=e,e'=-y](e^2+y^2=1\land e=x)}$$

Using the construction in Proposition 6, a corresponding proof uses only a single equational invariant to prove (4):

$$\text{DI}\;\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{2(e^2+y^2-1)(-y2e+e2y)+2(e-x)(-y-(-y))=0}}{\left(-y\frac{\partial}{\partial x}+e\frac{\partial}{\partial y}-y\frac{\partial}{\partial e}\right)\big((e^2+y^2-1)^2+(e-x)^2\big)=0}}{(e^2{+}y^2{-}1)^2+(e{-}x)^2=0\to[x'=-y,y'=e,e'=-y](e^2+y^2-1)^2+(e-x)^2=0}$$

Thus, DC and domain restrictions are not critical for proving (4). Observe, however, that the indirect proof of (4) in Example 11 worked with a single equational differential invariant and recall that the same formula was not provable directly in Counterexample 5. Thus, even when the evolution domain (here *true*) is a domain and the phenomena illustrated in Counterexample 10 are not an issue, indirect proofs with auxiliary invariants may succeed even if the direct use of DI_c fails. This makes Theorem 3 incomplete and invariant generation challenging.

Before we illustrate the reasons for this difference in the next section, we briefly show that the same phenomenon happens for the actual aircraft dynamics, not just the deconstructed aircraft-type dynamics.

Example 12 (Aircraft). We abbreviate $d_1^2 + d_2^2 = \omega^2 p^2 \land d_1 = -\omega x_2 \land d_2 = \omega x_1$ by F, which is equivalent to the condition $x_1^2 + x_2^2 = p^2 \land d_1 = -\omega x_2 \land d_2 = \omega x_1$ for safe separation by distance p of the aircraft (x_1, x_2) from the origin $(0, 0)$, when the aircraft flies in a roundabout in its current direction (d_1, d_2) with angular velocity $\omega \neq 0$. We prove invariance of F for an aircraft:

$$\mathrm{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{2d_1(-\omega d_2) + 2d_2\omega d_1 = 0 \land -\omega d_2 = -\omega d_2 \land \omega d_1 = \omega d_1}}{2d_1 d_1' + 2d_2 d_2' = 0 \land d_1' = -\omega x_2' \land d_2' = \omega x_1'}}{F \land \omega \neq 0 \rightarrow [x_1' = d_1, x_2' = d_2, d_1' = -\omega d_2, d_2' = \omega d_1]F}$$

The proof for collision freedom of an aircraft (x_1, x_2) in direction (d_1, d_2) from an aircraft (y_1, y_2) flying in direction (e_1, e_2) is similar to that in [19].

While differential cuts have, thus, turned out not to be required (though still practically useful) for these aircraft properties, differential cuts are still crucially necessary to prove other systems. We have recently shown that differential cuts increase the deductive power fundamentally [23]. That is, unlike in the first-order case, where Gentzen's cut elimination theorem [6] proves that first-order cuts can be eliminated, we have refuted the *differential cut elimination hypothesis*, by proving that some properties of differential equations can only be proved with a differential cut, not without.

Theorem 13 (Differential cut power [23]). *The deductive power with differential cuts (rule DC) exceeds the deductive power without differential cuts.*

We refer to previous work [23] for details on the differential cut elimination hypothesis [19], the proof of its refutation [23], and a complete investigation of the relative deductive power of several classes of differential invariants.

4 Invariant Equations and Invariant Functions

In this section, we study invariant equations and the closely related notion of invariant functions. The conclusion of rule DI_c expresses that the polynomial term p is an invariant function of the differential equation $x' = \theta$ on domain H:

Definition 14 (Invariant function). *The function p is an* invariant function *of the differential equation $x' = \theta$ on H iff*

$$\vDash \forall c \left(p = c \rightarrow [x' = \theta \,\&\, H] p = c\right)$$

That is, an invariant function p is one whose value $p(x(t))$ is constant along all solutions $x(t)$, as a function of time t, of the differential equation $x' = \theta$ within the domain H, i.e., $p(x(t)) = p(x(0))$ for all t. Rule DI_c provides a way to prove that p is an invariant function. A closely related notion is the following.

Definition 15 (Invariant equation). *For a function p, the equation $p = 0$ is an* invariant equation *of the differential equation $x' = \theta$ on H iff*

$$\vDash p = 0 \rightarrow [x' = \theta \,\&\, H] p = 0$$

Synonymously, we say that $p = 0$ is an equational invariant or that the variety $V(p)$ is an *invariant variety* of $x' = \theta \,\&\, H$. For a set S of functions (or polynomials), $V(S)$ is the *variety* of zeros of S:

$$V(S) \overset{\text{def}}{=} \{a \in \mathbb{R}^n : f(a) = 0 \text{ for all } f \in S\}$$

For a single function or polynomial p, we write $V(p)$ for $V(\{p\})$. Varieties of sets of polynomials are a fundamental object of study in algebraic geometry [3,10]. Rule $DI_=$ provides a way to prove that $p = 0$ is an invariant equation.

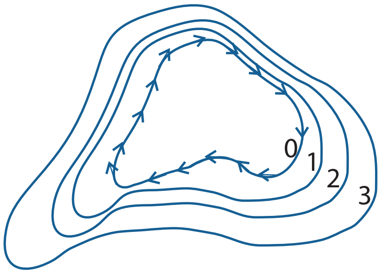

Fig. 2. Invariant equations $p = c$ for levels c of invariant function p

What is, at first, surprising, is that the premise of rule $DI_=$ does not depend on the constant term of the polynomial p. However, a closer look reveals that the premises of $DI_=$ and DI_c are equivalent, and, hence, rule $DI_=$ actually proves that p is an invariant function, not just that $p = 0$ is an equational invariant. Both notions of invariance are closely related but different. If p is an invariant function, then $p = 0$ is an equational invariant [17], but not conversely, since not every level set of p has to be invariant if $p = 0$ is invariant; compare Fig. 2 to general differential invariant Fig. 1.

Lemma 16 (Relation of invariant functions and invariant equations). *A (smooth) polynomial p is an invariant function of $x' = \theta \,\&\, H$ iff, for every $c \in \mathbb{R}$, $p = c$ is an invariant equation of $x' = \theta \,\&\, H$. In this case, if c is a constant that denotes the value of p at the initial state, then $p = c$ and $p = 0$ are invariant equations. Conversely, if $p = 0$ is an equational invariant then the product $I_{p=0}p$ is an invariant function (not necessarily C^1, i.e., continuously differentiable). If c is a fresh variable and $p = c$ an invariant equation of $x' = \theta, c' = 0 \,\&\, H$, then p is an invariant function of $x' = \theta \,\&\, H$ and $x' = \theta, c' = 0 \,\&\, H$.*

Proof. By definition. Recall that the characteristic or indicator function of $p = 0$ is defined as $I_{p=0}(x) = 1$ if $p(x) = 0$ and as $I_{p=0}(x) = 0$ if $p(x) \neq 0$. □

Counterexample 17 ($p = 0$ equational invariant $\not\Rightarrow$ p invariant function). We have $\vDash x = 0 \rightarrow [x' = x]x = 0$ but $\nvDash x = 1 \rightarrow [x' = x]x = 1$, hence $p = 0$ is an equational invariant of $x' = x$ but p is no invariant function, because $p = 1$ is no equational invariant. In particular, we can tell by simulation, whether a polynomial p can be an invariant function, which gives a good falsification test.

The structure of invariant functions is that they form an algebra.

Lemma 18 (Structure of invariant functions). *The invariant functions (or the invariant polynomials) of $x' = \theta \,\&\, H$ form an $\mathbb{R}$-algebra.*

Proof. As a function of time t, let $x(t)$ be a solution of the differential equation under consideration. If p, q are invariant functions and $\lambda \in \mathbb{R}$ is a number (or constant symbol), then $p + q, pq, \lambda p$ are invariant functions, because, for any operator $\oplus \in \{+, \cdot\}$:
$(p \oplus q)(x(t)) = p(x(t)) \oplus q(x(t()) = p(x(0)) \oplus q(x(0)) = (p \oplus q)(x(0))$ □

According to Lemma 18, it is enough to find a generating system of the algebra of invariant functions, because all algebraic expressions built from this generating set are invariant functions. A *generating system* of an algebra is a set S such that the set of all elements that can be formed from S by operations of the algebra coincides with the full algebra. More precisely, the smallest algebra containing S is the full algebra of invariant functions. This generating system is not necessarily small, however, because, whenever p is an invariant function and F an arbitrary (sufficiently smooth) function, e.g., polynomial, then $F(p)$ is an invariant function. This holds accordingly for (sufficiently smooth) functions F with multiple arguments. The situation improves if we take a *functional generating set G*. That is, a set G that gives all invariant functions when closing it under composition with any (sufficiently smooth) function F, i.e., $F(p_1, \ldots, p_n)$ is in the closure for all p_i in the closure.

A useful structure of the invariant equations is that they form an ideal. For a fixed dynamics $x' = \theta$ or $x' = \theta \,\&\, H$ we define the following sets of valid formulas and provable formulas, respectively:

$$\begin{aligned} \mathcal{I}_{=}(\Gamma) &:= \{p \in \mathbb{R}[\boldsymbol{x}] \;:\; \vDash \Gamma \rightarrow [x' = \theta \,\&\, H]p = 0\} \\ \mathcal{DCI}_{=}(\Gamma) &:= \{p \in \mathbb{R}[\boldsymbol{x}] \;:\; \vdash_{\mathrm{DI}_{=}+\mathrm{DC}} \Gamma \rightarrow [x' = \theta \,\&\, H]p = 0\} \\ r\mathcal{I}_{=} &:= \{p \in \mathbb{R}[\boldsymbol{x}] \;:\; \vDash p = 0 \rightarrow [x' = \theta \,\&\, H]p = 0\} \\ r\mathcal{DCI}_{=} &:= \{p \in \mathbb{R}[\boldsymbol{x}] \;:\; \vdash_{\mathrm{DI}_{=}+\mathrm{DC}} p = 0 \rightarrow [x' = \theta \,\&\, H]p = 0\} \end{aligned}$$

The set $\mathcal{I}_{=}(\Gamma)$ collects the polynomials whose variety forms an invariant equation ($p \in \mathcal{I}_{=}(\Gamma)$). The set $\mathcal{DCI}_{=}(\Gamma)$ collects the polynomials for whose zero set it is provable using equational differential invariants ($DI_{=}$) and differential cuts (DC) that they are invariant equations ($p \in \mathcal{DCI}_{=}(\Gamma)$). The sets $\mathcal{I}_{=}(\Gamma)$ and $\mathcal{DCI}_{=}(\Gamma)$ are relative to a $\mathsf{d}\mathcal{L}$ formula (or set) Γ that is used as assumption.

The reflexive sets $r\mathcal{I}_=$ and $r\mathcal{DCI}_=$, instead, assume that the precondition and postcondition are identical. It turns out that the reflexive versions do not have a very well-behaved structure (see the following proof). The invariant sets $\mathcal{I}_=(\Gamma)$ and $\mathcal{DCI}_=(\Gamma)$, instead, are well-behaved and form a chain of differential ideals.

Lemma 19 (Structure of invariant equations). *Let Γ be a set of* d$\mathcal{L}$ *formulas, then $\mathcal{DCI}_=(\Gamma) \subseteq \mathcal{I}_=(\Gamma)$ is a chain of differential ideals (with respect to the derivation $\theta \cdot \nabla$, in particular $(\theta \cdot \nabla)p \in \mathcal{DCI}_=(\Gamma)$ for all $p \in \mathcal{DCI}_=(\Gamma)$). Furthermore, the varieties of these ideals are generated by a single polynomial.*

Proof. We prove each of the stated properties.

1. The inclusion follows from soundness. The inclusion $r\mathcal{DCI}_= \subseteq r\mathcal{I}_=$ even still holds for $r\mathcal{I}_=$.
2. It is easy to see that $p, q \in \mathcal{I}_=(\Gamma)$ and $r \in \mathbb{R}[\boldsymbol{x}]$ imply $p + q, rp \in \mathcal{I}_=(\Gamma)$. Both properties do not hold for r$\mathcal{I}_=$, because $x, x^2 \in r\mathcal{I}_=$ for the dynamics $x' = x$, but the sum/product $x^2 + x = x(x + 1) \notin r\mathcal{I}_=$
3. Let $p, q \in \mathcal{DCI}_=(\Gamma)$, then $p + q \in \mathcal{DCI}_=(\Gamma)$, because $\Gamma \to p = 0 \land q = 0$ implies $\Gamma \to p + q = 0$ (for the antecedent) and $\theta \cdot \nabla$ is a linear operator:
$$(\theta \cdot \nabla)(p + q) = (\theta \cdot \nabla)p + (\theta \cdot \nabla)q = 0 + 0 = 0$$
The second equation holds after sufficiently many uses of DC that are needed to show that $p, q \in \mathcal{DCI}_=(\Gamma)$.
4. Let $p \in \mathcal{DCI}_=(\Gamma)$ and $r \in \mathbb{R}[\boldsymbol{x}]$, then $rp \in \mathcal{DCI}_=(\Gamma)$, because $\Gamma \to p = 0$ implies $\Gamma \to rp = 0$ (for the antecedent) and $\theta \cdot \nabla$ is a derivation operator:
$$(\theta \cdot \nabla)(rp) = p(\theta \cdot \nabla)r + r\underbrace{(\theta \cdot \nabla)p}_{0} = \underbrace{p}_{0}(\theta \cdot \nabla)r = 0$$
The second equation holds after sufficiently many uses of DC that are needed to show that $p \in \mathcal{DCI}_=(\Gamma)$. The last equation holds after one more use of DC by $p = 0$, which entails $p = 0$ on the (new) domain of evolution $H \land p = 0$.
5. The fact that the ideal $\mathcal{DCI}_=(\Gamma)$ is a differential ideal follows from [20, Lem 3.7], which just uses differential weakening. In detail: $p \in \mathcal{DCI}_=(\Gamma)$ implies that $(\theta \cdot \nabla)p = 0$ is provable after sufficiently many DC. Hence, after the same DC, invariance of $(\theta \cdot \nabla)p = 0$ is provable by DW.
6. From $p \in \mathcal{I}_=(\Gamma)$, we conclude $(\theta \cdot \nabla)p \in \mathcal{I}_=(\Gamma)$ as follows. Let $p(x(t)) = 0\ \forall t$. Then $((\theta \cdot \nabla)p)(x(t)) = \sum_i \theta_i(x(t)) \frac{\partial p}{\partial x_i}(x(t)) = 0$ follows from the necessity direction of Theorem 3.
7. $p = 0 \land q = 0$ is a propositional equation that is invariant iff $p^2 + q^2 \in \mathcal{I}(\Gamma)$, i.e., $p^2 + q^2 = 0$ gives an invariant equation. The same holds for $\mathcal{DCI}_=(\Gamma)$ by previous work [19,23]. By repeating this construction, we obtain a variety generated by a single polynomial, because, by Hilbert's basis theorem [12], every ideal in the (multivariate) polynomial ring of a Noetherian ring (e.g., a field) is finitely generated ideal. Yet the ring of polynomials is not a principal ideal domain except in dimension 1.

8. $p = 0 \lor q = 0$ is a propositional equational invariant iff $pq \in \mathcal{I}_=(\Gamma)$, i.e., $pq = 0$ gives an invariant equation. The same holds for $\mathcal{DCI}_=(\Gamma)$ by previous work [19,23]. □

Observe that the differential cut rule DC needs to be included to make $\mathcal{DCI}_=$ an ideal (not closed under multiplication with other polymials). Without differential cuts, the set of provable equational differential invariants is generally no ideal. As a corollary to Lemma 19, it is sufficient to find a complete set of differential ideal generators, because these generators describe all other invariants. Without taking functional generators into account, there are still infinitely many invariant equations, because every invariant function induces infinitely many invariant equations by Lemma 16.

According to Lemma 19, however, there is a *single generator of the variety of the differential ideals*, which is the most informative invariant.

5 Assuming Equations and Equational Invariants

Theorem 3 gives an equivalence characterization of invariant functions on open domains. Another seminal result due to Lie provides a similar equivalence characterization for invariant equations of full rank. This equivalence characterization assumes the invariant F during its proof, which is not sound in general; see Counterexample 8. In the case of full rank, this is different.

Theorem 20 (Lie [15,16][17, Theorem 2.8]). *The following rule is sound*

$$(\overleftarrow{DI}_p)\ \frac{\bigwedge_{i=1}^{n} p_i = 0 \rightarrow [x' = \theta \,\&\, H] \bigwedge_{i=1}^{n} p_i = 0}{H \land \bigwedge_{i=1}^{n} p_i = 0 \rightarrow \bigwedge_{i=1}^{n} (\theta \cdot \nabla) p_i = 0}$$

If rank $\frac{\partial p_i}{\partial x_j} = n$ *on* $H \land \bigwedge_{i=1}^{n} p_i = 0$*, then the premise and conclusion are equivalent.*

Rule $\overleftarrow{DI}_p$ provides a necessary condition for an equation system to be an invariant and can, thus, be used to disprove invariance. Rule $DI_=$ provides a sufficient condition, but implies a stronger property (invariant function instead of just invariant equation). In the full rank case, $\overleftarrow{DI}_p$ is an equivalence and can decide whether $\bigwedge_{i=1}^{n} p_i = 0$ is an invariant equation. Whether $\bigwedge_{i=1}^{n} p_i = 0$ satisfies the full rank condition is decidable in real-closed fields, but nontrivial without optimizations. The invariant in Example 9 has full rank 2, except when $x = y = 0$, which does not satisfy the invariant $x^2 + y^2 = 1$:

$$\begin{pmatrix} \frac{\partial(x^2+y^2-1)}{\partial x} & \frac{\partial(x^2+y^2-1)}{\partial y} & \frac{\partial(x^2+y^2-1)}{\partial e} \\ \frac{\partial(e-x)}{\partial x} & \frac{\partial(e-x)}{\partial y} & \frac{\partial(e-x)}{\partial e} \end{pmatrix} = \begin{pmatrix} 2x & 2y & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

In Counterexample 8, however, the full rank condition is, in fact, violated, since $\frac{\partial(x^2-6x+9)}{\partial y} = 0$ and $\frac{\partial(x^2-6x+9)}{\partial x} = 2x-6$ has a zero when $x=3$, which satisfies $x^2-6x+9=0$. This explains why it was not sound to assume $x^2-6x+9=0$ when attempting to prove it.

It is sound to use equations in the following style (also see [30]):

Theorem 21. *This rule is sound for any choice of smooth functions $Q_{i,j}$:*

$$(\overrightarrow{DI}_p)\ \frac{H \rightarrow \bigwedge_{i=1}^{n} (\theta \cdot \nabla) p_i = \sum_j Q_{i,j} p_j}{\bigwedge_{i=1}^{n} p_i = 0 \rightarrow [x' = \theta \,\&\, H] \bigwedge_{i=1}^{n} p_i = 0}$$

If rank $\frac{\partial p_i}{\partial x_j} = n$ *on* $H \wedge \bigwedge_{i=1}^{n} p_i = 0$*, then the premise of* $\overrightarrow{DI}_p$ *is equivalent to the conclusion of* $\overleftarrow{DI}_p$*.*

Proof. This result follows from [17], since the premise of $\overrightarrow{DI}_p$ is equivalent to the conclusion of $\overleftarrow{DI}_p$ by [17, Proposition 2.10] in the maximal rank case. We only sketch the (simple) soundness direction for $n=1$ and $H \equiv \mathit{true}$. At any ζ, by Lemma 2, the premise, and the antecedent of the conclusion:

$$\begin{aligned} \frac{\mathsf{d}\varphi(t)[\![p]\!]}{\mathsf{d}t}(\zeta) &= \varphi(\zeta)[\![(\theta \cdot \nabla)p]\!] = \varphi(\zeta)[\![Qp]\!] = \varphi(\zeta)[\![Q]\!] \cdot \varphi(\zeta)[\![p]\!] \\ \varphi(0)[\![p]\!] &= 0 \end{aligned}$$

The constant function zero solves this linear differential equation (system). Since solutions are unique (Q and p smooth), this implies $\varphi(\zeta)[\![p]\!] = 0$ for all ζ. □

According to Theorem 20, it is necessary for invariance of $\bigwedge_{i=1}^{n} p_i = 0$ that $(\theta \cdot \nabla)p_i$ is in the variety, i.e., $(\theta \cdot \nabla)p_i \in V(p_1, \dots, p_n)$ for all i. But, according to Theorem 21 it is only sufficient if $(\theta \cdot \nabla)p_i$ is in the ideal $(p_1, \dots, p_n)$ generated by the p_j, i.e., the set $\{\sum_j Q_j p_j : Q_j \in \mathbb{R}[x]\}$. In the full rank case, both conditions are equivalent.

Counterexample 22 (Full rank). Full rank is required for equivalence. For example, $h := x-1$ vanishes on $p := (x-1)^2 = 0$, but no smooth function Q satisfies $h = Qp$, since the required $Q := (x-1)^{-1}$ has a singularity at $p=0$.

6 Partial Differential Equations and the Inverse Characteristic Method

In this section, we study the connection of differential invariants with partial differential equations. The operator $\theta \cdot \nabla$ defined in (1) is a differential operator.

Then the premise $H \to (\theta \cdot \nabla)p$ of DI_c, which is the same as the premise of $DI_=$, is a partial differential equation on the domain H.

$$(\theta \cdot \nabla)p = 0 \quad \text{on } H \tag{5}$$

This equation is a first-order, linear, homogeneous partial differential equation, which are well-behaved partial differential equations. By Theorem 3, p is a solution of the partial differential equation (5) on domain H iff p is an invariant function of $x' = \theta \,\&\, H$. Thus, with the caveats explained in Section 3, solving partial differential equations gives a complete approach to generating invariant functions, which are the strongest type of differential invariants.

This approach first seems to be at odds with what we wanted to achieve in the first place. Differential equations are complicated, their solutions hard to compute. So we work with differential invariants instead, which are perfect for verification if only we find them. In order to find differential invariants, we solve a partial differential equation, which, in general, is even harder than solving ordinary differential equations. In fact, many numerical and symbolic algorithms for solving partial differential equations are based on solving a number of ordinary differential equation systems as subproblems. The *characteristic method*, see [5, Theorem 3.2.1][32, §1.13.1.1], studies the characteristic ordinary differential equations belonging to a partial differential equation in order to understand the partial differential equation.

We nevertheless proceed this way and call it the *inverse characteristic method*, i.e., the study of properties of ordinary differential equations by studying the partial differential equation belonging to its Lie-type differential operator.

Theorem 23 (Inverse characteristic method). *A (sufficiently smooth) function f is an invariant function of the differential equation $x' = \theta$ on the domain H iff f solves the partial differential equation* (5) *on H, i.e.,*

$$(\theta \cdot \nabla)f = 0 \quad \textit{on } H$$

Proof. This is a consequence of Theorem 3. □

The inverse characteristic method is insightful for two reasons. First, it identifies a mathematically well-understood characterization of the problem of generating differential invariants, at least for the equational case of invariant functions on domains. Second, the inverse characteristic method can be quite useful in practice, because the resulting partial differential equations are rather well-behaved, and solvers for partial differential equations are built on very mature foundations. Note that it is beneficial for the purposes of building a verification tool that the partial differential equation solver can work as an oracle and does not need to be part of the trusted computing base, since we can easily check its (symbolic) solutions for invariance by rule DI_c just using symbolic derivatives and polynomial algebra.

Example 24 (Deconstructed aircraft). For the deconstructed aircraft from Counterexample 5, the dynamics yields the corresponding partial differential equation

$$-y\frac{\partial f}{\partial x} + e\frac{\partial f}{\partial y} - y\frac{\partial f}{\partial e} = 0$$

whose solution can easily be computed to be

$$f(x,y,e) = g\left(e - x, \frac{1}{2}(2ex - x^2 + y^2)\right)$$

Thus, the solution is a function g of $e - x$ and of $\frac{1}{2}(2ex - x^2 + y^2)$, which turns both terms into invariant functions:

$$e - x \tag{6}$$

$$2ex - x^2 + y^2 \tag{7}$$

Contrast this with the invariant equation $(e^2 + y^2 - 1)^2 + (e - x)^2 = 0$ from the proof of (4) in Example 11. In order to relate this creative invariant to the systematically constructed invariants (6)–(7), we note that the initial state and postcondition in (4) is $x^2 + y^2 = 1 \land e = x$. Hence, $y^2 = 1 - x^2, e = x$, which we substitute in (7) to obtain $2xx - x^2 + (1 - x^2) = 1$. Thus, for the purpose of proving (4), the initial value for (6) is 0 and that for (7) is 1. Using $e - x = 0$, the invariant $e^2 + y^2 - 1$ can be obtained from (7) and the initial value 1 by polynomial reduction.

Example 25 (Aircraft). For the actual aircraft dynamics in Example 12, the corresponding partial differential equation

$$d_1 \frac{\partial f}{\partial x_1} + d_2 \frac{\partial f}{\partial x_2} - \omega d_2 \frac{\partial f}{\partial d_1} + \omega d_1 \frac{\partial f}{\partial d_2} = 0$$

whose solution can easily be computed to be (recall $\omega \neq 0$)

$$f(x_1, x_2, d_1, d_2) = g\left(d_2 - \omega x_1, \frac{d_1 + \omega x_2}{\omega}, \frac{1}{2}(d_1^2 + 2\omega d_2 x_1 - \omega^2 x_1^2)\right)$$

revealing the invariant functions $d_2 - \omega x_1, d_1 + \omega x_2, d_1^2 + 2\omega d_2 x_1 - \omega^2 x_1^2$. From these, the creative invariant in Example 12 can be constructed in retrospect with initial value 0, 0, and $\omega^2 p^2$, respectively. The value $\omega^2 p^2$ can be found either by polynomial reduction or by substituting $\omega x_1 = d_2$ in as follows

$$d_1^2 + 2\omega d_2 x_1 - \omega^2 x_1^2 = d_1^2 + 2d_2^2 - d_2^2 = d_1^2 + d_2^2 = \omega^2 p^2$$

7 Conclusions and Future Work

Differential invariants are a natural induction principle for differential equations. The structure of general differential invariants has been studied previously. Here, we took a differential operator view and have studied the case of equational differential invariants in more detail. We have related equational differential invariants to Lie's seminal work and subsequent results about Lie groups. We have shown how the resulting equivalence characterization of invariant equations on open domains can be used, carefully illustrate surprising challenges in invariant generation, explain why they exist, and show with which techniques they can be overcome. We have studied the structure of invariant functions and invariant equations, their relation, and have shown that, in the presence of differential cuts, the invariant equations and provable invariant equations form a chain of differential ideals and that their varieties are generated by a single invariant. Finally, we relate differential invariants to partial differential equations and explain how the inverse characteristic method reduces the problem of equational differential invariant generation to that of solving partial differential equations.

The results we present in this paper relate equational differential invariants to other problems. They show equivalence characterizations and methods for generating equational differential invariants. While the connection with other aspects of mathematics makes a number of classical results available, their complexity indicates that the study of differential invariants has the potential for many further discoveries. In this paper, we have focused exclusively on the equational case. In the theory of differential invariants, however, the equational and general case have quite different characteristics [23]. The general case of differential invariants that are logical formulas with equations and inequalities has been studied elsewhere [23].

Acknowledgements. I thank David Henriques and the PC chairs of ITP for helpful feedback.

References

1. Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T.A., Ho, P.H., Nicollin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. Theor. Comput. Sci. 138(1), 3–34 (1995)
2. Collins, G.E., Hong, H.: Partial cylindrical algebraic decomposition for quantifier elimination. J. Symb. Comput. 12(3), 299–328 (1991)
3. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer (1992)
4. Davenport, J.H., Heintz, J.: Real quantifier elimination is doubly exponential. J. Symb. Comput. 5(1/2), 29–35 (1988)
5. Evans, L.C.: Partial Differential Equations, Graduate Studies in Mathematics, vol. 19. AMS, 2nd edn. (2010)
6. Gentzen, G.: Untersuchungen über das logische Schließen. II. Math. Zeit. 39(3), 405–431 (1935)
7. Grigor'ev, D.Y.: Complexity of quantifier elimination in the theory of ordinary differential equations. In: Davenport, J.H. (ed.) EUROCAL. LNCS, vol. 378, pp. 11–25. Springer (1987)
8. Gulwani, S., Tiwari, A.: Constraint-based approach for analysis of hybrid systems. In: Gupta and Malik [9], pp. 190–203
9. Gupta, A., Malik, S. (eds.): Computer Aided Verification, CAV 2008, Princeton, NJ, USA, Proceedings, LNCS, vol. 5123. Springer (2008)
10. Hartshorne, R.: Algebraic Geometry, Graduate Texts in Mathematics, vol. 52. Springer (1977)

11. Henzinger, T.A.: The theory of hybrid automata. In: LICS. pp. 278–292. IEEE Computer Society, Los Alamitos (1996)
12. Hilbert, D.: Über die Theorie der algebraischen Formen. Math. Ann. 36(4), 473–534 (1890)
13. Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia. IEEE Computer Society (2012)
14. Lie, S.: Über Differentialinvarianten, vol. 6. Teubner (1884), english translation: Ackerman, M; R (1975), Sophus Lie's 1884 Differential Invariant Paper, Brookline, Mass.: Math Sci Press
15. Lie, S.: Vorlesungen über continuierliche Gruppen mit geometrischen und anderen Anwendungen. Teubner, Leipzig (1893)
16. Lie, S.: Über Integralinvarianten und ihre Verwertung für die Theorie der Differentialgleichungen. Leipz. Berichte 49, 369–410 (1897)
17. Olver, P.J.: Applications of Lie Groups to Differential Equations. Springer, 2nd edn. (1993)
18. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. 41(2), 143–189 (2008)
19. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. 20(1), 309–352 (2010)
20. Platzer, A.: Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics. Springer, Heidelberg (2010)
21. Platzer, A.: The complete proof theory of hybrid systems. In: LICS [13]
22. Platzer, A.: Logics of dynamical systems (invited tutorial). In: LICS [13]
23. Platzer, A.: The structure of differential invariants and differential cut elimination. Logical Methods in Computer Science (2012), to appear
24. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Gupta and Malik [9], pp. 176–189
25. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. Form. Methods Syst. Des. 35(1), 98–120 (2009), special issue for selected papers from CAV'08
26. Platzer, A., Clarke, E.M.: Formal verification of curved flight collision avoidance maneuvers: A case study. In: Cavalcanti, A., Dams, D. (eds.) FM. LNCS, vol. 5850, pp. 547–562. Springer (2009)
27. Platzer, A., Quesel, J.D., Rümmer, P.: Real world verification. In: Schmidt, R.A. (ed.) CADE. LNCS, vol. 5663, pp. 485–501. Springer (2009)
28. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) HSCC. vol. 2993, pp. 477–492. Springer (2004)
29. Prajna, S., Jadbabaie, A., Pappas, G.J.: A framework for worst-case and stochastic safety verification using barrier certificates. IEEE T. Automat. Contr. 52(8), 1415–1429 (2007)
30. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. Form. Methods Syst. Des. 32(1), 25–55 (2008)
31. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. University of California Press, Berkeley, 2nd edn. (1951)
32. Zeidler, E. (ed.): Teubner-Taschenbuch der Mathematik. Teubner (2003)