The Structure of Differential Invariants and Differential Cut Elimination

André Platzer

April 12, 2011
CMU-CS-11-112

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA

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. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution or government.

Keywords: Proof theory, differential equations, differential cut elimination, logics of programs, differential invariants, hybrid systems, dynamic logic.

Abstract

The biggest challenge in hybrid systems verification is the handling of differential equations. Because computable closed-form solutions only exist for very simple differential equations, proof certificates have been proposed for more scalable verification. Search procedures for these proof certificates are still rather ad-hoc, though, because the problem structure is only understood poorly. We investigate differential invariants, which can be checked for invariance along a differential equation just by using their differential structure and without having to solve the differential equation. We study the structural properties of differential invariants. To analyze trade-offs for proof search complexity, we identify more than a dozen relations between several classes of differential invariants and compare their deductive power. As our main results, we analyze the deductive power of differential cuts and the deductive power of differential invariants with auxiliary differential variables. We refute the differential cut elimination hypothesis and show that differential cuts are fundamental proof principles that strictly increase the deductive power. We also prove that the deductive power of differential invariants increases further when adding auxiliary differential variables to the dynamics.

1 Introduction

Hybrid systems [Tav87, Hen96, BBM98, DN00] are systems with joint discrete and continuous dynamics, e.g., aircraft that move continuously in space along differential equations for flight and that are controlled by discrete control decisions for flight control like collision avoidance maneuvers. Hybrid systems verification is an important but challenging and undecidable problem [Hen96, BBM98]. Several verification approaches for hybrid systems have been proposed. Verifying properties of differential equations is at the heart of hybrid systems verification. In fact, hybrid systems can be proved correct exactly as good as we can prove properties of differential equations. This surprising intuition is made formally rigorous by a relatively complete axiomatization of a verification logic for hybrid systems relative to properties of differential equations [Pla08]. Thus, the remaining (yet undecidable) question is how to prove properties of differential equations. If the differential equation has a simple polynomial solution, then this is easy [Pla08] using the decidable theory of first-order real arithmetic [Tar51]. Unfortunately, almost no differential equations have such simple solutions. Polynomial solutions arise in linear differential equations with constant coefficients where the coefficient matrix is nilpotent. But this is a very restricted class. For other differential equations, numerous approximation techniques have been considered to obtain approximate answers [GM99, ADG03, GP07, RS07, Fre08]. It is generally surprisingly difficult to get them formally sound, however, due to inherent numerical approximation and floating-point errors that make the numerical image computation problem itself undecidable [PC07, Col07], even when tolerating arbitrarily large error bounds on the decision.

As alternative approaches that are not based on approximation, proof certificate techniques have been proposed for hybrid systems verification, including barrier certificates [PJ04, PJP07], template equations [SSM08], differential invariants [Pla10a, PC08], and a constraint-based template approach [GT08]. Once a proof certificate has been found, it can be checked efficiently. But we first have to find it. Previous search procedures are based on fixing various user-specified templates [PJ04, PJP07, SSM08, GT08, PC08]. But these verification techniques fail if the template does not include the required form. How do we need to choose the templates? What are the trade-offs for choosing them? This can be a serious practical problem. Indeed, in an air traffic control study [PC08], templates with degree bound 2 already lead to a 10000-dimensional nonlinear continuous search problem when using, e.g., the approach of Prajna et al. [PJP07]. But this 10000-dimensional uncountable search space nevertheless does not contain a successful proof certificate. The reason that search procedures for these proof certificates are ad-hoc is that the structure of the certificates has not been well understood so far.

A more general question is what the structure of the search space looks like. What relationships exist between various choices for classes of proof certificates? Are there system properties that cannot be proven when focusing on a particular class of invariants? Are any of the choices superior to others or are they mutually incomparable? Invariants are well-understood for discrete systems but not for continuous and hybrid systems.

We consider differential invariants, which include several previous approaches as special cases (yet in modified forms to make the reasoning sound). Differential invariants have been instrumental in verifying several practical applications including separation properties in complex curved flight collision avoidance maneuvers for air traffic control [PC09], advanced safety, reactivity and

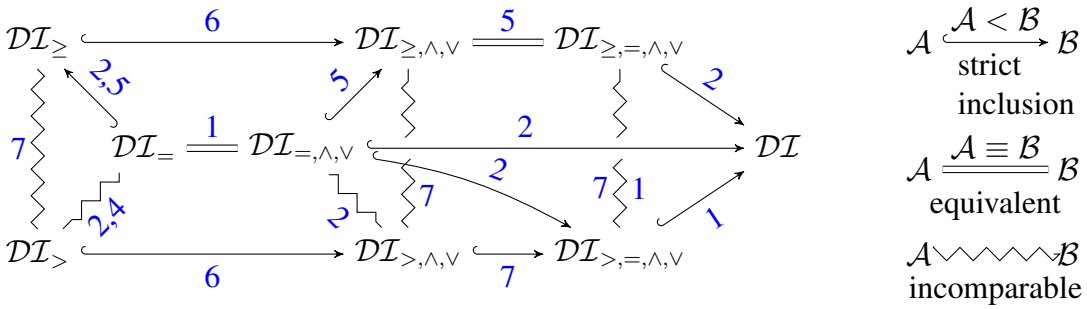

Figure 1: Differential invariance chart (proposition numbers are indicated for each relation)

controllability properties of train control systems with disturbance and PI controllers [PQ09], and properties of electrical circuits [Pla10b]. Our logic-based proof approach with differential invariants has been the key enabling technique to make formal verification of these systems possible.

Here, we study the structure of differential invariants from a more foundational perspective and develop their proof theory. Differential equations enjoy various universal computation properties, hence verification is not even semidecidable [Bra95, GCB07, BCGH07, Col07]. Consequently, every complete proof rule is unsound or ineffective. Hence, proof theory is not a study of completeness but a study of alignment and relative provability.

We analyze the relationships between several classes of differential invariants. Our main tool for this is the study of *relative deductive power*. For comparing two classes of differential invariants, $\mathcal{A}$ and $\mathcal{B}$, we investigate whether there is a system property that only $\mathcal{A}$ can prove or whether all properties that can be proven using $\mathcal{A}$ can also be proven using $\mathcal{B}$. If the answer is yes (inclusion), we give a construction that translates proofs using $\mathcal{A}$ into proofs using $\mathcal{B}$. If the answer is no (separation), we prove for a formal proof using $\mathcal{A}$ that there is no formal proof using $\mathcal{B}$. Of course, there are infinitely many possible proofs to check. We, thus, show the deductive power separation property by coming up with an indirect characteristic that separates the properties provable using $\mathcal{B}$ from the particular proof using $\mathcal{A}$. These separation properties that we identify in our proofs are of more general interest beyond the cases we show. We identify more than a dozen (16) relationships between nine classes of differential invariants (summarized in Figure 1), which shed light on how the classes compare in terms of their deductive power for systems analysis.

While our study is mostly one of logically fundamental properties like deductive power and provability, our proofs indicate additional computational implications, e.g., to what extent the polynomial degree or formula complexity increases with the respective inclusion and equivalence reductions shown in Figure 1. It is also easy to read off general limits of classes of differential invariants from our proofs of the separation properties.

Observe that the algebraic structure of nonlinear real arithmetic alone is not sufficient to explain the relations identified in Figure 1. Both the algebraic and the differential structure of differential invariants matter for the answer, because the dynamics along differential equations determines which properties hold when following the system dynamics. Consequently, the differential structure of the differential equation and of the property matter. Even if the real algebraic structures match, we still do not know if the corresponding differential structures align in a compatible

way. We will see that the joint differential-algebraic structure of the problem can be surprising even for very simple differential equations already. In particular, our observations are fundamental and cannot be sidestepped by restricting attention to simpler classes of differential equations. Even though topological considerations have also been successful for some aspects of continuous dynamical systems, invariance ultimately is not a topological question but depends on the differential-geometrical structure induced by the differential equation. We, thus, study the proof-theoretical properties of what can be proved about a differential equation based on its differential and algebraic invariant structure.

Most importantly, and most surprisingly, we refute the *differential cut elimination hypothesis*. Differential cuts have a simple intuition. Similar to a cut in first-order logic, they can be used to first prove a lemma and then use it. By the seminal cut elimination theorem of Gentzen [Gen35b, Gen35a], standard logical cuts can be eliminated. Unlike standard cuts, differential cuts work for differential equations and can be used to change the dynamics of the system. The question is whether this differential cut proof principle also supports differential cut elimination. Are differential cuts only a convenient proof shortcut? Or are differential cuts an independent fundamental proof principle? We show that the addition of differential cuts increases the deductive power. There are system properties that can only be proven using differential cuts, not without them. Hence, differential cuts indeed turn out to be a fundamental proof principle. Three years ago we had conjectured that differential cuts are necessary to prove a certain class of air traffic control properties [Pla10a]. We have now refuted this conjecture, since those differential cuts can still be eliminated with a clever construction. But we show that differential cuts are still necessary in general. This illustrates the subtle nature of proving properties of differential equations.

Furthermore, we present new proof rules for auxiliary differential variables and prove that the addition of auxiliary differential variables increases the deductive power, even in the presence of differential cuts. That is, there are system properties that can only be proven using auxiliary differential variables in the dynamics. Hence, auxiliary differential variables are also a fundamental proof principle. This is similar to discrete programs where auxiliary variables may also be necessary to prove some properties. We now show that the same also holds for differential equations. Refining differential equations with auxiliary differential variables adds to the deductive power, which, surprisingly, has not been considered before.

These alignments of the relative deductive power shed light on the properties and practical implications of various choices for verification. They help make informed decisions about which restrictions on proof search (and differential invariant search) are tolerable without changing the deductive power. In this paper we study the problem of proving properties of differential equations. This directly relates to a study of proving properties of hybrid systems by way of a proof calculus from previous work that we have shown to be a complete axiomatization of hybrid systems relative to properties of differential equations [Pla08]. This previous result makes it formally precise how the verification of hybrid systems can be reduced directly to the verification of properties of differential equations, which we consider here. Our new results about the structure of the continuous verification problem extend directly to the hybrid systems verification problem in our proof calculus [Pla08, Pla10a, Pla10b].

Our research requires a symbiosis of logic with elements of differential, semialgebraic, geo-

metrical, and real arithmetical principles. Based on the results presented in this paper, we envision a continuing development of a new field that we call *real differential semialgebraic geometry*. In this work, it is of paramount importance to distinguish semantical truth from deductive proof. We assume that the reader is familiar with the proof theory of classical logic [Fit96, And02], including the underlying notions of formal deduction, and the relationship and differences between syntax, semantics, and proof calculi. We also assume basic knowledge of differential equations [Wal98] and of first-order real arithmetic [Tar51].

2 Preliminaries

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 dynamic logic 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 terms, which we assume to be polynomials for simplicity. In particular, H describes a region that the continuous system cannot leave (e.g., because of physical restrictions or because the controller otherwise switches to another mode of the hybrid system). In contrast, F describes a region for which we want to prove that the continuous system $x' = \theta \,\&\, H$ will never leave it. If, for instance, the formula $H \to F$ is valid (i.e., the region F is contained in the evolution domain region H), then $[x' = \theta \,\&\, H]F$ is valid trivially. This reasoning alone rarely helps, because F will not be contained in H in the interesting cases.

Differential Dynamic Logic (Excerpt) The modal logical principle described above can be extended to a full dynamic logic for hybrid systems [Pla08, Pla10a]. Here we only need propositional operators and modalities for differential equations. For our purposes, it is sufficient to consider the fragment with the following grammar (where F, H are formulas of (quantifier-free) first-order real arithmetic, x is a vector of variables and θ a vector of terms of the same dimension):

$$\phi, \psi \;::=\; F \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \to \psi \mid \phi \leftrightarrow \psi \mid [x' = \theta \,\&\, H]F$$

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 time $\zeta \in [0,r]$:

$$\frac{\mathsf{d}\,\varphi(t)[\![x_i]\!]}{\mathsf{d}t}(\zeta) = \varphi(\zeta)[\![\theta_i]\!]$$

   in particular, $\varphi(t)[\![x_i]\!]$ has to be differentiable at ζ as a function of t

2. and the evolution domain is always respected, i.e., $\varphi(\zeta) \models H$ for each $\zeta \in [0,r]$.

Other details about the logic, its semantics, and proof rules that are not of immediate concern here can be found in [Pla08, Pla10a, Pla10b]. We do not need to consider the full logic and full proof calculus here, because both are strictly compositional. The other proof rules deal with handling other features like discrete dynamics, sequential compositions, nondeterministic choices, and loops. For our purposes, it is sufficient to assume a decision procedure for first-order logic of real-closed fields [Tar51] and a propositionally complete base calculus. For simplicity, we also allow standard cuts just to have a simple way of glueing multiple proofs together. In the sequel, we denote the use of instances of valid tautologies of first-order real arithmetic in proofs by $\mathbb{R}$. For reference, these background proof rules are summarized in Appendix A.

Solutions as Explicit Witnesses An explicit witness for the validity of a logical formula like $F \to [x' = \theta \,\&\, H]F$ would be a solution of the differential equation for which we can prove that, when starting in a state that satisfies F, formula F holds all along the solution of $x' = \theta$ as long as formula H holds. If we happen to know a (unique) solution $X(t) = f(t, x_0)$ of the differential equation $x' = \theta$ with a function $f(t, x_0)$ of time t and the initial state x_0, then we have the following sound rule

$$\frac{F \to \forall r \Big(r \geq 0 \land \forall \zeta \Big(0 \leq \zeta \leq r \to H_x^{f(\zeta,x)} \Big) \to F_x^{f(r,x)} \Big)}{F \to [x' = \theta \,\&\, H]F}$$

where $F_x^{f(r,x)}$ is the result of applying to F the substitution that replaces the variable x by $f(r,x)$ and similarly for $H_x^{f(\zeta,x)}$. It is very easy to see why this rule is sound [Pla08], because it directly follows the semantics. The problem is that it is usually not a good proof rule, because it is rarely effective. It only helps if we can effectively compute a (unique) solution $f(t, x_0)$, as a function of t and x_0, to the symbolic initial-value problem $x' = \theta, x(0) = x_0$ for a variable symbol x_0. Notice that conventional initial-value problems are numerical with concrete numbers $x_0 \in \mathbb{R}^n$ as initial values, not symbols [Wal98]. This is not enough for our purpose, because we need to prove that the formula holds for all states satisfying initial assumption F, which could be uncountably many. We can hardly solve uncountably many different initial-value problems to verify a system. Also, the rule only helps when the resulting arithmetic is computable and the formula with the (alternating) quantifiers $\forall r$ and $\forall \zeta$ in the premise can be decided. Even very simple linear differential equations like $x' = y, y' = -x$ have trigonometric functions as solutions, which gives undecidable arithmetic by a simple corollary to Gödel's incompleteness theorem [Göd31]. For most differential equations, the solutions cannot be computed effectively, fall outside decidable classes of arithmetic, or do not even exist in closed form.

Consequently, the semantic approach to proving properties of differential equations is not very informative for actual provability. We need to consider the problem from a proof-theoretic perspective and investigate syntactic proof rules that are computationally effective, because they lead to computable or decidable formulas and have computable side conditions. Coming up with computationally ineffective proof rules for differential equations would obviously be trivial, even if they are sound and complete. The right question to ask is how provability compares and aligns for different choices of sound and effective proof rules. This is what we address in this paper.

3 Differential Invariants & Differential Cuts

The most fundamental question about a differential equation for safety verification purposes is whether a formula F is an invariant, i.e., whether formula $F \to [x' = \theta \,\&\, H]F$ is valid (true in all states). At first sight, invariance questions may look like a somewhat special case (pre- and postcondition are the same F here), but they are really at the heart of the hybrid systems verification problem. All more complicated safety properties of hybrid systems reduce to a series of invariance questions using the proof calculus that we presented in previous work [Pla08, Pla10b]. For instance, formulas of the form $A \to [x' = \theta \,\&\, H]B$ can be derived using the usual variation

$$\frac{A \to F \quad F \to [x' = \theta \,\&\, H]F \quad F \to B}{A \to [x' = \theta \,\&\, H]B} \tag{1}$$

We will use this variation occasionally. Formally, this variation can be derived in proof calculi using standard propositional cuts and Gödel generalizations (validity of $G \to F$ implies validity of $[x' = \theta \,\&\, H]G \to [x' = \theta \,\&\, H]F$) [Pla08]. What we need to do to use (1) effectively is to find a good choice for the invariant F that makes $F \to [x' = \theta \,\&\, H]F$ valid. For this, we need to understand which formulas are good candidates for invariants.

Definition 1 (Invariant) *Formula F is called an* invariant *of the system $x' = \theta \,\&\, H$ if the formula $F \to [x' = \theta \,\&\, H]F$ is valid.*

Validity of formulas is a semantic concept. Thus, invariance is a semantic concept and neither decidable nor semidecidable. For verification purposes we need a computable approach.

One simple but computable proof rule is *differential weakening*:

$$(DW)\ \frac{H \to F}{F \to [x' = \theta \,\&\, H]F}$$

This rule is obviously sound, because the system $x' = \theta \,\&\, H$, by definition, can never leave H, hence, if H implies F, then F is an invariant, no matter what $x' = \theta$ does. Unfortunately, this simple proof rule cannot prove very interesting properties, because it only works when H is very informative. It can, however, be useful in combination with stronger proof rules (e.g., the differential cuts that we discuss later).

Differential Invariants As a proof rule for the central invariance properties of differential equations, we have identified the following rule, called *differential induction* [Pla10a, PC08]. It resembles induction for discrete loops but works for differential equations instead.

$$(DI)\ \frac{H \rightarrow {F'}^{\theta}_{x'}}{F \rightarrow [x' = \theta \,\&\, H]F}$$

This rule is a natural induction principle for differential equations. The difference compared to ordinary induction for discrete loops is that the evolution domain region H is assumed in the premise (because the continuous evolution is not allowed to leave its evolution domain region) and that the induction step uses the differential formula ${F'}^{\theta}_{x'}$ corresponding to the differential equation $x' = \theta$ instead of a statement that the loop body preserves the invariant. The formula ${F'}^{\theta}_{x'}$ intuitively captures that F is only getting more true when following the differential equation $x' = \theta$. Here F' is the conjunction of total derivations of all atomic formulas in F, and ${F'}^{\theta}_{x'}$ is the result of substituting the (vectorial) differential equation $x' = \theta$ into F':

$$F' \equiv \bigwedge_{(b \sim c) \in F} \left(\left(\sum_{i=1}^{n} \frac{\partial b}{\partial x_i} x_i' \right) \sim \left(\sum_{i=1}^{n} \frac{\partial c}{\partial x_i} x_i' \right) \right)$$

$$ {F'}^{\theta}_{x'} \equiv \bigwedge_{(b \sim c) \in F} \left(\left(\sum_{i=1}^{n} \frac{\partial b}{\partial x_i} \theta_i \right) \sim \left(\sum_{i=1}^{n} \frac{\partial c}{\partial x_i} \theta_i \right) \right)$$

The sums are over all atomic subformulas $b \sim c$ of F for any $\sim \in \{=, \geq, >, \leq, <\}$. We assume that formulas use dualities like $\neg(a \geq b) \equiv a < b$ to avoid negations; see [Pla10a] for a discussion of this and the $\neq$ operator. For a discussion why this definition of differential invariants gives a sound approach and many other attempts would be unsound, we refer to previous work [Pla10a, Pla10b]. In the interest of a self-contained presentation, the soundness proof is shown in Appendix B. A variable z of F that is not in the vector x does not change during the continuous evolution, so we assume $z' = 0$ and replace z' by 0 when forming ${F'}^{\theta}_{x'}$.

The basic idea is that the premise of DI shows that the total derivative F' holds within evolution domain H when substituting the differential equations $x' = \theta$ into F'. If F holds initially (antecedent of conclusion), then F itself stays true (succedent of conclusion). Intuitively, the premise gives a condition showing that, within H, the total derivative F' along the differential constraints is pointing inwards or transversally to F but never outwards to $\neg F$; see Figure 2. Hence, if we start in F and, as indicated by F', the local dynamics never points outside F, then the system always stays in F when following the dynamics. Observe that, unlike F', the premise of DI is a well-formed formula, because all differential expressions are replaced by non-differential terms when forming ${F'}^{\theta}_{x'}$. It is possible to give a meaning also to the differential formula F' itself in differential states [Pla10a], but this is not relevant for the questions we address in this paper.

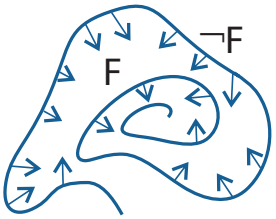

Figure 2: Differential invariant F

The formula F in rule DI is called *differential invariant*.

Definition 2 (Differential invariant) *The (quantifier-free) formula F of first-order real arithmetic is a* differential invariant *of the system $x' = \theta \,\&\, H$ if rule DI proves $F \rightarrow [x' = \theta \,\&\, H]F$ (because the premise is provable).*

We have proven that proof rule DI is sound, i.e., every provable formula is valid, hence, every differential invariant is an invariant [Pla10a, PC08]; also see Appendix B. 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 intractable semantics with a computationally effective, algebraic, syntactic total derivative along with mere substitution of differential equations.

Note that, because $F^{\theta}_{x'}$ is defined by a simple differential algebraic computation, which can be performed symbolically, it is decidable whether F is a differential invariant of a system $x' = \theta \,\&\, H$ based on the decidability of first-order real arithmetic [Tar51]. Furthermore, because differential equations are simpler than their solutions (which is part of the representational power of differential equations) and differential invariants are defined by differentiation (unlike solutions which are ultimately defined by integration), the differential induction rule DI is computationally attractive.

The big advantage of rule DI is that it can be used to prove properties of differential equations without having to know their solution (solutions may fall outside decidable classes of arithmetic, may not be computable, or may not even exist in closed form). A differential invariant F is an implicit proof certificate for the validity of $F \rightarrow [x' = \theta \,\&\, H]F$, because it establishes the same truth by a formal proof but does not need an explicit closed-form solution. **Example** The rotational dynamics $x' = y, y' = -x$ is complicated in that the solution involves trigonometric functions, which are generally outside decidable classes of arithmetic. Yet, we can easily prove interesting properties about it using DI and decidable polynomial arithmetic. For instance, we can prove the simple property that $x^2 + y^2 \geq p^2$ is a differential invariant of the dynamics using the following formal proof:

$$\mathbb{R}\,\frac{*}{\dfrac{2xy + 2y(-x) \geq 0}{\dfrac{(2xx' + 2yy' \geq 0)^{y\ -x}_{x'\ y'}}{DI\ x^2 + y^2 \geq p^2 \rightarrow [x' = y, y' = -x]x^2 + y^2 \geq p^2}}}$$

Differential invariant proofs of more involved properties of rotational and curved flight dynamics can be found in previous work [Pla10b].

Example Consider the dynamics $x' = y, y' = -\omega^2 x - 2d\omega y$ of the damped oscillator with the undamped angular frequency ω and the damping ratio d. General symbolic solutions of symbolic initial-value problems for this differential equation can become surprisingly difficult. Mathematica, for instance, produces a 6 line equation of exponentials. A differential invariant proof, instead, is very simple:

$$\mathbb{R}\,\frac{*}{\dfrac{\omega \geq 0 \wedge d \geq 0 \rightarrow 2\omega^2 xy - 2\omega^2 xy - 4d\omega y^2 \leq 0}{\dfrac{\omega \geq 0 \wedge d \geq 0 \rightarrow (2\omega^2 xx' + 2yy' \leq 0)^{y\ -\omega^2 x - 2d\omega y}_{x'\ y'}}{DI\ \omega^2 x^2 + y^2 \leq c^2 \rightarrow [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \wedge d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2}}}$$

Observe that rule DI directly makes the evolution domain constraint $\omega \geq 0 \wedge d \geq 0$ available as

an assumption in the premise, because the continuous evolution is never allowed to leave it. This is useful if we have a strong evolution domain constraint or can make it strong during the proof, which we consider in Sect. 7.

These are simple examples illustrating the power of differential invariants. Differential invariants make it possible to come up with very simple proofs even for tricky dynamics. Logical proofs with differential invariants have been the key enabling technique for the successful verification of case studies in air traffic, railway, automotive, and electrical circuit domains. Yet, if the original formula is not a differential invariant, one has to find the right differential invariant F like in (1), and, in particular, the search space for automatic procedures needs to include differential invariants of the right form. In this paper, we consider theoretical questions of how to trade-off deductive power with the size of the search space. We will answer the question which restrictions of differential invariants reduce the deductive power and which do not.

Because the premise of DI is in the (decidable) first-order theory of real arithmetic, it is obviously decidable whether a given formula F is a differential invariant of a given system $x' = \theta \,\&\, H$. For example, we can easily decide that $x^2 + y^2 \geq p^2$ is a differential invariant of the dynamics in Example 3 and that $\omega^2 x^2 + y^2 \leq c^2$ is a differential invariant of the dynamics in Example 3, just by deciding the resulting arithmetic in the proofs of those examples.

Similarly, when the user specifies a formula F with extra parameters $a_1, \ldots, a_n$, it is obviously decidable whether there is a choice for those parameters that makes F a differential invariant of a given system $x' = \theta \,\&\, H$. All we need to do to see why this is decidable, is to write appropriate quantifiers in front of the formulas; see [PC08, Pla10b] for formal details. This is a simple approach, but deceptively simple. If we choose the wrong template, it still will not work. Furthermore, the approach has a high computational complexity so that the choice of appropriate templates is crucial. For instance, a degree 2 template for Example 3 will result in a formula with 36 quantifiers. Quantifier elimination has doubly exponential lower bounds [DH88] and practical quantifier elimination implementations are doubly exponential in the number of variables. We, thus, need to understand the structure of the search space well to choose the right differential invariants or templates and avoid practically infinite computations that try to solve problems with the wrong templates.

Differential Cuts In the case of loops, invariants can be assumed to hold before the loop body in the induction step. It thus looks tempting to suspect that rule DI could be improved by assuming the differential invariant F in the antecedent of the premise:

$$(DI_{??})\ \frac{H \wedge F \rightarrow {F'}^{\theta}_{x'}}{F \rightarrow [x' = \theta \,\&\, H]F} \quad \text{sound?}$$

After all, we really only care about staying safe when we are still safe. But implicit properties of differential equations are a subtle business. Assuming F like in rule $DI_{??}$ would, in fact, be unsound, as the following simple counterexample shows, which "proves" an invalid property using

$DI_{??}$:

$$\dfrac{\dfrac{\dfrac{\qquad * \text{ (unsound)}}{-(x-y)^2 \geq 0 \rightarrow -2(x-y)(1-y) \geq 0}}{-(x-y)^2 \geq 0 \rightarrow (-2(x-y)(x'-y') \geq 0)^{1\ y}_{x'\ y'}}}{DI_{??}\ -(x-y)^2 \geq 0 \rightarrow [x'=1, y'=y](-(x-y)^2 \geq 0)} \tag{2}$$

Especially, it would be unsound to restrict the premise of DI to the border ∂F of F, which has often been suggested [PJ04, GT08]. The reason why some approaches try to add extra assumptions to the premise is that this would give more assumptions to prove the succedent from. Computationally, there is a trade-off, because ∂F may be computationally expensive to use (though computable to come up with for first-order real arithmetic F using quantifier elimination in real-closed fields [Tar51] with a large number of quantifiers). Yet, unsound ways of adding assumptions do not lead to reliable verification results anyhow, so we dismiss rule $DI_{??}$ and similar attempts.

We have come up with a complementary proof rule for *differential cuts* [Pla10a, PC08] that can be used to strengthen assumptions in a sound way:

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

It 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 appears to change the system dynamics but is a pseudo-restriction, because the left premise proves that C 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), 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 (see, e.g., the use of the evolution domain constraint in Example 3). In particular, the differential cut rule DC can be used to strengthen the right premise with more and more auxiliary differential invariants C that will be available as extra assumptions on the right premise, once they have been proven to be differential invariants in the left premise.

Using this differential cut process repeatedly has turned out to be extremely useful in practice and even simplifies the invariant search, because it leads to several simpler properties to find and prove instead of a single complex property [PC08, Pla10b]. But is it necessary in theory or just convenient in practice? Should we be searching for proofs without differential cuts or should we always conduct proof search including differential cuts? One central question that we answer in this paper is whether there is a differential cut elimination theorem showing that DC is admissible, or whether differential cuts are fundamental, because the addition of rule DC extends the deductive power of differential invariants (rule DI).

Prelude As a prelude to all subsequent (meta-)proofs, we ignore constant polynomials in differential invariants, because they do not contribute to the proof. For example, $5 \geq 0$ and $0 = 0$ are trivially true (do not contribute) and $0 \geq 1$ and $2 = 0$ are trivially false (not implied by any satisfiable precondition). We, thus, do not need to consider them for provability purposes, because

they do not constitute useful differential invariants. That is, whenever there is a proof using those trivial differential invariants, there also is a shorter proof not using them.

Furthermore, the subsequent proofs will go at an increasing pace. The first proofs will show elementary steps in detail, while subsequent proofs will proceed with a quicker pace and use the same elementary decompositions as previous proofs. One of the tricky parts in the proofs is coming up with the right counterexample to an inclusion or proving that there is none. The other tricky part is to show deductive power separation properties, i.e., that a valid formula cannot be proven using a given subset of the proof rules, which is a proof about infinitely many formal proofs.

This is similar to the fact that, in algebra, it is easier to prove that two structures are isomorphic than to prove that they are not. That they are isomorphic can be proven by constructing an isomorphism and proving that it satisfies all required properties. But proving that they are non-isomorphic requires a proof that *every* function between the two structures violates at least one of the properties of an isomorphism. Those proofs work by identifying a characteristic that is preserved by isomorphisms (e.g., dimension of vector spaces) but that the two structures under consideration do not agree on. We identify corresponding characteristics for the separation properties of deductive power.

4 Equivalences of Differential Invariants

First, we study whether there are equivalence transformations that preserve differential invariance. Every equivalence transformation that we have for differential invariant properties helps us with structuring the proof search space and also helps simplifying meta-proofs.

Lemma 1 (Differential invariants and propositional logic) *Differential invariants are invariant under propositional equivalences. That is, if $F \leftrightarrow G$ is an instance of a propositional tautology then F is a differential invariant of $x' = \theta \,\&\, H$ if and only if G is.*

Proof: Let F be a differential invariant of a differential equation system $x' = \theta \,\&\, H$ and let G be a formula such that $F \leftrightarrow G$ is an instance of a propositional tautology. Then G is a differential invariant of $x' = \theta \,\&\, H$, because of the following formal proof:

$$\dfrac{\dfrac{*}{H \rightarrow {G'}^{\theta}_{x'}}}{G \rightarrow [x' = \theta \,\&\, H]G}\,DI$$
$$F \rightarrow [x' = \theta \,\&\, H]F$$

The bottom proof step is easy to see using (1), because precondition F implies the new precondition G and postcondition F is implied by the new postcondition G. Subgoal $H \rightarrow {G'}^{\theta}_{x'}$ is provable, because $H \rightarrow {F'}^{\theta}_{x'}$ is provable and G' is defined as a conjunction over all literals of G. The set of literals of G is identical to the set of literals of F, because the literals do not change by using propositional tautologies. Furthermore, we assumed a propositionally complete base calculus (e.g., Appendix A). □

In subsequent proofs, we can use propositional equivalence transformations by Lemma 1. In the following, we will also implicitly use equivalence reasoning for pre- and postconditions as we have

done in Lemma 1. Because of Lemma 1, we can, without loss of generality, work with arbitrary propositional normal forms for proof search.

Unfortunately, not all logical equivalence transformations carry over to differential invariants. Differential invariance is not necessarily preserved under arithmetic equivalence transformations.

Example(DIFFERENTIAL INVARIANTS AND ARITHMETIC). Differential invariants are *not* invariant under equivalences of real arithmetic. There are two formulas that are equivalent over $\mathbb{R}$ but, for the same differential equation, one of them is a differential invariant, the other one is not (because their differential structures differ). Since $5 \geq 0$, the formula $x^2 \leq 5^2$ is equivalent to $-5 \leq x \wedge x \leq 5$ in first-order real arithmetic. Nevertheless, $x^2 \leq 5^2$ is a differential invariant of $x' = -x$ by the following formal proof:

$$\dfrac{\mathbb{R}\dfrac{*}{-2x^2 \leq 0}}{DI\dfrac{(2xx' \leq 0)^{-x}_{x'}}{x^2 \leq 5^2 \rightarrow [x' = -x]x^2 \leq 5^2}}$$

but $-5 \leq x \wedge x \leq 5$ is not a differential invariant of $x' = -x$:

$$\dfrac{\dfrac{\text{not valid}}{0 \leq -x \wedge -x \leq 0}}{DI\dfrac{(0 \leq x' \wedge x' \leq 0)^{-x}_{x'}}{-5 \leq x \wedge x \leq 5 \rightarrow [x' = -x](-5 \leq x \wedge x \leq 5)}}$$

Hence, when we want to prove the latter property, we need to use the principle (1) with the differential invariant $F \equiv x^2 \leq 5^2$.

Consequently, we cannot just use arbitrary equivalences when investigating differential invariance, but have to be more careful. The reason is that not just the *elementary equivalence* of having the same set of satisfying assignments matters, but even the differential structures need to be compatible.

Example 4 illustrates an important point about differential equations. Many different formulas characterize the same set of satisfying assignments. But not all of them have the same differential structure. Quadratic polynomials have inherently different differential structure than linear polynomials even when they have the same set of solutions over the reals. The differential structure is a more fine-grained information. This is similar to the fact that two elementary equivalent models of first-order logic can still be non-isomorphic. Both the set of satisfying assignments and the differential structure matter for differential invariance. In particular, there are many formulas with the same solutions but different differential structures. The formulas $x^2 \geq 0$ and $x^6 + x^4 - 16x^3 + 97x^2 - 252x + 262 \geq 0$ have the same solutions (all of $\mathbb{R}$), but very different differential structure; see Figure 3. The first two rows in Figure 3 correspond to the polynomials from the latter two cases. The third row is a structurally different degree 6 polynomial with again the same set of solutions ($\mathbb{R}$) but a rather different differential structure. The differential structure, of course, also depends on what value x' assumes according to the differential equation. But Figure 3 illustrates that p' alone can already have a very different characteristic even if the respective sets of satisfying assignments of $p \geq 0$ are identical.

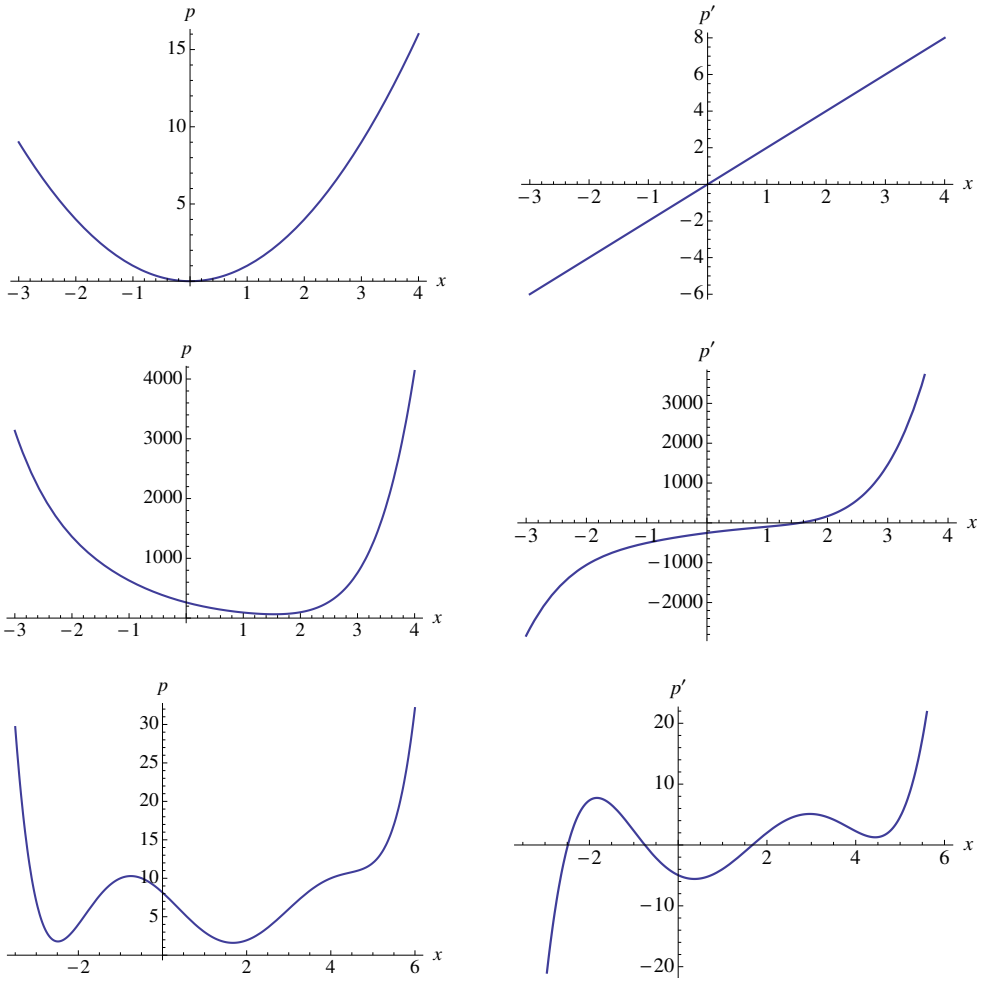

Figure 3: Equivalent solutions ($p \geq 0$ left) with different differential structure (p' plotted on the right)

We can, however, normalize all atomic subformulas to have right-hand side 0, that is, of the form $p = 0, p \geq 0$, or $p > 0$. For instance, $p \leq q$ is a differential invariant if and only if $q - p \geq 0$ is, because $p \leq q$ is equivalent (in first-order real arithmetic) to $q - p \geq 0$ and, moreover, for any variable x and term θ, $(p' \leq q')^{\theta}_{x'}$ is equivalent to $(q' - p' \geq 0)^{\theta}_{x'}$.

5 Relations of Differential Invariant Classes

We study the relations of classes of differential invariants in terms of their relative deductive power. As a basis, we consider a propositional sequent calculus with logical cuts (which simplify glueing derivations together) and real-closed field arithmetic (we denote all uses by proof rule $\mathbb{R}$); see Appendix A. By $\mathcal{DI}$ we denote the proof calculus that, in addition, has general differential invariants (rule DI with arbitrary quantifier-free first-order formula F) but no differential cuts (rule DC).

For a set $\Omega \subseteq \{\geq, >, =, \wedge, \vee\}$ of operators, we denote by $\mathcal{DI}_\Omega$ the proof calculus where the differential invariant F in rule DI is restricted to the set of formulas that uses only the operators in Ω. For example, $\mathcal{DI}_{=,\wedge,\vee}$ is the proof calculus that allows only and/or-combinations of equations to be used as differential invariants. Likewise, $\mathcal{DI}_{\geq}$ is the proof calculus that only allows atomic weak inequalities $p \geq q$ to be used as differential invariants.

We consider several classes of differential invariants and study their relations. If $\mathcal{A}$ and $\mathcal{B}$ are two classes of differential invariants, we write $\mathcal{A} \leq \mathcal{B}$ if all properties provable using differential invariants from $\mathcal{A}$ are also provable using differential invariants from $\mathcal{B}$. We write $\mathcal{A} \not\leq \mathcal{B}$ otherwise, i.e., when there is a valid property that can only be proven using differential invariants of $\mathcal{A} \setminus \mathcal{B}$. We write $\mathcal{A} \equiv \mathcal{B}$ if $\mathcal{A} \leq \mathcal{B}$ and $\mathcal{B} \leq \mathcal{A}$. We write $\mathcal{A} < \mathcal{B}$ if $\mathcal{A} \leq \mathcal{B}$ and $\mathcal{B} \not\leq \mathcal{A}$. Classes $\mathcal{A}$ and $\mathcal{B}$ are incomparable if $\mathcal{A} \not\leq \mathcal{B}$ and $\mathcal{B} \not\leq \mathcal{A}$. Our findings about classes of differential invariants are summarized in Figure 1 on p. 2. We prove these relations in the remainder of this section.

First we recall a simple result from previous work showing that propositional operators do not change the deductive power of differential invariants in the purely equational case. We have proven the following result in previous work; see [Pla10a, Proposition 1]. We repeat a variation of the proof here, because it is instructive to understand what we have to prove about the algebraic and differential structure of differential invariants.

Proposition 1 (Equational deductive power [Pla10a]) *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:*

$$\mathcal{DI}_{=} \equiv \mathcal{DI}_{=,\wedge,\vee}$$

Proof: Let $x' = \theta$ be the (vectorial) differential equation to consider. We show that every differential invariant that is a propositional combination F of polynomial equations is expressible as a single atomic polynomial equation (the converse inclusion is obvious). We can assume F to be in negation normal form by Lemma 1 (recall that negations are resolved and $\neq$ does not appear). Then we reduce F inductively to a single equation using the following transformations:

- If F is of the form $p_1 = p_2 \vee q_1 = q_2$, then F is equivalent to the single equation

  $$(p_1 - p_2)(q_1 - q_2) = 0$$

  Furthermore, ${F'}^{\theta}_{x'} \equiv (p_1' = p_2' \wedge q_1' = q_2')^{\theta}_{x'}$ directly implies

  $$\big(((p_1 - p_2)(q_1 - q_2))' = 0\big)^{\theta}_{x'} \equiv \big((p_1' - p_2')(q_1 - q_2) + (p_1 - p_2)(q_1' - q_2') = 0\big)^{\theta}_{x'}$$

- If F is of the form $p_1 = p_2 \wedge q_1 = q_2$, then F is equivalent to the single equation

  $$(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$$

  Furthermore, ${F'}^{\theta}_{x'} \equiv \big(p_1' = p_2' \wedge q_1' = q_2'\big)^{\theta}_{x'}$ implies

  $$\big(\ \big((p_1 - p_2)^2 + (q_1 - q_2)^2\big)' = 0\big)^{\theta}_{x'} \equiv \big(2(p_1 - p_2)(p_1' - p_2') + 2(q_1 - q_2)(q_1' - q_2') = 0\big)^{\theta}_{x'}$$

□

Note that the polynomial degree increases quadratically by the reduction in Proposition 1, but, as a trade-off, the propositional structure simplifies. Consequently, differential invariant search for the equational case can either exploit propositional structure with lower degree polynomials or suppress the propositional structure at the expense of higher degrees. Focusing exclusively on differential invariants with equations, however, reduces the deductive power. For instance, the approach by Sankaranarayanan et al. [SSM08] uses only equations and does not support inequalities.

Proposition 2 (Equational incompleteness) *The deductive power of differential induction with equational formulas is strictly less than the deductive power of general differential induction, because some inequalities cannot be proven with equations.*

$$\begin{aligned}\mathcal{DI}_{=} \equiv \mathcal{DI}_{=,\wedge,\vee} &< \mathcal{DI}\\ \mathcal{DI}_{\geq} &\not\leq \mathcal{DI}_{=} \equiv \mathcal{DI}_{=,\wedge,\vee}\\ \mathcal{DI}_{>} &\not\leq \mathcal{DI}_{=} \equiv \mathcal{DI}_{=,\wedge,\vee}\end{aligned}$$

Proof: Consider any term $a > 0$ (e.g., 5 or $x^2 + 1$ or $x^2 + x^4 + 2$). The following formula is provable by differential induction with the weak inequality $x \geq 0$:

$$\mathbb{R}\frac{*}{\overset{DI}{\dfrac{a \geq 0}{x \geq 0 \rightarrow [x' = a]x \geq 0}}}$$

It is not provable with an equational differential invariant. An invariant of the form $p = 0$ has (Lebesgue-)measure zero (except when p is the 0 polynomial, where $p = 0$ is trivially equivalent to $true$ and then useless for a proof, because it provides no interesting information) and, thus, cannot describe the region $x \geq 0$ of non-zero (Lebesgue-)measure, in which the system starts (precondition) and stays (postcondition). More formally, any (univariate) polynomial p that is zero on $x \geq 0$ is the zero polynomial and, thus, $p = 0$ cannot be equivalent to the half space $x \geq 0$. By the equational deductive power theorem, the formula then is not provable with any boolean combination of equations as differential invariant either. Similarly, the following formula is provable by differential induction with a strict inequality $x > 0$, but, for the same reason of different measures (respectively infinitely many zeros), not provable by an invariant of the form $p = 0$:

$$\mathbb{R}\frac{*}{\overset{DI}{\dfrac{a > 0}{x > 0 \rightarrow [x' = a]x > 0}}}$$

□

It might be tempting to think that at least equational postconditions (like those considered in [SSM08]) only need equational differential invariants for proving them. But that is not the case either. We show that there are even purely equational invariants that are only provable using inequalities, but not when using only equations as differential invariants.

Proposition 3 (No equational closure) *There is an equational invariant of a differential equation that is only provable using an inequality as a differential invariant, but not using equational propositional logic for differential invariants. This equational invariant is not even provable using equational propositional logic and differential cuts.*

Proof: The formula $x = 0 \rightarrow [x' = -x]x = 0$ is provable using $x^2 \leq 0$ as a differential invariant by the following simple formal proof:

$$\dfrac{\mathbb{R}\dfrac{*}{-2x^2 \leq 0}}{DI\dfrac{(2xx' \leq 0)^{-x}_{x'}}{x^2 \leq 0 \rightarrow [x' = -x]x^2 \leq 0}}$$

We need to show that this formula cannot be proven using equations as differential invariants. Suppose there was a differential invariant of the form $p = 0$ for a univariate polynomial p of the form $\sum_{i=0}^{n} a_i x^i$ in the only occurring variable x. Then

1. $\vDash p = 0 \leftrightarrow x = 0$, and
2. $\vDash {p'}^{-x}_{x'} = 0$, where

$$ {p'}^{-x}_{x'} = \left(\sum_{i=1}^{n} i a_i x^{i-1} x' \right)^{-x}_{x'} = -\sum_{i=1}^{n} i a_i x^i $$

From item 2, we obtain that $a_1 = a_2 = \cdots = a_0 = 0$ by comparing coefficients. Consequently, p must be the constant polynomial a_0, not involving x. Thus, the formula $p = 0$ is either trivially equivalent to $true$ (then it does not contribute to the proof) or equivalent to $false$ (then it is no consequence of the precondition). Thus the only equational invariants of $x = 0 \rightarrow [x' = -x]x = 0$ are trivial (equivalent to $true$ or to $false$). Consequently, that formula cannot be provable by an equational invariant, nor by a propositional combination of equations (because of Proposition 1). This result still holds in the presence of differential cuts. As above, differential cuts can only strengthen with trivial equational formulas that do not contain x, are equivalent to $true$ (and then do not contribute to the proof), or equivalent to $false$ (and then are not implied by the precondition). □

We show that, conversely, focusing on strict inequalities also reduces the deductive power, because equations are obviously missing and there is at least one proof where this matters. That is, strict barrier certificates do not prove (nontrivial) closed invariants.

Proposition 4 (Strict barrier incompleteness) *The deductive power of differential induction with strict barrier certificates (formulas of the form $p > 0$) is strictly less than the deductive power of general differential induction.*

$$\mathcal{DI}_{>} < \mathcal{DI}$$
$$\mathcal{DI}_{=} \not\leq \mathcal{DI}_{>}$$

Proof: The following formula is provable by equational differential induction:

$$\mathbb{R}\dfrac{*}{{}^{DI}\dfrac{2xy+2y(-x)=0}{x^2+y^2=c^2\rightarrow[x'=y,y'=-x]x^2+y^2=c^2}}$$

But it is not provable with a differential invariant of the form $p>0$. An invariant of the form $p>0$ describes an open set and, thus, cannot be equivalent to the (nontrivial) closed domain where $x^2+y^2=c^2$. The only sets that are both open and closed in $\mathbb{R}^2$ are $\emptyset$ and $\mathbb{R}^2$. □

Weak inequalities, however, do subsume the deductive power of equational differential invariants. This is obvious on the algebraic level but we will see that it also does carry over to the differential structure.

Proposition 5 (Equational definability) *The deductive power of differential induction with equations is subsumed by the deductive power of differential induction with weak inequalities:*

$$\mathcal{DI}_{=,\wedge,\vee}\leq\mathcal{DI}_{\geq}$$

Proof: By Proposition 1, we only need to show that $\mathcal{DI}_{=}\leq\mathcal{DI}_{\geq}$. Let $p=0$ be an equational differential invariant of a differential equation $x'=\theta\,\&\,H$. Then we can prove the following:

$$\dfrac{*}{{}^{DI}\dfrac{H\rightarrow(p'=0)^{\theta}_{x'}}{p=0\rightarrow[x'=\theta\,\&\,H]p=0}}$$

Then, the inequality $p^2\leq 0$, which is equivalent to $p=0$ in real arithmetic, also is a differential invariant of the same dynamics by the following formal proof:

$$\dfrac{*}{{}^{DI}\dfrac{H\rightarrow(2pp'\leq 0)^{\theta}_{x'}}{p^2\leq 0\rightarrow[x'=\theta\,\&\,H]p^2\leq 0}}$$

The subgoal for the differential induction step is provable: if we can prove that H implies $(p'=0)^{\theta}_{x'}$, then we can also prove that H implies $(2pp'\leq 0)^{\theta}_{x'}$, because $(p'=0)^{\theta}_{x'}$ implies $(2pp'\leq 0)^{\theta}_{x'}$. □
Note that the local state-based view of differential invariants is crucial to make the last proof work. Also note that the polynomial degree increases quadratically with the reduction in Proposition 5. In particular, the polynomial degree even increases quartically when using the reductions in Proposition 1 and Proposition 5 one after another to turn propositional equational formulas into single inequalities. This quartic increase of the polynomial degree is likely a too serious computational burden for practical purposes even if it is a valid reduction in theory.

When using propositional connectives and inequalities, the reduction is less counterproductive for the polynomial degree. The following result is an immediate corollary to Proposition 5 but of independent interest. We give a direct proof that shows a more natural reduction that does not increase the polynomial degree.

Corollary 1 (Atomic equational definability) *The deductive power of differential induction with atomic equations is subsumed by the deductive power of differential induction with formulas with weak inequalities.*

$$\mathcal{DI}_{=} \leq \mathcal{DI}_{\geq,\wedge,\vee}$$

Proof: Consider an atomic equational differential invariant of a differential equation system $x' = \theta \,\&\, H$. We can assume this atomic equational differential invariant to be of the form $p = 0$. If $p = 0$ is a differential invariant, then we can show that the formula $p \geq 0 \wedge p \leq 0$ also is a differential invariant by the following formal proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{H \rightarrow (p' = 0)^{\theta}_{x'}}}{H \rightarrow (p' \geq 0 \wedge p' \leq 0)^{\theta}_{x'}}}{p \geq 0 \wedge p \leq 0 \rightarrow [x' = \theta \,\&\, H](p \geq 0 \wedge p \leq 0)}\,{}^{DI}}{p = 0 \rightarrow [x' = \theta \,\&\, H]p = 0}$$

□

The same natural reduction works to show the inclusion $\mathcal{DI}_{=,\wedge,\vee} \leq \mathcal{DI}_{\geq,\wedge,\vee}$ without a penalty for the polynomial degree. Again, the local state-based view of differential invariants is helpful for this proof.

Now we see that, with the notable exception of pure equations (Proposition 1), propositional operators (which have been considered in [Pla10a, PC08] and for some cases also in [GT08] but not in [SSM08, PJ04, PJP07]) increase the deductive power.

Proposition 6 (Atomic incompleteness) *The deductive power of differential induction with propositional combinations of inequalities exceeds the deductive power of differential induction with atomic inequalities.*

$$\mathcal{DI}_{\geq} < \mathcal{DI}_{\geq,\wedge,\vee}$$
$$\mathcal{DI}_{>} < \mathcal{DI}_{>,\wedge,\vee}$$

Proof: Consider any term $a \geq 0$ (e.g., 1 or $x^2 + 1$ or $x^2 + x^4 + 1$ or $(x - y)^2 + 2$). Then the formula $x \geq 0 \wedge y \geq 0 \rightarrow [x' = a, y' = y^2](x \geq 0 \wedge y \geq 0)$ is provable using a conjunction in the differential invariant:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{a \geq 0 \wedge y^2 \geq 0}\,\mathbb{R}}{(x' \geq 0 \wedge y' \geq 0)^{a\ y^2}_{x'\ y'}}}{x \geq 0 \wedge y \geq 0 \rightarrow [x' = a, y' = y^2](x \geq 0 \wedge y \geq 0)}\,{}^{DI}$$

By a sign argument similar to that in the proof of [Pla10a, Theorem 2] no atomic formula is equivalent to $x \geq 0 \wedge y \geq 0$. Thus, the above property cannot be proven using a single differential induction. The proof for a postcondition $x > 0 \wedge y > 0$ is similar. □

Note that the formula in the proof of Proposition 6 would be provable, e.g., using differential cuts with two atomic differential induction steps, one for $x \geq 0$ and one for $y \geq 0$. Yet, a similar

argument can be made to show that the deductive power of differential induction with atomic formulas (even when using differential cuts) is strictly less than the deductive power of general differential induction; see previous work [Pla10a, Theorem 2].

Next, we show that differential induction with strict inequalities is incomparable with differential induction with weak inequalities. In particular, strict and weak barrier certificates are incomparable [PJ04, PJP07].

Proposition 7 (Elementary incomparability) *The deductive power of differential induction with strict inequalities is incomparable to the deductive power of differential induction with weak inequalities.*

$$\begin{array}{l} \mathcal{DI}_{>} \not\leq \mathcal{DI}_{\geq,\wedge,\vee} \quad \textit{even } \mathcal{DI}_{>} \not\leq \mathcal{DI}_{\geq,=,\wedge,\vee} \\ \mathcal{DI}_{\geq} \not\leq \mathcal{DI}_{>,\wedge,\vee} \\ \mathcal{DI}_{=} \not\leq \mathcal{DI}_{>,\wedge,\vee} \end{array}$$

Proof: Consider any term $a > 0$ (e.g., 5 or $x^2 + 1$ or $x^2 + x^4 + 5$). The following formula is provable with an atomic differential invariant with a strict inequality:

$$\mathbb{R}\frac{*}{\dfrac{a > 0}{x > 0 \rightarrow [x' = a]x > 0}\,DI}$$

But it is not provable with any conjunctive/disjunctive combination of weak inequalities $p_i \geq 0$. The reason is that the formula $x > 0$ describes a nontrivial open set, which cannot be equivalent to a boolean formula that is a combination of conjunctions, disjunctions and weak inequalities $p_i \geq 0$, because finite unions and intersections of closed sets are closed. Similarly, the above formula is not provable in $\mathcal{DI}_{\geq,=,\wedge,\vee}$, which describe closed regions.

Conversely, the following formula is provable with an atomic differential invariant with a weak inequality:

$$\mathbb{R}\frac{*}{\dfrac{a \geq 0}{x \geq 0 \rightarrow [x' = a]x \geq 0}\,DI}$$

But it is not provable with any conjunctive/disjunctive combination of strict inequalities $p_i > 0$. The reason is that the formula $x \geq 0$ describes a nontrivial closed set, which cannot be equivalent to a boolean formula that is a combination of conjunctions, disjunctions and strict inequalities $p_i > 0$, because unions and finite intersections of open sets are open.

Similarly, it is easy to see that $\mathcal{DI}_{=} \not\leq \mathcal{DI}_{>,\wedge,\vee}$. By the proof of Proposition 4, the formula $x^2 + y^2 = c^2 \rightarrow [x' = y, y' = -x]x^2 + y^2 = c^2$ is provable in $\mathcal{DI}_{=}$. The formula $x^2 + y^2 = c^2$ describes a nontrivial closed set, which, again, cannot be equivalent to any conjunctive/disjunctive combination of strict inequalities $p_i > 0$, which would describe an open set. □

Corollary 2 *We obtain simple consequences:*

$$\begin{aligned}\mathcal{DI}_{\geq,=,\wedge,\vee} &\not\leq \mathcal{DI}_{\geq,>,=,\wedge,\vee}\\ \mathcal{DI}_{=,\wedge,\vee} &\not\leq \mathcal{DI}_{>,\wedge,\vee}\\ \mathcal{DI}_{>,\wedge,\vee} &\not\leq \mathcal{DI}_{=,\wedge,\vee}\end{aligned}$$

Proof: The property $\mathcal{DI}_{\geq,=,\wedge,\vee} \not\leq \mathcal{DI}_{\geq,>,=,\wedge,\vee}$ follows from the proof for $\mathcal{DI}_{\geq} \not\leq \mathcal{DI}_{>,\wedge,\vee}$, because conjunctive/disjunctive combinations of weak inequalities and equations are closed, but the region where $x > 0$ is open.

The separation of $\mathcal{DI}_{=,\wedge,\vee}$ and $\mathcal{DI}_{>,\wedge,\vee}$ is a consequence of the facts $\mathcal{DI}_{=} \not\leq \mathcal{DI}_{>,\wedge,\vee}$ and $\mathcal{DI}_{>} \not\leq \mathcal{DI}_{\geq,\wedge,\vee}$, because $\mathcal{DI}_{\geq} \geq \mathcal{DI}_{=,\wedge,\vee}$ by Proposition 5 and $\mathcal{DI}_{=,\wedge,\vee}$ describes closed sets yet $\mathcal{DI}_{>,\wedge,\vee}$ describes open sets. □

Hence, strict inequalities are a necessary ingredient to retain full deductive power. The operator basis $\{\geq, =, \wedge, \vee\}$ is not sufficient. What about weak inequalities? Do we need those? The operator basis $\{>, \wedge, \vee\}$ is not sufficient by Proposition 7, but what about $\{>, =, \wedge, \vee\}$? Algebraically, this would be sufficient, because all semialgebraic sets can be defined with polynomials using the operators $\{>, =, \wedge, \vee\}$. We show that, nevertheless, differential induction with weak inequalities is not subsumed by differential induction with all other operators. Weak inequalities are thus an inherent ingredient. In particular, the subsets of operators that have been considered in related work [SSM08, PJ04, PJP07] are not sufficient.

Theorem 1 (Necessity of full operator basis) *The deductive power of differential induction with propositional combinations of strict inequalities and equations is strictly less than the deductive power of general differential induction.*

$$\begin{aligned}\mathcal{DI}_{>,=,\wedge,\vee} &< \mathcal{DI}_{\geq,>,=,\wedge,\vee}\\ \mathcal{DI}_{\geq} &\not\leq \mathcal{DI}_{>,=,\wedge,\vee}\end{aligned}$$

Proof: The following simple formula is provable with a weak inequality as a differential invariant:

$$\dfrac{\mathbb{R}\dfrac{*}{1 \geq 0}}{DI\, x \geq 0 \rightarrow [x' = 1]x \geq 0}$$

Suppose F is a propositional formula of strict inequalities and equations that is a differential invariant proving the above formula. Then F is equivalent to $x \geq 0$, which describes a closed region with a nonempty interior. Consequently, F must have an atom of the form $p > 0$ (otherwise the region has an empty interior or is trivially true and then useless) and an atom of the form $q = 0$ (otherwise the region is not closed). We can assume q to have a polynomial of degree ≥ 1 (otherwise the region is not closed if F only has trivially true equations $0 = 0$ or trivially false equations like $5 = 0$). A necessary condition for F to be a differential invariant of $x' = 1$ thus is that

$$\vDash (p' > 0 \wedge q' = 0)^1_{x'} \tag{3}$$

because all atoms need to satisfy the differential invariance condition. Now, q is of the form $\sum_{i=0}^{n} a_i x^i$ for some $n, a_0, \ldots, a_n$. Thus, $q' = \sum_{i=1}^{n} i a_i x^{i-1} x'$ and $q'^1_{x'} = \sum_{i=1}^{n} i a_i x^{i-1}$. Consequently, (3) implies that

$$\vDash \sum_{i=1}^{n} i a_i x^{i-1} = 0$$

If this formula is valid (true under all interpretations for x), then we must have $n \leq 1$. Otherwise if x occurs ($n > 1$), the above polynomial would not always evaluate to zero. Consequently q is of the form $a_0 + a_1 x$. Hence, $(q')^1_{x'} = a_1$. Again the validity (3) implies that a_1 must be zero. This contradicts the fact that q has degree ≥ 1. □

This finishes the study of the relations of classes of differential invariants that we summarize in Figure 1 on p. 2. The other relations are obvious transitive consequences of the ones summarized in Figure 1.

6 Auxiliary Differential Variable Power

After having studied the relationships of several classes of differential invariants, we now turn to extensions of differential induction. First, we consider auxiliary differential variables, and show that some properties can only be proven after introducing auxiliary differential variables into the dynamics. That is, the addition of auxiliary differential variables increases the deductive power of differential induction. Similar phenomena also hold for classical discrete systems. Up to now, it was unknown whether similar differences exist for the continuous dynamics of differential equations. In particular, auxiliary differential variables have not been considered in related work before. We present the following new proof rule DA for introducing auxiliary differential variables:

$$(DA)\ \frac{\phi \leftrightarrow \exists y\, \psi \quad \psi \rightarrow [x' = \theta, y' = \vartheta \,\&\, H]\psi}{\phi \rightarrow [x' = \theta \,\&\, H]\phi}$$

Rule DA is applicable if y is a new variable and the new differential equation $y' = \vartheta$ has global solutions (e.g., because term ϑ satisfies a Lipschitz condition, which is definable in first-order real arithmetic and thus decidable). Without that condition, adding $y' = \vartheta$ could limit the duration of system evolutions incorrectly. Soundness is easy to see, because precondition ϕ implies ψ for some choice of y (left premise). Yet, for any y, ψ is an invariant of the extended dynamics (right premise). Thus, ψ holds after the evolution for some y, which implies ϕ (left premise). Since y is fresh and its differential equation does not limit the duration of solutions, this implies the conclusion. Note that y is fresh and does not occur in H, and, thus, its solution does not leave H, which may incorrectly restrict the duration of the evolution.

Let $\mathcal{DCI}$ be the proof calculus with (unrestricted) differential induction (like $\mathcal{DI}$) plus differential cuts (rule DC).

Theorem 2 (Auxiliary differential variable power) *The deductive power of $\mathcal{DCI}$ with auxiliary differential variables (DA) exceeds the deductive power of $\mathcal{DCI}$ without auxiliary differential variables.*

Proof: We show that the formula

$$x > 0 \rightarrow [x' = -x]x > 0 \tag{4}$$

is provable in $\mathcal{DCI}$ with auxiliary differential variables (rule DA), but not provable without using auxiliary differential variables.

We first show that (4) is provable with auxiliary differential variables (variables that are added and do not affect other formulas or dynamics) using rule DA (and DI):

$$\dfrac{\mathbb{R}\dfrac{*}{x > 0 \leftrightarrow \exists y\, xy^2 = 1} \qquad {}^{DI}\dfrac{\mathbb{R}\dfrac{*}{-xy^2 + 2xy\frac{y}{2} = 0}}{(x'y^2 + x2yy' = 0)^{-x\ \frac{y}{2}}_{x'\ \ y'}}}{xy^2 = 1 \rightarrow [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \rightarrow [x' = -x]x > 0}\,{}^{DA}$$

In the remainder of the proof, we show that (4) is not provable without auxiliary differential variables like y. We suppose there was a proof without DA, which we assume cannot be made shorter (in the number of proof steps and the size of the formulas involved). Note that for any non-constant univariate polynomial p in the variable x, the limits at $\pm\infty$ exist and are $\pm\infty$, i.e.

$$\lim_{x\to-\infty} p(x) \in \{-\infty, \infty\} \text{ and } \lim_{x\to\infty} p(x) \in \{-\infty, \infty\} \tag{5}$$

For constant polynomials, the limits at $\pm\infty$ exist, are finite, and identical.

Suppose (4) were provable by a differential invariant of the form $p(x) > 0$ for a polynomial p in the only occurring variable x. Then $\vDash p(x) > 0 \leftrightarrow x > 0$. Hence $p(x)$ is not a constant polynomial and $p(x) \leq 0$ when $x \leq 0$ and $p(x) \geq 0$ when $x \geq 0$ by continuity. Thus, from (5) we conclude

$$\lim_{x\to-\infty} p(x) = -\infty \quad \text{and} \quad \lim_{x\to\infty} p(x) = \infty$$

In particular, $p(x)$ has the following property, which is equivalent to $p(x)$ having odd degree:

$$\lim_{x\to-\infty} p(x) \neq \lim_{x\to\infty} p(x) \tag{6}$$

Consequently, the degree of p is odd and the leading (highest-degree) term is of the form $c_{2n+1}x^{2n+1}$ for an $n \in \mathbb{N}$ and a number $c_{2n+1} \in \mathbb{R} \setminus \{0\}$. Since $p(x) > 0$ was assumed to be a differential invariant of $x' = -x$, the differential invariance condition $\vDash (p' > 0)^{-x}_{x'}$ holds. Abbreviate the polynomial $p'^{-x}_{x'}$ by $q(x)$. The leading term of p' is $(2n+1)c_{2n+1}x^{2n}x'$. Consequently, the leading term of $q(x)$ is $-(2n+1)c_{2n+1}x^{2n+1}$, hence of odd degree. Thus $q(x)$ also has the property (6), which contradicts the fact that the differential invariance condition $(p' > 0)^{-x}_{x'}$, i.e., $q(x) > 0$ needs to hold for all $x \in \mathbb{R}$.

Our proof where we suppose that (4) were provable by a differential invariant of the form $p(x) \geq 0$ for a polynomial p in the only occurring variable x, and show that this is impossible, is

similar, because $p(x)$ then also enjoys property (6). Again, a constant polynomial $p(x)$ does not satisfy the requirement $\vDash p(x) \geq 0 \leftrightarrow x > 0$.

Suppose (4) were provable by a differential invariant of the form $p(x) = 0$ for a polynomial p in the only occurring variable x. Then $p(x) = 0$ must be a consequence of the precondition $x > 0$. Thus, the polynomial p is zero at infinitely many points, which implies that this *univariate* polynomial is the zero polynomial. But $0 = 0$ is trivially true and there would be a shorter proof without this useless invariant. Consequently no single atomic formula can be a differential invariant proving (4).

Without differential cuts and DA, (4) is, thus, not provable. Next, suppose (4) was provable by differential cuts subsequently with differential invariants $F_1, F_2, \ldots, F_n$, where each F_i is a logical formula in the only occurring variable x. Then

1. $\vDash x > 0 \rightarrow F_i$ for each i (precondition implies each differential invariant), and
2. $\vDash F_1 \wedge \cdots \wedge F_n \rightarrow x > 0$ (finally implies postcondition), and
3. the respective differential induction step conditions hold.

We abbreviate the conjunction $F_1 \wedge \cdots \wedge F_i$ of the first i invariants by $F_{\leq i}$. Then conditions 1 and 2 imply $\vDash F_{\leq n} \leftrightarrow x > 0$.

By condition 2, the region described by $F_{\leq n}$ does not include $-\infty$ (more precisely, this means $-\infty \neq \inf\{x : x \vDash F_{\leq n}\}$). Hence, there is a smallest i such that the region described by $F_{\leq i}$ does not include $-\infty$ but $F_{\leq i-1}$ still includes $-\infty$.

Then this F_i must have an atomic subformula that distinguishes ∞ from $-\infty$ (otherwise $F_{\leq i}$ would have the same truth values for ∞ and $-\infty$, and $F_{\leq i}$ would still include $-\infty$, because, by condition 1, all F_i regions include ∞). This atomic subformula has the form $p(x) > 0$ or $p(x) \geq 0$ or $p(x) = 0$ with a univariate polynomial $p(x)$. It is easy to see why all univariate polynomial equations $p(x) = 0$ evaluate to false at both $-\infty$ and ∞, because of property (5). Hence, the atomic subformula has the form $p(x) > 0$ or $p(x) \geq 0$ and the univariate polynomial $p(x)$ has to satisfy property (6), because $p(x) > 0$ or $p(x) \geq 0$ is assumed to distinguish $-\infty$ and ∞. Since the previous domain $F_{\leq i-1}$ still includes $-\infty$ and ∞, the same argument as before leads to a contradiction. In detail. By property (6), $p(x)$ has an odd degree. Since $p(x) \geq 0$ or $p(x) > 0$ was assumed to satisfy the differential invariance condition for $x' = -c \,\&\, F_{\leq i-1}$, it at least satisfies $(p' \geq 0)^{-x}_{x'}$ on the evolution domain $F_{\leq i-1}$. Because $p(x)$ has odd degree, p' has even degree and the polynomial ${p'}^{-x}_{x'}$, which we abbreviate by $q(x)$, again has odd degree. Thus $q(x)$ has the property (6), which contradicts the fact that the differential invariance condition $(p' \geq 0)^{-x}_{x'}$, i.e., $q(x) \geq 0$ needs to hold for all x satisfying $F_{\leq i-1}$, hence, at least for $-\infty$ and ∞. □

Note that the same proof can also be used to show that $x > 0 \rightarrow [x' = x]x > 0$ cannot be proven by differential induction and differential cuts without auxiliary differential variables (similarly for other $x' = ax$ with a number $a \in \mathbb{R} \setminus \{0\}$). It is not a barrier certificate [PJP07] either. Further, the nontrivial open region $x > 0$ cannot be equivalent to the closed region of a barrier certificate $p \leq 0$. Yet, we do not use formula $x > 0 \rightarrow [x' = x]x > 0$ in the proof of Theorem 2, because it is still provable with what is called *open* differential induction ($\mathcal{DI}^\circ$), where it is sound

to assume the differential invariant in the differential induction step if the differential invariant $F \equiv x > 0$ is open [Pla10a]:

$$\mathbb{R}\,\frac{*}{\dfrac{x>0 \to (x'>0)^{x}_{x'}}{x>0 \to [x'=x]x>0}\,DI^\circ} \qquad \text{by} \quad (DI^\circ)\,\frac{H \wedge F \to F'^{\theta}_{x'}}{F \to [x'=\theta\,\&\,H]F} \quad \text{where } F \text{ is open}$$

But as an additional result, we show that, because (4) has a different sign in the differential equation, also open differential induction is still insufficient for proving (4) without the help of auxiliary differential variables. In particular, our approach can prove a property that related approaches [PJ04, PJP07, SSM08] cannot.

Let $\mathcal{DCI}^\circ$ be the calculus with open differential induction (DI°) and differential cuts (DC).

Theorem 3 (Open auxiliary differential variable power) *The deductive power of $\mathcal{DCI}^\circ$ with auxiliary differential variables exceeds the deductive power of $\mathcal{DCI}^\circ$ without auxiliary differential variables.*

Proof: In the proof of Theorem 2 we have shown a formal proof of (4) that uses only auxiliary differential variables (DA) and even only uses regular differential induction (DI) without differential cuts.

In order to see why (4) cannot be proven with regular differential induction, open differential induction, and differential cuts without the help of auxiliary differential variables, we continue the proof of Theorem 2. Again we consider the smallest F_i and an atomic subformula $p(x) > 0$ (or $p(x) \geq 0$) that distinguishes $-\infty$ and ∞ with a univariate polynomial $p(x)$. The point ∞ is in $F_{\leq n}$, so there must be such an atomic subformula that is true at ∞ and false at $-\infty$. Consequently, the leading coefficient of $p(x)$ is positive and $p(x)$ enjoys property (6). In open differential induction, the differential invariant F can be assumed in the differential induction step whenever the differential invariant F is open. Thus, the domain in which the differential induction step needs to hold is no longer $F_{\leq i-1}$ but now restricted to $F_{\leq i} \equiv F_{\leq i-1} \wedge F_i$. First note that $F_{\leq i-1}$ includes both ∞ and $-\infty$ but F_i (and $F_{\leq i}$) only include ∞, not $-\infty$. Then the rest of the proof of Theorem 2 does not work, because it assumes both ∞ and $-\infty$ to matter in the differential invariance condition.

Yet the leading coefficient c_{2n+1} of $p(x)$ is positive and, by (6), $p(x)$ is of odd degree. Abbreviate $p'^{-x}_{x'}$ again by $q(x)$. Then $q(x)$ is of odd degree and its leading coefficient is negative, because the leading term of $q(x)$ is $(2n+1)c_{2n+1}x^{2n}(-x)$ and $-(2n+1)c_{2n+1} < 0$. But then for $x \to \infty$ (which is in the domain of $F_{\leq i}$), the differential invariant condition $q(x) > 0$ or $q(x) \geq 0$ evaluates to false, which is a contradiction. □

7 Differential Cut Power

Differential cuts (rule DC on p. 10) can be used to first prove a lemma about a differential equation and then restrict the dynamics. They are very useful in practice [PC08, Pla10b] especially for finding proofs. But in some cases, they are just a shortcut for a more difficult proof with a more difficult differential invariant. This happens, for instance, in the class of air traffic control properties that we had originally conjectured to crucially require differential cuts three years ago [Pla10a]. Interestingly, no such single invariant was found by a template search with 252 unknowns [San10].

$$\dfrac{\dfrac{\dfrac{*}{\mathbb{R}\ 1 \geq 0}}{(y' \geq 0)^{y\ 1}_{x'\ y'}}}{DI\ x \geq 0 \wedge y \geq 0 \rightarrow [x' = y, y' = 1] y \geq 0} \qquad \dfrac{\dfrac{\dfrac{*}{\mathbb{R}\ y \geq 0 \rightarrow y \geq 0 \wedge 1 \geq 0}}{y \geq 0 \rightarrow (x' \geq 0 \wedge y' \geq 0)^{y\ 1}_{x'\ y'}}}{DI\ x \geq 0 \wedge y \geq 0 \rightarrow [x' = y, y' = 1 \,\&\, y \geq 0](x \geq 0 \wedge y \geq 0)}$$
$$\overline{DC\ x \geq 0 \wedge y \geq 0 \rightarrow [x' = y, y' = 1](x \geq 0 \wedge y \geq 0)}$$

Figure 4: Differential cut power: a proof of a simple property that requires differential cuts, not just differential invariants

But we have now found out that it still exists (omitted for space reasons). Is this always the case? Can all uses of differential cuts (DC) be eliminated and turned into a proof of the same property without using DC? Is there a differential cut elimination theorem for differential cuts just like there is Gentzen's cut elimination theorem for standard cuts [Gen35b, Gen35a]? Are all properties that are provable using DC also provable without DC?

As the major result of this work, we refute the differential cut elimination hypothesis. Differential cuts (rule DC) are *not* just admissible proof rules that can be eliminated, but an inherent proof rule that adds to the deductive power of the proof system. The addition of differential cuts to differential induction is a significant extension of the deductive power, because, when disallowing differential cuts (like all other approaches do), the deductive power of the proof system strictly decreases.

Theorem 4 (Differential cut power) *The deductive power of differential induction with differential cuts exceeds the deductive power without differential cuts.*

$$\mathcal{DCI} > \mathcal{DI}$$

The first key insight in the proof of Theorem 4 is that, for sufficiently large, but fixed, $y \gg 0$ or sufficiently small, but fixed, $y \ll 0$, the sign of a polynomial $p = \sum_{i,j} a_{i,j} x^i y^j$ in the limit where either $x \to \infty$ or $x \to -\infty$ is determined entirely by the sign of the leading monomial $a_{n,m} x^n y^m$ with respect to the lexicographical order induced by $x \succ y$. That is, the biggest $n, m \in \mathbb{N}$ with $a_{n,m} \neq 0$ such that there is no $N > n$ and no $j \in \mathbb{N}$ with $a_{N,j} \neq 0$ and there is no $M > m$ with $a_{n,M} \neq 0$. The reason why the leading monomial $a_{n,m} x^n y^m$ dominates is that, for $x \to \pm\infty$, the highest degree terms in variable x dominate smaller degree monomials. Furthermore, for sufficiently large $y \gg 0$ (and for sufficiently small $y \ll 0$), the highest degree term in variable y among those highest degree terms in x dominates the impact of coefficients of smaller degree.
Proof(Proof of Theorem 4): Consider the formula

$$x \geq 0 \wedge y \geq 0 \rightarrow [x' = y, y' = 1](x \geq 0 \wedge y \geq 0) \tag{7}$$

First, we show that formula (7) is provable easily with differential cuts; see Figure 4.

Now, we need to show that (7) is not provable without differential cuts, i.e., not provable by a differential induction step using any formula as differential invariant. Suppose (7) was provable by a single differential induction step with a formula F as differential invariant. Then

1. $\vDash x \geq 0 \land y \geq 0 \rightarrow F$ (precondition implies differential invariant), and
2. $\vDash F \rightarrow x \geq 0 \land y \geq 0$ (differential invariant implies postcondition), and
3. $\vDash F'^{y}_{x'\ y'}$ (differential induction step).

By condition 2, there has to be a subformula of F in which x occurs (with nonzero coefficient). This subformula is of the form $p \geq 0$ (or $p > 0$ or $p = 0$) with a polynomial $p := \sum_{i,j} a_{i,j} x^i y^j$. By condition 1, there even has to be such a formula of the form $p \geq 0$ or $p > 0$, because the set described by $p = 0$ has measure zero (as p is not the zero polynomial), yet the precondition has non-zero measure (otherwise, if F only had equational subformulas, then the region described by F would have measure zero, contradicting condition 1, or would be trivial $0 = 0$, contradicting condition 2).

Consider the leading term $a_{n,m} x^n y^m$ of p with respect to the lexicographical order induced by $x \succ y$. By condition 2, F needs to have a subformula ($p \geq 0$ or $p > 0$), in which the leading term $a_{n,m} x^n y^m$ with respect to $x \succ y$ has odd degree n in x (otherwise, if all leading terms had even degree in x, then, for sufficiently large $y \gg 0$, the truth-values for $x \rightarrow -\infty$ and for $x \rightarrow \infty$ would be identical and, thus, F cannot entail $x \geq 0$ as required by condition 2). By condition 3, we know, in particular, that the following holds:

$$\vDash p'^{y}_{x'\ y'} \geq 0 \quad (\text{or } \vDash p'^{y}_{x'\ y'} > 0 \text{ respectively}) \tag{8}$$

Note that, when forming F' and transforming p into $p'^{y}_{x'\ y'}$, the lexicographical monomial order induced by $x \succ y$ strictly decreases. The leading term (with respect to the lexicographical order induced by $x \succ y$) of $p'^{y}_{x'\ y'}$ comes from the leading term $a_{n,m} x^n y^m$ of p, and is identical to the leading term of

$$\begin{aligned} \ell &:= (n a_{n,m} x^{n-1} x' y^m + m a_{n,m} x^n y^{m-1} y')^{y}_{x'\ y'} \\ &= n a_{n,m} x^{n-1} y^{m+1} + m a_{n,m} x^n y^{m-1} \end{aligned}$$

Now, for sufficiently large $y \gg 0$ or sufficiently small $y \ll 0$, we see that, in the limit of $x \rightarrow \pm\infty$, the sign of $p'^{y}_{x'\ y'}$ is identical to the sign of ℓ, because $a_{n,m} x^n y^m$ is the leading term for the lexicographical order with $x \succ y$ and the forming of F' does not increase the degree of x. There are two cases to consider:

- Case $m = 0$: Then $\ell = n a_{n,0} x^{n-1} y$. Because (8) holds (for all x, y), we have, in particular, that
  1. $\ell \geq 0$ for $y \gg 0, x \rightarrow \pm\infty$. Hence, $n - 1$ is even and $a_{n,0} \geq 0$.
  2. $\ell \geq 0$ for $y \ll 0, x \rightarrow \pm\infty$. Hence, $n - 1$ is even and $a_{n,0} \leq 0$.

  Together, these imply $a_{n,0} = 0$, which contradicts the fact that $a_{n,m} \neq 0$, because $a_{n,m}$ is the leading term.
- Case $m \neq 0$: Because (8) holds (for all x, y), we have, in particular, that

1. $\ell \geq 0$ for $y \gg 0, x \to \pm\infty$. Then ℓ is dominated by the right term $ma_{n,m}x^n y^{m-1}$, which has higher degree in x. Hence, n is even and $a_{n,m} \geq 0$. But this contradicts the fact that n is odd.

In both cases, we have a contradiction, showing that (7) is not provable without differential cuts (DC). □

For traceability purposes, we use a very simple dynamics in this proof. This particular example could, in fact, still easily be solved with polynomial solutions using auxiliary differential variables (DA) instead. Yet, a similar example with more involved dynamics is, e.g., the following, which does not even have a polynomial solution, but is still easily provable by the differential cut $y \geq 0$:

$$x \geq 0 \land y \geq 0 \to [x' = y, y' = y^4](x \geq 0 \land y \geq 0)$$

8 Related Work

There are numerous approaches to verifying hybrid systems [Hen96, GM99, ADG03, GP07, Fre08]. Here we focus on approaches that are based on proof certificates or similar indirect witnesses for verification.

Approaches based on Lyapunov functions and tangent cones have a long history in control, including positively invariant sets and viability theory; see [Bla99] for an overview. These approaches are very successful for linear systems. Even though the overall theory is interesting, it is purely semantical and defined in terms of limit properties of general functions, which are not computable, even in rich computation frameworks [Col07]. Similarly, working with solutions of differential equations, which are defined in terms of limits of functions, lead to sound but generally not computable approaches (except for simple cases like nilpotent linear systems).

The whole point of our approach is that differential invariants are defined in terms of logic and differential algebra and allow us to replace semantic limit processes by decidable proof rules. The simplicity of our differential invariants makes them computationally attractive. The purpose of this paper is to study the proof theory of differential equations and differential invariants, not the semantics or mathematical limit processes, which would require higher-order logic.

Differential invariants are related to several other interesting approaches using variations of Lie derivatives, including barrier certificates [PJ04, PJP07], template equations [SSM08], and a constraint-based template approach [GT08]. Those approaches assume that the user provides the right template, but it is not clear how that has to be chosen. We answer the orthogonal question about provability trade-offs in classes of templates. Differential invariants are a generalization of several previous notions to general logical formulas, yet with some modifications of the verification principles that are required for soundness and make them computationally more attractive. The inclusion and soundness subtleties that we discuss in the following explain why we have chosen differential invariants for our study and generally emphasize the subtle nature of the problem of proving properties of differential equations.

Verification with barrier certificates [PJ04] fits to the general rule schema DI where F has the special form $p \leq 0$ for a polynomial p. Barrier certificates have also been strengthened [PJ04] with

an extra assumption $p = 0$ in the antecedent of the premise of DI. Even though this sounds intuitively convincing, it is generally unsound, however, because even the assumption of the weaker superset $F \equiv p \leq 0$ of $p = 0$ is unsound, as shown by counterexample (2). Those barrier certificates "prove" counterexample (2), which is not a valid formula. More recent work [PJP07] has modified the definition of barrier certificates to avoid this counterexample, but this becomes computationally more involved and cannot work for more general logical formulas.

An even stronger extra assumption for schema DI has been proposed in [GT08]. While it is perhaps interesting for other purposes, this variation is unsound, because it can also "prove" the counterexample (2). Variations of those rules for some special cases have been proposed later on [TT09], four of them either unsound or incomplete or ineffective. We do not consider those rules here, because no soundness proofs have been provided [TT09].

Template equations [SSM08] are equational differential invariants of the form $p = 0$ for a polynomial p, yet with a slightly modified extra assumption. They do not support inequalities. Soundness is again subtle, because the soundness proof [SSM08] is only correct when the differential equation has only globally convergent analytic solutions. This is not the case for $x' = -2tx^2, t' = 1$, whose solution $x(t) = 1/(t^2 + 1) = 1/((t + i)(t - i))$ has complex poles at $\pm i$ and, thus, only a convergence radius of 1 around 0. It is not the case for $x' = 2/t^3 x, t' = 1$ and for $x' = x^2 + 1$ either, which have non-analytic solutions and solutions with singular non-analytic points, respectively. It may be possible to fix the soundness proof in [SSM08]. Similar observations hold for [San10], which is a variation of the approach in [SSM08] where even a whole set of equations is required to be invariant.

We discard unsound approaches and focus exclusively on the sound approach of differential invariants. This is also the only sound approach that works for more general logical formulas. Since extra assumptions quickly result in unsound procedures, we stay away from using them here, like original barrier certificates. We consider differential cuts as a sound alternative in this paper, which is not only useful in practice but now also turns out to be a fundamental proof principle. For an analysis under which circumstances extra assumption F could be assumed in the premise without losing soundness, we refer to previous work [Pla10a]. In particular, differential invariants include some of the previous approaches (not the unsound ones) as special cases. Differential invariants are more general in that they do not focus on single polynomial equalities like [PJ04, PJP07] or on single polynomial equalities like [SSM08]. We have shown how the deductive power increases when considering more general formulas as differential invariants. Our findings in the setting of differential invariants translate into corresponding properties of other approaches as hinted at in this paper, but detailed technical constructions for other approaches are beyond the scope of this paper.

Other approaches also neither use differential cuts nor auxiliary differential variables, both of which we have proven to be fundamental proof principles.

9 Conclusions

We have considered the differential invariance problem, which, by a relative completeness argument, is at the heart of hybrid systems verification. To better understand structural properties of

hybrid systems, we have identified and analyzed more than a dozen (16) relations between the deductive power of several (9) classes of differential invariants, including subclasses that correspond to related approaches. Most crucially and surprisingly, we have refuted the differential cut elimination hypothesis and have shown that differential cuts increase the deductive power of differential invariants. Our answer to the differential cut elimination hypothesis is the central result of this work. We have also shown that auxiliary differential variables further increase the deductive power, even in the presence of arbitrary differential cuts. These findings shed light on fundamental provability properties of hybrid systems and are practically important for successful proof search.

Our results require a symbiosis of elements of logic with differential, semialgebraic, geometrical, and real arithmetical properties. Future work includes investigating this new field further that we call *real differential semialgebraic geometry*.

References

[ADG03] Eugene Asarin, Thao Dang, and Antoine Girard. Reachability analysis of nonlinear systems using conservative approximation. In Oded Maler and Amir Pnueli, editors, *HSCC*, volume 2623 of *LNCS*, pages 20–35. Springer, 2003.

[And02] Peter B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof*. Kluwer, 2nd edition, 2002.

[BBM98] Michael S. Branicky, Vivek S. Borkar, and Sanjoy K. Mitter. A unified framework for hybrid control: Model and optimal control theory. *IEEE T. Automat. Contr.*, 43(1):31–45, 1998.

[BCGH07] Olivier Bournez, Manuel Lameiras Campagnolo, Daniel S. Graça, and Emmanuel Hainry. Polynomial differential equations compute all real computable functions on computable compact intervals. *Journal of Complexity*, 23:317–335, 2007.

[Bla99] Franco Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[Bra95] Michael S. Branicky. Universal computation and other capabilities of hybrid and continuous dynamical systems. *Theor. Comput. Sci.*, 138(1):67–100, 1995.

[Col07] Pieter Collins. Optimal semicomputable approximations to reachable and invariant sets. *Theory Comput. Syst.*, 41(1):33–48, 2007.

[DH88] James H. Davenport and Joos Heintz. Real quantifier elimination is doubly exponential. *J. Symb. Comput.*, 5(1/2):29–35, 1988.

[DN00] Jennifer Mary Davoren and Anil Nerode. Logics for hybrid systems. *IEEE*, 88(7):985–1010, July 2000.

[Fit96] Melvin Fitting. *First-Order Logic and Automated Theorem Proving*. Springer, New York, 2nd edition, 1996.

[Fre08] Goran Frehse. PHAVer: algorithmic verification of hybrid systems past HyTech. *STTT*, 10(3):263–279, 2008.

[GCB07] Daniel Silva Graça, Manuel L. Campagnolo, and Jorge Buescu. Computability with polynomial differential equations. *Advances in Applied Mathematics*, 2007.

[Gen35a] Gerhard Gentzen. Untersuchungen über das logische Schließen. I. *Math. Zeit.*, 39(2):176–210, 1935.

[Gen35b] Gerhard Gentzen. Untersuchungen über das logische Schließen. II. *Math. Zeit.*, 39(3):405–431, 1935.

[GM99] Mark R. Greenstreet and Ian Mitchell. Reachability analysis using polygonal projections. In Frits W. Vaandrager and Jan H. van Schuppen, editors, *HSCC*, volume 1569 of *LNCS*, pages 103–116. Springer, 1999.

[GM08] Aarti Gupta and Sharad Malik, editors. *Computer Aided Verification, CAV 2008, Princeton, NJ, USA, Proceedings*, volume 5123 of *LNCS*. Springer, 2008.

[Göd31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Mon. hefte Math. Phys.*, 38:173–198, 1931.

[GP07] Antoine Girard and George J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE T. Automat. Contr.*, 52:782–798, 2007.

[GT08] Sumit Gulwani and Ashish Tiwari. Constraint-based approach for analysis of hybrid systems. In Gupta and Malik [GM08], pages 190–203.

[Hen96] Thomas A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.

[PC07] André Platzer and Edmund M. Clarke. The image computation problem in hybrid systems model checking. In Alberto Bemporad, Antonio Bicchi, and Giorgio Buttazzo, editors, *HSCC*, volume 4416 of *LNCS*, pages 473–486. Springer, 2007.

[PC08] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Gupta and Malik [GM08], pages 176–189.

[PC09] André Platzer and Edmund M. Clarke. Formal verification of curved flight collision avoidance maneuvers: A case study. In Ana Cavalcanti and Dennis Dams, editors, *FM*, volume 5850 of *LNCS*, pages 547–562. Springer, 2009.

[PJ04] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In Rajeev Alur and George J. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 477–492. Springer, 2004.

[PJP07] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE T. Automat. Contr.*, 52(8):1415–1429, 2007.

[Pla08] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008.

[Pla10a] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010. Advance Access published on November 18, 2008.

[Pla10b] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010.

[PQ09] André Platzer and Jan-David Quesel. European Train Control System: A case study in formal verification. In Karin Breitman and Ana Cavalcanti, editors, *ICFEM*, volume 5885 of *LNCS*, pages 246–265. Springer, 2009.

[RS07] Stefan Ratschan and Zhikun She. Safety verification of hybrid systems by constraint propagation-based abstraction refinement. *Trans. on Embedded Computing Sys.*, 6(1):8, 2007.

[San10] Sriram Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In Karl Henrik Johansson and Wang Yi, editors, *HSCC*, pages 221–230. ACM, 2010.

[SSM08] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. Constructing invariants for hybrid systems. *Form. Methods Syst. Des.*, 32(1):25–55, 2008.

[Tar51] Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley, 2nd edition, 1951.

[Tav87] Lucio Tavernini. Differential automata and their discrete simulators. *Non-Linear Anal.*, 11(6):665–683, 1987.

[TT09] Ankur Taly and Ashish Tiwari. Deductive verification of continuous dynamical systems. In Ravi Kannan and K. Narayan Kumar, editors, *FSTTCS*, volume 4 of *LIPIcs*, pages 383–394. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2009.

[Wal98] Wolfgang Walter. *Ordinary Differential Equations*. Springer, 1998.

A Background Proof Rules

Figure 5 shows the proof rules that we assume as background rules for our purposes. They consist of the standard propositional sequent proof rules including the axiom (ax) and cut rule (cut) for

glueing proofs together. Rule $\mathbb{R}$ allows us to use any valid instance of a first-order real arithmetic tautology as a proof rule. This rule is a simplification of more constructive deduction modulo proof rules for real arithmetic and modular quantifier elimination [Pla08, Pla10a, Pla10b], which we do not need to consider in detail in this paper. The rules in Figure 5 are standard and listed here just for the sake of a complete presentation.

$$(\neg\text{r})\ \frac{\Gamma, \phi \to \Delta}{\Gamma \to \neg\phi, \Delta} \qquad (\vee\text{r})\ \frac{\Gamma \to \phi, \psi, \Delta}{\Gamma \to \phi \vee \psi, \Delta} \qquad (\wedge\text{r})\ \frac{\Gamma \to \phi, \Delta \quad \Gamma \to \psi, \Delta}{\Gamma \to \phi \wedge \psi, \Delta}$$

$$(\neg\text{l})\ \frac{\Gamma \to \phi, \Delta}{\Gamma, \neg\phi \to \Delta} \qquad (\vee\text{l})\ \frac{\Gamma, \phi \to \Delta \quad \Gamma, \psi \to \Delta}{\Gamma, \phi \vee \psi \to \Delta} \qquad (\wedge\text{l})\ \frac{\Gamma, \phi, \psi \to \Delta}{\Gamma, \phi \wedge \psi \to \Delta}$$

$$(\to\text{r})\ \frac{\Gamma, \phi \to \psi, \Delta}{\Gamma \to \phi \to \psi, \Delta} \qquad (ax)\ \frac{}{\Gamma, \phi \to \phi, \Delta} \qquad (\mathbb{R})\ \frac{\tilde{\Gamma} \to \tilde{\Delta}}{\Gamma \to \Delta}\ [1]$$

$$(\to\text{l})\ \frac{\Gamma \to \phi, \Delta \quad \Gamma, \psi \to \Delta}{\Gamma, \phi \to \psi \to \Delta} \qquad (cut)\ \frac{\Gamma \to \phi, \Delta \quad \Gamma, \phi \to \Delta}{\Gamma \to \Delta}$$

[1] if $(\tilde{\Gamma} \to \tilde{\Delta}) \to (\Gamma \to \Delta)$ is an instance of a valid tautology of first-order real arithmetic

Figure 5: Basic proof rules

B Soundness of Differential Induction

We have proved soundness of proof rules DI and DC and the other rules in previous work [Pla10a]. In the interest of a self-contained presentation, we repeat the critical soundness proofs here in a simplified and adapted form that directly uses the notation of this paper.

For the proof of soundness of DI, we first prove that the valuation of syntactic total derivation ${F'}^{\theta}_{x'}$ (with differential equations substituted in) of formula F as defined in Sect. 3 coincides with analytic differentiation. We first show this derivation lemma for terms c.

Lemma 2 (Derivation lemma) *Let $x' = \theta \,\&\, H$ be a continuous evolution and let $\varphi : [0, r] \to (V \to \mathbb{R}^n)$ be a corresponding flow of duration $r > 0$. Then for all terms c and all $\zeta \in [0, r]$ we have the identity*

$$\frac{\mathsf{d}\,\varphi(t)[\![c]\!]}{\mathsf{d}t}(\zeta) = \varphi(\zeta)[\![{c'}^{\theta}_{x'}]\!] \ .$$

In particular, $\varphi(t)[\![c]\!]$ is continuously differentiable.

Proof: The proof is by induction on term c. The differential equation $x' = \theta$ is of the form $x'_1 = \theta_1, \ldots, x'_n = \theta_n$.

- If c is one of the variables x_j for some j (for other variables, the proof is simple because c is constant during φ) then:

$$\frac{\mathsf{d}\,\varphi(t)[\![x_j]\!]}{\mathsf{d}t}(\zeta) = \varphi(\zeta)[\![\theta_j]\!] = \varphi(\zeta)[\![\sum_{i=1}^{n} \frac{\partial x_j}{\partial x_i}\theta_i]\!] \ .$$

  The first equation holds by definition of the semantics. The last equation holds as $\frac{\partial x_j}{\partial x_j} = 1$ and $\frac{\partial x_j}{\partial x_i} = 0$ for $i \neq j$. The derivatives exist because φ is (continuously) differentiable for x_j.

- If c is of the form $a + b$, the desired result can be obtained by using the properties of derivatives and semantic valuation:

$$\begin{aligned}
&\frac{\mathsf{d}\,\varphi(t)[\![a+b]\!]}{\mathsf{d}t}(\zeta) \\
&= \frac{\mathsf{d}\,(\varphi(t)[\![a]\!] + \varphi(t)[\![b]\!])}{\mathsf{d}t}(\zeta) && \nu[\![\cdot]\!] \text{ is a linear operator for all } \nu \\
&= \frac{\mathsf{d}\,\varphi(t)[\![a]\!]}{\mathsf{d}t}(\zeta) + \frac{\mathsf{d}\,\varphi(t)[\![b]\!]}{\mathsf{d}t}(\zeta) && \frac{\mathsf{d}}{\mathsf{d}t} \text{ is a linear operator} \\
&= \varphi(\zeta)[\![{a'}^{\theta}_{x'}]\!] + \varphi(\zeta)[\![{b'}^{\theta}_{x'}]\!] && \text{by induction hypothesis} \\
&= \varphi(\zeta)[\![{a'}^{\theta}_{x'} + {b'}^{\theta}_{x'}]\!] && \nu[\![\cdot]\!] \text{ is a linear operator for } \nu = \varphi(\zeta) \\
&= \varphi(\zeta)[\![{(a+b)'}^{\theta}_{x'}]\!] && \text{derivation is linear, because } \frac{\partial}{\partial x_i} \text{ is linear}
\end{aligned}$$

- The case where c is of the form $a \cdot b$ is accordingly, using Leibniz's product rule for $\frac{\partial}{\partial x_i}$; see [Pla10b].

□

Proof(Proof of Soundness of DI): In order to prove soundness of rule DI, we need to prove that, whenever the premise is valid (true in all states), then the conclusion is valid. We have to show that $\nu \models F \to [x' = \theta \,\&\, H]F$ for all states ν. Let ν satisfy $\nu \models F$ as, otherwise, there is nothing to show. We can assume F to be in disjunctive normal form and consider any disjunct G of F that is true at ν. In order to show that F remains true during the continuous evolution, it is sufficient to show that each conjunct of G is. We can assume these conjuncts to be of the form $c \geq 0$ (or $c > 0$ where the proof is accordingly). Finally, using vectorial notation, we write $x' = \theta$ for the differential equation system. Now let $\varphi : [0, r] \to (V \to \mathbb{R}^n)$ be any flow of $x' = \theta \,\&\, H$ beginning in $\varphi(0) = \nu$. If the duration of φ is $r = 0$, we have $\varphi(0) \models c \geq 0$ immediately, because $\nu \models c \geq 0$. For duration $r > 0$, we show that $c \geq 0$ holds all along the flow φ, i.e., $\varphi(\zeta) \models c \geq 0$ for all $\zeta \in [0, r]$.

Suppose there was a $\zeta \in [0, r]$ with $\varphi(\zeta) \models c < 0$, which will lead to a contradiction. The function $h : [0, r] \to \mathbb{R}$ defined as $h(t) = \varphi(t)[\![c]\!]$ satisfies the relation $h(0) \geq 0 > h(\zeta)$, because $h(0) = \varphi(0)[\![c]\!] = \nu[\![c]\!]$ and $\nu \models c \geq 0$ by antecedent of the conclusion. By Lemma 2, h is continuous on $[0, r]$ and differentiable at every $\xi \in (0, r)$. By mean value theorem, there is

a $\xi \in (0,\zeta)$ such that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) \cdot (\zeta - 0) = h(\zeta) - h(0) < 0$. In particular, since $\zeta \geq 0$, we can conclude that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) < 0$. Now Lemma 2 implies that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) = \varphi(\xi)[\![{c'}^{\theta}_{x'}]\!] < 0$. This, however, is a contradiction, because the premise implies that the formula $H \rightarrow (c \geq 0)'^{\theta}_{x'}$ is true in all states along φ, including $\varphi(\xi) \models H \rightarrow (c \geq 0)'^{\theta}_{x'}$. In particular, as φ is a flow for $x' = \theta \,\&\, H$, we know that $\varphi(\xi) \models H$ holds, and we have $\varphi(\xi) \models (c \geq 0)'^{\theta}_{x'}$, which contradicts $\varphi(\xi)[\![{c'}^{\theta}_{x'}]\!] < 0$. □

Proof(Proof of Soundness of DC): Rule DC is sound using the fact that the left premise implies that every flow φ that satisfies $x' = \theta$ also satisfies H *all along* the flow. Thus, if flow φ satisfies $x' = \theta$, it also satisfies $x' = \theta \,\&\, H$, so that the right premise entails the conclusion. □