15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Differential Invariants & Proof Theory

André Platzer

Carnegie Mellon University
Lecture 13

1. Introduction

Lecture 10 on Differential Equations & Differential Invariants and Lecture 11 on Differential Equations & Proofs equipped us with powerful tools for proving properties of differential equations without having to solve them. *Differential invariants* (DI) [Pla10a] prove properties of differential equations by induction based on the right-hand side of the differential equation, rather than its much more complicated global solution. *Differential cuts* (DC) [Pla10a] made it possible to prove another property C of a differential equation and then change the dynamics of the system around so that it is restricted to never leave that region C. Differential cuts turned out to be very useful when stacking inductive properties of differential equations on top of each other, so that easier properties are proved first and then assumed during the proof of the more complicated properties. In fact, in some cases, differential cuts are crucial for proving properties in the first place [Pla10a, Pla12c, GSP14]. Differential weakening (DW) [Pla10a] proves simple properties that are entailed by the evolution domain, which becomes especially useful after the evolution domain constraint has been augmented sufficiently by way of a differential cut.

Just like in the case of loops, where the search for invariants is nontrivial, differential invariants also require some smarts (or good automatic procedures [PC08, Pla12b, GP14, GSP14]) to be found. Once a differential invariant has been identified, however, the proof follows easily, which is a computationally attractive property.

Finding invariants of loops is very challenging. It can be shown to be the only fundamental challenge in proving safety properties of conventional discrete programs [HMP77]. Likewise, finding invariants and differential invariants is the only fundamental challenge in proving safety properties of hybrid systems [Pla08, Pla10b, Pla12a].

A more careful analysis even shows that just finding differential invariants is the only fundamental challenge for hybrid systems safety verification [Pla12a].

That is reassuring, because we know that the proofs will work[1] as soon as we find the right differential invariants. But it also tells us that we can expect the search for differential invariants (and invariants) to be challenging, because cyber-physical systems are extremely challenging, albeit very important. Yet, differential equations also enjoy many pleasant properties that we can exploit to help us find differential invariants.

Since, at the latest after this revelation, we fully realize the importance of studying and understanding differential invariants, we subscribe to developing a deeper understanding of differential invariants right away. The part of their understanding that today's lecture develops is how various classes of differential invariants relate to each other in terms of what they can prove. That is, are there properties that only differential invariants of the form $\mathcal{A}$ can prove, because differential invariants of the form $\mathcal{B}$ cannot ever succeed in proving them? Or are all properties provable by differential invariants of the form $\mathcal{A}$ also provable by differential invariants of the form $\mathcal{B}$?

These relations between classes of differential invariants tell us which forms of differential invariants we need to search for and which forms of differential invariants we don't need to bother considering. A secondary goal of today's lecture besides this theoretical understanding is the practical understanding of developing more intuition about differential invariants and seeing them in action more thoroughly.

This lecture is based on [Pla12c] and strikes a balance between comprehensive handling of the subject matter and core intuition. The lecture mostly focuses on the core intuition at the heart of the proofs and leaves a more comprehensive argument and further study for the literature [Pla12c]. Many proofs in this lecture are simplified and only prove the core argument, while leaving out other aspects. Those—very important—further details are beyond the scope of this course, however, and can be found elsewhere [Pla12c]. For example, this lecture will not study whether indirect proofs could conclude the same properties. With a more careful analysis [Pla12c], it turns out that indirect proofs do not change the results reported in this lecture, but the proofs become significantly more complicated and require a more precise choice of the sequent calculus formulation. In this lecture, we will also not always prove all statements conjectured in a theorem. The remaining proofs can be found in the literature [Pla12c].

Note 1 (Proof theory of differential equations)**.** *The results in this lecture are part of the* proof theory *of differential equations, i.e. the theory of what can be proved about differential equations and with what techniques. They are proofs about proofs, because they prove relations between the provability of logical formulas with different proof calculi. That is, they relate "formula ϕ can be proved using $\mathcal{A}$" and "formula ϕ can be proved using $\mathcal{B}$."*

The most important learning goals of this lecture are:

Modeling and Control: This lecture helps in understanding the core argumentative

[1] Although it may still be a lot of work in practice to make the proofs work. At least they become possible.

principles behind CPS and sheds more light on the question how to tame their analytic complexity.

Computational Thinking: An important part of computer science studies questions about the *limits of computation* or, more generally, develops an understanding of *what can be done* and *what cannot be done*. Either in absolute terms (*computability theory* studies what is computable and what is not) or in relative terms (*complexity theory* studies what is computable in a characteristically quicker way or within classes of resource bounds on time and space). Often times, the most significant understanding of a problem space starts with what cannot be done (the theorem of Rice says that all nontrivial properties of programs are not computable) or what can be done (every problem that can be solved with a deterministic algorithm in polynomial time can also be solved with a nondeterministic algorithm in polynomial time, with the converse being the P versus NP problem).

The primary purpose of this lecture is to develop such an understanding of the limits of what can and what cannot be done in the land of *proofs about differential equations* with what techniques. Not all aspects of this deep question will be possible to answer in one lecture, but it will feature the beginning of the *proof theory of differential equations*, i.e. the theory of provability and proofs about differential equations. Proof theory is, of course, also of interest in other cases, but we will study it in the case that is most interesting and illuminating: the case of proofs about differential equations.

The primary, scientific learning goals of this lecture are, thus, to develop a fundamental understanding of what can and cannot be proved in which way about differential equations. This helps us in our search for differential invariants for applications, because such an understanding prevents us from asking the same analytic question again in equivalent ways (if two different classes of differential invariants prove the same properties and one of them already failed) and guides our search toward the required classes of differential invariants (by next choosing a class that can prove fundamentally more, and of properties of the requisite form). The secondary, pragmatic learning goals are to practice inductive proofs about differential equations using differential invariants and to develop an intuition which verification question to best address in which way. In these ways, both fundamentally and pragmatically, the primary direct impact of this lecture is on understanding rigorous reasoning about CPS models as well as helping to verify CPS models of appropriate scale, in which more than one mode of reasoning is often needed for the various parts and aspects of the system.

CPS Skills: This lecture serves no purpose in CPS Skills that the author could think of, except indirectly via its impact on their analysis.

2. Recap

Recall the following proof rules for differential equations from Lecture 11 on Differential Equations & Proofs:

Note 2 (Proof rules for differential equations).

$$\text{(DI)}\ \frac{H \vdash F'^{\theta}_{x'}}{F \vdash [x' = \theta \,\&\, H]F} \qquad \text{(DW)}\ \frac{H \vdash F}{\Gamma \vdash [x' = \theta \,\&\, H]F, \Delta}$$

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

With cuts and generalizations, earlier lectures have also shown that the following can be proved:

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

This is useful for replacing a precondition A and postcondition B by another invariant F that implies postcondition B and is implied by precondition A, which will be done frequently in this lecture.

3. Comparative Deductive Study: Relativity Theory for Proofs

In order to find out what we can do when we have been unsuccessfully searching for a differential invariant of one form, we need to understand which other form of differential invariants could work out better. If we have been looking for differential invariants of the form $p = 0$ with a term p without success and then move on to search for differential invariants of the form $p = q$, then we cannot expect to be any more successful than before, because $p = q$ can be rewritten as $p - q = 0$, which is of the first form again. So we should, for example, try finding inequational differential invariants of the form $p \geq 0$, instead. In general, this begs the question which generalizations would be silly (because differential invariants of the form $p = q$ cannot prove any more than those of the form $p = 0$) and when it might be smart (because $p \geq 0$ could still succeed even if everything of the form $p = 0$ failed).

As a principled answer to questions like these, we study the relations of classes of differential invariants in terms of their relative deductive power. That is, we study whether some properties are only provable using differential invariants from the class $\mathcal{A}$, not using differential invariants from the class $\mathcal{B}$, or whether all properties provable with differential invariants from class $\mathcal{A}$ are also provable with class $\mathcal{B}$.

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 of real arithmetic by proof rule $\mathbb{R}$) along the lines of what we say in Lecture 6 on

Truth & Proof; see [Pla12c] for precise details. 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 further 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 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 $\mathcal{B} \not\leq \mathcal{A}$.

4. Equivalences of Differential Invariants

Before we go any further, let us study whether there are equivalence transformations on formulas 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 the meta-proofs in the proof theory. For example, we should not expect $F \wedge G$ to be a differential invariant for proving a property when $G \wedge F$ was not. Neither would $F \vee G$ be any better as a differential invariant than $G \vee F$.

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. In order to prove this, we consider any property that proves with F as a differential invariant and show that G also works. 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:

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

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 propositionally. Subgoal $H \vdash {G'}^{\theta}_{x'}$ is provable, because $H \vdash {F'}^{\theta}_{x'}$ 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, $\mathsf{d}\mathcal{L}$ uses a propositionally complete base calculus [Pla12c]. □

In all 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 *à la* (1) 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.

5. Differential Invariants & Arithmetic

Depending on the reader's exposure to differential structures, it may come as a shock that not all logical equivalence transformations carry over to differential invariants. Differential invariance is not necessarily preserved under real arithmetic equivalence transformations.

Lemma 2 (Differential invariants and arithmetic). *Differential invariants are* not *invariant under equivalences of real arithmetic. That is, if $F \leftrightarrow G$ is an instance of a first-order real arithmetic tautology then F may be a differential invariant of $x' = \theta \,\&\, H$ yet G may not.*

Proof. There are two formulas that are equivalent over first-order real arithmetic 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:

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

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

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

□

For proving the property in the proof of Lemma 2 we need to use the principle (1) with the differential invariant $F \equiv x^2 \leq 5^2$ and cannot use $-5 \leq x \wedge x \leq 5$ directly.

By Lemma 2, we cannot just use arbitrary equivalences when investigating differential invariance, but have to be more careful. Not just the *elementary real arithmetical equivalence* of having the same set of satisfying assignments matters, but also the differential structures need to be compatible. Some equivalence transformations that preserve the solutions still destroy the differential structure. It is the equivalence of *real differential structures* that matters. Recall that differential structures are defined locally in terms of the behavior in neighborhoods of a point, not the point itself.

Lemma 2 illustrates a notable 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 Fig. 1.

The first two rows in Fig. 1 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 also depends on what value x' assumes according to the differential equation. Fig. 1 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.

We can, however, always 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 $(q' - p' \geq 0)^{\theta}_{x'}$ in first-order real arithmetic.

6. Differential Invariant Equations

For equational differential invariants $p = 0$, a.k.a. differential invariant equations, propositional operators do not add to the deductive power.

Proposition 3 (Equational deductive power [Pla10a, Pla12c]). *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:*

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

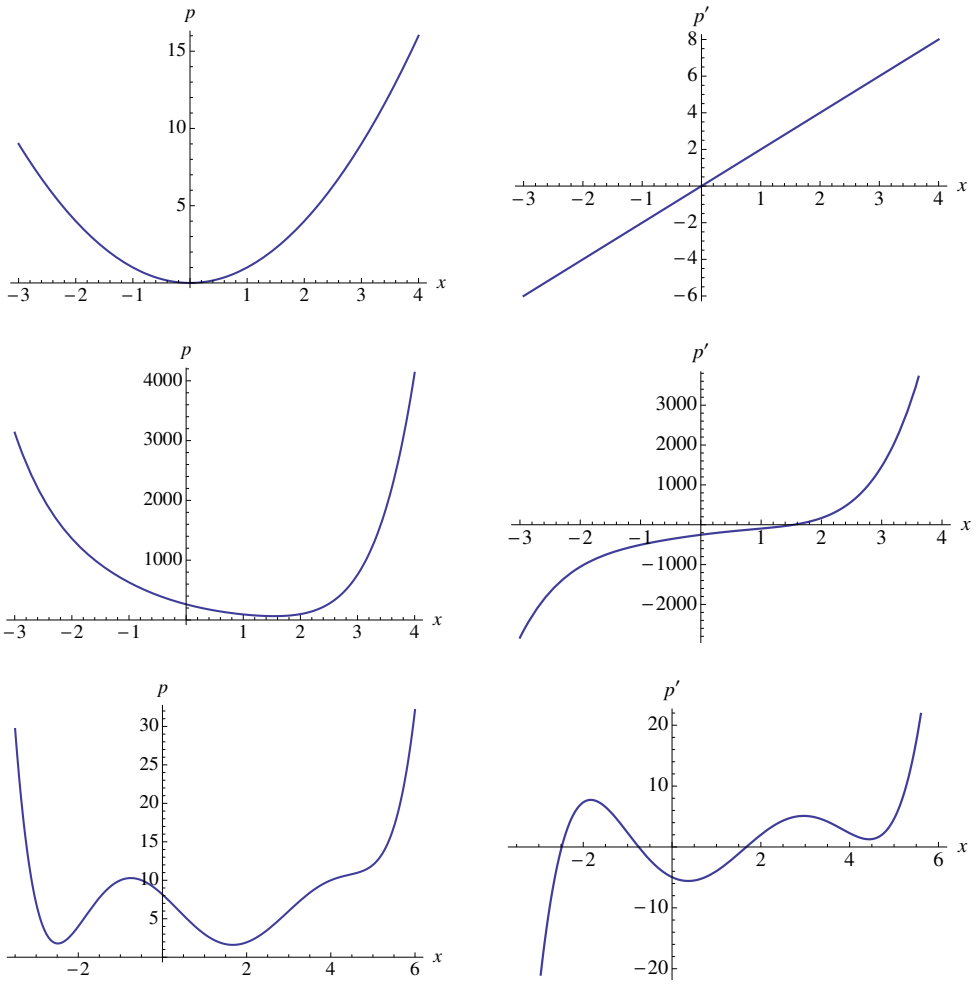


Figure 1: Equivalent solutions ($p \geq 0$ on the left) with quite different differential structure (p' plotted on the right)

How could we prove that?

Before you read on, see if you can find the answer for yourself.

One direction is simple. Proving $\mathcal{DI}_{=} \leq \mathcal{DI}_{=,\wedge,\vee}$ is obvious, because every proof using a differential invariant equation $p_1 = p_2$ also is a proof using a propositional combination of differential invariant equations. The propositional combination that just consists of the only conjunct $p_1 = p_2$ without making use of any propositional operators.

The other way around $\mathcal{DI}_{=} \geq \mathcal{DI}_{=,\wedge,\vee}$ is more difficult. If a formula can be proved using a differential invariant that is a propositional combination of equations, such as $p_1 = p_2 \wedge q_1 = q_2$, how could it possibly be proved using just a single equation?

Note 6 (Proofs of equal provability). *A proof of Proposition 3 needs to show that every such provable property is also provable with a structurally simpler differential invariant. It effectively needs to transform proofs with propositional combinations of equations as differential invariants into proofs with just differential invariant equations. And, of course, the proof of Proposition 3 needs to prove that the resulting equations are actually provably differential invariants and prove the same properties as before. This is a general feature of proof theory. It often involves proof transformations at the heart of the arguments.*

Proof of Proposition 3. 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 $\neq$ can be assumed not to 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

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

  which implies that the differential structure is the same so that the inductive steps are equivalent (either both succeed or both fail).

- 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

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

Consequently propositional connectives of equations can be replaced by their equivalent arithmetic equations in pre- and postconditions, and the corresponding induction steps are equivalent. □

Note that the polynomial degree increases quadratically by the reduction in Proposition 3, 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. This trade-off depends on the real arithmetic decision procedure, but is often enough in favor of keeping propositional structure, because the proof calculus can still exploit the logical structure to decompose the verification question before invoking real arithmetic. There are cases, however, where such reductions are formidably insightful [Pla12b].

Equational differential invariants, thus, enjoy a lot of beautiful properties, including characterizing invariant functions [Pla12b] and generalizing to a decision procedure for algebraic invariants of algebraic differential equations [GP14].

7. Equational Incompleteness

Focusing exclusively on differential invariants with equations reduces the deductive power, because sometimes only differential invariant inequalities can prove properties.

Proposition 4 (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.*

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

How could such a proposition be proved?

Before you read on, see if you can find the answer for yourself.

The proof strategy for the proof of Proposition 3 involved transforming proofs into proofs to prove the inclusion $\mathcal{DI}_{=} \geq \mathcal{DI}_{=,\wedge,\vee}$. Could the same strategy prove Proposition 4? No, because we need to show the opposite! Proposition 4 conjectures $\mathcal{DI}_{\geq} \not\leq \mathcal{DI}_{=,\wedge,\vee}$, which means that there are true properties that are only provable using a differential invariant inequality $p_1 \geq p_2$ and not using any differential invariant equations or propositional combinations thereof.

For one thing, this means that we ought to find a property that a differential invariant inequality can prove. That ought to be easy enough, because Lecture 11 on Differential Equations & Proofs showed us how useful differential invariants are. But then a proof of Proposition 4 also requires a proof why that very same formula cannot possibly ever be proved with any way of using only differential invariant equations or their propositional combinations. That is a proof about nonprovability. Proving provability in proof theory amounts to producing a proof (in sequent calculus). Proving nonprovability most certainly does not mean it would be enough to write something down that is not a proof. After all, just because one proof attempt fails does not mean that other attempts would not be successful. You have experienced this while you were working on proving your labs for this course. The first proof attempt might have failed miserably and was impossible to ever work out. But, come next day, you had a better idea with a different proof, and suddenly the same property turned out to be perfectly provable even if the first proof attempt failed.

How could we prove that all proof attempts do not work?

Before you read on, see if you can find the answer for yourself.

One way of showing that a logical formula cannot be proved is by giving a counterexample, i.e. a state which assigns values to the variables that falsify the formula. That is, of course, not what can help us proving Proposition 4, because a proof of Proposition 4 requires us to find a formula that can be proved with $\mathcal{DI}_{\geq}$ (so it cannot have any counterexamples, since it is perfectly valid), just cannot be proved with $\mathcal{DI}_{=,\wedge,\vee}$. Proving that a valid formula cannot be proved with $\mathcal{DI}_{=,\wedge,\vee}$ requires us to show that all proofs in $\mathcal{DI}_{=,\wedge,\vee}$ do not prove that formula.

Expedition 1 (Proving differences in set theory and linear algebra)**.** Recall sets. The way to prove that two sets M, N have the same "number" of elements is to come up with a pair of functions $\Phi : M \to N$ and $\Psi : N \to M$ between the sets and then prove that Φ, Ψ are inverses of each other, i.e. $\Phi(\Psi(y)) = y$ and $\Psi(\Phi(x)) = x$ for all $x \in M, y \in N$. Proving that two sets M, N do not have the same "number" of elements works entirely differently, because that has to prove for all pairs of functions $\Phi : M \to N$ and $\Psi : N \to M$ that there is is an $x \in M$ such that $\Psi(\Phi(x)) \neq x$ or an $y \in N$ such that $\Phi(\Psi(y)) \neq y$. Since writing down every such pair of functions Φ, Ψ is a lot of work (an infinite amount of work of M and N are infinite), indirect criteria such as cardinality or countability are used instead, e.g. for proving that the reals $\mathbb{R}$ and rationals $\mathbb{Q}$ cannot possibly have the same number of elements, because $\mathbb{Q}$ are countable but $\mathbb{R}$ are not (by Cantor's diagonal argument).

Recall vector spaces from linear algebra. The way to prove that two vector spaces V, W are isomorphic is to think hard and construct a function $\Phi : V \to W$ and a function $\Psi : W \to V$ and then prove that Φ, Ψ are linear functions and inverses of each other. Proving that two vector spaces V, W are *not* isomorphic works entirely differently, because that has to prove that all pairs of functions $\Phi : V \to W$ and $\Psi : W \to V$ are either not linear or not inverses of each other. Proving the latter literally is again a lot (usually infinite) amount of work. So instead, indirect criteria are being used. One proof that two vector spaces V, W are not isomorphic could show that both have different dimensions and then prove that isomorphic vector spaces always have the same dimension, so V and W cannot possibly be isomorphic.

By analogy, proving non-provability leads to a study of indirect criteria about proofs of differential equations.

Note 8 (Proofs of different provability)**.** *Proving non-reducibility $\mathcal{A} \not\leq \mathcal{B}$ for classes of differential invariants requires an example formula ϕ that is provable in $\mathcal{A}$ plus a proof that no proof using $\mathcal{B}$ proves ϕ. The preferred way of doing that is finding an indirect criterion that all proofs in $\mathcal{B}$ possess but that ϕ does not have, so that the proofs using $\mathcal{B}$ cannot possibly succeed in proving ϕ.*

Proof of Proposition 4. Consider any positive term $a > 0$ (e.g., 5 or $x^2 + 1$ or $x^2 + x^4 + 2$). The following proof proves a formula by differential induction with the weak inequal-

ity $x \geq 0$:

$$\mathbb{R}\,\frac{*}{\vdash a \geq 0}\qquad \text{DI}\,\frac{\vdash a \geq 0}{x \geq 0 \vdash [x' = a]x \geq 0}$$

The same formula is not provable with an equational differential invariant, however. Any univariate polynomial p that is zero on all $x \geq 0$ is the zero polynomial and, thus, an equation of the form $p = 0$ cannot be equivalent to the half space $x \geq 0$. By the equational deductive power theorem 3, the above formula then is not provable with any Boolean combination of equations as differential invariant either, because propositional combinations of equational differential invariants prove the same properties that single equational differential invariants do, and the latter cannot succeed in proving $x \geq 0 \to [x' = a]x \geq 0$.

The other parts of the theorem that involve generalizations of the non-provability argument to other indirect proofs using cuts and the like are proved elsewhere [Pla12c]. □

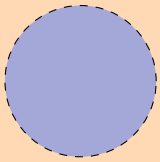
It might be tempting to think that at least equational postconditions only need equational differential invariants for proving them. But that is not the case either [Pla12c]. So even if the property you care to prove involves only equations, you may still need to generalize your proof arguments to consider inequalities instead.

8. Strict Differential Invariant Inequalities

We show that, conversely, focusing on strict inequalities $p > 0$ also reduces the deductive power, because equations are obviously missing and there is at least one proof where this matters. That is, what are called strict barrier certificates do not prove (non-trivial) closed invariants.

Expedition 2 (Topology in real analysis)**.** The following proofs distinguish open sets from closed sets, which are concepts from real analysis (or topology).cd Roughly: A closed set is one whose boundary belongs to the set. For example the solid unit disk of radius 1. An open set is one for which no point of the boundary belongs to the set, for example the unit disk of radius 1 without the outer circle of radius 1.

closed solid disk
$x^2 + y^2 \leq 1$
with boundary



open disk
$x^2 + y^2 < 1$
without
boundary

A set $O \subseteq \mathbb{R}^n$ is *open* iff there is a small neighborhood that is contained in O around every point of O. That is, for all points $a \in O$ there is an $\varepsilon > 0$ such that every point b of distance at most ε from a is still in O. A set $C \subseteq \mathbb{R}^n$ is *closed* iff its complement is open. Because $\mathbb{R}^n$ is what is called a complete metric space, a set $C \subseteq \mathbb{R}^n$ is closed iff every convergent sequence of elements in C converges to a limit in C.

Proposition 5 (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 proof proves a formula by equational differential induction:

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

But the same formula 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 set where $x^2 + y^2 = c^2$ holds true. The only sets that are both open and closed in (the Euclidean space) $\mathbb{R}^n$ are the empty set $\emptyset$ and the full space $\mathbb{R}^n$.

The other parts of the theorem are proved elsewhere [Pla12c]. □

One takeaway message is that it makes sense to check whether the desired invariant is an open or a closed set and use differential invariants of the suitable type for the job. Of course, both $p = 0$ and $p \geq 0$ might still work for closed sets.

9. Differential Invariant Equations as Differential Invariant Inequalities

Weak inequalities $p \geq 0$, however, do subsume the deductive power of equational differential invariants $p = 0$. This is obvious on the algebraic level but we will see that it also does carry over to the differential structure.

Proposition 6 (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 3, we only need to show that $\mathcal{DI}_{=} \leq \mathcal{DI}_{\geq}$, as $\mathcal{DI}_{=,\wedge,\vee} = \mathcal{DI}_{=}$. Let $p = 0$ be an equational differential invariant of a differential equation $x' = \theta \,\&\, H$. Then we can prove the following:

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

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

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

The subgoal for the differential induction step is provable: if we can prove that H implies $(p' = 0)^{\theta}_{x'}$ according to the first sequent proof, then we can also prove that H implies $(-2pp' \geq 0)^{\theta}_{x'}$ for the sequent sequent proof, because $(p' = 0)^{\theta}_{x'}$ implies $(-2pp' \geq 0)^{\theta}_{x'}$ in first-order real arithmetic. □

Note that the local state-based view of differential invariants is crucial to make the last proof work. By Proposition 6, differential invariant search with weak inequalities can suppress equations. Note, however, that the polynomial degree increases quadratically with the reduction in Proposition 6. In particular, the polynomial degree increases quartically when using the reductions in Proposition 3 and Proposition 6 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.

10. Differential Invariant Atoms

Next we see that, with the notable exception of pure equations (Proposition 3), propositional operators increase the deductive power.

Theorem 7 (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:

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

By a sign argument similar to that in the proof of [Pla10a, Theorem 2] and [Pla10b, Theorem 3.3], no atomic formula is equivalent to $x \geq 0 \wedge y \geq 0$. Basically, no formula of the form $p(x, y) \geq 0$ for a polynomial p can be equivalent to $x \geq 0 \wedge y \geq 0$, because that would imply that $p(x, 0) \geq 0 \leftrightarrow x \geq 0$ for all x, which, as $p(x, 0)$ is a univariate polynomial with infinitely many roots (for every $x \geq 0$), which implies that $p(x, 0)$ is the zero polynomial, which is not equivalent to $x \geq 0$, because the zero polynomial is also zero on $x < 0$. Similar arguments work for $p(x, y) > 0$ and $p(x, y) = 0$. Thus, the above property cannot be proven using a single differential induction. The proof for a postcondition $x > 0 \wedge y > 0$ is similar.

The other—quite substantial—parts of the proof are proved elsewhere [Pla12c]. □

Note that the formula in the proof of Theorem 7 is provable, e.g., using differential cuts (DC) with two atomic differential induction steps, one for $x \geq 0$ and one for $y \geq 0$. Yet, a similar, yet much more involved, 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 [Pla10a, Theorem 2].

Consequently, in the case of inequalities, propositional connectives can be quite crucial when looking for differential invariants.

11. Summary

Fig. 2 summarizes the findings on provability relations of differential equations explained in this lecture and others reported in the literature [Pla12c]. We have considered the differential invariance problem, which, by a relative completeness argument [Pla12a], 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. An understanding of these relations helps guide the search for suitable differential invariants and also provides an intuition for exploiting indirect criteria such as open/closedness of sets as a guide.

The results require a symbiosis of elements of logic with real arithmetical, differential, semialgebraic, and geometrical properties. Future work includes investigating this new

field further called *real differential semialgebraic geometry*, whose development has only just begun [Pla12c, GSP14, GSP15].

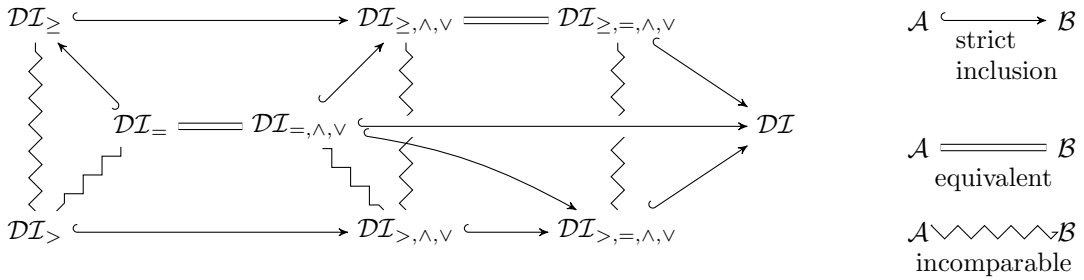


Figure 2: Differential invariance chart
(strict inclusions $\mathcal{A} < \mathcal{B}$, equivalences $\mathcal{A} \equiv \mathcal{B}$, and incomparabilities $\mathcal{A} \not\leq \mathcal{B}$, $\mathcal{B} \not\leq \mathcal{A}$ for classes of differential invariants are indicated)

A. Curves Playing with Norms and Degrees

The proof of Lemma 2 showed a case where a formula with a higher-degree polynomial was needed to prove a property that a lower-degree polynomial could not prove. The conclusion from the proof of Lemma 2 is not that it is always better to use differential invariants of higher degrees, just because that worked in this particular proof.

For example, the following proof for an upper bound t on the supremum norm $\|(x,y)\|_\infty$ of the vector (x,y) defined as

$$\|(x,y)\|_\infty \leq t \overset{\text{def}}{\equiv} -t \leq x \leq t \wedge -t \leq y \leq t \tag{2}$$

is significantly easier for the curved dynamics:

$$\mathbb{R}\ \frac{*}{d^2+e^2 \leq 1 \vdash -1 \leq d \leq 1 \wedge -1 \leq e \leq 1}$$
$$\frac{}{d^2+e^2 \leq 1 \vdash (-t' \leq x' \leq t' \wedge -t' \leq y' \leq t')^{d\ e\ \omega e\ -\omega d\ 1}_{x'\ y'\ d'\ e'\ t'}}$$
$$\text{DI}\ \frac{}{\triangleleft d^2+e^2 \leq 1 \wedge x=y=t=0 \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d,t'=1\,\&\,d^2+e^2\leq 1]\|(x,y)\|_\infty \leq t}$$
$$\text{DC}\ \frac{}{d^2+e^2 \leq 1 \wedge x=y=t=0 \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d,t'=1]\|(x,y)\|_\infty \leq t}$$

where the first premise of the differential cut (DC) above is elided (marked $\triangleleft$) and proves as in Lecture 11 on Differential Invariants & Proofs. This proof shows that a point (x,y) starting with linear velocity at most 1 and angular velocity ω from the origin will not move further than the time t in supremum norm.

This simple proof is to be contrasted with the following proof attempt for a corresponding upper bound on the Euclidean norm $\|(x,y)\|_2$ defined as

$$\|(x,y)\|_2 \leq t \overset{\text{def}}{\equiv} x^2+y^2 \leq t^2 \tag{3}$$

for which a direct proof fails:

not valid

$$\frac{}{d^2+e^2\leq 1 \vdash 2xd+2ye\leq 2t}$$

$$\frac{}{d^2+e^2\leq 1 \vdash (2xx'+2yy'\leq 2tt')^{d\ e\ \omega e\ -\omega d\ 1}_{x'\ y'\ d'\ e'\ t'}}$$

DI $$\frac{}{d^2+e^2\leq 1\wedge x=y=t=0 \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d,t'=1\,\&\,d^2+e^2\leq 1]\|(x,y)\|_2\leq t}$$

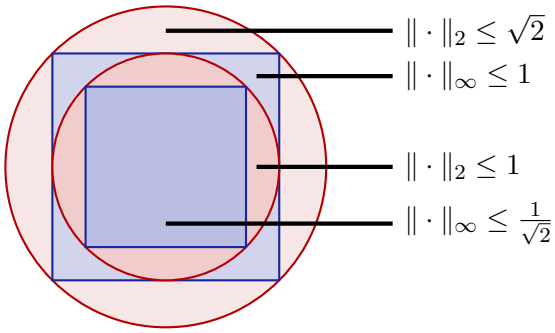
DC $$\frac{}{d^2+e^2\leq 1\wedge x=y=t=0 \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d,t'=1]\|(x,y)\|_2\leq t}$$

An indirect proof is still possible but much more complicated. But the proof using the supremum norm (2) is much easier than the proof using the Euclidean norm (3) in this case. In addition, the arithmetic complexity decreases, because supremum norms are definable in linear arithmetic (2) unlike the quadratic arithmetic required for Euclidean norms (3). Finally, the simpler proof is, up to a factor of $\sqrt{2}$ just as good, because quantifier elimination easily proves that the supremum norm $\|\cdot\|_\infty$ and the standard Euclidean norm $\|\cdot\|_2$ are equivalent, i.e., their values are identical up to constant factors:

$$\forall x\,\forall y\,(\|(x,y)\|_\infty \leq \|(x,y)\|_2 \leq \sqrt{n}\|(x,y)\|_\infty) \tag{4}$$

$$\forall x\,\forall y\,(\frac{1}{\sqrt{n}}\|(x,y)\|_2 \leq \|(x,y)\|_\infty \leq \|(x,y)\|_2) \tag{5}$$

where n is the dimension of the vector space, here 2. That makes sense, because if, e.g., the coordinate with maximal absolute value is at most 1, then the Euclidean distance can be at most 1. And the extra factor of $\sqrt{2}$ is easily justified by Pythagoras' theorem.



Exercises

Exercise 1. Prove the relation $\mathcal{DI}_{>} \leq \mathcal{DI}_{>,\wedge,\vee}$, i.e., that all properties provable using differential invariants of the form $p > q$ are also provable using propositional combinations of these formulas as differential invariants.

Exercise 2. Prove the relation $\mathcal{DI}_{\geq} \equiv \mathcal{DI}_{\leq,\wedge,\vee}$.

Exercise 3. Prove the relation $\mathcal{DI}_{\geq,\wedge,\vee} \equiv \mathcal{DI}_{\geq,=,\wedge,\vee}$.

Exercise 4. Let $\mathcal{DI}_{true}$ denote the proof calculus in which only the formula $true$ is allowed as a differential invariant. Prove the relation $\mathcal{DI}_{true} < \mathcal{DI}_{=}$.

Exercise 5. Let $\mathcal{DI}_{false}$ denote the proof calculus in which only the formula $false$ is allowed as a differential invariant. Prove the relation $\mathcal{DI}_{false} < \mathcal{DI}_{>}$.

Exercise 6. Prove the relation $\mathcal{DI}_{=,\wedge,\vee} < \mathcal{DI}_{\geq,\wedge,\vee}$.

Exercise 7. Prove the relation $\mathcal{DI}_{>,\wedge,\vee} < \mathcal{DI}_{>,=,\wedge,\vee}$.

Exercise 8. Prove the norm relations (4) and (5). Use these relations in a sequent proof to relate the successful proof with a bound on the supremum norm $\|(x,y)\|_\infty$ to a result about a bound on the Euclidean norm $\|(x,y)\|_2$.

References

[GP14] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. In Erika Ábrahám and Klaus Havelund, editors, *TACAS*, volume 8413 of *LNCS*, pages 279–294. Springer, 2014. doi:10.1007/978-3-642-54862-8_19.

[GSP14] Khalil Ghorbal, Andrew Sogokon, and André Platzer. Invariance of conjunctions of polynomial equalities for algebraic differential equations. In Markus Müller-Olm and Helmut Seidl, editors, *SAS*, volume 8723 of *LNCS*, pages 151–167. Springer, 2014. doi:10.1007/978-3-319-10936-7_10.

[GSP15] Khalil Ghorbal, Andrew Sogokon, and André Platzer. A hierarchy of proof rules for checking differential invariance of algebraic sets. In Deepak D'Souza, Akash Lal, and Kim Guldstrand Larsen, editors, *VMCAI*, LNCS. Springer, 2015.

[HMP77] David Harel, Albert R. Meyer, and Vaughan R. Pratt. Computability and completeness in logics of programs (preliminary report). In *STOC*, pages 261–268. ACM, 1977.

[PC08] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008. doi:10.1007/978-3-540-70545-1_17.

[Pla08] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008. doi:10.1007/s10817-008-9103-8.

[Pla10a] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010. doi:10.1093/logcom/exn070.

[Pla10b] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010. doi:10.1007/978-3-642-14509-4.

[Pla12a] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE, 2012. doi:10.1109/LICS.2012.64.

[Pla12b] André Platzer. A differential operator approach to equational differential invariants. In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48. Springer, 2012. doi:10.1007/978-3-642-32347-8_3.

[Pla12c] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012. doi:10.2168/LMCS-8(4:16)2012.