15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Differential Invariants & Proof Theory

André Platzer

Carnegie Mellon University

Lecture 14

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 can never leave 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. 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) to be found. Once a differential invariant has been identified, 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.

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 prove 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. 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 [Pla12b]. In this lecture, we try to strike a balance between comprehensive handling of the subject matter and core intuition. This lecture will mostly focus on the core intuition of the heart of the proofs and leaves a more comprehensive argument and further study for articles [Pla12b]. 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 and can be found elsewhere [Pla12b]. For example, this lecture will not study whether indirect proofs could conclude the same properties. With a more careful analysis [Pla12b], 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 [Pla12b].

Note 1 (Proof theory of differential equations). *The results in this lecture are part of the* proof theory *of differential equations. They are proofs about proofs, because they prove relations between the provability of logical formulas with different (sequent) proof calculi.*

2 Recap

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

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

Note 2 (Proof rules for differential equations)**.**

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

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

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

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

3 Comparative Deductive Study

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 invariant 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 by proof rule $\mathbb{R}$); see [Pla12b]. 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 $\Omega \subseteq \{\geq, >, =, \land, \lor\}$ 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, $\mathcal{DI}_{=,\land,\lor}$ 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

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:

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

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, we assumed a propositionally complete base calculus [Pla12b]. □

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.

5 Differential Invariants & Arithmetic

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 $-5 \leq x \land x \leq 5$ in first-order real arithmetic. Nevertheless, $x^2 \leq 5^2$ is a differential invariant of $x' = -x$ by the following formal proof:

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

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

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

□

When we want to prove 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 $-5 \leq x \land x \leq 5$.

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.

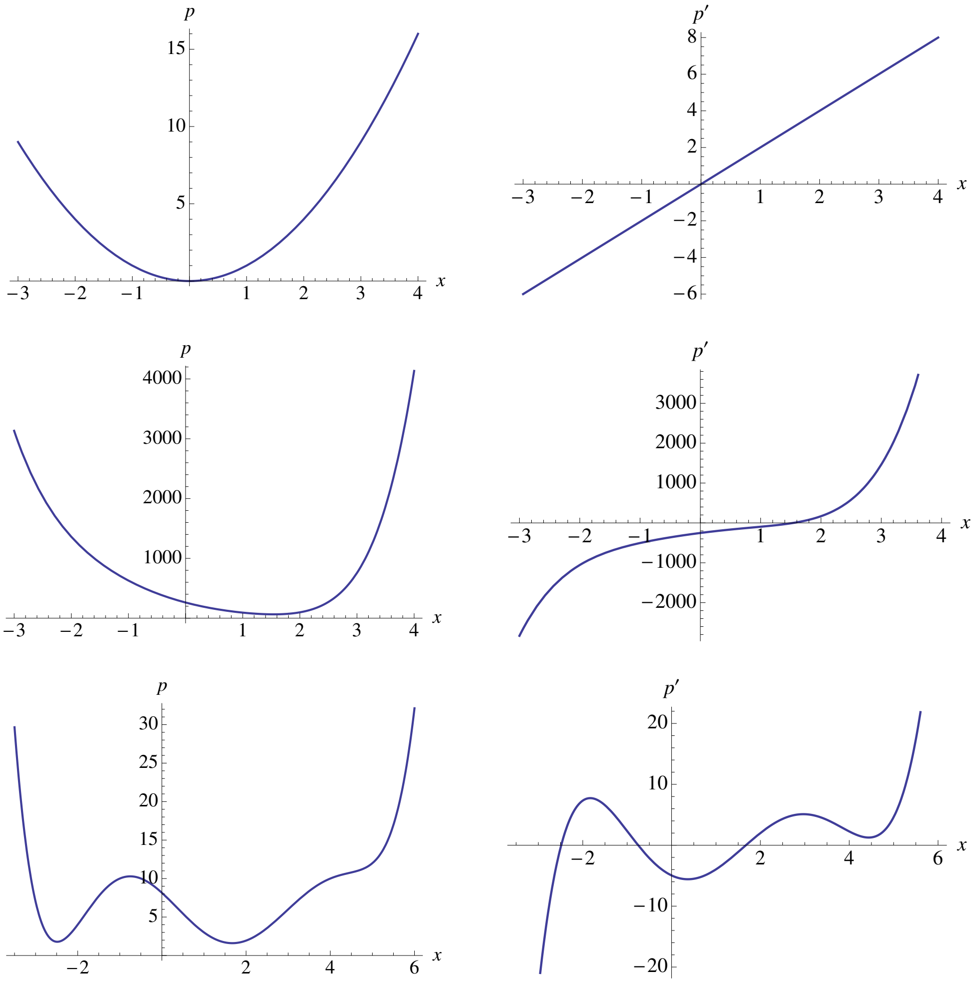

Figure 1: Equivalent solutions ($p \geq 0$ on the left) with different differential structure (p' plotted on the right)

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, a.k.a. differential invariant equations, propositional operators do not add to the deductive power.

Proposition 3 (Equational deductive power [Pla10a, Pla12b])**.** *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:*

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

How could we prove that?

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

One direction is simple. Proving $\mathcal{DI}_{=} \leq \mathcal{DI}_{=,\land,\lor}$ 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 $p_1 = p_2$.

The other way around $\mathcal{DI}_{=} \geq \mathcal{DI}_{=,\land,\lor}$ is more difficult. If a formula can be proved using a differential invariant that is a propositional combination of equations, such as $p_1 = p_2 \land q_1 = q_2$, 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.*

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 $p_1 = p_2 \lor q_1 = q_2$, then F is equivalent to the single equation $(p_1 - p_2)(q_1 - q_2) = 0$. Furthermore, $F'^{\theta}_{x'} \equiv (p_1' = p_2' \land q_1' = q_2')^{\theta}_{x'}$ 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 $p_1 = p_2 \land q_1 = q_2$, then F is equivalent to the single equation $(p_1 - p_2)^2 + (q_1 - q_2)^2 = 0$. Furthermore, $F'^{\theta}_{x'} \equiv \big(p_1' = p_2' \land q_1' = q_2'\big)^{\theta}_{x'}$ 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 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.

7 Equational Incompleteness

Focusing exclusively on differential invariants with equations, however, 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.*

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

How could such a proposition be proved?

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

The proof strategy in 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 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 others 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 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 a counterexample, since it is 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.

By analogy, 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 that is a lot of work, indirect criteria such as cardinality or countability are often used instead, e.g. for proving that the reals $\mathbb{R}$ and rationals $\mathbb{Q}$ do not have the same number of elements, because $\mathbb{Q}$ are countable but $\mathbb{R}$ are not (by Cantor's diagonal argument).

By analogy, 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 a lot of work. So instead, indirect criteria are being used. One proof that 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.

Consequently, 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.*

Proof of Proposition 4. 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 $x \geq 0$:

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

It is not provable with an equational differential invariant. 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 3, the above formula then is not provable with any Boolean combination of equations as differential invariant either.

The other parts of the theorem are proved elsewhere [Pla12b]. □

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 [Pla12b].

8 Strict Differential Invariant Inequalities

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.

Formal definitions of open and closed sets come from real analysis (or topology). Roughly: A closed set is one whose boundary belongs to the set. For example the solid unit disk. An open set is one whose boundary does not belong to the set, for example the unit disk without the circle of radius 1.

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 formula is provable by equational differential induction:

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

But 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 $\mathbb{R}^n$ are $\emptyset$ and $\mathbb{R}^n$.

The other parts of the theorem are proved elsewhere [Pla12b]. □

9 Differential Invariant Equations as Differential Invariant Inequalities

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 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 $\mathcal{DI}_{=} \leq \mathcal{DI}_{\geq}$. Let $p = 0$ be an equational differential invariant of a differential equation $x' = \theta \,\&\, H$. Then we can prove the following:

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

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:

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

The subgoal for the differential induction step is provable: if we can prove that H implies $(p' = 0)_{x'}^{\theta}$, then we can also prove that H implies $(-2pp' \geq 0)_{x'}^{\theta}$, because $(p' = 0)_{x'}^{\theta}$ implies $(-2pp' \geq 0)_{x'}^{\theta}$ 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:

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

By a sign argument similar to that in the proof of [Pla10a, Theorem 2] 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.

The other—quite substantial—parts of the proof are proved elsewhere [Pla12b]. □

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 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].

11 Summary

Fig. 2 summarizes the findings of this lecture and others reported in the literature [Pla12b]. 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.

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

$$\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, hook, squiggly] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, hook, squiggly] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dd, hook, squiggly] \arrow[dr, hook] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] \arrow[dl, hook, squiggly] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook, bend left] \arrow[dr, squiggly] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}$$

Figure 2: Differential invariance chart

Exercises

Exercise 1. Prove the relation $\mathcal{DI}_{>} \leq \mathcal{DI}_{>,\wedge,\vee}$.

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

Exercise 5. Prove the relation $\mathcal{DI}_{>,\wedge,\vee} < \mathcal{DI}_{>,=,\wedge,\vee}$.