André Platzer

Lecture Notes on Foundations of Cyber-Physical Systems

15-424/624/824 Foundations of Cyber-Physical Systems

Chapter 13
Differential Invariants & Proof Theory

Synposis This advanced chapter studies some meta-properties of differential equations proving. It investigates aspects of the proof theory of differential equations, i.e. the theory of proofs about differential equations. While the primary focus in this chapter is on theoretical significance, it also provides insights into the practical questions of what types of differential invariants to search for under which circumstances. The primary tool is the proof-theoretical device of relative deductive power, i.e. the question whether all properties provable with technique $\mathscr{A}$ are also provable with technique $\mathscr{B}$. These results leverage appropriate insights about properties of real arithmetic and of differential equations.

13.1 Introduction

Chapters 10 and 11 equipped us with powerful tools for proving properties of differential equations without having to solve them. *Differential invariants* (dI) [10, 16] 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) [10, 16] made it possible to prove another property C of a differential equation and then change the evolution domain of the dynamics of the system 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 [5, 10, 14]. *Differential weakening* (dW) [10] proves simple properties that are entailed directly by the evolution domain, which becomes especially useful after the evolution domain constraint has been augmented sufficiently by way of a differential cut. *Differential ghosts* (dG) can prove properties by changing the dynamics of the system when adding a new differential equation for a new variable that was not there before. Differential ghosts are useful to, e.g., prove properties of systems with changing energy, where it helps

to relate the change of state in the original system to auxiliary quantities that merely reflect a mathematical value for the sake of the argument, even if it is not part of the original system. In some cases, differential ghosts are crucial for proving properties, because they cannot be proved without them [14].

Just like in the case of loops, where the search for invariants is nontrivial, finding differential invariants also requires considerable smarts (or good automatic procedures [4, 7, 12, 17]) 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 [8]. Likewise, finding invariants and differential invariants is the only fundamental challenge in proving safety properties of hybrid systems [9, 11, 13, 15]. A more delicate analysis even shows that just finding differential invariants is the only fundamental challenge for hybrid systems safety verification [13].

That is reassuring, because we, at least, 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 quite challenging, because cyber-physical systems are extremely challenging. But it is worth the trouble, because CPSs are so important. Fortunately, differential equations also enjoy many pleasant properties that we can exploit to help us find differential invariants.

At the latest after this revelation, we fully realize the importance of studying and understanding differential invariants. So let us subscribe to developing a deeper understanding of differential invariants right away. The part of their understanding that this chapter 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 $\mathscr{A}$ can prove, because differential invariants of the form $\mathscr{B}$ cannot ever succeed in proving them? Or are all properties provable by differential invariants of the form $\mathscr{A}$ also provable by differential invariants of the form $\mathscr{B}$?

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 this chapter besides this theoretical understanding is the practical understanding of developing more intuition about differential invariants and seeing them in action more thoroughly. Some attention during the theoretical proofs will give us a generalizable understanding which cases can or cannot be proved by which shape of differential invariants.

This chapter is based on prior work [14] and strikes a balance between comprehensive handling of the subject matter and core intuition. Many proofs in this chapter are simplified and only prove the core argument, while leaving out other aspects. Those—very important—further details of a comprehensive argument are beyond the scope of this textbook, however, and can be found elsewhere [14]. For example, this chapter will not study whether indirect proofs could conclude the same

[1] Even if it may still be a lot of work to make the proofs work out in practice, at least they become possible.

properties but will focus on the easier base case of direct proofs. With a more thorough analysis [14], it turns out that indirect proofs do not change the results reported in this chapter, but the proofs become significantly more complicated and require a more precise choice of the sequent calculus formulation. In this chapter, we will also not always prove all statements conjectured in a theorem. The remaining proofs can be found in the literature [14].

Note 66 (Proof theory of differential equations) *The results in this chapter 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 the statements "formula P can be proved using $\mathscr{A}$" and "formula P can be proved using $\mathscr{B}$."*

The most important learning goals of this chapter are:

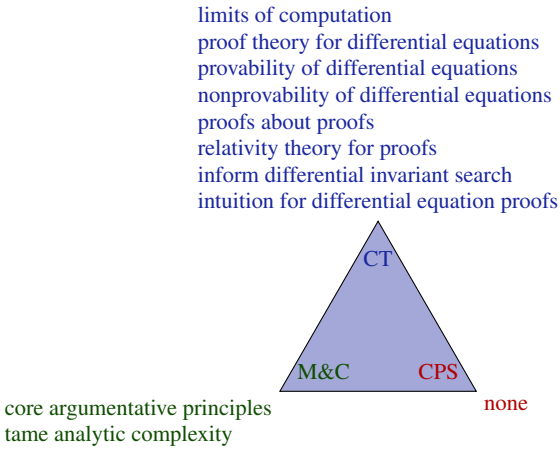
Modeling and Control: This chapter helps in understanding the core argumentative principles behind CPS and sheds more light on the pragmatic question how to tame their analytic complexity.

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). The answer is especially fundamental because it is independent of the model of computation by the Church-Turing thesis [2, 20]. Often times, the most significant understanding of a problem space starts with what cannot be done (the theorem of Rice [19] 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 [3] problem).
The primary purpose of this chapter 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*. Not all aspects of this deep question will be possible to answer in one chapter, 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 for cyber-physical systems: the case of proofs about differential equations.
The primary, scientific learning goals of this chapter 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 differen-

tial invariants prove the same properties and one of them already failed then there is no need to try the other) 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 goal is 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 chapter is to further our understanding of 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. Finally this chapter has beneficial side effects informing differential invariant search and deepening our intuition about differential equations proofs.

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



13.2 Recap

Recall the following proof rules for differential equations from Chaps. 11 and 12:

Note 67 (Proof rules for differential equations)

$$\text{dI}\ \frac{Q \vdash [x':=f(x)](F)'}{F \vdash [x'=f(x)\,\&\,Q]F} \qquad \text{dW}\ \frac{Q \vdash P}{\Gamma \vdash [x'=f(x)\,\&\,Q]P,\Delta}$$

$$\text{dC}\ \frac{\Gamma \vdash [x' = f(x)\,\&\,Q]C, \Delta \quad \Gamma \vdash [x' = f(x)\,\&\,(Q \wedge C)]P, \Delta}{\Gamma \vdash [x' = f(x)\,\&\,Q]P, \Delta}$$

$$\text{dG}\ \frac{\Gamma \vdash \exists y\,[x' = f(x), y' = a(x)\cdot y + b(x)\,\&\,Q]P, \Delta}{\Gamma \vdash [x' = f(x)\,\&\,Q]P, \Delta}$$

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

$$\text{cut,MR}\,\frac{A \vdash F \quad F \vdash [x' = f(x)\,\&\,Q]F \quad F \vdash B}{A \vdash [x' = f(x)\,\&\,Q]B} \tag{13.1}$$

This proof step is useful for replacing a precondition A and a postcondition B by another invariant F that implies postcondition B (third premise) and is implied by precondition A (first premise) and is an invariant (second premise), which will be done frequently in this chapter without further notice.

13.3 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 $e = 0$ with a term e without success and then move on to search for differential invariants of the form $e = k$, then we cannot expect to be any more successful than before, because $e = k$ can be rewritten as $e - k = 0$, which is of the first shape again. So we should, for example, try finding inequational differential invariants of the form $e \geq 0$, instead. In general, this begs the question which generalizations would be silly (because differential invariants of the form $e = k$ cannot prove any more than those of the form $e = 0$) and when it might be smart (because $e \geq 0$ could still succeed even if everything of the form $e = 0$ 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 $\mathscr{A}$, not using differential invariants from the class $\mathscr{B}$, or whether all properties provable with differential invariants from class $\mathscr{A}$ are also provable with class $\mathscr{B}$.

As a basis, we consider a propositional sequent calculus with logical cuts (which simplify glueing derivations together) and real arithmetic (denoted by proof rule $\mathbb{R}$) along the lines of what we say in Chap. 6; see [14] for precise details. By $\mathscr{DI}$ 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) or differential ghosts (rule dG). For a set $\Omega \subseteq \{\geq, >, =, \wedge, \vee\}$ of operators, we denote by $\mathscr{DI}_\Omega$ 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 the set Ω. For example, $\mathscr{DI}_{=,\wedge,\vee}$ is the proof calculus that allows only and/or-combinations of

equations to be used as differential invariants. Likewise, $\mathscr{DI}_{\geq}$ is the proof calculus that only allows atomic weak inequalities $e \geq k$ to be used as differential invariants.

We consider classes of differential invariants and study their relations. If $\mathscr{A}$ and $\mathscr{B}$ are two classes of differential invariants, we write $\mathscr{A} \leq \mathscr{B}$ if all properties provable using differential invariants from $\mathscr{A}$ are also provable using differential invariants from $\mathscr{B}$. We write $\mathscr{A} \not\leq \mathscr{B}$ otherwise, i.e., when there is a valid property that can only be proven using differential invariants of $\mathscr{A} \setminus \mathscr{B}$. We write $\mathscr{A} \equiv \mathscr{B}$ if $\mathscr{A} \leq \mathscr{B}$ and $\mathscr{B} \leq \mathscr{A}$. We write $\mathscr{A} < \mathscr{B}$ if $\mathscr{A} \leq \mathscr{B}$ and $\mathscr{B} \not\leq \mathscr{A}$. Classes $\mathscr{A}$ and $\mathscr{B}$ are incomparable if $\mathscr{A} \not\leq \mathscr{B}$ and $\mathscr{B} \not\leq \mathscr{A}$.

For example, the properties provable by differential invariants of the form $e = 0$ are the same as the properties provable by differential invariants of the form $e = k$. That justifies $\mathscr{DI}_{=} \equiv \mathscr{DI}_{=0}$ when $\mathscr{DI}_{=0}$ denotes the class of properties provable with differential invariants of the form $e = 0$. Trivially, $\mathscr{DI}_{=} \leq \mathscr{DI}_{=,\wedge,\vee}$, because every property provable with differential invariants of the form $e = k$ is also provable with differential invariants that additional are allowed to use conjunctions and disjunctions. Likewise, $\mathscr{DI}_{\geq} \leq \mathscr{DI}_{\geq,\wedge,\vee}$. But the converses are not so clear, because one might suspect that propositional connectives help.

13.4 Equivalences of Differential Invariants

Before we go any further, let us study whether there are straight out 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 of differential equations. 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 13.1 (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 $x' = f(x) \,\&\, Q$ 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 the propositionally equivalent formula G also works. Let F be a differential invariant of a differential equation system $x' = f(x) \,\&\, Q$ 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 $x' = f(x) \,\&\, Q$, because of the following formal proof:

$$\dfrac{\dfrac{\dfrac{*}{Q \vdash [x':=f(x)](G)'}}{G \vdash [x'=f(x)\,\&\,Q]G}}{F \vdash [x'=f(x)\,\&\,Q]F}\;\begin{matrix}[:=]\\ \text{dI}\end{matrix}$$

The bottom proof step is easy to see using (13.1), which follows from rules cut and MR, because precondition F implies the new precondition G and postcondition F is implied by the new postcondition G propositionally. Subgoal $Q \vdash [x':=f(x)](G)'$ is provable, because $Q \vdash [x':=f(x)](F)'$ is provable and $(G)'$ is ultimately a conjunction formed over the differentials of all atomic formulas of G. The set of atoms of G is identical to the set of atoms of F, because atoms do not change by propositional tautologies. Furthermore, dL has a propositionally complete base calculus [14]. □

In all subsequent proofs, we can use propositional equivalence transformations by Lemma 13.1. In the following, we will also implicitly use equivalence reasoning for pre- and postconditions *à la* (13.1) as we have done in Lemma 13.1. Because of Lemma 13.1, we can, without loss of generality, work with arbitrary propositional normal forms for proof search.

13.5 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 13.2 (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 $x' = f(x)\,\&\,Q$ 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:

$$\dfrac{\dfrac{\dfrac{*}{\vdash -2x^2 \leq 0}\,\mathbb{R}}{\vdash [x':=-x]2xx' \leq 0}\,[:=]}{x^2 \leq 5^2 \vdash [x'=-x]x^2 \leq 5^2}\,\text{dI}$$

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

$$\dfrac{\dfrac{\dfrac{}{\text{not valid}}}{\vdash 0 \le -x \land -x \le 0}}{\vdash [x' := -x](0 \le x' \land x' \le 0)}\,[:=]$$
$$\overline{-5 \le x \land x \le 5 \vdash [x' = -x](-5 \le x \land x \le 5)}\,\text{dI}$$

□

For proving the property in the proof of Lemma 13.2 we need to use (13.1) with the differential invariant $F \equiv x^2 \le 5^2$ and cannot use $-5 \le x \land x \le 5$ directly.

By Lemma 13.2, 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, because differential invariance depends on the differential structure. Some equivalence transformations that preserve the set of 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 13.2 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 in cases where they happen to 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 $x^2 \ge 0$ and $x^6 + x^4 - 16x^3 + 97x^2 - 252x + 262 \ge 0$ have the same solutions (all of $\mathbb{R}$), but very different differential structure; see Fig. 13.1.

The first two rows in Fig. 13.1 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. Figure 13.1 illustrates that $(p)'$ alone can already have a very different characteristic even if the respective sets of satisfying assignments of $p \ge 0$ are identical.

We can, however, always normalize all atomic subformulas to have right-hand side 0, that is, of the form $p = 0, p \ge 0$, or $p > 0$. For instance, $p \le q$ is a differential invariant if and only if $q - p \ge 0$ is, because $p \le q$ is equivalent (in first-order real arithmetic) to $q - p \ge 0$. Moreover, for any variable x and term e, $[x' := e](p)' \le (q)'$ is equivalent to $[x' := e](q)' - (p)' \ge 0$ in first-order real arithmetic, because the postcondition $(p)' \le (q)'$ is equivalent to $(q)' - (p)' \ge 0$ in real arithmetic.

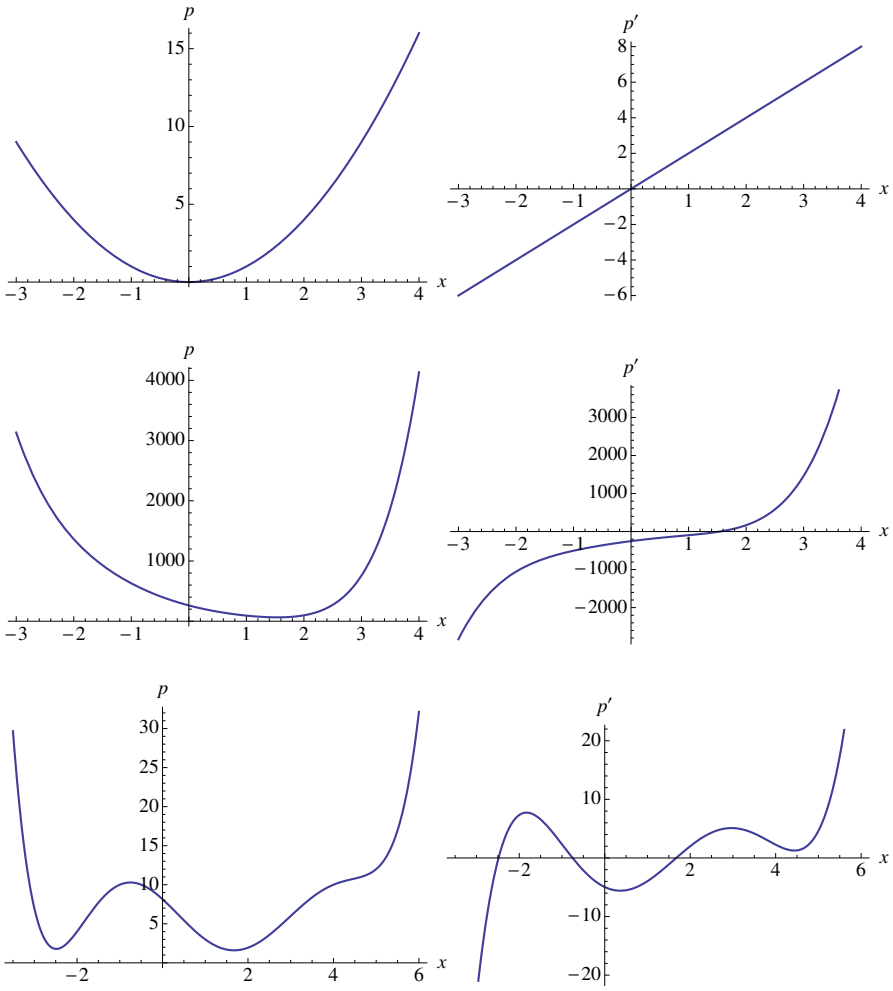


Fig. 13.1 Equivalent solutions ($p \geq 0$ on the left) with quite different differential structure ($(p)'$ plotted on the right)

13.6 Differential Invariant Equations

Of course, we already know that $\mathscr{DI}_{=} \leq \mathscr{DI}_{=,\wedge,\vee}$ by definition, because every property provable without proposal logic in the differential invariants is also provable if we are allowed to use propositional logic. Indeed, for equational differential invariants $e = k$, alias differential invariant equations, propositional operators do not add to the deductive power [10, 14].

Proposition 13.1 (Equational deductive power). *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:*

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

How could we prove this positive statement about provability?

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

One direction is simple. Proving $\mathscr{DI}_{=} \leq \mathscr{DI}_{=,\wedge,\vee}$ is obvious, because every proof using a single differential invariant equation $e_1 = e_2$ also is a proof that is allowed to use a propositional combination of differential invariant equations. The propositional combination that just consists of the only conjunct $e_1 = e_2$ without making use of any of the propositional operators.

The other way around $\mathscr{DI}_{=} \geq \mathscr{DI}_{=,\wedge,\vee}$ is more difficult. If a formula can be proved using a differential invariant that is a propositional combination of equations, such as $e_1 = e_2 \wedge k_1 = k_2$, how could it possibly be proved using just a single equation?

Note 68 (Proofs of equal provability) *A proof of Proposition 13.1 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 13.1 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. At the heart of the arguments, it often involves proof transformations. This explains why proof theory is a meta-theory conducting proofs about proofs: mathematical proofs about formal proofs.

Proof (of Proposition 13.1). Let $x' = f(x)$ 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 13.1 (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 $e_1 = e_2 \vee k_1 = k_2$, then F is equivalent to the single equation $(e_1 - e_2)(k_1 - k_2) = 0$. Furthermore, the formula in the induction step of dI,

$[x':=f(x)](F)' \equiv [x':=f(x)]((e_1)' = (e_2)' \wedge (k_1)' = (k_2)')$ directly implies

$$[x':=f(x)]((e_1-e_2)(k_1-k_2))' = 0$$
$$\equiv [x':=f(x)]\big(((e_1)'-(e_2)')(k_1-k_2)+(e_1-e_2)((k_1)'-(k_2)') = 0\big)$$

which implies that the differential structure is compatible. So, the inductive step for $(e_1-e_2)(k_1-k_2)=0$ will succeed if the inductive step for $e_1=e_2 \vee k_1=k_2$ succeeded. The converse implication does not hold, but also does not have to hold for this proof to work out, because we are merely saying that if the disjunction of equations would have been a differential invariant then the more complex single equation will also be, not vice versa.

- If F is of the form $e_1=e_2 \wedge k_1=k_2$, then F is equivalent to the single equation $(e_1-e_2)^2+(k_1-k_2)^2=0$. Also, the formula in the induction step of rule dI, $[x':=f(x)](F)' \equiv [x':=f(x)]\big((e_1)' = (e_2)' \wedge (k_1)' = (k_2)'\big)$ implies

$$[x':=f(x)]\big(((e_1-e_2)^2+(k_1-k_2)^2)'=0\big)$$
$$\equiv [x':=f(x)]\big(2(e_1-e_2)((e_1)'-(e_2)')+2(k_1-k_2)((k_1)'-(k_2)') = 0\big)$$

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

Observe that the polynomial degree increases quadratically by the reduction in Proposition 13.1, 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. 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 [12].

Equational differential invariants, thus, enjoy a lot of beautiful properties, including characterizing invariant functions [12] and generalizing to a decision procedure for algebraic invariants of algebraic differential equations [4].

13.7 Equational Incompleteness

Despite the fact that Proposition 13.1 confirms how surprisingly expressive single equations are, focusing exclusively on differential invariants with equations reduces the deductive power, because sometimes only differential invariant inequalities can prove properties.

Proposition 13.2 (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.*

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

How could such a proposition with a negative answer about provability be proved?

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

The proof strategy for the proof of Proposition 13.1 involved transforming dL proofs into other dL proofs to prove the inclusion $\mathscr{DI}_{=} \geq \mathscr{DI}_{=,\wedge,\vee}$. Could the same strategy prove Proposition 13.2? No, because we need to show the opposite! Proposition 13.2 conjectures $\mathscr{DI}_{\geq} \not\leq \mathscr{DI}_{=,\wedge,\vee}$, which means that there are true properties that are only provable using a differential invariant inequality $e_1 \geq e_2$ 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 Chap. 11 showed us how useful differential invariants are. But then a proof of Proposition 13.2 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 dL's 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 the more challenging exercises of this textbook. 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 13.2, because a proof of Proposition 13.2 requires us to find a formula that can be proved with $\mathscr{DI}_{\geq}$ (so it cannot have any counterexamples, since it is perfectly valid), just cannot be proved

with $\mathscr{DI}_{=,\wedge,\vee}$. Proving that a valid formula cannot be proved with $\mathscr{DI}_{=,\wedge,\vee}$ requires us to show that all proofs in $\mathscr{DI}_{=,\wedge,\vee}$ do not prove that formula.

Expedition 13.1 (Proving differences in set theory and linear algebra)

Recall what you know about 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 $x \in M, y \in N$ to show that there is a bijection between the sets M and 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 if 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 $\mathbb{Q}$ is countable but $\mathbb{R}$ is not (by Cantor's diagonal argument [1, 18]).

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

Proof (of Proposition 13.2). 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 invariants with the weak inequality $x \geq 0$:

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

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 (Proposition 13.1), 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 $x \geq 0 \rightarrow [x' = a]x \geq 0$.

The other parts of the theorem that involve generalizations of the non-provability argument to other indirect proofs using cuts etc. are proved elsewhere [14]. □

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 [14]. 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.

13.8 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 (nontrivial) closed invariants.

Proposition 13.3 (Strict barrier incompleteness). *The deductive power of differential induction with strict barrier certificates (formulas of the form $e > 0$) is strictly less than the deductive power of general differential induction.*

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

Proof. The following proof proves a formula by equational differential induction:

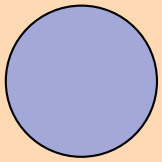
$$\mathbb{R}\,\dfrac{\dfrac{*}{\vdash 2xy + 2y(-x) = 0}}{[:=]\,\dfrac{}{\vdash [x':=y][y':=-x]2xx' + 2yy' = 0}}{\text{dI}\,\dfrac{}{x^2+y^2 = c^2 \vdash [x' = y, y' = -x]x^2 + y^2 = c^2}}$$

But the same formula is not provable with a differential invariant of the form $e > 0$. An invariant of the form $e > 0$ 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 $\emptyset$ (described by the formula *false*) and the full space $\mathbb{R}^n$ (described by the formula *true*), both of which do not prove the property of interest, because *true* does not imply the postcondition and *false* does not hold initially.

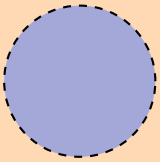
The other parts of the theorem are proved elsewhere [14]. □

Expedition 13.2 (Topology in real analysis)

The following proofs distinguish open sets from closed sets, which are concepts from real analysis (or topology). 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.

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 $e = 0$ and $e \geq 0$ might still work for closed sets.

Beware, however, that openness and closedness depends on the ambient space. One proof in Chap. 12, for example, proved the strict inequality $x > 0$ to be an invariant of the differential equation $x' = -x$ by reducing it to a proof of invariance of the equation $xy^2 = 1$ with an additional differential ghost $y' = \frac{y}{2}$. Seemingly, this proves an open set to be an invariant by using a closed set, but the whole dimension of the state space changes due to the new variable y. And, indeed, the set of all x for which there is a y such that $xy^2 = 1$ is again the open set described by $x > 0$.

13.9 Differential Invariant Equations as Differential Invariant Inequalities

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

Proposition 13.4 (Equational definability). *The deductive power of differential induction with equations is subsumed by the deductive power of differential induction with weak inequalities:*

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

Proof. By Proposition 13.1, we only need to show that $\mathscr{DI}_{=} \leq \mathscr{DI}_{\geq}$, because Proposition 13.1 implies $\mathscr{DI}_{=,\wedge,\vee} = \mathscr{DI}_{=}$. Let $e = 0$ be an equational differential invariant of a differential equation $x' = f(x)\,\&\,Q$. Then we can prove the following:

$$\dfrac{\dfrac{*}{Q \vdash [x' := f(x)](e)' = 0}\,[:=],\mathbb{R}}{e = 0 \vdash [x' = f(x)\,\&\,Q]e = 0}\,\text{dI}$$

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

$$\dfrac{\dfrac{*}{Q \vdash [x' := f(x)] - 2e(e)' \geq 0}\,[:=],\mathbb{R}}{-e^2 \geq 0 \vdash [x' = f(x)\,\&\,Q](-e^2 \geq 0)}\,\text{dI}$$

The subgoal for the differential induction step is provable: if we can prove that Q implies $[x' := f(x)](e)' = 0$ according to the first sequent proof, then we can also prove that Q implies $[x' := f(x)] - 2e(e)' \geq 0$ for the sequent sequent proof, because the postcondition $(e)' = 0$ implies $-2e(e)' \geq 0$ in first-order real arithmetic. □

Note that the differential invariant view of reducing properties of differential equations to differential properties in local states is crucial to make the last proof work. It is obvious that $(e)' = 0$ implies $-2e(e)' \geq 0$ holds in any single state. Without differential invariance arguments, it is harder to relate this to the truth-values of corresponding properties along differential equations. By Proposition 13.4, differential invariant search with weak inequalities can suppress equations. Note, however, that the polynomial degree increases quadratically with the reduction in Proposition 13.4. In particular, the polynomial degree increases quartically when using the reductions in Proposition 13.1 and Proposition 13.4 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.

13.10 Differential Invariant Atoms

Next we see that, with the notable exception of pure equations (Proposition 13.1), propositional operators do increase the deductive power of differential invariants.

Theorem 13.1 (Atomic incompleteness). *The deductive power of differential induction with propositional combinations of inequalities exceeds the deductive power of differential induction with atomic inequalities.*

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

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:

$$\cfrac{\cfrac{\cfrac{*}{\vdash a \geq 0 \wedge y^2 \geq 0}\,\mathbb{R}}{\vdash [x':=a][y':=y^2](x' \geq 0 \wedge y' \geq 0)}\,[:=]}{x \geq 0 \wedge y \geq 0 \vdash [x' = a, y' = y^2](x \geq 0 \wedge y \geq 0)}\,\mathrm{dI}$$

By a sign argument similar to that in the proof of [10, Theorem 2] and [11, 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 [14]. □

Note that the formula in the proof of Theorem 13.1 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, significantly more involved, argument can be made to show that the deductive power of differential induction with atomic formulas (even when using differential cuts) is still strictly less than the deductive power of gen-

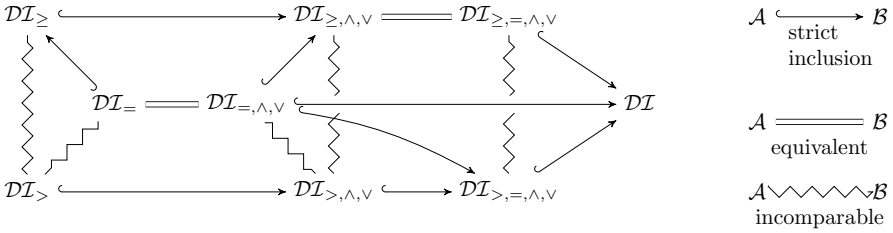
eral differential induction; see [10, Theorem 2]. This just needs another choice of differential equation and a more involved proof.

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

13.11 Summary

Figure 13.2 summarizes the findings on provability relations of differential equations explained in this chapter and others reported in the literature [14]. We have considered the differential invariance problem, which, by a relative completeness argument [9, 13], 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 [5–7, 14].



$\mathcal{DI}_{\Omega}$: properties verifiable using differential invariants built with operators from Ω

Fig. 13.2 Differential invariance chart (strict inclusions $\mathscr{A} < \mathscr{B}$, equivalences $\mathscr{A} \equiv \mathscr{B}$, and incomparabilities $\mathscr{A} \not\leq \mathscr{B}$, $\mathscr{B} \not\leq \mathscr{A}$ for classes of differential invariants are indicated)

13.12 Appendix: Curves Playing with Norms and Degrees

The proof of Lemma 13.2 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 13.2 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

$$\|(x,y)\|_\infty \leq t \stackrel{\text{def}}{\equiv} -t \leq x \leq t \wedge -t \leq y \leq t \tag{13.2}$$

is significantly easier for the curved dynamics:

$$\mathbb{R}\,\frac{*}{v^2+w^2\leq 1 \vdash -1\leq v\leq 1\wedge -1\leq w\leq 1}$$
$$[:=]\,\frac{v^2+w^2\leq 1 \vdash -1\leq v\leq 1\wedge -1\leq w\leq 1}{v^2+w^2\leq 1 \vdash [x':=v][y':=w][v':=\omega w][w':=-\omega v][t':=1](-t'\leq x'\leq t'\wedge -t'\leq y'\leq t')}$$
$$\text{dI}\,\frac{v^2+w^2\leq 1 \vdash [x':=v][y':=w][v':=\omega w][w':=-\omega v][t':=1](-t'\leq x'\leq t'\wedge -t'\leq y'\leq t')}{\lhd v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1\,\&\,v^2+w^2\leq 1]\|(x,y)\|_\infty\leq t}$$
$$\text{dC}\,\frac{\lhd v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1\,\&\,v^2+w^2\leq 1]\|(x,y)\|_\infty\leq t}{v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1]\|(x,y)\|_\infty\leq t}$$

where the first premise of the differential cut (dC) above is elided (marked $\lhd$) and proved as in Example 11.3. 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

$$\|(x,y)\|_2 \leq t \stackrel{\text{def}}{\equiv} x^2+y^2 \leq t^2 \tag{13.3}$$

for which a direct proof fails:

$$\frac{\text{not valid}}{v^2+w^2\leq 1 \vdash 2xv+2yw\leq 2t}$$
$$[:=]\,\frac{v^2+w^2\leq 1 \vdash 2xv+2yw\leq 2t}{v^2+w^2\leq 1 \vdash [x':=v][y':=w][v':=\omega w][w':=-\omega v][t':=1](2xx'+2yy'\leq 2tt')}$$
$$\text{dI}\,\frac{v^2+w^2\leq 1 \vdash [x':=v][y':=w][v':=\omega w][w':=-\omega v][t':=1](2xx'+2yy'\leq 2tt')}{\lhd v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1\,\&\,v^2+w^2\leq 1]\|(x,y)\|_2\leq t}$$
$$\text{dC}\,\frac{\lhd v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1\,\&\,v^2+w^2\leq 1]\|(x,y)\|_2\leq t}{v^2+w^2\leq 1\wedge x=y=t=0 \vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v,t'=1]\|(x,y)\|_2\leq t}$$

An indirect proof is still possible but much more complicated. But the proof using the supremum norm (13.2) is much easier than the proof using the Euclidean norm (13.3) in this case. In addition, the arithmetic complexity decreases, because supremum norms are definable in linear arithmetic (13.2) unlike the quadratic arithmetic required for Euclidean norms (13.3). 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:

$$\forall x\forall y\,(\|(x,y)\|_\infty \leq \|(x,y)\|_2 \leq \sqrt{n}\|(x,y)\|_\infty) \tag{13.4}$$

$$\forall x\forall y\,(\frac{1}{\sqrt{n}}\|(x,y)\|_2 \leq \|(x,y)\|_\infty \leq \|(x,y)\|_2) \tag{13.5}$$

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 Pythago-

ras' theorem. An illustration of the inclusion relationships of the unit discs in the various norms can be found in Fig. 13.3.

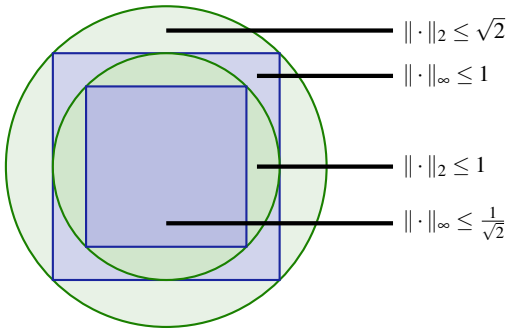


Fig. 13.3 Illustration of p-norm inclusions

Exercises

13.1. Prove the norm relations (13.4) and (13.5). Use these relations in a sequent proof to relate the successful proof with a bound on the supremum norm $\|(x,y)\|_\infty$ to a corresponding result about a bound on the Euclidean norm $\|(x,y)\|_2$.

13.2. Prove the relation $\mathscr{DI}_{>} \leq \mathscr{DI}_{>,\wedge,\vee}$, 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.

13.3. Prove the relation $\mathscr{DI}_{\geq} \equiv \mathscr{DI}_{\leq,\wedge,\vee}$.

13.4. Prove the relation $\mathscr{DI}_{\geq,\wedge,\vee} \equiv \mathscr{DI}_{\geq,=,\wedge,\vee}$.

13.5. Let $\mathscr{DI}_{\mathit{true}}$ denote the proof calculus in which only the formula *true* is allowed as a differential invariant. Prove the relation $\mathscr{DI}_{\mathit{true}} < \mathscr{DI}_{=}$.

13.6. Let $\mathscr{DI}_{\mathit{false}}$ denote the proof calculus in which only the formula *false* is allowed as a differential invariant. Prove the relation $\mathscr{DI}_{\mathit{false}} < \mathscr{DI}_{>}$.

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

13.8. Prove the relation $\mathscr{DI}_{>,\wedge,\vee} < \mathscr{DI}_{>,=,\wedge,\vee}$.

References

1. Cantor, G. Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **1,** 75–78 (1891).

2. Church, A. A Note on the Entscheidungsproblem. *J. Symb. Log.* **1,** 40–41 (1936).
3. Cook, S. A. *The Complexity of Theorem-Proving Procedures* in *STOC* (eds Harrison, M. A., Banerji, R. B. & Ullman, J. D.) (ACM, 1971), 151–158. doi:10.1145/800157.805047.
4. Ghorbal, K. & Platzer, A. *Characterizing Algebraic Invariants by Differential Radical Invariants* in *TACAS* (eds Ábrahám, E. & Havelund, K.) **8413** (Springer, 2014), 279–294. doi:10.1007/978-3-642-54862-8_19.
5. Ghorbal, K., Sogokon, A. & Platzer, A. *Invariance of Conjunctions of Polynomial Equalities for Algebraic Differential Equations* in *SAS* (eds Müller-Olm, M. & Seidl, H.) **8723** (Springer, 2014), 151–167. doi:10.1007/978-3-319-10936-7_10.
6. Ghorbal, K., Sogokon, A. & Platzer, A. *A Hierarchy of Proof Rules for Checking Differential Invariance of Algebraic Sets* in *VMCAI* (eds D'Souza, D., Lal, A. & Larsen, K. G.) **8931** (Springer, 2015), 431–448. doi:10.1007/978-3-662-46081-8_24.
7. Ghorbal, K., Sogokon, A. & Platzer, A. A Hierarchy of Proof Rules for Checking Positive Invariance of Algebraic and Semi-Algebraic Sets. *Computer Languages, Systems & Structures* **47,** 19–43 (2017).
8. Harel, D., Meyer, A. R. & Pratt, V. R. *Computability and Completeness in Logics of Programs (Preliminary Report)* in *STOC* (ACM, 1977), 261–268.
9. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
10. Platzer, A. Differential-Algebraic Dynamic Logic for Differential-Algebraic Programs. *J. Log. Comput.* **20,** 309–352 (2010).
11. Platzer, A. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics* doi:10.1007/978-3-642-14509-4 (Springer, Heidelberg, 2010).
12. Platzer, A. *A Differential Operator Approach to Equational Differential Invariants* in *ITP* (eds Beringer, L. & Felty, A.) **7406** (Springer, 2012), 28–48. doi:10.1007/978-3-642-32347-8_3.
13. Platzer, A. *The Complete Proof Theory of Hybrid Systems* in *LICS* (IEEE, 2012), 541–550. doi:10.1109/LICS.2012.64.
14. Platzer, A. The Structure of Differential Invariants and Differential Cut Elimination. *Log. Meth. Comput. Sci.* **8,** 1–38 (2012).
15. Platzer, A. Differential Game Logic. *ACM Trans. Comput. Log.* **17,** 1:1–1:51 (2015).
16. Platzer, A. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reas.* doi:10.1007/s10817-016-9385-1 (2016).
17. Platzer, A. & Clarke, E. M. Computing Differential Invariants of Hybrid Systems as Fixedpoints. *Form. Methods Syst. Des.* **35.** Special issue for selected papers from CAV'08, 98–120 (2009).
18. Quine, W. V. On Cantor's Theorem. *J. Symb. Log.* **2,** 120–124 (1937).

19. Rice, H. G. Classes of recursively enumerable sets and their decision problems. *Trans. AMS* **74,** 358–366 (1953).
20. Turing, A. M. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society 2* **42,** 230–265 (1937).