Chapter 10
Differential Equations & Differential Invariants

Synopsis This chapter leaves the realm of cyber-physical systems whose differential equations are solvable in closed form. Without closed-form solvable differential equations, the continuous dynamics of cyber-physical systems becomes much more challenging. The change is as noticeable and significant as the change from single-shot control systems to systems with an unbounded number of interactions in a control loop. All of a sudden, we can no longer pretend each differential equation could be replaced by an explicit representation of a function that describes the resulting state at time t along with a quantifier for t. Instead, differential equations have to be handled implicitly based on their actual dynamics as opposed to their solution. This leads to a remarkable shift in perspective opening up a new world of fascination in the continuous dynamical aspects of cyber-physical systems, and it begins by ascribing an entirely new meaning to primes in cyber-physical system models.

10.1 Introduction

So far, this textbook explored only one way to deal with differential equations: the $[']$ axiom schema from Lemma 5.3. Just like almost all other axioms, this axiom $[']$ is an equivalence, so it can be used to reduce a property of a more complex HP, in this case a differential equation, to a structurally easier logical formula.

$$[']\quad [x' = f(x)]p(x) \leftrightarrow \forall t{\geq}0\,[x := y(t)]p(x) \qquad (y'(t) = f(y))$$

However, in order to use the $[']$ axiom for a differential equation $x' = f(x)$, we must first find a symbolic solution to the symbolic initial value problem (i.e., a function $y(t)$ such that $y'(t) = f(y)$ and $y(0) = x$). But what if the differential equation does not have such an explicit closed-form solution $y(t)$? Or what if $y(t)$ cannot be written down in first-order real arithmetic? Chapter 2 allows many more differential equations to be part of CPS models than just the ones that happen to have simple solutions. These are the differential equations we will look at in this chapter

A. Platzer, *Logical Foundations of Cyber-Physical Systems*,
https://doi.org/10.1007/978-3-319-63588-0_10

to provide rigorous reasoning techniques for them. In fact, the rigorous proofs for differential equations that this part of the textbook explores even simplify proofs of solvable differential equations and will ultimately make the solution axiom schema $[']$ superfluous.

You may have previously seen a whole range of methods for solving differential equations. These are indubitably useful for many common cases. But, in a certain sense, "most" differential equations are impossible to solve, because they have no explicit closed-form solution with elementary functions, for instance [18]:

$$x''(t) = e^{t^2}$$

Even if they do have solutions, the solution may no longer be in first-order real arithmetic. Example 2.5 showed that, for certain initial values, the solution of

$$x' = y, y' = -x$$

is $x(t) = \sin(t), y(t) = \cos(t)$, which is not expressible in real arithmetic (recall that both are infinite power series) and leads to undecidable arithmetic [6]. The sine function, for example, needs infinitely many powers, which does not give a finite term in first-order real arithmetic:

$$\sin(t) = t - \frac{t^3}{3!} + \frac{t^5}{5!} - \frac{t^7}{7!} + \frac{t^9}{9!} - \dots$$

This chapter reinvestigates differential equations from a more fundamental perspective, which will lead to a way of proving properties of differential equations without using their solutions. It seeks unexpected analogies among the seemingly significantly different dynamical aspects of discrete dynamics and of continuous dynamics. The first and quite influential observation is that differential equations and loops have more in common than one might suspect.[1] Discrete systems may be complicated, but have a powerful ally: induction as a way of establishing truth for discrete dynamical systems by generically analyzing the one step that it performs (repeatedly like the body of a loop). What if we could use induction for differential equations? What if we could prove properties of differential equations directly by analyzing how these properties change along the differential equation rather than having to find a global solution first and inspecting whether it satisfies that property at all times? What if we could tame the analytic complexity of differential equations by analyzing the generic local "step" that a continuous dynamical system performs (repeatedly). The biggest conceptual challenge will, of course, be in understanding what exactly the counterpart of a step even is for continuous dynamical systems, because there is no such thing as a next step for a differential equation that evolves in continuous time.

This chapter is of central significance for the Foundations of Cyber-Physical Systems. The analytic principles begun in this chapter will be a crucial basis for analyzing all complex CPSs. The most important learning goals of this chapter are:

[1] In fact, discrete and continuous dynamics turn out to be proof-theoretically quite related [12].

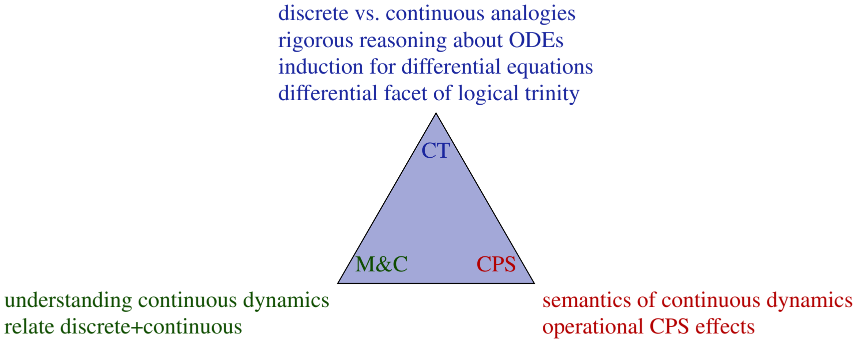
Modeling and Control: This chapter will advance the core principles behind CPS by developing a deeper understanding of their continuous dynamical behavior. This chapter will also illuminate another facet of how discrete and continuous systems relate to one another, which ultimately leads to a fascinating view on understanding hybrid systems [12].

Computational Thinking: This chapter exploits the computational thinking principles in their purest form by seeking and exploiting surprising analogies between discrete dynamics and continuous dynamics, however different the two may appear at first sight. This chapter is devoted to rigorous reasoning about the differential equations in CPS models. Such rigorous reasoning is crucial for understanding the continuous behavior that CPSs exhibit over time. Without sufficient rigor in their analysis it can be impossible to understand their intricate behavior and spot subtle flaws in their control or say for sure whether and why a design is no longer faulty. This chapter systematically develops one reasoning principle for equational properties of differential equations that is based on *induction for differential equations* [8, 13]. It follows an axiomatic logical understanding of differential invariants via differential forms [14]. Subsequent chapters expand the same core principles developed in this chapter to the study of general invariant properties of differential equations. This chapter continues the *axiomatization* of differential dynamic logic dL [11, 12] pursued since Chap. 5 and lifts dL's proof techniques to systems with more complex differential equations. The concepts developed in this chapter form the differential facet illustrating the more general relation of *syntax* (which is notation), *semantics* (which carries meaning), and *axiomatics* (which internalizes semantic relations into universal syntactic transformations). These concepts and their relations jointly form the significant *logical trinity* of syntax, semantics, and axiomatics. This chapter studies the differential facet of this logical trinity. Finally, the verification techniques developed in this chapter are critical for verifying CPS models of appropriate scale and technical complexity.

CPS Skills: We will develop a deeper understanding of the semantics of the continuous dynamical aspects of CPS models and develop and exploit a significantly better intuition for the operational effects involved in CPS. In addition to exhibiting semantic nuances, this understanding is critical to rigorous reasoning for all but the most elementary cyber-physical systems.

10.2 A Gradual Introduction to Differential Invariants

This section provides a gradual development of the intuition behind differential invariants. Such an incremental development is useful to understand the working principles and to understand why differential invariants work the way they do. It can also support our intuition when designing systems or proofs for them.


discrete vs. continuous analogies
rigorous reasoning about ODEs
induction for differential equations
differential facet of logical trinity
CT
M&C
CPS
understanding continuous dynamics
relate discrete+continuous
semantics of continuous dynamics
operational CPS effects

10.2.1 Global Descriptive Power of Local Differential Equations

Differential equations let the physics evolve continuously, possibly for longer periods of time. They describe such global behavior locally, however, just by the right-hand side of the differential equation.

Note 54 (Local descriptions of global behavior by differential equations) The key principle behind the descriptive power of differential equations is that they describe the evolution of a continuous system over time using only a local description of the direction in which the system evolves at any point in space. The solution of a differential equation is a global description of how the system evolves. The differential equation itself is a local characterization. While the global behavior of a continuous system can be subtle, complex, and challenging, its local description as a differential equation is much simpler. This difference between local description and global behavior, which is fundamental to the descriptive power of differential equations, can be exploited for proofs.

Recall the semantics of differential equations from Chap. 3:

Definition 3.3 (Transition semantics of ODEs).

$$[\![x' = f(x) \,\&\, Q]\!] = \big\{(\omega,\nu) : \varphi(0) = \omega \text{ except at } x' \text{ and } \varphi(r) = \nu \text{ for a solution}$$
$$\varphi{:}[0,r] \to \mathscr{S} \text{ of any duration } r \text{ satisfying } \varphi \models x' = f(x) \land Q\big\}$$

where $\varphi \models x' = f(x) \land Q$, iff for all times $0 \le z \le r$: $\varphi(z) \in [\![x' = f(x) \land Q]\!]$ with $\varphi(z)(x') \stackrel{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$ and $\varphi(z) = \varphi(0)$ except at x, x'.

The solution φ describes the global behavior of the system, which is specified locally by the right-hand side $f(x)$ of the differential equation $x' = f(x)$.

Chap. 2 has shown a number of examples illustrating the descriptive power of differential equations, that is, examples in which the solution was very complicated even though the differential equation was rather simple. This is a strong property of differential equations: they can describe even complicated processes in simple ways. However, this representational advantage of differential equations does not carry over into the verification when verification is stuck with proving properties of differential equations only by way of their solutions, which, by the very nature of differential equations, are more complicated again.

This chapter, thus, investigates ways of proving properties of differential equations using the differential equations themselves, not their solutions. This leads to *differential invariants* [8, 13, 14], which can perform induction for differential equations just based on their local dynamics. In fact, loops and differential equations have a lot more in common [12] than meets the eye (Sect. 10.8.1).

10.2.2 Intuition for Differential Invariants

Just as inductive invariants are the premier technique for proving properties of loops, differential invariants [7–9, 13, 14] provide the primary inductive technique we use for proving properties of differential equations (without having to solve them). Recall the loop induction proof rule from Sect. 7.3.3

$$\text{loop}\ \frac{\Gamma \vdash F, \Delta \quad F \vdash [\alpha]F \quad F \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

The core principle behind loop induction is that the induction step for proving $[\alpha^*]P$ investigates the loop body as the local generator α and shows that it never changes the truth-value of the invariant F (see the middle premise $F \vdash [\alpha]F$ of proof rule loop from Sect. 7.3.3 or the only premise of the core essentials induction proof rule ind from Sect. 7.3.2). Let us try to establish the same inductive principle, just for differential equations. The first and third premise of the loop rule transfer easily to differential equations. The challenge is to figure out what the counterpart of the induction step $F \vdash [\alpha]F$ would be since, unlike loops, differential equations do not have a notion of "one step."

What does the local generator of a differential equation $x' = f(x)$ tell us about the evolution of a system? And how does it relate to the truth of a formula F all along the solution of that differential equation? That is, to the truth of the dL formula $[x' = f(x)]F$ expressing that all runs of $x' = f(x)$ lead to states satisfying F. Figure 10.1 depicts an example of a vector field for a differential equation (plotting the right-hand side of the differential equation as a vector at every point in the state space), a global solution (in red), and an unsafe region $\neg F$ (shown in blue). The safe region F is the complement of the blue unsafe region $\neg F$. Of course, it is quite impossible to draw the appropriate direction vector of the differential equation at literally every point in the state space in Fig. 10.1, so we have to settle for a few.

One way of proving that $[x' = f(x)]F$ is true in a state ω would be to compute the solution from that state ω, and check every point in time along the solution to

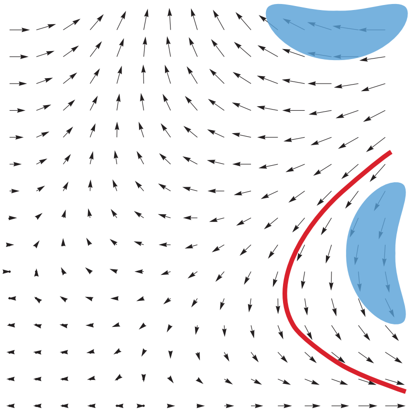


Fig. 10.1 Vector field and one solution of a differential equation that does not enter the blue unsafe regions

see whether it is in the safe region F or the unsafe region $\neg F$. Unfortunately, there are uncountably infinitely many points in time to check. Furthermore, that only considers a single initial state ω, so proving validity of a formula would require considering all of the uncountably infinitely many possible initial states and computing and following a solution in each of them. That is why this naïve approach does not compute.

A similar idea can still be made to work when the symbolic initial-value problem can be solved with a symbolic initial value x and a quantifier for time can be used, which is what the solution axiom $[']$ does. Yet, even that only works when a solution to the symbolic initial-value problem can be computed and the arithmetic resulting from the quantifier for time can be decided. For polynomial solutions, this works by Tarski's quantifier elimination (Sect. 6.5). But polynomial solutions come from very simple systems only (the nilpotent linear differential equation systems from Sect. 2.9.3).

Reexamining the illustration in Fig. 10.1, we suggest an entirely different way of checking whether the system could ever lead to an unsafe state in $\neg F$ when following the differential equation $x' = f(x)$. The intuition is the following. If there were a vector in Fig. 10.1 that pointed from a safe state in F to an unsafe state $\neg F$ (in the blue region), then following the differential equation along that vector would get the system into the unsafe region $\neg F$. If, instead, all vectors only pointed from safe states to safe states in F, then, intuitively, following such a chain of vectors would only lead from safe states to safe states. So if the system also started in a safe state, it would stay safe forever. In fact, this also illustrates that we have some leeway in how we show $[x' = f(x)]F$. We do not need to know where exactly the system evolves to, just that it remains somewhere in F.

Let us make this intuition rigorous to obtain a sound proof principle that is perfectly reliable in order to be usable in CPS verification. What we need to do is to find a way of characterizing how the truth of F changes when moving along the differential equation. That will then enable us to show that the system only evolves in directions in which the formula F stays true.

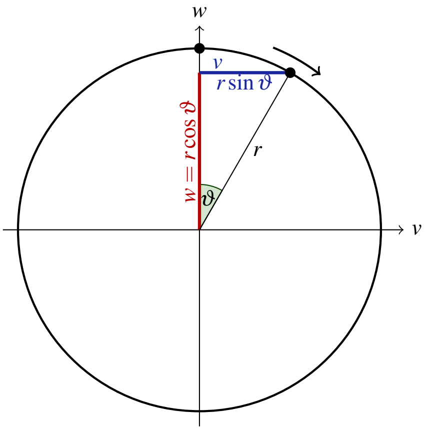


Fig. 10.2 One scenario for the rotational dynamics and relationship of direction vector (v,w) to radius r and angle ϑ

10.2.3 Deriving Differential Invariants

How can the intuition about directions of evolution of a logical formula F with respect to differential equation $x' = f(x)$ be made rigorous? Let's develop step by step.

Example 10.1 (Rotational dynamics). As a guiding example, consider a conjecture about the rotational dynamics from Example 2.5 where v and w represent the coordinates of a direction vector rotating clockwise in a circle of radius r (Fig. 10.2):

$$v^2 + w^2 = r^2 \rightarrow [v' = w, w' = -v]\, v^2 + w^2 = r^2 \tag{10.1}$$

The conjectured dL formula (10.1) is valid, because, indeed, if the vector (v,w) is initially at distance r from the origin (0,0), then it will always remain at that distance when rotating around the origin, which is what the dynamics does. That is, the point (v,w) will always remain on the circle of radius r. But how can we prove that? In this particular case, we could possibly investigate solutions, which are trigonometric functions (although the solutions indicated in Fig. 10.2 are not at all the only solutions). With those solutions, we could perhaps find an argument why they stay at distance r from the origin. But the resulting arithmetic will involve power series, which makes it unnecessarily difficult. The argument for why the simple dL formula (10.1) is valid should be an easy one. And it is, after we have discovered the right proof principle as this chapter will do.

First, what is the direction in which a continuous dynamical system evolves? The direction is exactly described by the differential equation, because the whole point of a differential equation is to describe in which direction the state evolves at every point in space. So the direction which a continuous system obeying $x' = f(x)$ follows from state ω is described by the time-derivative, which is exactly the value $\omega[\![f(x)]\!]$ of term $f(x)$ in state ω. Recall that the term $f(x)$ can mention x and other variables so its value $\omega[\![f(x)]\!]$ depends on the present state ω.

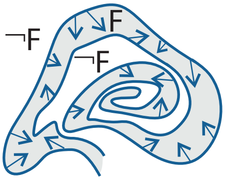


Fig. 10.3 Differential invariant F remains true in the direction of the dynamics

Note 55 ("Formulas that remain true in the direction of the dynamics") Proving dL formula $[x' = f(x)]F$ does not really require us to answer where exactly the system evolves to but just how the evolution of the system relates to the formula F and the set of states ω in which F evaluates to *true*. It is enough to show that the system only evolves in directions in which formula F will stay *true* (Fig. 10.3).

A logical formula F is ultimately built from atomic formulas that are comparisons of (polynomial or rational) terms such as $e = 5$ or $v^2 + w^2 = r^2$. Let e denote such a (polynomial) term in the variable (vector) x that occurs in the formula F. The semantics of a polynomial term e in a state ω is the real number $\omega[\![e]\!]$ to which it evaluates. In which direction does the value of e evolve when following the differential equation $x' = f(x)$ for some time? That depends both on the term e that is being evaluated and on the differential equation $x' = f(x)$ that describes how the respective variables x evolve over time.

Note 56 (Directions) Directions of evolutions are described by derivatives. After all, the differential equation $x' = f(x)$ states that the time-derivative of x is $f(x)$.

To find out how the value of a term changes, let's differentiate the term of interest and see what that tells us about how its value evolves over time. Wait, what do the resulting derivatives actually mean? That is a crucial question, but let us, nevertheless, take the inexcusable liberty of postponing this question till later and just develop a first intuition for now.

Example 10.2 (Differentiating terms in rotational dynamics). Which of the terms should be differentiated when trying to understand how the truth-value of the postcondition in (10.1) changes? Since that is not necessarily clear so far, let's rewrite formula (10.1) and consider the following equivalent (Exercise 10.2) dL formula, which only has a single interesting term to worry about:

$$v^2 + w^2 - r^2 = 0 \rightarrow [v' = w, w' = -v]\, v^2 + w^2 - r^2 = 0 \tag{10.2}$$

Differentiating the only relevant term $v^2 + w^2 - r^2$ in the postcondition of (10.2) gives

$$(v^2 + w^2 - r^2)' = 2vv' + 2ww' - 2rr' \tag{10.3}$$

Of course, differentiating $v^2 + w^2 - r^2$ does not just result in $2v + 2w - 2r$, because its value also depends on how the variables themselves change so on the derivative v' of v, etc. If only we knew what the symbols v', w', and r' mean in (10.3). The differential equation of (10.2) seems to indicate that v' equals w and w' equals $-v$. Would it be okay to replace the left-hand side w' of the differential equation with its right-hand side $-v$ in (10.3)? That would lead to

$$2vv' + 2ww' - 2rr' = 2vw + 2w(-v) - 2rr' \tag{10.4}$$

which clearly would be 0 if only r' were 0. Well, maybe we could consider r' to be 0, since r does not come with a differential equation, so r is not supposed to change, which is what the differential equation $r' = 0$ would tell us, too.

Lo and behold! This might lead to a possible proof because $2vw + 2w(-v)$ is indeed 0. We just do not know whether it is a proof yet. What proof rules should we have applied to prove (10.2)? Why are they sound proof rules? Was it okay to substitute the right-hand side of the differential equation for its left-hand side in (10.4)? Can we differentiate terms to find out how they change over time? What do the respective primed symbols v', w', r' mean? What is the meaning of the operator $(\cdot)'$ that we used on the term $v^2 + w^2 - r^2$ in (10.3)? How do we know that this operator makes the two sides of (10.3) equal? Or maybe even: do differential equations mind being substituted in?

These are a bunch of important questions on the road to turning the intuition of Example 10.2 into sound proof principles. Let's answer them one at a time.

10.3 Differentials

In order to clarify the intuition we followed for motivating differential invariant reasoning, we first add x' and $(e)'$ officially to the syntax since we used them in our reasoning in Example 10.2. The second step is to define their meaning. And the third step of the logical trinity is to develop axioms that can be proved sound with respect to the semantics and that enable correct syntactic reasoning about such primes.

10.3.1 Syntax of Differentials

The first step for understanding reasoning with differentiation is to ennoble the primes of x' and $(e)'$ and officially consider them as part of the language of differential dynamic logic by adding them to its syntax. For every variable x add a corresponding *differential symbol* x' that can be used like any other variable, but, in a differential equation $x' = f(x)$, of course, x' serves the special purpose of denoting the time-derivative of its associated variable x. For every term e, add the *differential term* $(e)'$. Formally, both really should have been part of differential dynamic logic all along, but our understanding only caught up with that fact in this chapter. Besides, it was easier to first suppress these primes and exclusively have them in differential equations in Part I.

Definition 10.1 (dL Terms). A *term e* of *(differential-form) differential dynamic logic* is defined by the grammar (where $e,\tilde{e}$ are terms, x is a variable with corresponding differential symbol x', and c a rational number constant):

$$e ::= x \mid x' \mid c \mid e+\tilde{e} \mid e-\tilde{e} \mid e\cdot\tilde{e} \mid e/\tilde{e} \mid (e)'$$

For emphasis, when primes are allowed, the logic is also called *differential-form* differential dynamic logic [14], but we will continue to just call it differential dynamic logic. The formulas and hybrid programs of (differential-form) differential dynamic logic are built as in Sects. 3.3 and 4.4. The semantics remains unchanged except that the new additions of differential terms $(e)'$ and differential symbols x' need to be outfitted with a proper meaning.

It is, of course, important to take care that division $e/\tilde{e}$ only makes sense in a context where the divisor $\tilde{e}$ is guaranteed not to be zero in order to avoid undefinedness. *We only allow division to be used in a context where the divisor is ensured not to be zero!*

10.3.2 Semantics of Differential Symbols

The meaning of a variable symbol x is defined by the state ω as $\omega(x)$, so its value $\omega[\![x]\!]$ in state ω is directly looked up from the state via $\omega[\![x]\!] = \omega(x)$. It is crucial to understand the significant subtleties and substantial challenges that arise when trying to give meaning to a differential symbol x' or anything else with a derivative connotation such as the differential term $(e)'$ of term e. The meaning of term e in state ω is $\omega[\![e]\!]$ and, thus, the meaning of the differential term $(e)'$ in state ω is written $\omega[\![(e)']\!]$. But now that we know how it's written, how is $\omega[\![(e)']\!]$ defined?

The first mathematical reflex may be to set out for a definition of x' and $(e)'$ in terms of a time-derivative $\frac{\mathrm{d}}{\mathrm{d}t}$ of something. But there is no time and, thus, no time-derivative in an isolated state ω. We cannot possibly define something like

$$\omega[\![(e)']\!] \overset{???}{=} \frac{\mathrm{d}\omega[\![e]\!]}{\mathrm{d}t}$$

because time t does not even occur anywhere on the right-hand side. In fact, it is entirely meaningless to ask for the rate of change of the value of anything over time in a single isolated state ω! For time-derivatives to make sense, we at least need a concept of time and the values understood as a function of time. That function needs to be defined on a big enough interval for derivatives to have a chance to become meaningful. And the function needs to be differentiable so that the time-derivatives even exist to begin with. In the presence of discrete state change, not every value will always have a time-derivative even if we were to keep its history around. None of this is the case when we try to define what the value $\omega[\![(e)']\!]$ of the syntactic term $(e)'$ would be in the state ω.

The next mathematical reflex may be to say that the meaning of x' and $(e)'$ depends on the differential equation. But the meaning of $(e)'$ in state ω is $\omega[\![(e)']\!]$, so there simply is no differential equation to speak of. Nothing can have a meaning that depends on something else outside, because that violates all principles of denotational semantics. Notice how useful it is that the principles of logic prompted us to be precise about the definition $\omega[\![(e)']\!]$ of the meaning of $(e)'$. Without the help of the mathematical rigor of logic, we might have just fallen for innocently writing down some primes and differential operators, and ultimately would have woken up surprised if this led us to "conclude" something that is not actually true.

While neither time-derivatives nor differential equations can come to the rescue to give x' or $(e)'$ a meaning, it is important to understand why the lack of having a value and a meaning would cause complications for the fabrics of logic. Denotational semantics defines the meaning of all expressions compositionally in a modular fashion and without reference to outside elements, such as the differential equation in which they also happen to occur. The meaning of terms is a function of the state, and not a function of the state and the context or purpose for which it happens to have been mentioned at the moment.

The mystery of giving meaning to differential symbols is resolved by declaring the state to be responsible for assigning a value not just to all variables $x \in \mathscr{V}$ but also to all differential symbols $x' \in \mathscr{V}'$. A *state* ω is a mapping $\omega : \mathscr{V} \cup \mathscr{V}' \to \mathbb{R}$ assigning a real number $\omega(x) \in \mathbb{R}$ to each variable $x \in \mathscr{V}$ and also a real number $\omega(x') \in \mathbb{R}$ to each differential symbol $x' \in \mathscr{V}'$. For example, when $\omega(v) = 1/2, \omega(w) = \sqrt{3}/2, \omega(r) = 5$ and $\omega(v') = \sqrt{3}/2, \omega(w') = -1/2, \omega(r') = 0$ the term $2vv' + 2ww' - 2rr'$ evaluates to

$$\omega[\![2vv' + 2ww' - 2rr']\!] = 2\omega(v) \cdot \omega(v') + 2\omega(w) \cdot \omega(w') - 2\omega(r) \cdot \omega(r') = 0$$

A differential symbol x' can have any arbitrary real value in a state ω. Along the solution $\varphi : [0,r] \to \mathscr{S}$ of a differential equation, however, we know precisely what value x' has. Or at least we do, if its duration r is nonzero so that we are not just talking about an isolated point $\varphi(0)$ again. At any point in time $z \in [0,r]$ along such a continuous evolution φ, the differential symbol x' has the same value as the time-derivative $\frac{\mathrm{d}}{\mathrm{d}t}$ of the value $\varphi(t)(x)$ of x over time t at the specific time z [8, 11, 14], because that is what we needed to make sense of the equation $x' = f(x)$.

Definition 3.3 (Transition semantics of ODEs).

$$[\![x' = f(x) \,\&\, Q]\!] = \big\{(\omega, \nu) : \varphi(0) = \omega \text{ except at } x' \text{ and } \varphi(r) = \nu \text{ for a solution } \varphi{:}[0,r] \to \mathscr{S} \text{ of any duration } r \text{ satisfying } \varphi \models x' = f(x) \wedge Q\big\}$$

where $\varphi \models x' = f(x) \wedge Q$, iff for all times $0 \le z \le r$: $\varphi(z) \in [\![x' = f(x) \wedge Q]\!]$ with $\varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$ and $\varphi(z) = \varphi(0)$ except at x, x'.

The value of differential symbol x' at time $z \in [0,r]$ along a solution $\varphi : [0,r] \to \mathscr{S}$ of a differential equation $x' = f(x) \,\&\, Q$ is equal to the analytic time-derivative at z:

Expedition 10.1 (Denotational semantics)

The whole paradigm of *denotational semantics*, initiated for programming languages by Dana Scott and Christopher Strachey [16], is based on the principle that the semantics of an expression of a programming language should be the mathematical object that it denotes. That is, a denotational semantics is a function assigning a mathematical object $\omega[\![e]\!]$ from a semantic domain (here $\mathbb{R}$) to each term e, depending on the state ω.

The *meaning of terms*, thus, is a function $[\![\cdot]\!] : \mathrm{Trm} \to (\mathscr{S} \to \mathbb{R})$ that maps each term $e \in \mathrm{Trm}$ to the function $[\![e]\!] : \mathscr{S} \to \mathbb{R}$ giving the real value $\omega[\![e]\!] \in \mathbb{R}$ that the term e has in each state $\omega \in \mathscr{S}$. In fact, this is exactly how the semantics of terms of dL has been defined in Chap. 2 in the first place. For classical logics such as first-order logic, this denotational semantics has always been the natural and dominant approach since Gottlob Frege [1].

Scott and Strachey [16], however, pioneered the idea of leveraging the denotational style of semantics to give meaning to programming languages. And, indeed, dL's hybrid programs have a denotational semantics. The meaning of an HP α is the reachability relation $[\![\alpha]\!] \subseteq \mathscr{S} \times \mathscr{S}$ that it induces on the states $\mathscr{S}$. Correspondingly, the (denotational) *meaning of hybrid programs* as defined in Chap. 3 is a function $[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S})$ assigning a relation $[\![\alpha]\!] \subseteq \mathscr{S} \times \mathscr{S}$ in the powerset $\wp(\mathscr{S} \times \mathscr{S})$ of the product $\mathscr{S} \times \mathscr{S}$ to each HP α.

A crucial feature of denotational semantics, however, is *compositionality*. The meaning $[\![e + \tilde{e}]\!]$ of a compound such as $e + \tilde{e}$ should be a simple function of the meanings $[\![e]\!]$ and $[\![\tilde{e}]\!]$ of its pieces e and $\tilde{e}$. This compositionality is exactly the way the meaning of differential dynamic logic is defined. For example,

$$\omega[\![e + \tilde{e}]\!] = \omega[\![e]\!] + \omega[\![\tilde{e}]\!] \quad \text{for all states } \omega$$

With a point-wise understanding of $+$, this can be summarized as

$$[\![e + \tilde{e}]\!] = [\![e]\!] + [\![\tilde{e}]\!]$$

$$\varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z) \tag{10.5}$$

Intuitively, the value $\varphi(z)(x')$ of x' is, thus, determined by considering how the value $\varphi(z)(x)$ of x changes along the solution φ when we change time z "only a little bit." Visually, it corresponds to the slope of the tangent of the value of x at time z; see Fig. 10.4. A subtlety poses the case of a solution of duration $r = 0$, in which case there still is no time-derivative to speak of. If $r = 0$, the more detailed explanation of Definition 3.3 in Sect. 3.3.2 ignores condition (10.5) leaving only the requirement that ω and ν agree except for the value of x' and that $\nu \in [\![x' = f(x) \wedge Q]\!]$.

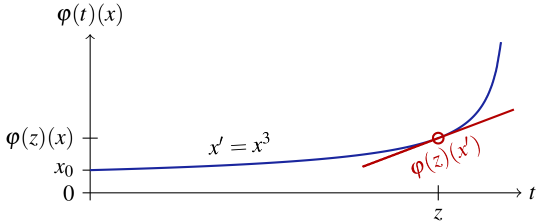


Fig. 10.4 Semantics of differential symbol x' along differential equation

Now we finally figured out the answer to the question of what symbol x' means and what its value is. It all depends on the state. And nothing but the state! Along differential equations, we know a lot about the value of x', otherwise we know less.

The values assigned to x' by the states $\varphi(z)$ visited along a solution $\varphi : [0,r] \to \mathcal{S}$ of a differential equation $x' = f(x) \,\&\, Q$ will have a close relationship, namely (10.5) and $\varphi(z) \in [\![x' = f(x)]\!]$. But that relationship is by virtue of φ being a solution of a differential equation, so that the family of states $\varphi(z)$ for $z \in [0,r]$ have a unique link. It is perfectly consistent to have one state ω in which $\omega(x') = 1$ and another equally isolated state ν in which $\nu(x') = \sqrt{8}$. In fact, that is just what happens for the initial state ω and final state ν when following the differential equation $x' = x^3$ from $\omega(x) = 1$ for $\frac{1}{4}$ time units. If we do not know that ω and ν are the initial and final states of that differential equation or if we do not know that it was exactly for $\frac{1}{4}$ time units that we followed it, there is no reason to suspect much of a relationship between the values of $\omega(x')$ and $\nu(x')$.

Differential symbols x' have a meaning now as being interpreted directly by the state. Yet, what is the meaning of a differential term $(e)'$ such as $(v^2 + w^2 - r^2)'$?

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

10.3.3 Semantics of Differential Terms

At this point it should no longer be a surprise that the first mathematical reflex of understanding differential terms $(e)'$ as time-derivatives will quickly fall short of its own expectations, because there still is no time-derivative in the isolated state ω that the value $\omega[\![(e)']\!]$ has at its disposal. Likewise, we still cannot ask any differential equations occurring somewhere else in the context, because that would break compositionality and would not explain the meaning in an isolated formula such as (10.3). Unfortunately, though, we cannot follow the same solution and ask the state to assign any arbitrary real value to each differential term. After all, there should be a close relationship of $\omega[\![(2x^2)']\!]$ and $\omega[\![(8x^2)']\!]$ namely that $4\omega[\![(2x^2)']\!] = \omega[\![(8x^2)']\!]$, and an arbitrary state would not respect this relationship if it were to remember arbitrary and unrelated real values for all possible differential terms. Thus, the structure and meaning of the term e should contribute to the meaning of $(e)'$.

The value of $(e)'$ is supposed to tell us something about how the value of e changes. But it is not and could not possibly be change over time to which this is referring, because there is no time or time-derivative to speak of in an isolated state ω. The trick is that we can still determine how the value of e will change, just not over time. We can tell just from the term e itself how its value will change locally depending on how its constituents change.

Recall that the *partial derivative* $\frac{\partial f}{\partial x}(\xi)$ of a function f with respect to the variable x at the point ξ characterizes how the value of f changes as the variable x changes at the point ξ, so when keeping all values of all variables at the point ξ, except for small local changes of the value of x. The term $2x^2$ will locally change according to the partial derivative of its value with respect to x, but the overall change will also depend on how x itself changes locally. The term $5x^2y$ also changes according to the partial derivative of its value with respect to x but it additionally changes according to its partial derivative with respect to y and overall also depends on how x and y themselves change locally.

The clou is that the state ω already has the values $\omega(x')$ of all differential symbols x' at its disposal, which, qua Definition 3.3, are reminiscent of the direction that x would be evolving to locally, if only state ω were part of a solution of a differential equation. The value $\omega(x')$ of differential symbol x' acts like the "local shadow" of the time-derivative $\frac{dx}{dt}$ at ω if only that derivative even existed at that point to begin with. But even if that time-derivative cannot exist at a general isolated state, we can still understand the value $\omega(x')$ that x' happens to have in that state as the direction that x would evolve in locally at that state. Likewise the value $\omega(y')$ of y' can be taken to indicate the direction that y would evolve in locally at that state. Now all it takes is a way to accumulate the change by summing it all up to lead to the meaning of differentials [14].

Definition 10.2 (Semantics of differentials). The semantics of differential term $(e)'$ in state ω is the value $\omega[\![(e)']\!]$ defined as

$$\omega[\![(e)']\!] = \sum_{x\in\mathscr{V}} \omega(x') \cdot \frac{\partial [\![e]\!]}{\partial x}(\omega)$$

The value $\omega[\![(e)']\!]$ is the sum of all (analytic) spatial partial derivatives at ω of the value $[\![e]\!]$ of e by each variable $x \in \mathscr{V}$ multiplied by the corresponding direction of evolution (*tangent*) described by the value $\omega(x')$ of differential symbol $x' \in \mathscr{V}'$.

That sum over all variables $x \in \mathscr{V}$ has finite support (only finitely many summands are nonzero), because term e only mentions finitely many variables x and the partial derivative with respect to variables x that do not occur in e is 0, so does not contribute to the sum. The spatial derivatives exist since the evaluation $\omega[\![e]\!]$ is a composition of smooth functions such as addition, multiplication, etc., so is itself smooth. Recall that the *partial derivative* with respect to variable $x \in \mathscr{V}$ of the value $[\![e]\!]$ of e at state $\omega \in \mathscr{S}$ represents how the value of $\omega[\![e]\!]$ changes with the value of x. It is defined as the limit of the corresponding difference quotient as the new value

$\kappa \in \mathbb{R}$ that x has in state ω_x^κ converges to the value $\omega(x)$ that x has in state ω:

$$\frac{\partial [\![e]\!]}{\partial x}(\omega) = \lim_{\kappa \to \omega(x)} \frac{\omega_x^\kappa[\![e]\!] - \omega[\![e]\!]}{\kappa - \omega(x)}$$

Overall the (real) value of $(e)'$ depends not just on e itself and the values in the current state ω of the variables x that occur in e but also on the direction in which these variables are taken to evolve according to the values of the respective differential symbols x' in ω; see Fig. 10.5.

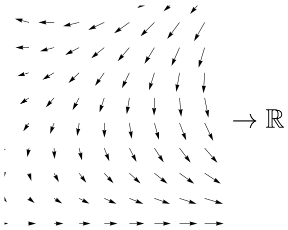


Fig. 10.5 Differential form semantics of differentials: their value depends on the point as well as on the direction of the vector field at that point

Example 10.3 (Rotational dynamics). In state ω, the differential term $(v^2+w^2-r^2)'$ from the rotational dynamics has the semantics:

$$\omega[\![(v^2+w^2-r^2)']\!] = \omega(v') \cdot \omega[\![2v]\!] + \omega(w') \cdot \omega[\![2w]\!] - \omega(r') \cdot \omega[\![2r]\!]$$

Example 10.4. In a state ω, the differential term $(x^3y+2x+1)'$ has the semantics:

$$\omega[\![(x^3y+2x+5)']\!] = \omega(x') \cdot \omega[\![3x^2y+2]\!] + \omega(y') \cdot \omega[\![x^3]\!]$$

10.3.4 Derivation Lemma with Equations of Differentials

Observe one quite crucial byproduct of adopting differentials as first-class citizens in dL. Differentiation, the process of forming derivatives that we used in (10.2), was previously an amorphous operation without proper semantic counterparts. While it might have been clear how to differentiate a term, it was quite unclear what that really meant in a state. Using Definition 10.2, both sides of the equation (10.2) now have a precise semantics and, indeed, both sides always have the same value.

Differentiation has now simply become the perfectly meaningful use of equations of differential terms. For example, the use of Leibniz's product rule of differentiation simply corresponds to the use of the following equation:

$$(e \cdot k)' = (e)' \cdot k + e \cdot (k)' \tag{10.6}$$

Equations have a well-defined meaning on reals and both sides of the equation (10.6) have a semantics by Definition 10.2, which can be shown to agree. Equation (10.6) is an ordinary formula that is an equation of differential terms equating the differential $(e \cdot k)'$ of the product term $e \cdot k$ to the sum of terms $(e)' \cdot k$ and $e \cdot (k)'$. After establishing that the equation (10.6) is a valid formula, differentiating a product such as $x^3 \cdot y$ simply amounts to using the corresponding instance of (10.6) to justify

$$(x^3 \cdot y)' = (x^3)' \cdot y + x^3 \cdot (y)'$$

Corresponding equations of differentials hold for all other term operators.

Lemma 10.1 (Derivation lemma). *The following equations of differentials are valid formulas so sound axioms:*

$+'$ $(e+k)' = (e)' + (k)'$

$-'$ $(e-k)' = (e)' - (k)'$

$\cdot'$ $(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$

$/'$ $(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2$

c' $(c())' = 0$ (for numbers or constants $c()$)

x' $(x)' = x'$ (for variable $x \in \mathcal{V}$)

Proof. We only consider the summation case of the proof, which is reported in full elsewhere [14].

$$\begin{aligned}
\omega[\![(e+k)']\!] &= \sum_x \omega(x') \frac{\partial [\![e+k]\!]}{\partial x}(\omega) = \sum_x \omega(x') \frac{\partial ([\![e]\!] + [\![k]\!])}{\partial x}(\omega) \\
&= \sum_x \omega(x') \Big(\frac{\partial [\![e]\!]}{\partial x}(\omega) + \frac{\partial [\![k]\!]}{\partial x}(\omega) \Big) \\
&= \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega) + \sum_x \omega(x') \frac{\partial [\![k]\!]}{\partial x}(\omega) \\
&= \omega[\![(e)']\!] + \omega[\![(k)']\!] = \omega[\![(e)' + (k)']\!]
\end{aligned}$$

□

This gives us a way of computing simpler forms for differentials of terms by applying the equations of Lemma 10.1 from left to right, which will, incidentally, lead us to the same result that differentiation would have, except now the result has been obtained by a chain of logical equivalence transformations on differentials each of which is individually grounded semantically with a soundness proof. It also becomes possible to selectively apply equations of differentials as needed in a proof without endangering soundness. Who would have figured that our study of differential equations would lead us down a path to study equations of differentials?

By axiom x', the differential $(x)'$ of a variable x is simply its corresponding differential symbol x', because they have the same semantics. The differential $(c())'$

of a constant symbol $c()$ is 0, because constant symbols do not change their value when the value of any variable changes, because no variables even occur. The differential of a division e/k uses a division, which is where we need to make sure not to accidentally divide by zero. Yet, in the definition of $(e/k)'$, the division is by k^2, which, fortunately, has the same roots that k already has, as $k=0 \leftrightarrow k^2=0$ is valid for any term k. Hence, in any context in which e/k is defined, its differential $(e/k)'$ will also be defined.

Example 10.5. Computing the differential of a term like v^2+w^2 is now easy just by using the respective equations from Lemma 10.1 in sequence as indicated:

$$\begin{aligned}(v^2+w^2)' &\overset{+'}{=} (v\cdot v)' + (w\cdot w)' \\ &\overset{\cdot'}{=} ((v)'\cdot v + v\cdot (v)') + ((w)'\cdot w + w\cdot (w)') \\ &\overset{x'}{=} v'\cdot v + v\cdot v' + w'\cdot w + w\cdot w' = 2vv' + 2ww'\end{aligned}$$

When r is a constant function symbol, an additional use of axiom c' also justifies

$$(v^2+w^2-r^2)' = 2vv' + 2ww'$$

10.3.5 Differential Lemma

Now that we have obtained a precise semantics of differential symbols x' and differentials $(e)'$ that is meaningful in any arbitrary state ω, no matter how isolated it may be, it is about time to come back to the question of what we can now learn from studying their values *along a differential equation*.

Along the solution φ of a differential equation, differential symbols x' do not have arbitrary values but, at all times z, are interpreted as time-derivatives of the value of x by Definition 3.3:

$$\varphi(z)[\![(x)']\!] = \varphi(z)(x') \overset{\text{def}}{=} \frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(z) \qquad (10.5^*)$$

The key insight is that this equality of the value of differentials with analytic time-derivatives along a differential equation continues to hold not just for differentials of variables x but also for differentials $(e)'$ of arbitrary terms e.

The following central lemma [14], which is the differential counterpart of the substitution lemma, establishes the connection between the semantics of syntactic differentials of terms and semantic differentiation as an analytic operation to obtain analytic time-derivatives of the semantics of terms along differential equations. It will allow us to draw analytic conclusions about the behavior of a system along a differential equation from the values of differentials obtained syntactically.

Lemma 10.2 (Differential lemma). *Let* $\varphi \models x' = f(x) \land Q$ *for some solution* $\varphi : [0,r] \to \mathscr{S}$ *of duration* $r > 0$*. Then for all times* $0 \le z \le r$ *and all terms* e *defined all along* φ *with* $FV(e) \subseteq \{x\}$*:*

$$\varphi(z)[\![(e)']\!] = \frac{\mathsf{d}\,\varphi(t)[\![e]\!]}{\mathsf{d}t}(z)$$

Proof. Prior work reports the full proof [14], which is mostly by chain rule:

$$\frac{\mathsf{d}\varphi(t)[\![e]\!]}{\mathsf{d}t}(z) \overset{\text{chain}}{=} \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z))\frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(z) = \sum_x \frac{\partial [\![e]\!]}{\partial x}(\varphi(z))\varphi(z)(x') = \varphi(z)[\![(e)']\!]$$

The proof uses that $\varphi(z)(x')$ equals $\frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(z)$ along the solution φ of $x' = f(x)$. □

In particular, $\varphi(z)[\![e]\!]$ is continuously differentiable in z. The same result applies to vectorial differential equations as long as all free variables of the term e have some differential equation so that their differential symbols agree with the time-derivatives.

Note 57 (Differential lemma clou) Lemma 10.2 shows that the analytic time-derivatives coincide with the values of differentials. The clou with Lemma 10.2 is that it equates precise but sophisticated analytic time-derivatives with purely syntactic differentials. The analytic time-derivatives on the right-hand side of Lemma 10.2 are mathematically precise and pinpoint exactly what we are interested in: the rate of change of the value of e along solution φ. But they are unwieldy for computers, because analytic derivatives are ultimately defined in terms of limit processes and also need a whole solution to be well-defined. The syntactic differentials on the left-hand side of Lemma 10.2 are purely syntactic (putting a prime on a term) and even their simplifications via the recursive use of the axioms from Lemma 10.1 are computationally tame.

Having said that, in order to be useful, the syntactic differentials need to be aligned with the intended analytic time-derivatives, which is exactly what Lemma 10.2 achieves. To wit, even differentiating polynomials and rational functions is much easier syntactically than by unpacking the meaning of analytic derivatives in terms of limit processes every time.

10.3.6 Differential Invariant Term Axiom

The differential lemma immediately leads to a first proof principle for differential equations. If the differential $(e)'$ is always zero along a differential equation, then e will always be zero if and only if it was zero initially. For emphasis, we use the backwards implication $P \leftarrow Q$ as alternative notation for the converse forward implication $Q \to P$.

Lemma 10.3 (Differential invariant term axiom). *This axiom is sound:*

$$\text{DI} \quad \big([x' = f(x)]\, e = 0 \leftrightarrow e = 0\big) \leftarrow [x' = f(x)]\, (e)' = 0$$

Proof. To prove that axiom DI is sound, we need to show the validity of the formula

$$[x' = f(x)]\, (e)' = 0 \rightarrow \big([x' = f(x)]\, e = 0 \leftrightarrow e = 0\big)$$

Consider any state ω in which the assumption is true, so $\omega \in [\![[x' = f(x)]\, (e)' = 0]\!]$, and show that $\omega \in [\![[x' = f(x)]\, e = 0 \leftrightarrow e = 0]\!]$. Now, $\omega \in [\![[x' = f(x)]\, e = 0]\!]$ directly implies $\omega \in [\![e = 0]\!]$ when following the differential equation for duration 0. To show the converse implication, assume $\omega \in [\![e = 0]\!]$. If φ is a solution of $x' = f(x)$, then the assumption implies that $\varphi \models (e)' = 0$ since all restrictions of solutions are again solutions. Consequently, Lemma 10.2 implies

$$0 = \varphi(z)[\![(e)']\!] = \frac{\mathsf{d}\,\varphi(t)[\![e]\!]}{\mathsf{d}t}(z) \tag{10.7}$$

This implies that the term e always evaluates to zero along φ by the mean-value theorem (Lemma 10.4 below), since it initially started out 0 (by initial $\omega \in [\![e = 0]\!]$) and had 0 change over time by (10.7). Hold on, that use of Lemma 10.2 was, of course, predicated on having a solution φ of duration $r > 0$ (otherwise there are no time-derivatives to speak of). Yet, solutions of duration $r = 0$ also already satisfy $e = 0$ from the assumption $\omega \in [\![e = 0]\!]$. Strictly speaking [14], this proof requires that x' is not free in e. □

This proof uses the mean-value theorem [17, §10.10]:

Lemma 10.4 (Mean-value theorem). *If $g : [a,b] \to \mathbb{R}$ is continuous and differentiable in the open interval (a,b), then there is a $\xi \in (a,b)$ such that:*

$$g(b) - g(a) = g'(\xi)(b - a)$$

The only nuisance with axiom DI is that it never proves any interesting properties on its own. It reduces a proof of the postcondition $e = 0$ for a differential equation to the question of whether $e = 0$ is true initially but also to a proof of the postcondition $(e)' = 0$ for the same differential equation. This is similar to how the loop induction axiom I from Lemma 7.1 reduced the proof of postcondition P of a loop to another postcondition $P \rightarrow [\alpha]P$ of the same loop, so that we ultimately still needed the generalization rule G to get rid of the loop entirely. But just generalization rule G alone will not quite suffice for differential equations.

For Example 10.1, a use of axiom DI would lead to

$$\text{→R}\ \dfrac{\text{DI}\ \dfrac{\vdash [v'=w,w'=-v]\,2vv'+2ww'-2rr'=0}{v^2+w^2-r^2=0 \vdash [v'=w,w'=-v]\,v^2+w^2-r^2=0}}{\vdash v^2+w^2-r^2=0 \to [v'=w,w'=-v]\,v^2+w^2-r^2=0}$$

Without knowing anything about v' and w' and r' in the postcondition, we have no chance of finishing this proof. Certainly the generalization rule G cannot succeed because the postcondition $2vv'+2ww'-2rr'=0$ alone is not always true. In fact, it should not be valid, because whether a postcondition $e=0$ is an invariant of a differential equation does not just depend on the differential $(e)'$ of the term in the postcondition, but also on the differential equation itself. What stands to reason is to use the right-hand sides of the differential equations for their left-hand sides; the two sides of the equation are supposed to be equal! The question is how to justify that that's sound.

10.3.7 Differential Substitution Lemmas

Lemma 10.2 shows that, along a differential equation, the value of the differential $(e)'$ of term e coincides with the analytic time-derivative of the value of term e. The value of a differential term $(e)'$ depends on the term itself as well as the value of its variables x and their corresponding differential symbols x'. Along a differential equation $x'=f(x)$, the differential symbols x' themselves actually have a simple interpretation: their values equal the right-hand side $f(x)$.

> The direction in which the value of a term e evolves as the system follows a differential equation $x'=f(x)$ depends on the differential $(e)'$ of the term e as well as on the differential equation $x'=f(x)$ that locally describes the evolution of its variable x over time.

What we need is a way of using the differential equation $x'=f(x)$ to soundly replace occurrences of the differential symbol x' from its left-hand side with the corresponding right-hand side $f(x)$ of the differential equation. Naïve replacement would be unsound, because that might violate the scope of the formula where x' equals $f(x)$. Discrete assignments $x:=e$ were ultimately handled in axiom [:=] from Lemma 5.2 by substituting the new value e for the variable x, and the axiom is already mindful of scoping challenges. The trick is to use the same assignments but for assigning terms to differential symbols x' instead of variables x. Since x' already always has the value $f(x)$ when following the differential equation $x'=f(x)$ along its solution φ, assigning $f(x)$ to x' by a discrete assignment $x':=f(x)$ has no effect.

Lemma 10.5 (Differential assignment). *If $\varphi \models x' = f(x) \land Q$ for a solution $\varphi : [0,r] \to \mathscr{S}$ of any duration $r \geq 0$, then*

$$\varphi \models P \leftrightarrow [x' := f(x)]P$$

Proof. The proof [14] is a direct consequence of the fact that the semantics of differential equations (Definition 3.3) requires that $\varphi(z) \in [\![x' = f(x)]\!]$ holds for all times z all along φ. Consequently, the assignment $x' := f(x)$ that changes the value of x' to be the value of $f(x)$ will have no effect, since x' already does have that value along the differential equation. Thus, P and $[x' := f(x)]P$ are equivalent along φ. □

Using this equivalence at any state along a differential equation $x' = f(x)$ gives rise to a simple axiom characterizing the effect that a differential equation has on its differential symbol x'. Following a differential equation $x' = f(x)$ requires x' and $f(x)$ to always have the same value along the differential equation.

Lemma 10.6 (DE differential effect axiom). *This axiom is sound:*

$$\text{DE} \quad [x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q][x' := f(x)]P$$

While axiom DE performs a no-op, its benefit is that it makes the effect that a differential equation has on the differential symbol available as a discrete assignment.

The last ingredient is to use the assignment axiom [:=] from Lemma 5.2 also for discrete assignments $x' := e$ to differential symbol x' instead of just for discrete assignments $x := e$ to variable x:

$$[:=] \quad [x' := e]p(x') \leftrightarrow p(e)$$

Let's continue the proof for Example 10.1:

$$\begin{array}{lr}
 & \vdash [v' = w, w' = -v]\,2v(w) + 2w(-v) - 2rr' = 0\\ \hline
[:=] & \vdash [v' = w, w' = -v][v' := w][w' := -v]\,2vv' + 2ww' - 2rr' = 0\\ \hline
\text{DE} & \vdash [v' = w, w' = -v]\,2vv' + 2ww' - 2rr' = 0\\ \hline
\text{DI} & v^2 + w^2 - r^2 = 0 \vdash [v' = w, w' = -v]\,v^2 + w^2 - r^2 = 0\\ \hline
\to\text{R} & \vdash v^2 + w^2 - r^2 = 0 \to [v' = w, w' = -v]\,v^2 + w^2 - r^2 = 0
\end{array}$$

Oops, that did not make all differential symbols disappear, because r' is still around, since r did not have a differential equation in (10.2) to begin with. Stepping back, what we mean by a differential equation like $v' = w, w' = -v$ that does not mention r' is that r is not supposed to change. If r were supposed to change during a continuous evolution, then there would have to be a differential equation for r describing how exactly r changes.

Note 58 (Explicit change) Hybrid programs are *explicit change*. Nothing changes unless an assignment or differential equation specifies how (compare the semantics from Chap. 3 and the bound variables in Sect. 5.6.5). In particular, if a differential equation (system) $x' = f(x)$ does not mention z', then the variable z does not change during $x' = f(x)$, so $x' = f(x)$ and $x' = f(x), z' = 0$ are the same. Strictly speaking this equivalence only holds when z' itself also does not occur elsewhere in the program or formula, which is a condition that is usually met. The subtle nuance is that only $x' = f(x)$ will leave the value of z' untouched, but $x' = f(x), z' = 0$ will change z' to 0 by Definition 3.3.
Even if KeYmaera X has a rigorous treatment with uniform substitutions of free constant symbols, it suffices for our paper proofs to assume $z' = 0$ without further notice for variables z that do not change during a differential equation.

Since (10.2) does not have an r', Note 58 implies that instead of its differential equation $v' = w, w' = -v$ we could have used $v' = w, w' = -v, r' = 0$, which, with DE, would give rise to an extra $[r':=0]$, which we will assume implicitly from now on after showing its use explicitly just once.

$$
\rightarrow\!\mathrm{R}\ \dfrac{\mathrm{DI}\ \dfrac{\mathrm{DE}\ \dfrac{[:=]\ \dfrac{\mathrm{G}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2vw - 2wv - 0 = 0}}{\vdash [v' = w, w' = -v]2v(w) + 2w(-v) - 0 = 0}}{\vdash [v' = w, w' = -v][v':=w][w':=-v][r':=0]2vv' + 2ww' - 2rr' = 0}}{\vdash [v' = w, w' = -v]2vv' + 2ww' - 2rr' = 0}}{v^2 + w^2 - r^2 = 0 \vdash [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}}{\vdash v^2 + w^2 - r^2 = 0 \rightarrow [v' = w, w' = -v]v^2 + w^2 - r^2 = 0}
$$

This is amazing, because we found out that the value of $v^2 + w^2 - r^2$ does not change over time along the differential equation $v' = w, w' = -v$. And we found that out without ever solving the differential equation, just by a few lines of simple but mathematically rigorous symbolic proof steps.

10.4 Differential Invariant Terms

In order to be able to use the above reasoning as part of a sequent proof efficiently, let's package up the argument in a simple proof rule. As a first shot, we stay with equations of the form $e = 0$, which gives us soundness for the following proof rule.

Lemma 10.7 (Differential invariant term rule). *The following special case of the differential invariants proof rule is sound, i.e., if its premise is valid then so is its conclusion:*

$$\text{dI}\ \frac{\vdash [x':=f(x)](e)'=0}{e=0 \vdash [x'=f(x)]e=0}$$

Proof. We could prove soundness of this proof rule by going back to the semantics and lemmas we proved about it. The easier soundness proof is to prove that it is a derived rule, meaning that it can be expanded into a sequence of other axiom and proof rule applications that we have already seen to be sound:

$$\text{DI}\ \dfrac{\text{DE}\ \dfrac{\text{G}\ \dfrac{\vdash [x':=f(x)](e)'=0}{\vdash [x'=f(x)\,\&\,Q][x':=f(x)](e)'=0}}{\vdash [x'=f(x)\,\&\,Q](e)'=0}}{e=0 \vdash [x'=f(x)\,\&\,Q]e=0}$$

This proof shows dI to be a derived rule because it starts with the premise of rule dI as the only open goal and ends with the conclusion of rule dI, using only proof rules we already know are sound. □

Notice that Gödel's generalization rule G was used to derive dI, so it would not be sound to retain a sequent context Γ,Δ in its premise (except, as usual, assumptions about constants). After all, its premise represents an induction step for a differential equation. Just like in loop invariants, we cannot assume the state considered in the induction step will still satisfy whatever we knew in the initial state.

This proof rule enables us to prove dL formula (10.2) easily in sequent calculus:

$$\to\text{R}\ \dfrac{\text{dI}\ \dfrac{[:=]\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2vw+2w(-v)-0=0}}{\vdash [v':=w][w':=-v]\,2vv'+2ww'-0=0}}{v^2+w^2-r^2=0 \vdash [v'=w,w'=-v]\,v^2+w^2-r^2=0}}{\vdash v^2+w^2-r^2=0 \to [v'=w,w'=-v]\,v^2+w^2-r^2=0}$$

Taking a step back, this is an exciting development, because, thanks to differential invariants, the property (10.2) of a differential equation with a nontrivial solution has a very simple proof that we can easily check. The proof did not need to solve the differential equation, which has infinitely many solutions with combinations of trigonometric functions.[2] The proof only required deriving the postcondition and substituting in the differential equation.

[2] Granted, the solutions in this case are not quite so terrifying. They are all of the form

$$v(t)=a\cos t+b\sin t,\ w(t)=b\cos t-a\sin t$$

But the special functions sin and cos still fall outside the decidable parts of arithmetic.

10.5 A Differential Invariant Proof by Generalization

So far, the differential invariant term proof rule dI works for

$$v^2+w^2-r^2=0 \rightarrow [v'=w,w'=-v]v^2+w^2-r^2=0 \tag{10.2*}$$

with an equation $v^2+w^2-r^2=0$ normalized to having 0 on the right-hand side. But it does not work for the original formula

$$v^2+w^2=r^2 \rightarrow [v'=w,w'=-v]v^2+w^2=r^2 \tag{10.1*}$$

because its postcondition is not of the form $e=0$. Yet, the postcondition $v^2+w^2-r^2=0$ of (10.2) is trivially equivalent to the postcondition $v^2+w^2=r^2$ of (10.1), just by rewriting the polynomials on one side, which is a minor change. That is an indication that differential invariants can perhaps do more than what proof rule dI already knows about.

But before we pursue any further our discovery of what else differential invariants can do for us, let us first understand a very important proof principle.

Note 59 (Proof by generalization) If you do not find a proof of a formula, it can sometimes be easier to prove a more general property from which the one you were looking for follows.

This principle, which may at first appear paradoxical, turns out to be very helpful. In fact, we have made ample use of Note 59 when proving properties of loops by induction. The loop invariant that needs to be proved is usually more general than the particular postcondition one is interested in. The desirable postcondition follows from having proved a more general inductive invariant.

Recall the monotonicity right rule MR from Lemma 7.4:

$$\mathrm{MR}\ \frac{\Gamma \vdash [\alpha]Q,\Delta \quad Q \vdash P}{\Gamma \vdash [\alpha]P,\Delta}$$

Instead of proving the desirable postcondition P of α (conclusion), proof rule MR makes it possible to prove the postcondition Q instead (left premise) and prove that Q is more general than the desired P (right premise). Generalization MR can help us prove the original dL formula (10.1) by first turning the postcondition into the form of the (provable) (10.2) and adapting the precondition using a corresponding cut with $v^2+w^2-r^2=0$, whose first premise $v^2+w^2=r^2 \vdash v^2+w^2-r^2=0$ is elided but is proved by $\mathbb{R}$:

$$\text{→R}\,\dfrac{\text{MR}\,\dfrac{\text{cut}\,\dfrac{\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2vw+2w(-v)-0=0}}{\vdash [v':=w][w':=-v]2vv'+2ww'-0}}{v^2+w^2-r^2=0 \vdash [v'=w,w'=-v]v^2+w^2-r^2=0}}{v^2+w^2=r^2 \vdash [v'=w,w'=-v]v^2+w^2-r^2=0} \qquad \mathbb{R}\,\dfrac{*}{v^2+w^2-r^2=0 \vdash v^2+w^2=r^2}}{v^2+w^2=r^2 \vdash [v'=w,w'=-v]v^2+w^2=r^2}}{\vdash v^2+w^2=r^2 \rightarrow [v'=w,w'=-v]v^2+w^2=r^2}$$

This is a possible way of proving the original (10.1), but also unnecessarily complicated. Differential invariants can prove (10.1) directly once we generalize proof rule dI appropriately. For other purposes, however, it is still important to have the principle of generalization Note 59 in our repertoire of proof techniques.

10.6 Example Proofs

Of course, differential invariants are just as helpful for proving properties of other differential equations, of which this section lists a few.

Example 10.6. A simple proof shows the differential invariant illustrated in Fig. 10.6.

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

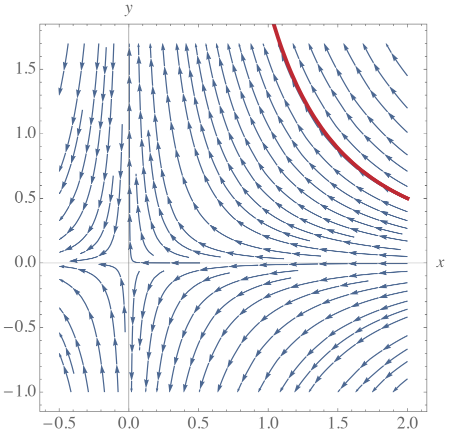


Fig. 10.6 Differential invariant (illustrated in thick red) of the indicated dynamics

Example 10.7 (Self-crossing). Another example is the invariant property illustrated in Fig. 10.7. It is proved easily using dI:

$$\to\mathrm{R}\;\dfrac{\mathrm{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash 2x(-2y)+3x^2(-2y)-2y(-2x-3x^2)=0}}{\vdash [x':=-2y][y':=-2x-3x^2]2xx'+3x^2x'-2yy'-0=0}}{x^2+x^3-y^2-c=0 \vdash [x'=-2y,y'=-2x-3x^2]x^2+x^3-y^2-c=0}}{\vdash x^2+x^3-y^2-c=0 \to [x'=-2y,y'=-2x-3x^2]x^2+x^3-y^2-c=0}$$

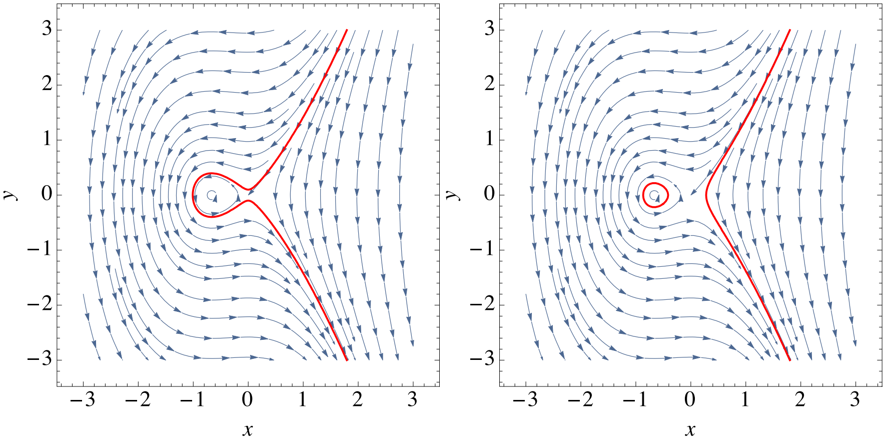


Fig. 10.7 Two differential invariants (illustrated in thick red) of the indicated self-crossing dynamics for Example 10.7 for different values of c

Example 10.8 (Motzkin). Another nice example is the Motzkin polynomial, which is an invariant of the following dynamics (see Fig. 10.8):

$$x^4y^2+x^2y^4-3x^2y^2+1=c \to$$
$$[x'=2x^4y+4x^2y^3-6x^2y, y'=-4x^3y^2-2xy^4+6xy^2]\,x^4y^2+x^2y^4-3x^2y^2+1=c$$

This dL formula is proved directly by dI, again after normalizing the equation to have right-hand side 0 (where .. abbreviates the antecedent):

$$\to\mathrm{R}\;\dfrac{\mathrm{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash 0=0}}{\vdash [x':=2x^4y+4x^2y^3-6x^2y][y':=-4x^3y^2-2xy^4+6xy^2](x^4y^2+x^2y^4-3x^2y^2+1-c)'=0}}{..\vdash [x'=2x^4y+4x^2y^3-6x^2y, y'=-4x^3y^2-2xy^4+6xy^2]x^4y^2+x^2y^4-3x^2y^2+1-c=0}}{\vdash .. \to [x'=2x^4y+4x^2y^3-6x^2y, y'=-4x^3y^2-2xy^4+6xy^2]x^4y^2+x^2y^4-3x^2y^2+1-c=0}$$

The proof step [:=] is simple, but requires some space:

$$(x^4y^2+x^2y^4-3x^2y^2+1-c)' = (4x^3y^2+2xy^4-6xy^2)x' + (2x^4y+4x^2y^3-6x^2y)y'$$

After substituting in the differential equation, this gives

$$\begin{gathered}(4x^3y^2+2xy^4-6xy^2)(2x^4y+4x^2y^3-6x^2y)\\ +(2x^4y+4x^2y^3-6x^2y)(-4x^3y^2-2xy^4+6xy^2)\end{gathered}$$

which simplifies to 0 after expanding the polynomials, and, thus, leads to the equation $0=0$, which is easy arithmetic. Note that the arithmetic complexity is reduced when we hide unnecessary contexts as shown in Sect. 6.5.3.

(Thanks to Andrew Sogokon for the nice Example 10.8.)

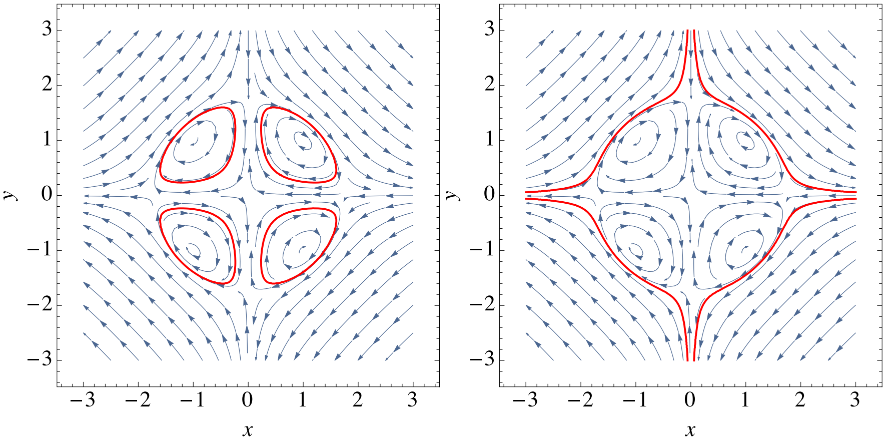


Fig. 10.8 Two differential invariants (illustrated in thick red) of the indicated dynamics for the Motzkin polynomial for Example 10.8 for different values of c

10.7 Summary

This chapter showed one form of differential invariants: the form where the differential invariants are terms whose value always stays 0 along all solutions of a differential equation. The next chapter will use the tools developed in this chapter to investigate more general forms of differential invariants and more advanced proof principles for differential equations. They all share the important discovery in this chapter: that properties of differential equations can be proved using the differential equation rather than its solution.

The most important technical insight of this chapter was that even very complicated behavior that is defined by mathematical properties of the semantics can be captured by purely syntactical proof principles using differentials. The differential lemma proved that the values of differentials of terms coincide with the analytic derivatives of the values. The derivation lemma gave us the usual rules for computing derivatives as equations of differentials. The differential assignment lemma allowed us the intuitive operation of substituting differential equations into terms. Proving properties of differential equations using a mix of these simple proof principles is much more civilized and effective than working with solutions of differential equations. The proofs are also computationally easier, because the proof arguments are local and derivatives even decrease the polynomial degrees. The resulting axioms are summarized in Fig. 10.9 except the differential induction axiom DI since it will be generalized in Chap. 11.

DE $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' := f(x)]P$

$+'$ $(e+k)' = (e)' + (k)'$

$-'$ $(e-k)' = (e)' - (k)'$

$\cdot'$ $(e \cdot k)' = (e)' \cdot k + e \cdot (k)'$

$/'$ $(e/k)' = \big((e)' \cdot k - e \cdot (k)'\big)/k^2$

c' $(c())' = 0$ (for numbers or constants $c()$)

x' $(x)' = x'$ (for variable $x \in \mathcal{V}$)

Fig. 10.9 Axioms for differential invariant terms of differential equations without solutions

The principles begun in this chapter have significantly more potential, though, and are not limited to proving only properties of the rather limited form $e = 0$. Subsequent chapters will make use of the results obtained and build on the differential lemma, derivation lemma, and differential assignment lemma to develop more general proof principles for differential equations. But at least on open and connected evolution domains, the differential invariance proof rule dI is pretty powerful, because it is able to prove all invariant terms, i.e., all terms that never change their value along the differential equation (as Sect. 10.8.2 will explore). There also is a way of deciding equational invariants of algebraic differential equations using a higher-order generalization of differential invariants called differential radical invariants [2].

10.8 Appendix

This appendix discusses optional topics such as the relationship of differential equations to loops, the relationship to differential algebra, and the relationship of the differential invariant term proof rule to Sophus Lie's characterization of invariant functions.

10.8.1 Differential Equations Versus Loops

One way of developing an intuition for the purpose of differential invariants leads through a comparison of differential equations with loops. This perhaps surprising relation can be made completely rigorous and is at the heart of a deep connection equating discrete and continuous dynamics proof-theoretically [12]. This chapter will stay at the surface of this surprising connection but it still leverages the relation of differential equations to loops for our intuition.

To get started with relating differential equations to loops, compare

$$x' = f(x) \qquad \text{vs.} \qquad (x' = f(x))^*$$

How does the differential equation $x' = f(x)$ compare to the same differential equation in a loop $(x' = f(x))^*$ instead? Unlike the differential equation $x' = f(x)$, the repeated differential equation $(x' = f(x))^*$ can run the differential equation $x' = f(x)$ repeatedly any number of times. Albeit, on second thoughts, does that get the repetitive differential equation $(x' = f(x))^*$ to any more states than where the differential equation $x' = f(x)$ could evolve to?

Not really, because chaining lots of solutions of differential equations from a repetitive differential equation $(x' = f(x))^*$ together will still result in a single solution for the same differential equation $x' = f(x)$ that we could have followed all the way. This is precisely what a classical result about the continuation of solutions is about (Proposition 2.2).

Note 60 (Looping differential equations) The loop $(x' = f(x))^*$ over a differential equation is equivalent to $x' = f(x)$, written $(x' = f(x))^* \equiv (x' = f(x))$, i.e., they have the same transition semantics:

$$[\![(x' = f(x))^*]\!] = [\![x' = f(x)]\!]$$

That is, differential equations "are their own loop".[3]

In light of Note 60, differential equations already have some aspects in common with loops. Like nondeterministic repetitions, differential equations might stop right

[3] Beware not to confuse this with the case for differential equations with evolution domain constraints, which is subtly different (Exercise 10.1).

away. Like nondeterministic repetitions, differential equations can evolve for longer or shorter durations and the choice of duration is nondeterministic. Like in nondeterministic repetitions, the outcome of the evolution of the system up to an intermediate state influences what happens in the future. And, in fact, in a deeper sense, differential equations actually really do correspond to loops executing their discrete Euler approximations [12].

With this rough relation in mind, let's advance the dictionary translating differential equation phenomena into loop phenomena and back. The local description of a differential equation as a relation $x' = f(x)$ of the state to its derivative corresponds to the local description of a loop by a repetition operator * applied to the loop body α. The global behavior of a global solution of a differential equation $x' = f(x)$ corresponds to the full global execution trace of a repetition α^*, but they are similarly unwieldy objects to handle. Because the local descriptions are so much more concise than the respective global behaviors, but still carry all information about how the system will evolve over time, we also say that the local relation $x' = f(x)$ is the *generator* of the global system solution and that the loop body α is the *generator* of the global behavior of repetition of the loop. Proving a property of a differential equation in terms of its solution corresponds to proving a property of a loop by unwinding it (infinitely often) using axiom $[^*]$ from Chap. 5. These comparisons are summarized in Table 10.1.

Table 10.1 Correspondence map between loops and differential equations

loop α^*	differential equation $x' = f(x)$
can repeat 0 times	can evolve for duration 0
repeat any number $n \in \mathbb{N}$ of times	evolve for any duration $r \in \mathbb{R}, r \geq 0$
effect depends on previous loop iteration	effect depends on the past solution
local generator is loop body α	local generator is $x' = f(x)$
full global execution trace	global solution $\varphi : [0,r] \to \mathscr{S}$
proof by unwinding iterations with axiom $[^*]$	proof by global solution with axiom $[']$
proof by induction with loop invariant rule loop	proof by differential invariant

Now, Chap. 7 made the case that unwinding the iterations of a loop can be a rather tedious way of proving properties about the loop, because there is no good way of ever stopping unwinding, unless a counterexample can be found after a finite number of unwindings. This is where working with a global solution of a differential equation with axiom $[']$ is actually more useful, because the solution, if we can write it down in first-order real arithmetic, can be handled completely because of the quantifier $\forall t \geq 0$ over all durations. But Chap. 7 introduced induction with invariants as the preferred way of proving properties of loops, by, essentially, cutting the loop open and arguing that the generic state after any run of the loop body has the same characterization as the generic state before. After all these analogous correspondences between loops and differential equations, the obvious question is what the differential equation analogue of a proof concept would be that corresponds to proofs by induction for loops, which is the premier technique for proving loops.

Induction can be defined for differential equations using what are called *differential invariants* [8, 13, 14]. They have a similar principle to the proof rules for induction for loops. Differential invariants prove properties of the solution of the differential equation using only its local generator: the right-hand side of the differential equation.

Expedition 10.2 (Differential algebra)

Even though the following names and concepts are not needed for this textbook, let's take a brief scientific expedition to align the findings on equations of differentials with the algebraic structures from differential algebra [3, 15] in order to illustrate their systematic principle. The condition in axiom c' defines (rational) number symbols alias literals as *differential constants*, which do not change their value during continuous evolution. Their derivative is zero. The number symbol 5 will always have the value 5 and never change by anything other than 0. The condition in axiom $+'$ and the *Leibniz* or *product rule* from $\cdot'$ are the defining conditions for *derivation operators on rings*. The derivative of a sum is the sum of the derivatives (additivity or a homomorphic property with respect to addition, i.e., the operator $(\cdot)'$ applied to a sum equals the sum of the operator applied to each summand) according to axiom $+'$. Furthermore, the derivative of a product is the derivative of one factor times the other factor plus the one factor times the derivative of the other factor as in axiom $\cdot'$. The condition in axiom $-'$ is a derived rule for subtraction according to the identity $e-k=e+(-1)\cdot k$ and again expresses a homomorphic property, now with respect to subtraction rather than addition.

The equation in axiom x' uniquely defines the operator $(\cdot)'$ on the *differential polynomial algebra* spanned by the *differential indeterminates* $x \in \mathscr{V}$, i.e., the symbols x that have indeterminate derivatives x'. It says that we understand the differential symbol x' as the derivative of the symbol x for all state variables $x \in \mathscr{V}$. Axiom $/'$ canonically extends the derivation operator $(\cdot)'$ to the *differential field of quotients* by the usual *quotient rule*. As the base field $\mathbb{R}$ has no zero divisors[a], the right-hand side of axiom $/'$ is defined whenever the original division e/k can be carried out, which, as we assumed for well-definedness, is guarded by $k \neq 0$.

[a] In this setting, $\mathbb{R}$ has no zero divisors, because the formula $ab=0 \rightarrow a=0 \vee b=0$ is valid, i.e., a product is zero only if a factor is zero.

Expedition 10.3 (Semantics of differential algebra)

The view of Expedition 10.2 sort of gave $(e)'$ a meaning, but, when we think about it, did not actually define it. Differential algebra studies the structural algebraic relations of, e.g., the derivative $(e+k)'$ to the derivatives $(e)'$ plus $(k)'$ and is incredibly effective at capturing and understanding them. But algebra—and differential algebra is no exception—is, of course, deliberately abstract about the question of what the individual pieces mean, because algebra is the study of structure, not the study of the meaning of the objects that are being structured in the first place. That is why we can learn all about the structure of derivatives and derivation operators from differential algebra, but have to go beyond differential algebra to complement it with a precise semantics that relates to what is needed to understand the mathematics of real CPSs.

10.8.2 *Differential Invariant Terms and Invariant Functions*

It is not a coincidence that the examples in this chapter were provable by differential invariant proof rule dI, because that proof rule can handle arbitrary invariant functions.

Despite the power that differential invariant terms offer, challenges lie ahead in proving properties. Theorem 10.1 from Expedition 10.4 gives an indication where challenges remain.

Example 10.9 (Generalizing differential invariants). This dL formula is valid

$$x^2+y^2=0 \rightarrow [x'=4y^3, y'=-4x^3]\, x^2+y^2=0 \tag{10.9}$$

but cannot be proved directly using dI, because x^2+y^2 is not an invariant function of the dynamics. In combination with generalization (MR to change the postcondition to the equivalent $x^4+y^4=0$) and a cut (to change the antecedent to the equivalent $x^4+y^4=0$), however, there is a proof using differential invariants dI:

$$\begin{prooftree}
\AxiomC{$*$}
\LeftLabel{$\mathbb{R}$}
\UnaryInfC{$\vdash 4x^3(4y^3)+4y^3(-4x^3)=0$}
\LeftLabel{$[:=]$}
\UnaryInfC{$\vdash [x':=4y^3][y':=-4x^3]4x^3x'+4y^3y'=0$}
\LeftLabel{dI}
\UnaryInfC{$x^4+y^4=0 \vdash [x'=4y^3, y'=-4x^3]\, x^4+y^4=0$}
\LeftLabel{cut,MR}
\UnaryInfC{$x^2+y^2=0 \vdash [x'=4y^3, y'=-4x^3]\, x^2+y^2=0$}
\LeftLabel{$\rightarrow$R}
\UnaryInfC{$\vdash x^2+y^2=0 \rightarrow [x'=4y^3, y'=-4x^3]\, x^2+y^2=0$}
\end{prooftree}$$

The use of MR leads to another branch $x^4+y^4=0 \vdash x^2+y^2=0$ that is elided above. Similarly, the cut rule leads to another branch $x^2+y^2=0 \vdash x^4+y^4=0$ that is also elided. Both is proved easily using real arithmetic ($\mathbb{R}$).

Expedition 10.4 (Lie characterization of invariant functions)

The proof rule dI works by deriving the postcondition and substituting the differential equation in:

$$\text{dI}\ \frac{\vdash [x':=f(x)](e)'=0}{e=0 \vdash [x'=f(x)]e=0}$$

There is something quite peculiar about rule dI. Its premise is independent of the constant term in e. If, for any constant symbol c, the formula $e=0$ is replaced by $e-c=0$ in the conclusion, then the premise of rule dI stays the same, because $c'=0$. Consequently, if dI proves

$$e=0 \vdash [x'=f(x)]e=0$$

then it also proves

$$e-c=0 \vdash [x'=f(x)]e-c=0 \tag{10.8}$$

for any constant c. This observation is the basis for a more general result, which simultaneously proves all formulas (10.8) for all c from the premise of dI.

On open connected domains, equational differential invariants are even a necessary and sufficient characterization of *invariant functions*, i.e., functions that are invariant along the dynamics of a system, because, whatever value c that function had in the initial state, the value will stay the same forever. The equational case of differential invariants is intimately related [10] to the seminal work by Sophus Lie on what are now called Lie groups [4, 5].

Theorem 10.1 (Lie's characterization of invariant terms). *Let $x'=f(x)$ be a differential equation system and let Q be a* domain, *i.e., a first-order formula of real arithmetic characterizing a connected open set. The following proof rule is a sound global equivalence rule, i.e., the conclusion is valid if and only if the premise is:*

$$\text{dI}_c\ \frac{Q \vdash [x':=f(x)](e)'=0}{\vdash \forall c\,\big(e=c \rightarrow [x'=f(x)\,\&\,Q]e=c\big)}$$

How could this happen? How could the original formula (10.9) be provable only after generalizing its postcondition to $x^4+y^4=0$ and not before?

Note 61 (Strengthening induction hypotheses) An important phenomenon we already encountered in Chap. 7 and other uses of induction is that, sometimes, the only way to prove a property is to strengthen the induction hypothesis. Differential invariants are no exception. It is worth noting, however, that the inductive structure in differential invariants includes their differential structure. And, indeed, the derivatives of $x^4 + y^4 = 0$ are different and more conducive to an inductive proof for Example 10.9 than those of $x^2 + y^2 = 0$ even if both have the same set of solutions.

Theorem 10.1 explains why $x^2 + y^2 = 0$ was doomed to fail as a differential invariant while $x^4 + y^4 = 0$ succeeded. All formulas of the form $x^4 + y^4 = c$ for all c are invariants of the dynamics in (10.9), because the proof succeeded. But $x^2 + y^2 = c$ is only an invariant for the lucky choice $c = 0$ and only equivalent to $x^4 + y^4 = 0$ for this case.

Exercises

10.1 (Repeating differential equations with domains). Note 60 explained that $(x' = f(x))^*$ is equivalent to $x' = f(x)$. Does the same hold for differential equations with evolution domain constraints? Are the hybrid programs $(x' = f(x) \,\&\, Q)^*$ and $x' = f(x) \,\&\, Q$ equivalent or not? Justify or modify the statement and justify the variation.

10.2. We argued that dL formulas (10.1) and (10.2) are equivalent and then went on to find a proof of (10.2). Continue this proof of (10.2) to a proof of (10.1) using the generalization rule MR and the cut rule.

10.3 (Derivation lemma proof). Prove the other cases of Lemma 10.1 where the term is a variable x or a subtraction $e - k$ or multiplication $e \cdot k$ or division e/k.

10.4 (Absence of solutions). What happens in the proof of Lemma 10.3 if there is no solution φ? Show that this is not a counterexample to axiom DI, but that the axiom is sound in that case, too.

10.5. Carry out the polynomial computations needed to prove Example 10.8 using proof rule dI.

10.6 (Rotation with angular velocity ω). Example 10.1 considered a rotation of vector (v, w) with angular velocity 1. Suppose the vector (v, w) is rotating with an arbitrary fixed angular velocity ω. Even if the vector rotates more quickly or slowly, it still always remains on the circle of radius r. Prove the resulting dL formula using differential invariants:

$$v^2 + w^2 = r^2 \rightarrow [v' = \omega w, w' = -\omega v \,\&\, \omega \neq 0]v^2 + w^2 = r^2$$

10.7. Prove the following dL formulas using differential invariants:

$$xy = c \to [x' = -x, y' = y, z' = -z]\, xy = c$$
$$4x^2 + 2y^2 = 1 \to [x' = 2y, y' = -4x]\, 4x^2 + 2y^2 = 1$$
$$x^2 + \frac{y^3}{3} = c \to [x' = y^2, y' = -2x]\, x^2 + \frac{y^3}{3} = c$$
$$x^2{+}4xy{-}2y^3{-}y = 1 \to [x' = -1 + 4x - 6y^2, y' = -2x - 4y]\, x^2{+}4xy{-}2y^3{-}y = 1$$

10.8 (Hénon-Heiles). Prove a differential invariant of a Hénon-Heiles system for the motion of a star at (x,y) flying in direction (u,v) around the center of the galaxy:

$$\begin{aligned}&\frac{1}{2}(u^2 + v^2 + Ax^2 + By^2) + x^2y - \frac{1}{3}\varepsilon y^3 = 0 \to \\ &\qquad [x' = u, y' = v, u' = -Ax - 2xy, v' = -By + \varepsilon y^2 - x^2] \\ &\qquad\qquad \frac{1}{2}(u^2 + v^2 + Ax^2 + By^2) + x^2y - \frac{1}{3}\varepsilon y^3 = 0\end{aligned}$$

References

[1] Gottlob Frege. *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. Halle: Verlag von Louis Nebert, 1879.

[2] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. In: *TACAS*. Ed. by Erika Ábrahám and Klaus Havelund. Vol. 8413. LNCS. Berlin: Springer, 2014, 279–294. DOI: 10.1007/978-3-642-54862-8_19.

[3] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. New York: Academic Press, 1972.

[4] Sophus Lie. *Vorlesungen über continuierliche Gruppen mit geometrischen und anderen Anwendungen*. Leipzig: Teubner, 1893.

[5] Sophus Lie. Über Integralinvarianten und ihre Verwertung für die Theorie der Differentialgleichungen. *Leipz. Berichte* **49** (1897), 369–410.

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

[7] André Platzer. Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems. PhD thesis. Department of Computing Science, University of Oldenburg, 2008.

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

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

[10] André Platzer. A differential operator approach to equational differential invariants. In: *ITP*. Ed. by Lennart Beringer and Amy Felty. Vol. 7406. LNCS. Berlin: Springer, 2012, 28–48. DOI: 10.1007/978-3-642-32347-8_3.

[11] André Platzer. Logics of dynamical systems. In: *LICS*. Los Alamitos: IEEE, 2012, 13–24. DOI: 10.1109/LICS.2012.13.

[12] André Platzer. The complete proof theory of hybrid systems. In: *LICS*. Los Alamitos: IEEE, 2012, 541–550. DOI: 10.1109/LICS.2012.64.

[13] André Platzer. The structure of differential invariants and differential cut elimination. *Log. Meth. Comput. Sci.* **8**(4:16) (2012), 1–38. DOI: 10.2168/LMCS-8(4:16)2012.

[14] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.* **59**(2) (2017), 219–265. DOI: 10.1007/s10817-016-9385-1.

[15] Joseph Fels Ritt. *Differential equations from the algebraic standpoint*. Vol. 14. Colloquium Publications. New York: AMS, 1932.

[16] Dana Scott and Christopher Strachey. *Towards a mathematical semantics for computer languages*. Tech. rep. PRG-6. Oxford Programming Research Group, 1971.

[17] Wolfgang Walter. *Analysis 1*. 3rd ed. Berlin: Springer, 1992. DOI: 10.1007/978-3-662-38453-4.

[18] Eberhard Zeidler, ed. *Teubner-Taschenbuch der Mathematik*. Wiesbaden: Teubner, 2003. DOI: 10.1007/978-3-322-96781-7.