Chapter 11
Differential Equations & Proofs

Synopsis Furthering the remarkable shift in perspective toward a more thorough investigation of the wonders of the continuous dynamics of cyber-physical systems, this chapter advances logical induction techniques for differential equations from differential invariant terms to differential invariant formulas. Its net effect will be that not just the real value of a term can be proved to be invariant during a differential equation but also the truth-value of a formula. Differential invariants can prove that, e.g., the sign of a term never changes even if its value changes. Continuing the axiomatization of the differential equation aspects of differential dynamic logic, this chapter exploits a differential equation twist of Gerhard Gentzen's cut principle to obtain differential cuts that prove and then subsequently use properties of differential equations. The chapter will also advance the intuitions behind the continuous operational effects involved in CPS.

11.1 Introduction

Chapter 10 introduced equational differential invariants of the form $e = 0$ for differential equations that are significantly more general than the ones supported by the solution axiom $[']$ from Chap. 5. Axiom $[']$ equivalently replaces properties of differential equations with universally quantified properties of solutions, but is limited to differential equations that have explicit closed-form solutions whose resulting arithmetic can be handled (mostly polynomials or rational functions). But axiom $[']$ at least works for any arbitrary postcondition. The equational differential invariant proof rule dI supports general differential equations, but is limited to equational postconditions of the form $e = 0$.

The goal of this chapter is to generalize the differential invariant proof rule to work for more general postconditions but retain the flexibility with the more complicated differential equations that differential invariants provide. Indeed, the principles developed in Chap. 10 generalize beautifully to logical formulas other than the limited form $e = 0$. While $[x' = f(x)]\, e = 0$ expresses that the value of term e

A. Platzer, *Logical Foundations of Cyber-Physical Systems*,
https://doi.org/10.1007/978-3-319-63588-0_11

never changes and remains 0 along the differential equation $x' = f(x)$, other logical formulas such as $[x' = f(x)]\, e \geq 0$ allow term e to change its value as long as its sign remains nonnegative so that $e \geq 0$ is invariant and its truth-value remains *true*.

This chapter will establish generalizations that make the differential invariant proof rule work for formulas F of more general forms. The core of the differential invariant proof rule is its use of the differential $(e)'$ of the involved terms to determine quantities that, along the differential equation, are locally equal to the rate of change of the term e over time. The tricky bit is that it is conceptually significantly more challenging to apply derivative-based invariant principles to formulas than to terms. While invariant terms already had enough surprises in store for us in Chap. 10, they ultimately ended up relating in simple, sound, and well-defined ways to the intuitive concept of time-derivatives of values as rates of change along differential equations. But what could possibly be the counterpart of the rate of change or time-derivative for a formula? Formulas are either *true* or *false*, which makes it difficult to understand what their rate of change should be. While derivatives of terms can, at least intuitively, be understood as the question of how a function changes its value in the reals $\mathbb{R}$ at close-by points, it is not at all clear how to understand a small change to a close-by value when the only possible values of the formula are boolean in the set $\{true, false\}$. We cannot just say "the truth-value of formula P changes just a little bit when the state changes its values just a little bit along the differential equation" in any particularly simple meaningful way.

Fortunately, these considerations already provide some intuitive guidance toward an answer. Even if there is no wiggle room in the set of truth-values $\{true, false\}$, we still want to use differential reasoning to argue that small changes of the points lead to close-by truth-values, so stay *true* if they were *true* initially, because there simply are no truth-values close to *true* other than *true* itself. Of course, the most subtle and most crucial part will be defining and justifying the differential $(F)'$ of a formula such that the shape of the differential invariant proof rule is sound:

$$\text{dI}\quad \frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x)\,\&\,Q]F}$$

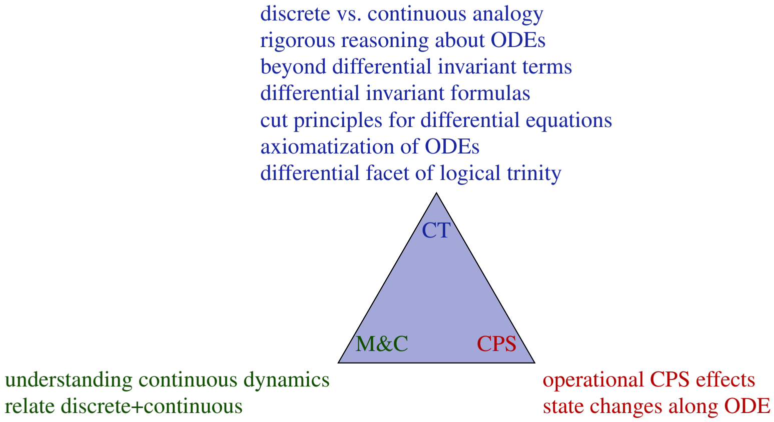
If, for example, the formula F in the conclusion is $e = 0$ and the evolution domain constraint Q is *true*, then Chap. 10 demonstrated that $(e)' = 0$ is a sound choice for the formula $(F)'$ in the premise of rule dI. This chapter investigates generalizations of rule dI that work for more general shapes of formula F than just $e = 0$. Differential invariants were originally introduced with another semantics [4, 5], but we follow an advanced axiomatic logical reading of differential invariants via differential forms [12] that also simplifies their intuitive understanding.

This chapter advances the capabilities of differential invariants that Chap. 10 started and continues to be of central significance for the Foundations of Cyber-Physical Systems in all but the most elementary CPSs. The most important learning goals of this chapter are:

Modeling and Control: This chapter continues the study of the core principles behind CPS by developing a deeper understanding of how continuous dynamical behavior affects the truth of logical formulas. The differential invariants developed in this chapter also have significance for developing models and controls using the design-by-invariant principle.

Computational Thinking: This chapter exploits computational thinking, continuing the surprising analogies between discrete dynamics and continuous dynamics discovered in Chap. 10. It is devoted to rigorous reasoning about differential equations in CPS models, which is crucial for understanding the continuous behavior that CPSs exhibit over time. This chapter systematically expands on the differential invariant terms for equational properties of differential equations developed in Chap. 10 and generalizes the same core principles to the study of general properties of differential equations. Computational thinking is exploited in a second way by generalizing Gentzen's cut principle, which is of seminal significance in discrete logic, to differential equations. This chapter continues the *axiomatization* of differential dynamic logic dL [9, 10] pursued since Chap. 5 and lifts dL's proof techniques to systems with more complex properties of more complex differential equations. The concepts developed in this chapter continue 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. Finally, the verification techniques developed in this chapter are critical for verifying CPS models of appropriate scale and technical complexity.

CPS Skills: The focus in this chapter is on reasoning about differential equations. As a beneficial side effect, we will develop better intuition for the operational effects involved in CPS by getting better tools for understanding how exactly state changes while the system follows a differential equation and what properties of the system will not change.


discrete vs. continuous analogy
rigorous reasoning about ODEs
beyond differential invariant terms
differential invariant formulas
cut principles for differential equations
axiomatization of ODEs
differential facet of logical trinity
CT
M&C
CPS
understanding continuous dynamics
relate discrete+continuous
operational CPS effects
state changes along ODE

11.2 Recap: Ingredients for Differential Equation Proofs

Before studying differential invariant formulas in greater detail, we first recall the semantics of differential equations from Chap. 3 and the semantics of differentials from Chap. 10:

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 $\varphi(z)(x') \overset{\text{def}}{=} \frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(z)$ and $\varphi(z) = \varphi(0)$ except at x, x'.

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

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

Our approach for more general differential invariants will leverage the fact that the following results from Chap. 10 already capture differential terms $(e)'$ and how their values relate to the change of the value of the term e over time, as well as the differential effects of differential equations on differential symbols. Equations of differentials can be used to compute with differentials akin to the process of forming derivatives which is called differentiation.

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 $x \in \mathscr{V}$)

The value of a differential, at least along a differential equation, equals the analytic time-derivative.

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

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

Differential equations can be substituted in via their differential effect.

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

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

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

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

These results are already more general and work for any postcondition P, not just normalized equations $e = 0$. Lemma 10.1 covers differentials of any polynomial (and rational) term. Lemma 10.2 relates their values to the change of value over time. Just the specific formulation of the differential invariant axiom needs to be generalized based on Lemma 10.2 to cover more general postconditions.

11.3 Differential Weakening

Just as the differential effect axiom DE perfectly internalizes the effect that differential equations have on the differential symbols, the differential weakening axiom internalizes the semantic effect of their evolution domain constraints (Definition 3.3). Of course, the effect of an evolution domain constraint Q is not to change the values of variables, but rather to limit the continuous evolution to always remain within the set of states $[\![Q]\!]$ where Q is true. There are multiple ways of achieving that [12] and you are invited to discover them.

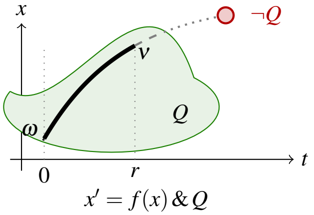
One simple but useful way is the following *differential weakening* axiom, somewhat reminiscent of the way axiom DE is phrased but for domain Q.

Lemma 11.1 (DW differential weakening axiom). *This axiom is sound:*

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

Since differential equations can never leave their evolution domain constraints (Fig. 11.1), any property P is true after the differential equation if and only if it is true whenever the evolution domain constraint Q is. The evolution domain constraint Q is always true throughout all evolutions of $x' = f(x) \,\&\, Q$ by Definition 3.3. We will see later that axiom DW justifies once and for all that the evolution domain constraint Q can be assumed soundly during any proof reasoning about differential equation $x' = f(x) \,\&\, Q$.

Fig. 11.1 Differential weakening axiom DW



On its own, the differential weakening axiom DW has the same shortcoming as the differential effect axiom DE and differential invariant axiom DI. They reduce one property of a differential equation to another property of that differential equation. Following up with a generalization rule G after the differential weakening axiom DW leads to the following differential weakening sequent proof rule that can be quite useful.

Lemma 11.2 (dW differential weakening proof rule). *The differential weakening proof rule derives from axiom DW:*

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

The system $x' = f(x) \,\&\, Q$ will stop before it leaves Q, hence, if Q implies P (i.e., the region Q is contained in the region P), then P is always true after the continuous evolution, no matter what the actual differential equation $x' = f(x)$ does.

Of course, it is crucial for soundness that rule dW drops the context Γ, Δ, which could not soundly be available in the premise (Exercise 11.3). The context Γ contains information about the initial state, which is no longer guaranteed to remain true in the final state. As usual, keeping assumptions about constants around would be acceptable (Sect. 7.5). Yet, on its own, even rule dW cannot prove particularly interesting properties, because it only work when Q is rather informative. Differential weakening can, however, be useful to obtain partial information about the domains of differential equations or in combination with stronger proof rules (Sect. 11.8). If an entire system model is proved with just differential weakening dW, then this indicates that the model may have assumed overly strong evolution domain constraints, because its property would be true independently of the differential equations (Sect. 8.2.2).

11.4 Operators in Differential Invariants

This section develops ways of handling logical and arithmetical operators in differential invariants. Thanks to axiom DW, we will soon see that the evolution domain constraint Q can be assumed during the induction step. All differential invariant rules have the same shape but differ in how they define the *differential formula* $(F)'$ in the induction step depending on F:

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

For the case where F is of the form $e = 0$ and Q is *true*, Chap. 10 justifies that this rule dI is sound when defining $(e = 0)'$ to be $(e)' = 0$. This leaves other shapes of the postcondition F and the evolution domain constraint Q to worry about. The differential invariant proof rules can also all be derived directly from corresponding differential induction axioms, given an appropriate definition and justification of $(F)'$. We first emphasize an intuitive gradual development, postponing the soundness proof until all cases of the rule have been developed.

11.4.1 Equational Differential Invariants

While Chap. 10 provided a way of proving postconditions of the form $e = 0$ for unsolvable differential equations, there are more general logical formulas that we would like to prove to be invariants of differential equations, not just the polynomial equations normalized such that they are single terms equaling 0. Direct proofs for postconditions of the form $e = k$ should work in almost the same way. In order to set the stage for the rest of this chapter, we develop an induction axiom and proof rule for differential equations with postcondition $e = k$ and simultaneously generalize it to the presence of evolution domain constraints Q using our newly discovered differential weakening principles captured in axiom DW.

Thinking back to the soundness proof for the case $e = 0$ in Sect. 10.3.6, the argument was based on the value of $\varphi(t)[\![e]\!]$ as a function of time t. The same argument can be made by considering the difference $\varphi(t)[\![e - k]\!]$ for postconditions of the form $e = k$. How does the inductive step for formula $e = k$ need to be defined to make a corresponding differential invariant proof rule sound? That is, for what premise is the following a sound proof rule when e and k are arbitrary terms?

$$\frac{\vdash ???}{e = k \vdash [x' = f(x)]e = k}$$

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

The following rule would make sense:

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

This rule for equational differential invariants captures the intuition that e always stays equal to k if it was initially (antecedent of conclusion) and the differential of term e is the same as the differential of k when using the right-hand side $f(x)$ of the differential equation $x' = f(x)$ for its left-hand side x'. For the case $Q \equiv \mathit{true}$, this rule fits the general shape of rule dI when we mnemonically define the "differential" of an equation $e = k$ as the formula

$$(e = k)' \overset{\text{def}}{\equiv} ((e)' = (k)')$$

This definition as the equation $(e)' = (k)'$ of the differentials of the two sides makes intuitive sense, because the truth-value of an equation $e = k$ does not change if the left- and right-hand side quantities have the same rate of change (Fig. 11.2).

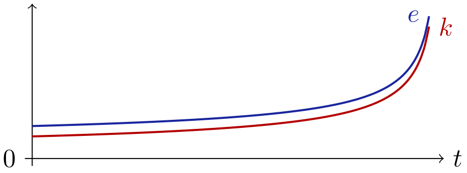


Fig. 11.2 Equal rate of change from equal initial value (drawn slightly apart for visualization)

The way we justified the soundness of the $e = 0$ case of the differential invariant proof rule dI in Sect. 10.4 was by deriving it from a corresponding differential invariant axiom DI, which captured the fundamental induction principle for terms along differential equations in more elementary ways. Let us pursue the same approach for the invariant $e = k$.

$$\text{DI}_= \quad \big([x' = f(x) \,\&\, Q]e = k \leftrightarrow [?Q]e = k\big) \leftarrow [x' = f(x) \,\&\, Q)](e)' = (k)'$$

This axiom expresses that, if $(e)' = (k)'$ always holds after the differential equation so that terms e and k always have the same rate of change, then e and k always have the same value after the differential equation if and only if they have the same value initially after the test $?Q$. The reason for the test $?Q$ is that the postcondition $e = k$ is vacuously true always after the differential equation $x' = f(x) \,\&\, Q$ when it starts outside its evolution domain constraint Q, because there is no evolution of the differential equation then. Correspondingly, the initial check $[?Q]e = k$ gets to assume the test $?Q$ passes, because otherwise there is nothing to show. Overall, axiom $\text{DI}_=$ expresses that two quantities that evolve with the same rate of change will always remain the same iff they start from the same value initially (Fig. 11.2).

Instead of going through a soundness proof for $\text{DI}_=$, however, we directly generalize the proof principles further and see whether differential invariants can prove even more formulas for us. We will later prove the soundness of the general differential invariant axiom, from which $\text{DI}_=$ derives as a special case.

11.4.2 Differential Invariant Proof Rule

Just as Sect. 11.4.1 did with axiom $\mathrm{DI}_=$ for the case of equational postconditions $e = k$, this section provides induction axioms for postconditions of differential equations that are all of the form

$$\mathrm{DI}\quad \big([x' = f(x)\,\&\,Q]P \leftrightarrow [?Q]P\big) \leftarrow [x' = f(x)\,\&\,Q)](P)'$$

This axiom expresses that, if a yet-to-be-defined differential formula $(P)'$ always holds after the differential equation so that P never changes its truth-value, then P is always true after the differential equation if and only if P was true initially after the test $?Q$. Since $[x' = f(x)\,\&\,Q]P$ always implies $[?Q]P$ by Definition 3.3 (using that $x' \notin \mathrm{FV}(P) \cup \mathrm{FV}(Q)$), only the converse implication needs the assumption $[x' = f(x)\,\&\,Q](P)'$. For each of the subsequently considered cases of $(P)'$, we only need to prove the validity of the following formula to prove the soundness of DI:

$$[x' = f(x)\,\&\,Q](P)' \rightarrow ([?Q]P \rightarrow [x' = f(x)\,\&\,Q]P)$$

For each case of this differential induction axiom DI, we obtain a corresponding differential invariant proof rule for free.

Lemma 11.3 (dI differential invariant proof rule). *The differential invariant proof rule derives from axiom DI:*

$$\mathrm{dI}\ \frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x)\,\&\,Q]F}$$

Proof. Proof rule dI derives from axiom DI as follows:

$$\text{DI}\ \dfrac{\text{[?]}\ \dfrac{\text{→R}\ \dfrac{\text{id}\ \dfrac{*}{F, Q \vdash F}}{F \vdash Q \rightarrow F}}{F \vdash [?Q]F} \qquad \text{DE}\ \dfrac{\text{DW}\ \dfrac{\text{G}\ \dfrac{\text{→R}\ \dfrac{Q \vdash [x' := f(x)](F)'}{\vdash Q \rightarrow [x' := f(x)](F)'}}{\vdash [x' = f(x)\,\&\,Q](Q \rightarrow [x' := f(x)](F)')}}{\vdash [x' = f(x)\,\&\,Q][x' := f(x)](F)'}}{\vdash [x' = f(x)\,\&\,Q](F)'}}{F \vdash [x' = f(x)\,\&\,Q]F}$$

□

The basic idea behind rule dI is that the premise of dI shows that the differential $(F)'$ holds within evolution domain Q when substituting the differential equations $x' = f(x)$ into $(F)'$. If F holds initially (antecedent of conclusion), then F itself always stays true (succedent of conclusion). Intuitively, the premise gives a condition showing that, within Q, the differential $(F)'$ along the differential constraints points inwards or transversally to F but never outwards to $\neg F$, as illustrated in

Fig. 11.3 Differential invariant F for safety

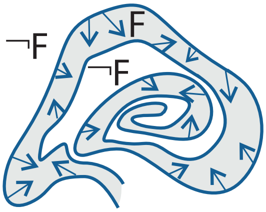


Fig. 11.3. Hence, if we start in F and, as indicated by $(F)'$, the local dynamics never points outside F, then the system always stays in F when following the dynamics.

Observe how useful it is that we have assembled an array of independent reasoning principles, differential effect DE, differential weakening DW, and generalization G, to combine and bundle the logically more elementary axiom DI to the more useful proof rule dI. Such modular combinations of reasoning principles are not just easier to prove sound, but also more flexible because they allow free variations in the argument structure. Recall, though, that the use of Gödel's generalization rule G for the derivation of dI implies it would be unsound to retain a sequent context Γ, Δ in its premise (except, as usual, assumptions about constants).

Example 11.1 (Rotational dynamics). Consider the system of rotational dynamics $v' = w, w' = -v$ from Example 10.1 on p. 293 once again. This dynamics is complicated in that the solution involves trigonometric functions, which are generally outside decidable classes of arithmetic. Yet, we can easily prove interesting properties about it using dI and decidable polynomial arithmetic. For instance, dI can directly prove formula (10.1), i.e., that $v^2 + w^2 = r^2$ is a differential invariant of the dynamics, using the following proof:

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

This proof is easier and more direct than the MR monotonicity proof in Chap. 10.

11.4.3 Differential Invariant Inequalities

The differential invariant axioms and proof rules considered so far give a good understanding of how to prove equational invariants. What about inequalities? How can they be proved?

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

The primary question to generalize the differential invariant proof rule is again how to mnemonically define a "differential," which we do as follows:

$$(e \leq k)' \overset{\text{def}}{\equiv} ((e)' \leq (k)')$$

This gives the following differential invariant axiom, which we simply call DI again:

$$\big([x' = f(x) \,\&\, Q]e \leq k \leftrightarrow [?Q]e \leq k\big) \leftarrow [x' = f(x) \,\&\, Q)](e \leq k)'$$

The only difference to the general axiom DI is the definition of the differential $(e \leq k)'$ and its soundness proof. The intuition is that a quantity e with smaller or equal rate of change than that of k starting from a smaller or equal value initially will always remain smaller or equal (Fig. 11.4). Lemma 11.3 derives the corresponding case of the differential induction rule dI from this axiom:

$$\frac{Q \vdash [x' := f(x)](e \leq k)'}{e \leq k \vdash [x' = f(x) \,\&\, Q]e \leq k}$$

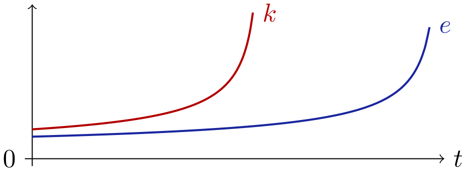


Fig. 11.4 Lesser or equal rate of change from lesser or equal initial value

Example 11.2 (Cubic dynamics). Similarly, differential induction can easily prove that $\frac{1}{3} \leq 5x^2$ is an invariant of the cubic dynamics $x' = x^3$; see the proof in Fig. 11.5 for the dynamics in Fig. 11.6. To apply the differential induction rule dI, we form the derivative of the differential invariant $F \equiv \frac{1}{3} \leq 5x^2$, which results in the dL formula $(F)' \equiv (\frac{1}{3} \leq 5x^2)' \equiv 0 \leq 5 \cdot 2xx'$. Now, the differential induction rule dI takes into account that the derivative of state variable x along the dynamics is known. Substituting the differential equation $x' = x^3$ into the inequality yields $[x' := x^3](F)' \equiv 0 \leq 5 \cdot 2xx^3$, which is a valid formula and is closed by quantifier elimination with rule $\mathbb{R}$.

Differential invariants that are inequalities are not just a minor variation of equational differential invariants, because they can prove more. That is, it can be shown [11] that there are valid formulas that can be proved using differential invariant inequalities but *cannot* be proved just using equations as differential invariants. Sometimes, you need to be prepared to look for inequalities that you can use as differential invariants. The converse is not true. Everything that is provable using equational differential invariants is also provable using differential invariant inequalities [11], but you should still look for equational differential invariants if they give easier proofs.

$$\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash 0 \le 5\cdot 2x(x^3)}}{\vdash [x':=x^3]0 \le 5\cdot 2xx'}}{\frac{1}{3} \le 5x^2 \vdash [x' = x^3]\frac{1}{3} \le 5x^2}$$

Fig. 11.5 Cubic dynamics proof

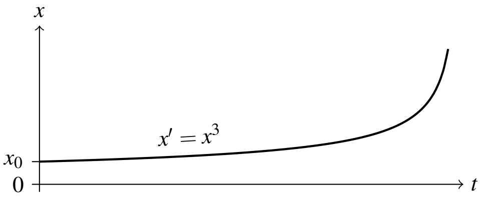


Fig. 11.6 Cubic dynamics

Strict inequalities could also be used as differential invariants when defining their "differentials" mnemonically as

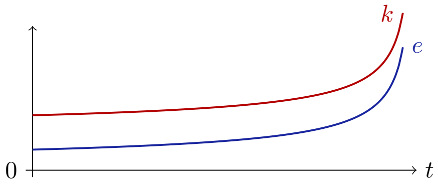
$$(e < k)' \overset{\text{def}}{\equiv} ((e)' < (k)')$$

However, we, instead, prefer a slightly relaxed definition that is also sound:

$$(e < k)' \overset{\text{def}}{\equiv} ((e)' \le (k)')$$

The intuition is again that a quantity e that starts from a smaller initial value than k and has *no larger rate of change* than that of k will always remain smaller (Fig. 11.7). The cases $e \ge k$ and $e > k$ work analogously.

Fig. 11.7 Lesser or equal rate of change from lesser initial value



Example 11.3 (Rotational dynamics). An inequality property can be proved easily for the rotational dynamics $v' = w, w' = -v$ using the following proof:

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

Example 11.4 (Odd-order dynamics). The following proof easily proves a simple invariant with only even powers of a dynamics with only odd powers:

$$\text{↯}\,\dfrac{\dfrac{*\ (\text{unsound})}{\vdash 1\neq 0}}{x\neq 5\vdash [x'=1]x\neq 5}$$

Fig. 11.8 Unsound attempt to use disequalities

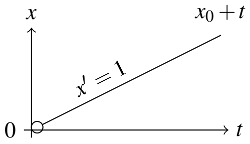


Fig. 11.9 Linear evolution of $x'=1$

$$\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2x^6+14x^4+4x^2\geq 0}}{\vdash [x':=x^5+7x^3+2x]\,2xx'\geq 0}}{x^2\geq 2\vdash [x'=x^5+7x^3+2x]x^2\geq 2}$$

Example 11.5 (Even-order dynamics). The following proof easily proves a simple invariant with only odd powers of a dynamics with only even powers:

$$\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2x^6+12x^4+10x^2\geq 0}}{\vdash [x':=x^4+6x^2+5]\,2x^2x'\geq 0}}{x^3\geq 2\vdash [x'=x^4+6x^2+5]x^3\geq 2}$$

Similar straightforward proofs work for any other appropriate sign condition on an odd power of a purely even dynamics or an even power of a purely odd dynamics, because the resulting arithmetic has only even powers and, thus, positive signs when added.

11.4.4 Disequational Differential Invariants

The case that is missing in differential invariant proof rules of atomic formulas is for postconditions that are disequalities $e\neq k$? How can they be proved?

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

By analogy to the previous cases, one might expect the following definition:

$$(e\neq k)' \overset{?}{\equiv} ((e)'\neq (k)') \quad ???$$

It is crucial for soundness of differential invariants that $(e\neq k)'$ is *not* defined that way! In the counterexample in Fig. 11.8, variable x can reach $x=0$ without its derivative ever being 0; again, see Fig. 11.9 for the dynamics. Of course, just because e and k start out different, does not mean they will always stay different if they evolve with different derivatives. *Au contraire*, it is because they evolve with different derivatives that they might catch each other (Fig. 11.10).

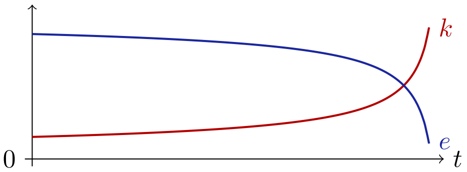


Fig. 11.10 Different rates of change from different initial values do not prove anything

Instead, if e and k start out different and evolve with the same derivative, they will always stay different. So the sound definition is slightly unexpected:

$$(e \neq k)' \overset{\text{def}}{\equiv} ((e)' = (k)')$$

11.4.5 Conjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a conjunction $F \land G$. The crucial question then is again what a "differential" $(F \land G)'$ would be that measures the rate of change in truth-values of the conjunction $F \land G$.

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

Of course, there aren't many changes of truth-values to speak of, because there are only two: *true* and *false*. But, still, no change in truth-value is a good thing for an invariant argument. An invariant should always stay *true* if it is *true* initially. To show that a conjunction $F \land G$ is invariant it is perfectly sufficient to prove that both are invariant. This can be justified separately, but is more obvious when recalling how box distributes over conjunctions.

Lemma 5.10 ([]∧ boxes distribute over conjunctions). *This axiom is sound:*

$$[]\land \quad [\alpha](P \land Q) \leftrightarrow [\alpha]P \land [\alpha]Q$$

Consequently, the mnemonic "differential" for conjunction is the conjunction of the differentials:

$$(A \land B)' \equiv (A)' \land (B)'$$

Soundness of this definition can be established by deriving it with the help of derived axiom []∧ to split each of the postconditions into separate conjuncts; see Fig. 11.11. The remaining premise in Fig. 11.11 is equivalent to the conjunction

$$\begin{aligned}&\big([x' = f(x) \,\&\, Q](A)' \to [?Q]A \to [x' = f(x) \,\&\, Q]A\big)\\ \land&\big([x' = f(x) \,\&\, Q](B)' \to [?Q]B \to [x' = f(x) \,\&\, Q]B\big)\end{aligned}$$

Both conjuncts derive from axiom DI by induction hypothesis, because they have simpler postconditions.

$$[]\wedge\;\dfrac{\vdash [x'=f(x)\,\&\,Q](A)'\wedge[x'=f(x)\,\&\,Q](B)' \to [?Q]A\wedge[?Q]B\to[x'=f(x)\,\&\,Q]A\wedge[x'=f(x)\,\&\,Q]B}{\vdash [x'=f(x)\,\&\,Q](A\wedge B)' \to [?Q](A\wedge B) \to [x'=f(x)\,\&\,Q](A\wedge B)}$$

Fig. 11.11 Soundness proof for conjunctive differential invariant axiom

Lemma 11.3 derives the corresponding case of the differential induction rule dI from this axiom, which enables us to prove conjunctions as in this example:

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

Of course, a manual proof using axiom []∧ to conduct two separate proofs that the left conjunct is a differential invariant and that, separately, the right conjunct also is a differential invariant would have worked equally well. As the invariant $v^2+w^2\le r^2\wedge v^2+w^2\ge r^2$ is equivalent to $v^2+w^2=r^2$, the above proof gives yet another proof of (10.1) when combined with a corresponding use of the generalization rule MR.

Example 11.6 (Bouncing ball's gravity). One of the major complications in the bouncing-ball proofs in Chap. 5 and Chap. 7 was the somewhat unwieldy arithmetic resulting from solving the differential equations. Its loop invariant can be proved more easily without solutions directly by differential invariants:

$$\mathrm{j}(x,v) \overset{\mathrm{def}}{\equiv} 2gx = 2gH - v^2 \wedge x\ge 0 \tag{7.10*}$$

The only complication is that this conjunction is not a differential invariant for the bouncing ball's dynamics $x'=v,v'=-g\,\&\,x\ge 0$, because $x\ge 0$ is not inductive since the resulting induction step $v\ge 0$ obtained from the differential $(x\ge 0)'$ is not valid because the velocity is negative on the way down.

Just like the justification for $(A\wedge B)'\equiv(A)'\wedge(B)'$ did, the proof in Fig. 11.12 also uses the []∧ axiom to split the postcondition and conduct independent proofs for independent questions. The trend for the conjunct $x\ge 0$ is potentially unsafe, because negative velocities would ultimately violate $x\ge 0$ if it wasn't for the evolution domain constraint keeping the ball above ground. Only the first conjunct is a differential invariant. The second conjunct can be proved by differential weakening (dW), because $x\ge 0$ is the evolution domain. Observe how the arithmetic in differential invariant reasoning is rather tame, because it is obtained by differentiation. This is quite unlike the arithmetic with solutions, which is obtained by integration.

$$[]\wedge\,\dfrac{\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{x\geq 0 \vdash 2gv=-2v(-g)}}{x\geq 0 \vdash [x':=v][v':=-g]2gx'=-2vv'}}{2gx=2gH-v^2 \vdash [x''=-g\,\&\,x\geq 0]2gx=2gH-v^2} \qquad \text{dW}\,\dfrac{\text{id}\,\dfrac{*}{x\geq 0 \vdash x\geq 0}}{\vdash [x''=-g\,\&\,x\geq 0]x\geq 0}}{2gx=2gH-v^2, x\geq 0 \vdash [x''=-g\,\&\,x\geq 0](2gx=2gH-v^2 \wedge x\geq 0)}$$

Fig. 11.12 Differential invariant proof for bouncing ball in gravity

11.4.6 Disjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a disjunction $A \vee B$. Our other lemmas take care of how to handle differential effects and differential weakening, if only we define the correct "differential" $(A \vee B)'$. How?

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

The "differential" of a conjunction is the conjunction of the differentials. So, by analogy, it might stand to reason to define the "differential" of a disjunction as the disjunction of the differentials.

$$(A \vee B)' \overset{?}{\equiv} (A)' \vee (B)' \quad ???$$

Let's give it a try:

$$↯\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{\text{unsound}}{\vdash 2vw+2w(-v)=0 \vee 5v+rw\geq 0}}{\vdash [v':=w][w':=-v]2vv'+2ww'=0 \vee r'v+rv'\geq 0}}{v^2+w^2=r^2 \vee rv\geq 0 \vdash [v'=w, w'=-v, r'=5](v^2+w^2=r^2 \vee rv\geq 0)}$$

That would be spectacularly wrong, however, because the formula at the bottom is not actually valid, so it does not deserve a proof, even if the formula at the top is valid. We have no business proving formulas that are not valid and if we ever could, we would have found a serious unsoundness in the proof rules.

For soundness of differential invariants, it is crucial that the "differential" $(A \vee B)'$ of a disjunction is defined, e.g., conjunctively as $(A)' \wedge (B)'$ instead of as $(A)' \vee (B)'$. From an initial state ω that satisfies $\omega \in [\![A]\!]$, and hence $\omega \in [\![A \vee B]\!]$, the formula $A \vee B$ is only sustained differentially if A itself is a differential invariant, not if B is. For instance, $v^2+w^2=r^2 \vee rv \geq 0$ is not an invariant of the above differential equation, because $rv \geq 0$ will be invalidated if we just follow the circle dynamics long enough. So if the disjunction was true because $rv \geq 0$ was true at the beginning, it does not stay invariant, even if the other disjunct $v^2+w^2=r^2$ is invariant.

Instead, splitting differential invariant proofs over disjunctions by the $\vee$L rule is the way to go, and, in fact, by axiom $[]\wedge$, also justifies the choice

$$(A \lor B)' \overset{\text{def}}{\equiv} (A)' \land (B)'$$

$$\text{→R}\dfrac{\text{∨L}\dfrac{\text{MR}\dfrac{\text{∨R}\dfrac{\text{id}\dfrac{*}{A \vdash A, B}}{A \vdash A \lor B} \qquad \text{dI}\dfrac{\vdash [x':=f(x)](A)'}{A \vdash [x' = f(x)]A}}{A \vdash [x' = f(x)](A \lor B)} \qquad \text{MR}\dfrac{\text{∨R}\dfrac{\text{id}\dfrac{*}{B \vdash A, B}}{B \vdash A \lor B} \qquad \text{dI}\dfrac{\vdash [x':=f(x)](B)'}{B \vdash [x' = f(x)]B}}{B \vdash [x' = f(x)](A \lor B)}}{A \lor B \vdash [x' = f(x)](A \lor B)}}{\vdash A \lor B \to [x' = f(x)](A \lor B)}$$

Soundness of the differential induction axiom with this definition of the differentials of disjunctions can be proved directly (Fig. 11.13). The proof uses that $[?Q](A \lor B)$ is indeed equivalent to $[?Q]A \lor [?Q]B$ because both are equivalent to $Q \to A \lor B$. From disjunct $[?Q]A$, the assumption $[x' = f(x) \,\&\, Q](A)'$ makes it possible to derive $[x' = f(x) \,\&\, Q]A$ from axiom DI by induction hypothesis (it has a simpler postcondition), from which $[x' = f(x) \,\&\, Q](A \lor B)$ derives by monotonicity rule M$[\cdot]$. Similarly, disjunct $[?Q]B$ derives $[x' = f(x) \,\&\, Q]B$, from which $[x' = f(x) \,\&\, Q](A \lor B)$ also derives by monotonicity rule M$[\cdot]$.

11.5 Differential Invariants

Differential invariants are a general proof principle for proving invariants of differential equations. Summarizing what this chapter has discovered so far leads to a single axiom DI for differential invariants, from which the corresponding differential invariant proof rule dI derives.

Definition 11.1 (Differential). The following definition generalizes the differential operator $(\cdot)'$ from terms to real-arithmetic formulas:

$$\begin{aligned}
(F \land G)' &\equiv (F)' \land (G)' && \\
(F \lor G)' &\equiv (F)' \land (G)' && \\
(e \geq k)' &\equiv (e)' \geq (k)' && \text{accordingly for } \leq, = \\
(e > k)' &\equiv (e)' \geq (k)' && \text{accordingly for } < \\
(e \neq k)' &\equiv (e)' = (k)' &&
\end{aligned}$$

The operation mapping F to $[x':=f(x)](F)'$ is also called the *Lie-derivative* of F with respect to $x' = f(x)$.

$$[]\land\dfrac{\vdash [x' = f(x) \,\&\, Q](A)' \land [x' = f(x) \,\&\, Q](B)' \to ([?Q]A \lor [?Q]B \to [x' = f(x) \,\&\, Q](A \lor B))}{\vdash [x' = f(x) \,\&\, Q](A \lor B)' \to [?Q](A \lor B) \to [x' = f(x) \,\&\, Q](A \lor B)}$$

Fig. 11.13 Soundness proof for disjunctive differential invariant axiom

By Definition 11.1, the "differential" $(F)'$ of formula F uses the differential $(e)'$ of the terms e that occur within F. It is possible to lift differential invariants to quantifiers [7], but for our purposes here, it is enough to assume quantifier elimination has been applied to first eliminate the quantifiers equivalently (Sect. 6.5).

Just like for the initial condition check $[?Q]P$, a minor twist on the DI axiom shows that the induction step $[x' = f(x) \,\&\, Q](P)'$ can also assume Q, because no evolution is possible if the system starts outside Q.

Lemma 11.4 (DI differential invariant axiom). *This axiom is sound:*

$$\text{DI} \quad \big([x' = f(x) \,\&\, Q]P \leftrightarrow [?Q]P\big) \leftarrow \big(Q \rightarrow [x' = f(x) \,\&\, Q](P)'\big)$$

The general form of the differential invariant proof rule is derived as in Sect. 11.4.2.

Lemma 11.3 (dI differential invariant proof rule). *The differential invariant proof rule derives from axiom DI:*

$$\text{dI} \quad \frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \,\&\, Q]F}$$

This proof rule enables us to easily prove (10.2) and all previous proofs as well. The following version dI' can be derived easily from the more fundamental, essential form dI similarly to how the most useful loop induction rule loop derives from the essential form ind. We do not use the version dI' in practice, because it is subsumed by a more general proof technique investigated in Sect. 11.8.

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

Proof (of Lemma 11.4). A detailed axiomatic proof of axiom DI is located elsewhere [12]. The proof of one implication was already in Sect. 11.4.2:

$$[x' = f(x) \,\&\, Q]P \rightarrow [?Q]P$$

The proof of the following implication will be by induction on the structure of P:

$$[x' = f(x) \,\&\, Q](P)' \rightarrow \big([?Q]P \rightarrow [x' = f(x) \,\&\, Q]P\big) \tag{11.1}$$

This proof directly implies the validity of the following direction, because the differential equation cannot run if Q is not initially true and then also fails test $?Q$:

$$\big(Q \rightarrow [x' = f(x) \,\&\, Q](P)'\big) \rightarrow \big([?Q]P \rightarrow [x' = f(x) \,\&\, Q]P\big)$$

The proof of the validity of (11.1) is by structural induction on P. The case of solutions of duration 0 follows directly from the assumption $[?Q]P$ by Definition 3.3 (using that $x' \notin \mathrm{FV}(P) \cup \mathrm{FV}(Q)$).

1. If P is of the form $e \geq 0$, so $(P)'$ is $(e)' \geq 0$, then consider a state ω satisfying $[x' = f(x) \,\&\, Q](e)' \geq 0$ and $[?Q]e \geq 0$. To show that $\omega \in [\![[x' = f(x) \,\&\, Q]e \geq 0]\!]$, consider any solution $\varphi : [0,r] \to \mathscr{S}$ with $\varphi \models x' = f(x) \land Q$ and $\varphi(0) = \omega$ except at x'. By Lemma 10.2, the function $h(t) \overset{\text{def}}{=} \varphi(t)[\![e]\!]$ is differentiable on $[0,r]$ if $r > 0$ and, provided $\mathrm{FV}(e) \subseteq \{x\}$, its time-derivative is
$$\frac{\mathsf{d}h(t)}{\mathsf{d}t}(z) = \frac{\mathsf{d}\varphi(t)[\![e]\!]}{\mathsf{d}t}(z) = \varphi(z)[\![(e)']\!] \geq 0$$
for all times $z \in [0,r]$ by the assumption $\omega \in [\![[x' = f(x) \,\&\, Q](e)' \geq 0]\!]$. Since h is differentiable, there is some $0 < \xi < r$ by the mean-value theorem such that:
$$h(r) - \underbrace{h(0)}_{\geq 0} = \underbrace{(r-0)}_{>0} \underbrace{\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi)}_{\geq 0} \geq 0 \tag{11.2}$$
Since $h(0) \geq 0$ by $\omega \in [\![[?Q]e{\geq}0]\!]$, this implies $h(r) \geq 0$. Hence, $\varphi(r) \in [\![e \geq 0]\!]$. Thus, $\omega \in [\![[x' = f(x) \,\&\, Q]e \geq 0]\!]$ since this proof works for any solution φ.
2. If P is of the form $e \geq k$ the above case applies to the equivalent $e - k \geq 0$, whose differential $(e)' - (k)' \geq 0$ is equivalent to the differential $(e)' \geq (k)'$.
3. If P is of the form $e = k$, a simple variation of the above proof applies. Alternatively, consider the equivalent $e \geq k \land k \geq e$, which has a differential $(e)' \geq (k)' \land (k)' \geq (e)'$ that is equivalent to the differential $(e)' = (k)'$. The minor twist is that this needs a shift in the well-founded induction to artificially consider conjunctions of inequalities smaller than equations.
4. If P is of the form $e > k$, a simple variation of the above proof applies, since its differential $(e)' \geq (k)'$ is equivalent to the differential of $e \geq 0$. The only additional thought is that the initial assumption $h(0) > 0$ implies $h(r) > 0$ by (11.2).
5. If P is of the form $A \land B$, then the derivation in Fig. 11.11 concludes the validity of (11.1) for postcondition $A \land B$ from the validity of (11.1) for the smaller postcondition A as well as the smaller postcondition B, which are both valid by induction hypothesis.
6. If P is of the form $A \lor B$, then the derivation in Fig. 11.13 concludes the validity of (11.1) for postcondition $A \lor B$ from the validity of (11.1) for the smaller postcondition A as well as the smaller postcondition B, which are both valid by induction hypothesis. □

Generalizations to systems of differential equations are quite straightforward.

11.6 Example Proofs

So that we gain more experience with differential invariants, this section studies a few example proofs.

Example 11.7 (Quartic dynamics). The following simple dL proof uses rule dI to prove an invariant of a quartic dynamics:

$$\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{a \geq 0 \vdash 3x^2((x-3)^4+a) \geq 0}}{a \geq 0 \vdash [x':=(x-3)^4+a]3x^2x' \geq 0}}{x^3 \geq -1 \vdash [x' = (x-3)^4+a \,\&\, a \geq 0]x^3 \geq -1}$$

Rule dI directly makes the evolution domain constraint $a \geq 0$ available as an assumption in the premise, because the continuous evolution is never allowed to leave it.

Example 11.8 (Damped oscillator). Consider $x' = y, y' = -\omega^2 x - 2d\omega y$, which is the differential equation for the damped oscillator with the undamped angular frequency ω and the damping ratio d. See Fig. 11.14 for one example of an evolution along this continuous dynamics. Figure 11.14 shows an evolution of x over time t on the left and a trajectory in the x,y state space on the right, which does not leave the green elliptic region $\omega^2 x^2 + y^2 \leq c^2$. General symbolic solutions of symbolic initial-value problems for this differential equation can become surprisingly difficult. A differential invariant proof, instead, is very simple:

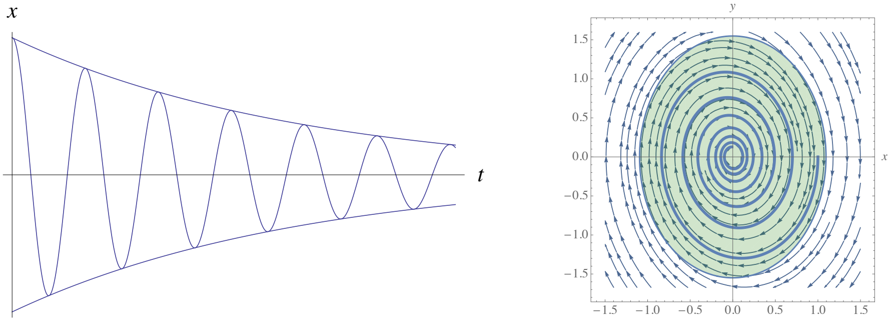


Fig. 11.14 Damped-oscillator time trajectory (**left**) and invariant in phase space (**right**)

$$\text{dI}\,\dfrac{[:=]\,\dfrac{\mathbb{R}\,\dfrac{*}{\omega \geq 0 \land d \geq 0 \vdash 2\omega^2 xy - 2\omega^2 xy - 4d\omega y^2 \leq 0}}{\omega \geq 0 \land d \geq 0 \vdash [x':=y][y':=-\,\omega^2 x - 2d\omega y]2\omega^2 xx' + 2yy' \leq 0}}{\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \land d \geq 0)]\, \omega^2 x^2 + y^2 \leq c^2}$$

Observe that rule dI directly makes the evolution domain constraint $\omega \geq 0 \land d \geq 0$ available as an assumption in the premise, because the continuous evolution is never allowed to leave it.

11.7 Assuming Invariants

Let's make the dynamics more interesting and see what happens. Suppose there is a robot at a point with coordinates (x,y) that is facing in direction (v,w). Suppose the robot moves with constant (linear) velocity into direction (v,w). Suppose the direction (v,w) is simultaneously rotating as in Example 10.1 with an angular velocity ω as in Example 2.7 (Fig. 3.9). Then the resulting differential equations are:

$$x' = v, y' = w, v' = \omega w, w' = -\omega v$$

because the derivative of the x coordinate is the component v of the direction and the derivative of the y coordinate is the component w of the direction. The angular velocity ω determines how fast the direction (v,w) rotates. Consider the conjecture

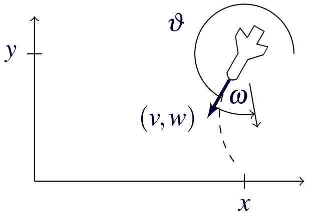


Fig. 11.15 Illustration of the Dubins dynamics of a point (x,y) moving in direction (v,w) along a dashed curve with angular velocity ω

$$(x-1)^2+(y-2)^2 \geq p^2 \rightarrow [x' = v, y' = w, v' = \omega w, w' = -\omega v](x-1)^2+(y-2)^2 \geq p^2 \tag{11.3}$$

This conjecture expresses that the robot at position (x,y) will always stay at distance $\geq p$ from the point $(1,2)$ if it started there. Let's try to prove conjecture (11.3):

$$\dfrac{\dfrac{\vdash 2(x-1)v+2(y-2)w \geq 0}{\vdash [x':=v][y':=w]2(x-1)x'+2(y-2)y' \geq 0}[:=]}{(x-1)^2+(y-2)^2 \geq p^2 \vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v](x-1)^2+(y-2)^2 \geq p^2}\text{dI}$$

Unfortunately, this differential invariant proof does not work. As a matter of fact, *fortunately* it does not work out, because conjecture (11.3) is not valid, so we will not be able to prove it with a sound proof technique. Conjecture (11.3) is too optimistic. Starting from a bad direction far far away, the robot will get too close to the point (1,2). Other directions may be fine.

Inspecting the above failed proof attempt, we could prove (11.3) if we knew something about the direction (v,w) that would allow the remaining premise to be proved. What could that be?

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

Certainly, if we knew $v = w = 0$, the resulting premise would be proved. Yet, that case is pretty boring because it corresponds to the point (x,y) being stuck forever. A more interesting case in which the premise would easily be proved is if we knew

$x-1=-w$ and $y-2=v$. In what sense could we “know” $x-1=-w\land y-2=v$? Certainly, we would have to assume this compatibility condition for directions versus position is true in the initial state, otherwise we would not necessarily know the condition holds true where we need it. So let’s modify (11.3) to include this assumption:

$$x-1=-w\land y-2=v\land (x-1)^2+(y-2)^2\geq p^2\rightarrow \\ [x'=v,y'=w,v'=\omega w,w'=-\omega v](x-1)^2+(y-2)^2\geq p^2 \tag{11.4}$$

Yet, the place in the proof where we need to know $x-1=-w\land y-2=v$ for the above sequent proof to continue is in the middle of the inductive step. How can we make that happen?

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

One step in the right direction is to check whether $x-1=-w\land y-2=v$ is a differential invariant of the dynamics, so it stays true forever if it is true initially:

$$\text{dI}\;\dfrac{[{:=}]\;\dfrac{\dfrac{\text{not valid}}{\vdash v=-(-\omega v)\land w=\omega w}}{\vdash [x'{:=}v][y'{:=}w][v'{:=}\omega w][w'{:=}-\omega v](x'=-w'\land y'=v')}}{x-1=-w\land y-2=v\vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v](x-1=-w\land y-2=v)}$$

This prove does not quite work out, because the two sides of the equations are off by a factor of ω and, indeed, $x-1=-w\land y-2=v$ is not an invariant unless $\omega=1$. On second thoughts, that makes sense, because the angular velocity ω determines how quickly the robot turns, so if there is any relation between position and direction at all, it should somehow depend on the angular velocity ω.

Let’s refine the conjecture to incorporate the angular velocity on the side of the equation where it was missing in the above proof and consider $\omega(x-1)=-w\land\omega(y-2)=v$ instead. That knowledge would still help the proof of (11.3), just with the same extra factor on both terms. So let’s modify (11.4) to use this assumption on the initial state:

$$\omega(x-1)=-w\land\omega(y-2)=v\land (x-1)^2+(y-2)^2\geq p^2\rightarrow \\ [x'=v,y'=w,v'=\omega w,w'=-\omega v](x-1)^2+(y-2)^2\geq p^2 \tag{11.5}$$

A simple proof shows that the new addition $\omega(x-1)=-w\land\omega(y-2)=v$ is a differential invariant of the dynamics, so it holds always if it holds at the beginning:

$$\text{dI}\;\dfrac{[{:=}]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash \omega v=-(-\omega v)\land \omega w=\omega w}}{\vdash [x'{:=}v][y'{:=}w][v'{:=}\omega w][w'{:=}-\omega v](\omega x'=-w'\land \omega y'=v')}}{\omega(x-1)=-w\land\omega(y-2)=v\vdash [x'=v,y'=w,v'=\omega w,w'=-\omega v](\omega(x-1)=-w\land\omega(y-2)=v)}$$

Now, how can this freshly proved invariant $\omega(x-1) = -w \land \omega(y-2) = v$ be made available in the previous proof? Perhaps we could prove (11.5) using the conjunction of the invariant we want with the additional invariant we need:

$$(x-1)^2 + (y-2)^2 \geq p^2 \land \omega(x-1) = -w \land \omega(y-2) = v$$

That does not work (eliding the antecedent in the conclusion just for space reasons):

$$\begin{array}{rl}
 & \vdash 2(x-1)v + 2(y-2)w \geq 0 \land \omega v = -(-\omega v) \land \omega w = \omega w \\ \hline
[:=] & \vdash [x':=v][y':=w][v':=\omega w][w':=-\,\omega v](2(x-1)x' + 2(y-2)y' \geq 0 \land \omega x' = -w' \land \omega y' = v') \\ \hline
\mathrm{dI} & ..\vdash [x' = v, y' = w, v' = \omega w, w' = -\omega v]((x-1)^2 + (y-2)^2 \geq p^2 \land \omega(x{-}1){=}{-}w \land \omega(y{-}2){=}v)
\end{array}$$

because the right conjunct in the premise is still proved beautifully but the left conjunct in the premise needs to know the invariant, while the differential invariant proof rule dI does not make the invariant F available in the antecedent of the premise.

In the case of loops, the invariant F can be assumed to hold before the loop body in the induction step (the other form loop of the loop invariant rule):

$$\text{ind}\ \frac{P \vdash [\alpha]P}{P \vdash [\alpha^*]P}$$

By analogy, we could augment the differential invariant proof rule dI similarly to include the invariant in the assumptions. Is that a good idea?

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

It looks tempting to suspect that rule dI could be improved by assuming the differential invariant F in the antecedent of the premise:

$$\mathrm{dI}_{??}\ \frac{Q \land F \vdash [x':=f(x)](F)'}{F \vdash [x' = f(x)\,\&\,Q]F} \quad \text{sound?}$$

After all, we really only care about staying safe when we are still safe since we start safe. Rule $\mathrm{dI}_{??}$ would indeed easily prove the formula (11.5), which might make us cheer. But implicit properties of differential equations are a subtle business. Assuming F as in rule $\mathrm{dI}_{??}$ would, in fact, be *unsound*, as the following simple counterexample shows, which "proves" an invalid property using the unsound proof rule $\mathrm{dI}_{??}$:

$$\begin{array}{rl}
 & \text{(unsound)} \\ \hline
 & v^2 - 2v + 1 = 0 \vdash 2vw - 2w = 0 \\ \hline
 & v^2 - 2v + 1 = 0 \vdash [v':=w][w':=-\,v](2vv' - 2v' = 0) \\ \hline
\text{↯} & v^2 - 2v + 1 = 0 \vdash [v' = w, w' = -v]v^2 - 2v + 1 = 0
\end{array}$$

Of course, $v^2 - 2v + 1 = 0$ does *not* stay true for the rotational dynamics, because v changes! And there are many other invalid properties that the unsound proof rule $\mathrm{dI}_{??}$ would claim to "prove," for example.

$$\text{↯}\;\dfrac{\dfrac{\dfrac{\text{(unsound)}}{-(x-y)^2 \geq 0 \vdash -2(x-y)(1-y) \geq 0}}{-(x-y)^2 \geq 0 \vdash [x':=1][y':=y](-2(x-y)(x'-y') \geq 0)}}{-(x-y)^2 \geq 0 \vdash [x' = 1, y' = y](-(x-y)^2 \geq 0)}$$

Assuming an invariant of a differential equation during its own proof is, thus, terribly incorrect, even though it has been suggested numerous times in the literature. There are some cases for which rule dI$_{??}$ or variations of it are still sound, but these are nontrivial [2, 3, 5, 8, 11]. The reason why assuming invariants for their own proof is problematic for the case of differential equations is subtle [5, 11]. In a nutshell, the proof rule dI$_{??}$ assumes more than it knows, so that the argument becomes cyclic. The antecedent only provides the invariant at a single point and Chap. 10 already explained that derivatives are not particularly well defined at a single point. That is one of the reasons why we had to exercise extraordinary care in our arguments to define precisely what derivatives and differentials were to begin with in Chap. 10. Unlike time-derivatives, differentials have meaning in isolated states.

11.8 Differential Cuts

Instead of these ill-guided attempts to assume invariants for their own proof, there is a complementary proof rule for *differential cuts* [4, 5, 8, 11] that can be used to strengthen assumptions about differential equations in a sound way.

Lemma 11.5 (dC differential cut proof rule). *The differential cut proof rule is sound and derives from axiom DC, which will be considered subsequently:*

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

The differential cut rule works like a logical cut, but for differential equations. Recall the cut rule from Chap. 6, which can be used to prove a formula C in the left premise as a lemma and then assume it in the right premise:

$$\text{cut}\quad \frac{\Gamma \vdash C, \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta}$$

Similarly, differential cut rule dC proves a property C of a differential equation in the left premise and then assumes C to hold in the right premise, except that it assumes C to hold *during* a differential equation by restricting the behavior of the system. To prove the original postcondition P from the conclusion, rule dC restricts the system evolution in the right premise to the subdomain $Q \land C$ of Q, which changes the system dynamics but is a pseudo-restriction, because the left premise proves that C is an invariant anyhow (e.g., using rule dI). Note that rule dC is special in that it *changes the dynamics of the system* (it adds a constraint to the system evolution domain region), but it is still sound, because this change does not reduce the reachable set, thanks to the left premise; see Fig. 11.16

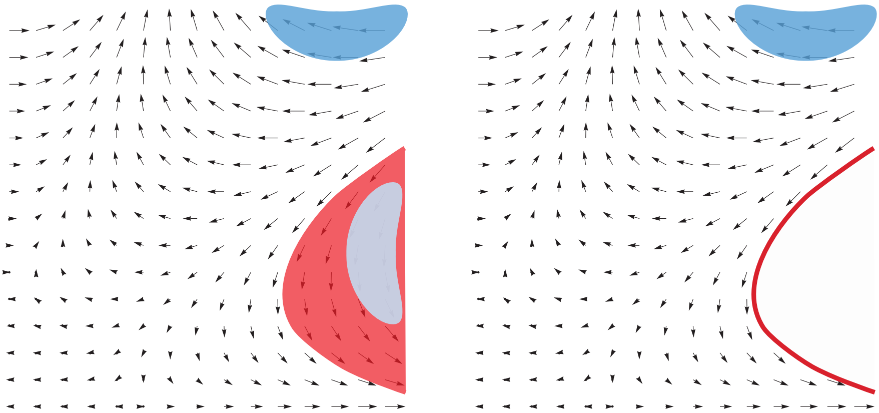


Fig. 11.16 If the solution of the differential equation can never leave region C and enter the red region $\neg C$ (**left**), then this unreachable region $\neg C$ can be cut out of the state space without changing the dynamics of the system by restricting it to C (**right**)

The benefit of rule dC is that C will (soundly) be available as an extra assumption for all subsequent dI uses in the right premise (see, e.g., the use of the evolution domain constraint in Example 11.8). In particular, the differential cut rule dC can be used to strengthen the right premise with more and more auxiliary differential invariants C that will be available as extra assumptions in the right premise, once they have been proven to be differential invariants in the left premise.

Example 11.9 (Increasingly damped oscillator). The damped oscillator in Example 11.8 was easily provable, but its proof crucially depended on having the damping coefficient $d \geq 0$ in the evolution domain constraint so that the induction step knew that the damping coefficient was not negative. In the following increasingly damped oscillator, the damping coefficient changes (albeit in arbitrary ways):

$$\omega^2x^2+y^2 \leq c^2 \wedge d \geq 0 \rightarrow [x' = y, y' = -\omega^2x - 2d\omega y, d' = 7 \,\&\, \omega \geq 0]\, \omega^2x^2+y^2 \leq c^2$$

This makes the damped oscillator apply increasing damping, but the system still always stays in the ellipse (Fig. 11.17). A direct proof with a differential invariant will fail, because of the lack of knowledge about the damping coefficient d, which, after all, is now changing. But the indirect proof in Fig. 11.18 succeeds. It uses a differential cut with $d \geq 0$ to first prove, in the left branch, that d always remains nonnegative by a differential invariant argument, and then continues the right branch as in Example 11.8 using the new added evolution domain constraint $d \geq 0$.

Proposition 11.1 (Increasingly damped oscillation). *This* dL *formula is valid:*

$$\omega^2x^2+y^2 \leq c^2 \wedge d \geq 0 \rightarrow [x' = y, y' = -\omega^2x - 2d\omega y, d' = 7 \,\&\, \omega \geq 0]\, \omega^2x^2+y^2 \leq c^2$$

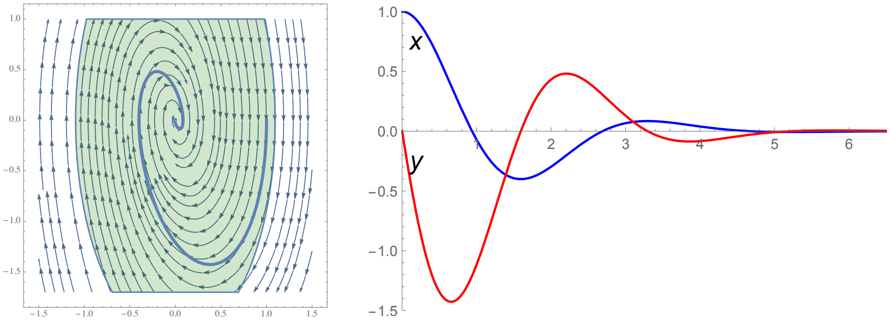


Fig. 11.17 Trajectory with vector field and evolution of an increasingly damped oscillator

$$\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\omega\geq0\vdash 7\geq0}}{\omega\geq0\vdash[d':=7]\,d'\geq0}}{d\geq0\vdash[x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,d\geq0}$$

proof as in Example 11.8

$$\text{dC}\;\dfrac{d\geq0\vdash[\text{above}]\,d\geq0\qquad \omega^2x^2+y^2\leq c^2\vdash[x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0\wedge d\geq0]\,\omega^2x^2+y^2\leq c^2}{\omega^2x^2+y^2\leq c^2,d\geq0\vdash[x'=y,y'=-\omega^2x-2d\omega y,d'=7\,\&\,\omega\geq0]\,\omega^2x^2+y^2\leq c^2}$$

Fig. 11.18 Differential cut proof for the increasingly damped oscillator

Example 11.10 (Robot formula). Proving the robot formula (11.5) in a sound way is now easy using a differential cut dC by $\omega(x-1)=-w\wedge\omega(y-2)=v$ after we abbreviate $(x-1)^2+(y-2)^2\geq p^2$ by A and $\omega(x-1)=-w\wedge\omega(y-2)=v$ by B:

$$\text{dC}\;\dfrac{\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{B\vdash 2(x-1)v+2(y-2)w\geq0}}{B\vdash[x':=v][y':=w](2(x-1)x'+2(y-2)y'\geq0)}}{\lhd\quad A\vdash[x'=v,y'=w,v'=\omega w,w'=-\omega v\,\&\,\omega(x-1)=-w\wedge\omega(y-2)=v](x-1)^2+(y-2)^2\geq p^2}}{A,B\vdash[x'=v,y'=w,v'=\omega w,w'=-\omega v](x-1)^2+(y-2)^2\geq p^2}$$

The first premise of the use of rule dC that is elided above (marked by $\lhd$) is proved:

$$\text{dI}\;\dfrac{[:=]\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash\omega v=-(-\omega v)\wedge\omega w=\omega w}}{\vdash[x':=v][y':=w][v':=\omega w][w':=-\,\omega v](\omega x'=-w'\wedge\omega y'=v')}}{\omega(x-1)=-w\wedge\omega(y-2)=v\vdash[x'=v\,..](\omega(x-1)=-w\wedge\omega(y-2)=v)}$$

Amazing. Now we have a proper sound proof of the quite nontrivial robot motion property (11.5). And it even is a surprisingly short proof.

It is not always enough to just do a single differential cut. Sometimes, you may want to do a differential cut with a formula C, then use C on the right premise of dC to prove a second differential cut with a formula D and then on its right premise have $C\wedge D$ available to continue the proof; see Fig. 11.19. For example, we could also have gotten a proof of (11.5) by first doing a differential cut with $\omega(x-1)=-w$, then continuing with a differential cut with $\omega(y-2)=v$, and then finally uising both to prove the postcondition (Exercise 11.6). Using this differential cut process repeatedly has turned out to be extremely useful in practice and even simplifies the invariant search, because it leads to several simpler properties to find and prove instead of a single complex property [6, 13, 14].

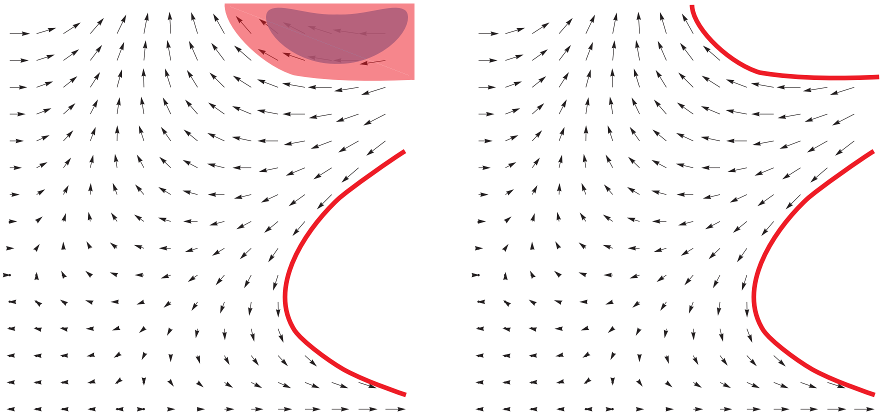


Fig. 11.19 If the solution of the differential equation can never leave region D and enter the top red region $\neg D$ (**left**), then this unreachable region $\neg D$ can also be cut out of the state space without changing the dynamics of the system by restricting it further to D (**right**)

It is straightforward to prove the differential cut rule dC sound from the semantics. The other differential equation proof rules were, however, proved sound by deriving them from corresponding axioms, which are, in turn, proved sound from the semantics. That approach also works for differential cuts.

Lemma 11.6 (DC differential cut axiom). *This axiom is sound:*

$$\text{DC} \quad \big([x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q \land C]P\big) \leftarrow [x' = f(x)\,\&\,Q]C$$

Proof. Any state that satisfies $[x' = f(x)\,\&\,Q]P$ also satisfies $[x' = f(x)\,\&\,Q \land C]P$, because every solution of $\varphi \models x' = f(x) \land Q \land C$ also solves $\varphi \models x' = f(x) \land Q$.

Conversely, consider an initial state ω satisfying the assumption $[x' = f(x)\,\&\,Q]C$. Thus, starting in ω, every solution φ that satisfies $\varphi \models x' = f(x) \land Q$ also satisfies C after the solution, so *all along* the solution, because every restriction of a solution is a solution. Thus, if solution φ starts in ω and satisfies $\varphi \models x' = f(x) \land Q$, it also satisfies $\varphi \models x' = f(x) \land Q \land C$, so that the assumption $\omega \in [\![[x' = f(x)\,\&\,Q \land C]P]\!]$ implies $\omega \in [\![[x' = f(x)\,\&\,Q]P]\!]$. □

The differential cut rule dC derives directly from the differential cut axiom DC. Compared to rule dC, the axiom DC has the additional information that the right premise and conclusion of rule dC are, indeed, *equivalent* if the left premise is valid.

11.9 Differential Weakening Again

Observe how differential weakening from Sect. 11.3 can be useful in combination with differential cuts. For example, after having performed the differential cut illustrated in Fig. 11.16 and, then, subsequently, performing the differential cut illustrated in Fig. 11.19, all unsafe blue regions have been cut out of the state space, so that the system in Fig. 11.19(right) is trivially safe by differential weakening, because there are no more unsafe blue regions. That is, the ultimate evolution domain constraint $Q \land C \land D$ after the two differential cuts with C and with D trivially implies the safety condition F, i.e., $Q \land C \land D \vdash F$ is valid. But notice that it took the two differential cuts to make differential weakening useful. The original evolution domain constraint Q was not strong enough to imply safety, since there were still unsafe blue regions in the original system in Fig. 11.16(left) and even still in the intermediate system in Fig. 11.19(left) obtained after one differential cut with C.

If the system starts in an initial state where the evolution domain constraint is not satisfied, the system is stuck so cannot evolve for any duration, not even for duration 0. Any postcondition holds after *all* continuous evolutions of $x' = f(x) \& Q$ if there simply are *none*. In particular in a state where the evolution domain constraint Q is *false*, the differential invariant axiom DI proves $[x' = f(x) \& Q]\mathit{false}$, because the assumption Q in the induction step is not satisfied and the test $?Q$ in $[?Q]\mathit{false}$ fails.

Such a proof, thus, is closed by a differential cut dC with *false* followed by a use of differential invariant axiom DI and differential weakening dW to show that the original postcondition follows from the augmented evolution domain constraint $Q \land \mathit{false}$. An easier proof is to use the monotonicity rule MR to prove the new postcondition *false*, which trivially implies the original postcondition P, and is proved by differential invariant axiom DI if the initial condition A implies $\neg Q$ so that the conjunction $A \land Q$ is a contradiction (even $(\mathit{false})' \equiv \mathit{true}$ holds by Exercise 11.10):

$${\scriptstyle \mathrm{MR}}\,\dfrac{{\scriptstyle \mathrm{DI}}\,\dfrac{{\scriptstyle [?]}\,\dfrac{{\scriptstyle \to\mathrm{R}}\,\dfrac{A, Q \vdash \mathit{false}}{A \vdash Q \to \mathit{false}}}{A \vdash [?Q]\mathit{false}} \qquad {\scriptstyle \mathrm{WR}}\,\dfrac{A, Q \vdash}{A, Q \vdash [x' = f(x) \& Q](\mathit{false})'}}{A \vdash [x' = f(x) \& Q]\mathit{false}} \qquad {\scriptstyle \mathbb{R}}\,\dfrac{*}{\mathit{false} \vdash P}}{A \vdash [x' = f(x) \& Q]P}$$

11.10 Differential Invariants for Solvable Differential Equations

The primary motivation for studying differential invariants, differential cuts, and differential weakening was the need for advanced induction techniques for advanced differential equations that have no closed-form solutions in decidable arithmetic. For such advanced differential equations, the solution axiom schema $[']$ cannot be used or leads to undecidable arithmetic. But differential invariant style reasoning is still helpful even for simpler differential equations that have (rational) solutions.

Example 11.11 (Differential cuts prove falling balls). Recall the dL formula for a falling ball that was a part of the bouncing-ball proof from Chap. 7:

$$2gx = 2gH - v^2 \land x \geq 0 \rightarrow [x'' = -g \,\&\, x \geq 0](2gx = 2gH - v^2 \land x \geq 0) \tag{11.6}$$

$$\text{where } \{x'' = -g \,\&\, x \geq 0\} \overset{\text{def}}{\equiv} \{x' = v, v' = -g \,\&\, x \geq 0\}$$

Chap. 7 proved dL formula (11.6) using the solution of the differential equations with the solution axiom schema [′]. Yet, dL formula (11.6) can also be proved with a mix of differential invariants, differential cuts, and differential weakening, instead:

$$\dfrac{\triangleleft \qquad \dfrac{\dfrac{*}{x\geq 0 \land 2gx{=}2gH{-}v^2 \vdash 2gx = 2gH - v^2 \land x \geq 0}\,{\scriptstyle\text{id}}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x{\geq}0 \land 2gx{=}2gH{-}v^2](2gx{=}2gH{-}v^2 \land x{\geq}0)}\,{\scriptstyle\text{dW}}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x \geq 0](2gx = 2gH - v^2 \land x \geq 0)}\,{\scriptstyle\text{dC}}$$

The elided premise (marked ◁) after dC is proved by differential invariants:

$$\dfrac{\dfrac{\dfrac{*}{x \geq 0 \vdash 2gv = -2v(-g)}\,{\scriptstyle\mathbb{R}}}{x \geq 0 \vdash [x'{:=}v][v'{:=}-g]2gx' = -2vv'}\,{\scriptstyle[:=]}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x \geq 0]2gx = 2gH - v^2}\,{\scriptstyle\text{dI}}$$

Note that differential weakening (dW) works for proving the postcondition $x \geq 0$, but dI would not work for proving $x \geq 0$, because its derivative is $(x \geq 0)' \equiv v \geq 0$, which is not an invariant of the bouncing ball since its velocity ultimately becomes negative when it is falling again under gravity.

The above proof is elegant and has notably easier arithmetic than the arithmetic required when working with solutions of the bouncing ball in Chap. 7.

Note 62 (Differential invariants lower degrees) Differential invariant proof rule dI works by differentiation, which *lowers* polynomial degrees. The differential equation solution axiom [′] works with solutions, which ultimately integrate the differential equation and, thus, increase the degree. The computational complexity of the resulting arithmetic is, thus, often in favor of differential invariants even in cases where the differential equations can be solved so that the solution axiom [′] would be applicable.

Since the first conjunct of the postcondition in (11.6) is not needed for the proof of the second conjunct, a similar differential invariant proof can also be obtained using derived axiom []∧ to split the postcondition instead of dC to nest it:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{x \geq 0 \vdash 2gv = -2v(-g)}\,{\scriptstyle\mathbb{R}}}{x \geq 0 \vdash [x'{:=}v][v'{:=}-g]2gx' = -2vv'}\,{\scriptstyle[:=]}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x \geq 0]2gx = 2gH - v^2}\,{\scriptstyle\text{dI}} \qquad \dfrac{\dfrac{*}{x \geq 0 \vdash x \geq 0}\,{\scriptstyle\text{id}}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x \geq 0]x \geq 0}\,{\scriptstyle\text{dW}}}{2gx = 2gH - v^2 \vdash [x'' = -g \,\&\, x \geq 0](2gx = 2gH - v^2 \land x \geq 0)}\,{\scriptstyle[]\land}$$

This is how it pays to pay attention to which parts of a postcondition hold by which principle. The second conjunct $x \geq 0$ follows from the evolution domain alone and, thus, holds by dW. The first conjunct is inductive and follows by dI.

Besides the favorably simple arithmetic coming from differential invariants, the other reason why the above proofs worked so elegantly is that the invariant was a clever choice that we came up with in a creative way in Chap. 4. There is nothing wrong with being creative. On the contrary! Please always be creative!

11.11 Summary

This chapter introduced very powerful proof rules for differential invariants, with which you can prove even complicated properties of differential equations in easy ways. Just like in the case of loops, where the search for invariants is nontrivial, differential invariants require some smarts (or good automatic procedures) to be found. Yet, once differential invariants have been identified, the proof follows easily.

The new proof rules and axioms that they are based on are summarized in Fig. 11.20. For convenience, the derivation axioms and axiom DE from Chap. 10 are included again. Differential invariants follow the intuition of proving properties of differential equations that get more true over time along the differential equation. Or they prove properties that at least do not get less true along a differential equation, so will remain true if they start true. The differential invariant proof rule determines locally whether a property remains true along a differential equation by inspecting the differential of the postcondition in the direction that the right-hand side of the differential equation indicates. Since the resulting premise is formed by differentiation and substitution, it is relatively easy to check whether the resulting real arithmetic is true.

If the postcondition of a differential equation is getting less true along the dynamics of the differential equation, however, then additional thoughts are needed. For example, differential cuts (axiom DC and corresponding rule dC) provide a way of enriching the dynamics with a property C that is first proved to be an invariant itself. The differential cut principle makes it possible to prove a sequence of additional properties of differential equations and then to use them subsequently in the proof. Differential cuts are powerful reasoning principles, because they can exploit additional implicit structure in the system by proving and then using lemmas about the behavior of the system. In particular, differential cuts can make into differential invariants properties that have not been differential invariants before by first restricting the domain to a smaller subset on which the property actually is an invariant. Indeed, differential cuts are a fundamental proof principle for differential equations, satisfying the *No Differential Cut Elimination* theorem [11], because some properties can only be proved with differential cuts, not without them. Yet another way properties of differential equations that are not differential invariants directly can be made inductive will be explored in the next chapter.

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

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

$$\text{DW}\ [x'=f(x)\,\&\,Q]P \leftrightarrow [x'=f(x)\,\&\,Q](Q \to P)$$

$$\text{DI}\ \big([x'=f(x)\,\&\,Q]P \leftrightarrow [?Q]P\big) \leftarrow (Q \to [x'=f(x)\,\&\,Q](P)')$$

$$\text{DC}\ \big([x'=f(x)\,\&\,Q]P \leftrightarrow [x'=f(x)\,\&\,Q \land C]P\big) \leftarrow [x'=f(x)\,\&\,Q]C$$

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

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

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

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

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

$$c'\ (c())' = 0 \qquad \text{(for numbers or constants } c()\text{)}$$

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

Fig. 11.20 Axioms and proof rules for differential invariants and differential cuts of differential equations

11.12 Appendix: Proving Aerodynamic Bouncing Balls

This section studies a hybrid system with differential invariants. Remember the bouncing ball whose safety was proved in Chap. 7?

The little acrophobic bouncing ball has graduated from its study of loops and control and yearningly thinks back to its joyful time when it was studying continuous behavior. Caught up in nostalgia, Quantum the bouncing ball suddenly discovers that it unabashedly neglected the effect that air has on bouncing balls all the time. It sure is fun to fly through the air, so the little bouncing ball swiftly decides to make up for that oversight by including a proper aerodynamical model in its favorite differential equation. The effect that air has on the bouncing ball is air resistance and, it turns out, air resistance gets stronger the faster the ball is flying. After a couple of experiments, the little bouncing ball finds out that air resistance is quadratic in the velocity with an aerodynamic damping factor $r > 0$.

Now the strange thing with air is that air is always against the flying ball! Air always provides resistance, no matter in which direction the ball is flying. If the ball is hurrying upwards, the air holds it back and slows it down by decreasing its positive speed $v > 0$. If the ball is rushing back down to the ground, the air still holds the ball back and slows it down, only then that actually means *increasing* the negative velocity $v < 0$, because that corresponds to decreasing the absolute value $|v|$. How can that be modeled properly?

One way of modeling this situation would be to use the (discontinuous) sign function $\operatorname{sign} v$ that has value 1 for $v > 0$, value -1 for $v < 0$, and value 0 for $v = 0$:

$$x' = v, v' = -g - (\operatorname{sign} v) r v^2 \,\&\, x \geq 0 \tag{11.7}$$

That, however, gives a differential equation with a discontinuous right-hand side [1]. Instead, the little bouncing ball has learned to appreciate the philosophy behind hybrid systems, which advocates for keeping the continuous dynamics simple and moving discontinuities and switching aspects to where they belong: the discrete dynamics. After all, switching and discontinuities are what the discrete dynamics is good at.

Consequently, the little bouncing ball decides to split modes and separate the upward-flying part $v \geq 0$ from the downward flying part $v \leq 0$ and offer the system a nondeterministic choice between the two:[1]

$$\begin{aligned}
& x \leq H \land v = 0 \land x \geq 0 \land g > 0 \land 1 \geq c \geq 0 \land r \geq 0 \rightarrow \\
& \big[\big(\mathsf{if}(x = 0)\, v := -cv; \\
& \quad (\{x' = v, v' = -g - rv^2 \,\&\, x{\geq}0 \land v{\geq}0\} \cup \{x' = v, v' = -g + rv^2 \,\&\, x{\geq}0 \land v{\leq}0\})\big)^* \\
& \big]\,(0 \leq x \leq H)
\end{aligned} \tag{11.8}$$

In pleasant anticipation of the new behavior that this *aerodynamic bouncing ball* model provides, the little bouncing ball is eager to give it a try. Before daring to bounce around with this model, though, the acrophobic bouncing ball first wants to be convinced that it would be safe to use, i.e., the model actually satisfies the height limit property in (11.8). So the bouncing ball first sets out on a proof adventure. After writing down several ingenious proof steps, the bouncing ball finds out that its previous proof does not carry over. For one thing, the nonlinear differential equations can no longer be solved quite so easily. That makes the solution axiom $[']$ rather useless. But, fortunately, the little bouncing ball brightens up again as it remembers that unsolvable differential equations were what differential invariants were good at. And the ball is rather keen on trying them in the wild, anyhow.

However, first things first. The first step of the proof after rule →R is the search for an invariant for the loop induction proof rule loop. Yet, since the proof of (11.8) cannot work by solving the differential equations, we will also need to identify differential invariants for the differential equations. If we are lucky, maybe the same invariant could even work for both? Whenever we are in such a situation, we can search from both ends and either identify an invariant for the loop first and then try to adapt it to the differential equation, or, instead, look for a differential invariant first.

[1] Note that the reasons for splitting modes and offering a nondeterministic choice between them are not controller events as they have been in Chap. 8, but, rather, come from the physical model itself. The mechanism is the same, though, whatever the reason for splitting.

Since we know the loop invariant for the ordinary bouncing ball from (7.10), let's look at the loop first. The loop invariant for the ordinary bouncing ball was

$$2gx = 2gH - v^2 \land x \geq 0$$

We cannot really expect the equation in this invariant to work out for the aerodynamic ball (11.8) as well, because the whole point of the air resistance is that it slows the ball down. Since air resistance always works against the ball's motion, the height is expected to be less:

$$\mathrm{J}_{x,v} \overset{\text{def}}{\equiv} 2gx \leq 2gH - v^2 \land x \geq 0 \tag{11.9}$$

In order to check right away whether this invariant that we suspect to be a loop invariant works for the differential equations as well, let's check for differential invariance:

$$\text{dI}\;\dfrac{[:=]\;\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{g>0\land r\geq 0, x\geq 0\land v\geq 0 \vdash 2gv \leq 2gv+2rv^3}}{g>0\land r\geq 0, x\geq 0\land v\geq 0 \vdash 2gv \leq -2v(-g-rv^2)}}{g>0\land r\geq 0, x\geq 0\land v\geq 0 \vdash [x':=v][v':=-g-rv^2](2gx' \leq -2vv')}}{g>0\land r\geq 0, 2gx \leq 2gH-v^2 \vdash [x'=v, v'=-g-rv^2\,\&\,x\geq 0\land v\geq 0]\,2gx \leq 2gH-v^2}$$

Note that for this proof to work, it is essential to keep the constants $g > 0 \land r \geq 0$ around, or at least $r \geq 0$. The easiest way of doing that is to perform a differential cut dC with $g > 0 \land r \geq 0$ and prove it to be a (trivial) differential invariant, because both parameters do not change, to make $g > 0 \land r \geq 0$ available in the evolution domain constraint for the rest of the proof.[2]

The differential invariant proof for the other ODE in (11.8) works as well:

$$\text{dI}\;\dfrac{[:=]\;\dfrac{\dfrac{\mathbb{R}\;\dfrac{*}{g>0\land r\geq 0, x\geq 0\land v\leq 0 \vdash 2gv \leq 2gv-2rv^3}}{g>0\land r\geq 0, x\geq 0\land v\leq 0 \vdash 2gv \leq -2v(-g+rv^2)}}{g>0\land r\geq 0, x\geq 0\land v\leq 0 \vdash [x':=v][v':=-g+rv^2]2gx' \leq -2vv'}}{g>0\land r\geq 0, 2gx \leq 2gH-v^2 \vdash [x'=v, v'=-g+rv^2\,\&\,x\geq 0\land v\leq 0]\,2gx \leq 2gH-v^2}$$

After this preparation, the rest of the proof of (11.8) is a matter of checking whether (11.9) is also a loop invariant. Except that the above two sequent proofs do not actually quite prove that (11.9) is a differential invariant, but only that its left conjunct $2gx \leq 2gH - v^2$ is. Would it work to add the right conjunct $x \geq 0$ and prove it to be a differential invariant?

Not exactly, because rule dI would lead to $[x':=v](x' \geq 0) \equiv v \geq 0$, which is obviously not always true for bouncing balls (except in the mode $x \geq 0 \land v \geq 0$). However, after proving the above differential invariant after a differential cut (elided use of the above proof is marked by $\triangleleft$ in the next proof), a differential weakening argument by dW easily shows that the relevant part $x \geq 0$ of the evolution domain constraint always holds after the differential equation:

[2] Since this happens so frequently, KeYmaera X keeps constant parameter assumptions in the context using the vacuous axiom V as in Sect. 7.5.

$$\text{dC}\;\dfrac{\text{dW}\;\dfrac{\text{id}\;\dfrac{*}{x\geq0\land v\leq0\land 2gx\leq 2gH-v^2 \vdash 2gx\leq 2gH-v^2\land x\geq 0}}{\triangleleft\, 2gx\leq 2gH-v^2 \vdash [x'=v,v'=-g+rv^2\,\&\,x\geq0\land v\leq0\land 2gx\leq 2gH-v^2](2gx\leq 2gH-v^2\land x\geq0)}}{..\,2gx\leq 2gH-v^2 \vdash [x'=v,v'=-g+rv^2\,\&\,x\geq0\land v\leq0](2gx\leq 2gH-v^2\land x\geq0)}$$

From these pieces it now remains to prove that (11.9) is a loop invariant of (11.8). Without abbreviations, this proof will not fit on a page:

$$A_{x,v} \overset{\text{def}}{\equiv} x\leq H\land v=0\land x\geq 0\land g>0\land 1\geq c\geq 0\land r\geq 0$$

$$B_{x,v} \overset{\text{def}}{\equiv} 0\leq x\land x\leq H$$

$$x''\&v{\geq}0 \overset{\text{def}}{\equiv} \{x'=v,v'=-g-rv^2\,\&\,x\geq0\land v\geq 0\}$$

$$x''\&v{\leq}0 \overset{\text{def}}{\equiv} \{x'=v,v'=-g+rv^2\,\&\,x\geq0\land v\leq 0\}$$

$$\mathrm{J}_{x,v} \overset{\text{def}}{\equiv} 2gx\leq 2gH-v^2\land x\geq 0$$

$$\text{loop}\;\dfrac{A_{x,v}\vdash \mathrm{J}_{x,v} \quad [;]\;\dfrac{\text{MR}\;\dfrac{\mathrm{J}_{x,v}\vdash[\mathsf{if}(x=0)\,v:=-cv]\mathrm{J}_{x,v} \quad [\cup]\;\dfrac{\land\text{R}\;\dfrac{\mathrm{J}_{x,v}\vdash[x''\&v{\geq}0]\mathrm{J}_{x,v} \quad \mathrm{J}_{x,v}\vdash[x''\&v{\leq}0]\mathrm{J}_{x,v}}{\mathrm{J}_{x,v}\vdash[x''\&v{\geq}0]\mathrm{J}_{x,v}\land[x''\&v{\leq}0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[x''\&v{\geq}0\cup x''\&v{\leq}0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[\mathsf{if}(x=0)\,v:=-cv][x''\&v{\geq}0\cup x''\&v{\leq}0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[\mathsf{if}(x=0)\,v:=-cv;(x''\&v{\geq}0\cup x''\&v{\leq}0)]\mathrm{J}_{x,v}} \quad \mathrm{J}_{x,v}\vdash B_{x,v}}{A_{x,v}\vdash[(\mathsf{if}(x=0)\,v:=-cv;(x''\&v{\geq}0\cup x''\&v{\leq}0))^*]B_{x,v}}$$

The first and last premise are proved by simple arithmetic using $g>0\land v^2\geq 0$. The third and fourth premise have been proved above by a differential cut with a subsequent differential invariant and differential weakening. That only leaves the second premise to worry about, which is proved as follows:

$$\dfrac{[\cup]\;\dfrac{\land\text{R}\;\dfrac{[;]\;\dfrac{[?]\;\dfrac{\to\text{R}\;\dfrac{[:=]\;\dfrac{\mathrm{J}_{x,v},x=0\vdash\mathrm{J}_{x,-cv}}{\mathrm{J}_{x,v},x=0\vdash[v:=-cv]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash x=0\to[v:=-cv]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[?x=0][v:=-cv]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[?x=0;v:=-cv]\mathrm{J}_{x,v}} \quad [?]\;\dfrac{\to\text{R}\;\dfrac{\text{id}\;\dfrac{*}{\mathrm{J}_{x,v},x\neq0\vdash\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash x\neq0\to\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[?x\neq0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[?x=0;v:=-cv]\mathrm{J}_{x,v}\land[?x\neq0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[?x=0;v:=-cv\cup ?x\neq0]\mathrm{J}_{x,v}}}{\mathrm{J}_{x,v}\vdash[\mathsf{if}(x=0)\,v:=-cv]\mathrm{J}_{x,v}}$$

This sequent proof first expands the $\mathsf{if}()$ with the axiom from Exercise 5.15 since $\mathsf{if}(Q)\,\alpha$ is an abbreviation for $?Q;\alpha\cup ?\neg Q$. The resulting right premise is proved trivially by axiom (there was no state change in the corresponding part of the execution), the left premise is proved by arithmetic, because $2gH-v^2\leq 2gH-(-cv)^2$ since $1\geq c\geq 0$. This completes the sequent proof for the safety of the aerodynamic bouncing ball expressed in dL formula (11.8). That is pretty neat!

Proposition 11.2 (Aerodynamic Quantum is safe). *This* dL *formula is valid:*

$$\begin{aligned}
&x \leq H \wedge v = 0 \wedge x \geq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge r \geq 0 \rightarrow\\
&\big[\big(\mathsf{if}(x = 0)\, v := -cv;\\
&\quad (\{x' = v, v' = -g - rv^2 \,\&\, x{\geq}0 \wedge v{\geq}0\} \cup \{x' = v, v' = -g + rv^2 \,\&\, x{\geq}0 \wedge v{\leq}0\})\big)^*\\
&\big]\,(0 \leq x \leq H)
\end{aligned}$$

It is about time for the newly upgraded aerodynamic acrophobic bouncing ball to notice a subtlety in its (provably safe) model. The bouncing ball innocently split the differential equation (11.7) into two modes, one for $v \geq 0$ and one for $v \leq 0$, when developing the model (11.8). This seemingly innocuous step required more thought than the little bouncing ball put into it at the time. Of course, the single differential equation (11.7) could, in principle, switch between velocity $v \geq 0$ and $v \leq 0$ any arbitrary number of times during a single continuous evolution. The HP in (11.8) that splits the mode, however, enforces that the ground controller $\mathsf{if}(x = 0)\, v := -cv$ will run in between switching from the mode $v \geq 0$ to the mode $v \leq 0$ or back. On its way up when gravity is just about to win out and pull the ball back down again, that is of no consequence, because the trigger condition $x = 0$ will not hold then anyhow, unless the ball really started the day without much energy ($x = v = 0$). On its way down, the condition may very well be true, namely when the ball is currently on the ground and just inverted its velocity. In that case, however, the evolution domain constraint $x \geq 0$ would have forced a ground controller action in the original system already anyhow.

So even if, in this particular model, the system could not in fact actually switch back and forth between the two modes too often in ways that would really matter, it is important to understand how to properly split modes in general, because that will be crucial for other systems. What the little bouncing ball should have done to become aerodynamical in a systematic way is to add an additional mini-loop around just the two differential equations, so that the system could switch modes repeatedly without requiring a discrete ground controller action to happen. This leads to the following dL formula with a systematic mode split, which is provably safe just the same (Exercise 11.7):

$$\begin{aligned}
&x \leq H \wedge v = 0 \wedge x \geq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge r \geq 0 \rightarrow\\
&\big[\big(\mathsf{if}(x = 0)\, v := -cv;\\
&\quad (\{x' = v, v' = -g - rv^2 \,\&\, x{\geq}0 \wedge v{\geq}0\} \cup \{x' = v, v' = -g + rv^2 \,\&\, x{\geq}0 \wedge v{\leq}0\})^*\big)^*\\
&\big]\,(0 \leq x \leq H)
\end{aligned} \tag{11.10}$$

Exercises

11.1. Since ω does not change in this dL formula, its assumption $\omega \geq 0$ can be preserved soundly during the induction step for differential invariants (rule dI):

$$\omega \geq 0 \land x = 0 \land y = 3 \to [x' = y, y' = -\omega^2 x - 2\omega y]\, \omega^2 x^2 + y^2 \leq 9$$

Give a corresponding dL sequent calculus proof. How does the proof change if you do not preserve assumptions about constants in the context?

11.2 (Differential invariant practice). Prove the following formulas using differential invariants, differential cuts, and differential weakening as required:

$$\begin{aligned}
xy^2 + x \geq 7 &\to [x' = -2xy, y' = 1 + y^2]\, xy^2 + x \geq 7 \\
x \geq 1 \lor x^3 \geq 8 &\to [x' = x^4 + x^2](x \geq 1 \lor x^3 \geq 8) \\
x - x^2 y \geq 2 \land y \neq 5 &\to [x' = -x^2, y' = -1 + 2xy]\, x - x^2 y \geq 2 \\
x \geq 2 \land y \geq 22 &\to [x' = 4x^2, y' = x + y^4]\, y \geq 22 \\
x \geq 2 \land y = 1 &\to [x' = x^2 y + x^4, y' = y^2 + 1]\, x^3 \geq 1 \\
x = -1 \land y = 1 &\to [x' = -6x^2 + 6xy^2, y' = 12xy - 2y^3]\, -2xy^3 + 6x^2 y \geq 0 \\
x \geq 2 \land y = 1 &\to [x' = x^2 y^3 + x^4 y, y' = y^2 + 2y + 1]\, x^3 \geq 8 \\
x = 1 \land y = 2 \land z \geq 8 &\to [x' = x^2, y' = 4x, z' = 5y]\, z \geq 8 \\
x^3 - 4xy \geq 99 &\to [x' = 4x, y' = 3x^2 - 4y]\, x^3 - 4xy \geq 99
\end{aligned}$$

11.3 (Wrong differential weakening). Show that the following variation of the differential weakening rule dW would be unsound:

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

11.4 (Weak differentials of strong inequations). Prove that both of the following alternative definitions yield a sound differential invariant proof rule:

$$(e < k)' \equiv ((e)' < (k)')$$
$$(e < k)' \equiv ((e)' \leq (k)')$$

11.5 (Disequalities). We have defined

$$(e \neq k)' \equiv ((e)' = (k)')$$

Suppose you remove this definition so that you can no longer use the differential invariant proof rule for formulas involving $\neq$. Can you derive a proof rule to prove such differential invariants regardless? If so, how? If not, why not?

11.6. Prove dL formula (11.5) by first doing a differential cut with $\omega(x-1) = -w$, then continue with a differential cut with $\omega(y-2) = v$, and then finally use both to prove the original postcondition. Compare this proof to the proof in Sect. 11.8.

11.7 (Aerodynamic bouncing ball). The aerodynamic-bouncing-ball model silently imposed that no mode switching could happen without ground control being executed first. Even if that is not an issue for the bouncing ball, prove the more general formula (11.10) with its extra loop for more mode switching regardless. Compare the resulting proof to the sequent proof for (11.8).

11.8 (Generalizations). Sect. 5.6.4 explained how the proof of the dL formula $[x:=1;x'=x^2+2x^4]x^3 \geq x^2$ can be reduced by monotonicity rule M$[\cdot]$ to a proof of $[x:=1;x'=x^2+2x^4]x \geq 1$. Prove both formulas in the dL calculus. Is there a direct proof of the first formula using rule dI without first generalizing it to a proof of the second formula?

11.9 (Differential invariants assuming initial domains). The least that the proof rules for differential equations get to assume is the evolution domain constraint Q, because the system does not evolve outside it. Prove soundness for the following slightly stronger formulation of dI that assumes Q to hold initially:

$$\frac{\Gamma, Q \vdash F, \Delta \quad Q \vdash [x':=f(x)](F)'}{\Gamma \vdash [x'=f(x)\,\&\,Q]F, \Delta}$$

11.10 (Differentials of logical constants). Prove the following definitions to be sound for the differential invariant proof rule:

$$(true)' \equiv true$$
$$(false)' \equiv true$$

Show how you can use them to prove the formula

$$A \to [x'=f(x)\,\&\,Q]B$$

in the case where $A \to \neg Q$ is provable, i.e., where the system initially starts outside the evolution domain constraint Q. Can you derive both definitions from arithmetic definitions of the formulas *true* and *false*?

11.11 (Runaround robot). Identify differential cuts and differentials to prove the runaround robot control model from Exercise 3.9.

11.12 (Solutions without solution axiom schemata). Prove the following formula with differential cuts, differential invariants, and differential weakening and without using the solution axiom schema $[']$.

$$x=6 \land v \geq 2 \land a=1 \to [x'=v, v'=a]x \geq 5$$

Grab a big sheet of paper and then also similarly prove

$$x=6 \land v \geq 2 \land a=1 \land j \geq 0 \to [x'=v, v'=a, a'=j]x \geq 5$$

References

[1] Jorge Cortés. Discontinuous dynamical systems: a tutorial on solutions, nonsmooth analysis, and stability. *IEEE Contr. Syst. Mag.* **28**(3) (2008), 36–73.

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

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

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

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

[7] André Platzer. Quantified differential invariants. In: *HSCC*. Ed. by Marco Caccamo, Emilio Frazzoli, and Radu Grosu. New York: ACM, 2011, 63–72. DOI: 10.1145/1967701.1967713.

[8] 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.

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

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

[11] 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.

[12] 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.

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

[14] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. *Form. Methods Syst. Des.* **35**(1) (2009). Spe-

cial issue for selected papers from CAV’08, 98–120. DOI: 10.1007/s10703-009-0079-8.