15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Differential Equations & Proofs

André Platzer

Carnegie Mellon University
Lecture 11

1. Introduction

Lecture 10 on Differential Equations & Differential Invariants introduced equational differential invariants of the form $\eta = 0$ for differential equations that are much more general than the ones supported by axiom [′] from Lecture 5 on Dynamical Systems & Dynamic Axioms. Axiom [′] replaces properties of differential equations with universally quantified properties of solutions, but is limited to differential equations that have explicit closed-form solutions whose arithmetic can be handled (mostly polynomials or rational functions). But axiom [′] works for any arbitrary postcondition. The equational differential invariant proof rule $\text{DI}_{=0}$ supports general differential equations, but was limited to equational postconditions of the form $\eta = 0$.

The goal of this lecture is to generalize the differential invariant proof rules to work for more general postconditions but retaining the flexibility with the differential equations that differential invariants provide. Indeed, the principles developed in Lecture 10 generalize beautifully to logical formulas other than the limited form $\eta = 0$. This lecture will establish generalizations that make the differential invariant proof rule work for formulas F of more general forms. The most important part will be soundly defining the total derivative F', because the basic shape of the differential invariants proof rule stays the same:

$$\frac{\vdash (F')^{\theta}_{x'}}{F \vdash [x' = \theta]F}$$

More details can be found in [Pla10b, Chapter 3.5] and [Pla10a, Pla12d, Pla12a, Pla12b]. Differential invariants were originally conceived in 2008 [Pla10a, Pla08] and later used for an automatic proof procedure for hybrid systems [PC08].

This lecture advances the capabilities of differential invariants begun in Lecture 10 on Differential Equations & Differential Invariants and continues to be of central significance for the Foundations of Cyber-Physical Systems. The most important learning goals of this lecture are:

Modeling and Control: This lecture 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 lecture also have a significance for developing models and controls using the design-by-invariant principle.

Computational Thinking: This lecture exploits computational thinking continuing the surprising analogies among discrete dynamics and continuous dynamics discovered in Lecture 10. This lecture is devoted to rigorous reasoning about the differential equations in CPS models, which is crucial for understanding the continuous behavior that CPS exhibit over time. This lecture systematically expands on the differential invariant terms for equational properties of differential equations developed in Lecture 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 lecture continues the *axiomatization* of differential dynamic logic $\mathsf{d}\mathcal{L}$ [Pla12c, Pla12a] pursued since Lecture 5 on Dynamical Systems & Dynamic Axioms and lifts $\mathsf{d}\mathcal{L}$'s proof techniques to systems with more complex properties of more complex differential equations. The concepts developed in this lecture continue the differential facet illustrating the more general relation of *syntax* (which is notation), *semantics* (what 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 lecture are critical for verifying CPS models of appropriate scale and technical complexity.

CPS Skills: The focus in this lecture is on reasoning about differential equations. As a beneficial side effect, we will develop a 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 it will not change.

2. Recall

Recall the following results from Lecture 10 on Differential Equations & Differential Invariants:

Definition 1 (Derivation). The operator $(\cdot)'$ that is defined as follows on terms is called *syntactic (total) derivation*:

$$(r)' = 0 \qquad \text{for numbers } r \in \mathbb{Q} \tag{1a}$$
$$(x)' = x' \qquad \text{for variable } x \in \Sigma \tag{1b}$$
$$(a+b)' = (a)' + (b)' \tag{1c}$$
$$(a-b)' = (a)' - (b)' \tag{1d}$$
$$(a \cdot b)' = (a)' \cdot b + a \cdot (b)' \tag{1e}$$
$$(a/b)' = ((a)' \cdot b - a \cdot (b)')/b^2 \tag{1f}$$

Definition 2 (Semantics of differential symbols). The value of x' at time $\zeta \in [0,r]$ of a differentiable function $\varphi : [0,r] \to \mathcal{S}$ of some duration $r \in \mathbb{R}$ is defined as the analytic time-derivative at ζ:

$$[\![x']\!]_{\varphi(\zeta)} = \frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta)$$

Lemma 3 (Derivation lemma). *Let $\varphi : [0,r] \to \mathcal{S}$ be a differentiable function of duration $r > 0$. Then for all terms η that are defined all along φ and all times $\zeta \in [0,r]$:*

$$\frac{\mathsf{d}\,[\![\eta]\!]_{\varphi(t)}}{\mathsf{d}t}(\zeta) = [\![(\eta)']\!]_{\varphi(\zeta)}$$

where differential symbols are interpreted according to Def. 2. In particular, $[\![\eta]\!]_{\varphi(\zeta)}$ is continuously differentiable.

Lemma 4 (Differential substitution property for terms). *If $\varphi : [0,r] \to \mathcal{S}$ solves the differential equation $x' = \theta$, i.e. $\varphi \models x' = \theta$, then $\varphi \models (\eta)' = (\eta)'^{\theta}_{x'}$ for all terms η, i.e.:*

$$[\![(\eta)']\!]_{\varphi(\zeta)} = [\![(\eta)'^{\theta}_{x'}]\!]_{\varphi(\zeta)} \quad \text{for all } \zeta \in [0,r]$$

3. Differential Invariant Terms

Lecture 10 on Differential Equations & Differential Invariants proved soundness for a proof rule for differential invariant terms, which can be used to prove normalized invariant equations of the form $\eta = 0$.

Lemma 5 (Differential invariant terms)**.** *The following special case of the differential invariants proof rule is sound, i.e. if its premise is valid then so is its conclusion:*

$$(DI_{=0})\ \frac{\vdash \eta'^{\theta}_{x'} = 0}{\eta = 0 \vdash [x' = \theta]\eta = 0}$$

Differential invariant terms led to an indirect proof of

$$d^2 + e^2 = r^2 \rightarrow [d' = e, e' = -d]d^2 + e^2 = r^2 \tag{2}$$

by generalizing the formula using $[]gen'$ and *cut* to

$$d^2 + e^2 - r^2 = 0 \rightarrow [d' = e, e' = -d]d^2 + e^2 - r^2 = 0 \tag{3}$$

after normalizing the equation to have 0 on the right-hand side as required by the differential invariant term proof rule $DI_{=0}$.

4. Equational Differential Invariants

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. For example, we should generalize differential invariants to enable a direct proof of (2) with an invariant of the form $\kappa = \eta$, rather than insisting on normalizing equations to the form $\eta = 0$ by generalization $[]gen'$ first.

Thinking back of the soundness proof for $DI_{=0}$ in Lecture 10, the argument was based on the value of the left-hand side term $h(t) = [\![\eta]\!]_{\varphi(t)}$ as a function of time t. The same argument can be made by considering the difference $h(t) = [\![\kappa - \eta]\!]_{\varphi(t)}$ instead to prove postconditions of the form $\kappa = \eta$. How does the inductive step for formula $\kappa = \eta$ need to be define to make a corresponding differential invariant proof rule sound? That is, for what premise is the following a sound proof rule?

$$\frac{\vdash ???}{\kappa = \eta \vdash [x' = \theta]\kappa = \eta}$$

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

Defining the total derivative of an equation $\kappa = \eta$ as

$$(\kappa = \eta)' \equiv ((\kappa)' = (\eta)')$$

results in a sound proof rule by a simple variation of the soundness proof for DI$_{=0}$ as sketched above. The resulting proof rule

$$(\text{DI}_=)\ \frac{\vdash (\kappa' = \eta')^{\theta}_{x'}}{\kappa = \eta \vdash [x' = \theta]\kappa = \eta}$$

for equational differential invariants captures the basic intuition that κ always stays equal to η if it has been initially (antecedent of conclusion) and the derivative of κ is the same as the derivative of η with respect to the differential equation $x' = \theta$. This intuition is made precise by Lemma 3 and Lemma 4. Instead of going through a proper soundness proof for DI$_=$, however, let's directly generalize the proof principles further and see if differential invariants can prove even more formulas for us. We will later prove soundness for the general differential invariant rule, from which DI$_=$ derives as a special case.

Example 6 (Rotational dynamics). The rotational dynamics $d' = e, e' = -d$ 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 (2), i.e. that $d^2 + e^2 = r^2$ is a differential invariant of the dynamics, using the following proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 2de + 2e(-d) = 0}\,\mathbb{R}}{\vdash (2dd' + 2ee' = 0)^{e\ -d}_{d'\ e'}}}{d^2 + e^2 = r^2 \vdash [d' = e, e' = -d]d^2 + e^2 = r^2}\,\text{DI}}{\vdash d^2 + e^2 = r^2 \to [d' = e, e' = -d]d^2 + e^2 = r^2}\,{\to}\text{r}$$

This proof is certainly much easier and more direct than the previous proof based on $[]gen'$.

5. Differential Invariant Inequalities

The differential invariant proof rules considered so far give a good (initial) 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 define the total derivative

$$(\kappa \leq \eta)' \equiv ((\kappa)' \leq (\eta)')$$

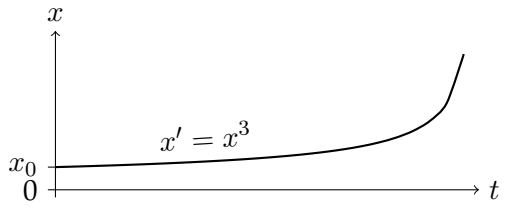
which gives the differential invariant proof rule:

$$\frac{\vdash (\kappa' \leq \eta')^{\theta}_{x'}}{\kappa \leq \eta \vdash [x' = \theta]\kappa \leq \eta}$$

Example 7 (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. 7 for the dynamics in Fig. 1. To apply the differential induction rule DI, we again form the total deriva-

$$\mathbb{R}\,\frac{*}{\vdash 0 \leq 5 \cdot 2x(x^3)}\,\frac{}{\vdash (0 \leq 5 \cdot 2xx')^{x^3}_{x'}}\,\mathrm{DI}\,\frac{}{\frac{1}{3} \leq 5x^2 \vdash [x' = x^3]\frac{1}{3} \leq 5x^2}$$

Figure 1: **a** Cubic dynamics proof



1**b**: Cubic dynamics

tive of the differential invariant $F \equiv \frac{1}{3} \leq 5x^2$, which gives the differential expression $F' \equiv (\frac{1}{3} \leq 5x^2)' \equiv 0 \leq 5 \cdot 2xx'$. 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 $F'^{x^3}_{x'} \equiv 0 \leq 5 \cdot 2xx^3$, which is a valid formula and closes by quantifier elimination with $\mathbb{R}$.

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 [Pla12d] that there are valid formulas that can be proved using differential invariant inequalities but cannot be proved just using equations as differential invariants ($\mathrm{DI}_{=}$). So 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 $\mathrm{DI}_{=}$ is also provable using differential invariant inequalities [Pla12d], but you should still look for equational differential invariants if they give easier proofs.

Strict inequalities can also be used as differential invariants when defining their total derivatives as:

$$(\kappa < \eta)' \equiv ((\kappa)' < (\eta)')$$

It is easy to see (Exercise 1) that the following slightly relaxed definition would also be sound:

$$(\kappa < \eta)' \equiv ((\kappa)' \leq (\eta)')$$

Understanding that differential substitution is sound for formulas, i.e. replacing the left-hand side of the differential equation by its right-hand side, requires a few more

thoughts now, because the equational differential substitution principle Lemma 4 does not apply directly. The differential substitution principle not only works for terms, however, but also for *differential first-order formulas*, i.e. first-order formulas in which differential symbols occur:

Lemma 8 (Differential substitution property for differential formulas)**.** *If $\varphi : [0, r] \to \mathcal{S}$ solves the differential equation $x' = \theta$, i.e. $\varphi \models x' = \theta$, then $\varphi \models \mathcal{D} \leftrightarrow \mathcal{D}^{\theta}_{x'}$ for all differential first-order formulas $\mathcal{D}$, i.e. first-order formulas over $\Sigma \cup \Sigma'$.*

Proof. The proof is by using the Substitution Lemma [Pla10b, Lemma 2.2] for first-order logic on the basis of $[\![x']\!]_{\varphi(\zeta)} = [\![\theta]\!]_{\varphi(\zeta)}$ at each time ζ in the domain of φ by Def. 2. □

By Lemma 8, differential equations can always be substituted in along their solutions. Hence, the focus on developing differential invariant proof rules is in defining appropriate total derivatives, since Lemma 8 shows how to handle differential symbols by substitution.

Where do differential first-order formulas come from? They come from the analogue of the total derivation operator on formulas. On formulas, the total derivation operator applies the total derivation operator from Def. 1 to all terms in a first-order formula, yet it also flips disjunctions into conjunctions and existential quantifiers into universal quantifiers.

Example 9 (Rotational dynamics). An inequality property can be proved easily for the rotational dynamics $d' = e, e' = -d$ using the following proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 2de + 2e(-d) \leq 0}\,\mathbb{R}}{\vdash (2dd' + 2ee' \leq 0)^{e\ -d}_{d'\ e'}}}{d^2 + e^2 \leq r^2 \vdash [d' = e, e' = -d]d^2 + e^2 \leq r^2}\,\text{DI}}{\vdash d^2 + e^2 \leq r^2 \to [d' = e, e' = -d]d^2 + e^2 \leq r^2}\,\to\text{r}$$

Example 10 (Damped oscillator). This proof shows the invariant illustrated in Fig. 2:

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

6. Disequational Differential Invariants

The case that is missing in differential invariant proof rules are for postconditions that are disequalities $\kappa \neq \eta$? How can they be proved?

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

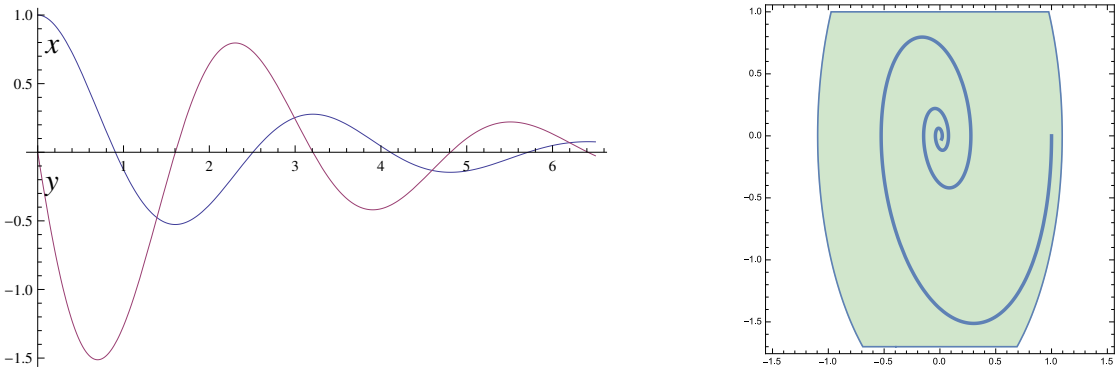


Figure 2: Damped oscillator time trajectory (**left**) and invariant in phase space (**right**)

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

$$(\kappa \neq \eta)' \stackrel{?}{\equiv} ((\kappa)' \neq (\eta)') \quad ???$$

It is crucial for soundness of differential invariants tha $(\kappa \neq \eta)'$ is *not* defined that way! In the following counterexample, variable x can reach $x = 0$ without its derivative ever being 0; again, see Fig. 3 for the dynamics. Of course, just because κ and η start out

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

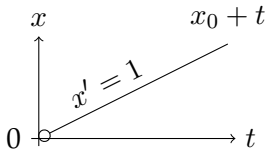


Figure 3: **a** Unsound attempt of using disequalities 3**b**: Linear dynamics

different, does not mean they would always stay different if they evolve with different derivatives. Au contraire, it is because both evolve with different derivatives that they might catch each other.

Instead, if κ and η start out differently and evolve with the same derivatives, they will always stay different. So the sound definition is slightly unexpected:

$$(\kappa \neq \eta)' \equiv ((\kappa)' = (\eta)')$$

7. Conjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a conjunction $F \wedge G$. Lemma 8 takes care of how to handle differential substitution for the differential equations, if only we define the correct total derivative of $(F \wedge G)'$.

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

To show that a conjunction $F \wedge G$ is invariant it is perfectly sufficient to prove that both are invariant. This can be justified separately, but is more obvious when recalling the following equivalence from Lecture 7:

$$([]\wedge) \quad [\alpha](\phi \wedge \psi) \leftrightarrow [\alpha]\phi \wedge [\alpha]\psi$$

which is valid for all hybrid programs α, also when α is just a differential equation. Consequently, the total derivative of a conjunction is the conjunction of the total derivatives (i.e. $(\cdot)'$ is a homomorphism for $\wedge$):

$$(F \wedge G)' \equiv (F)' \wedge (G)'$$

Again, we will not develop a proper soundness argument, because it will follow from the general differential invariant proof rule.

With a corresponding proof rule that enables us to do the following proof:

$$\dfrac{\dfrac{\dfrac{}{\mathbb{R}}\,* \quad \vdash 2de + 2e(-d) \le 0 \wedge 2de + 2e(-d) \ge 0}{\vdash (2dd' + 2ee' \le 0 \wedge 2dd' + 2ee' \ge 0)^{e\ -d}_{d'\ e'}}}{\text{DI}\ d^2 + e^2 \le r^2 \wedge d^2 + e^2 \ge r^2 \vdash [d' = e, e' = -d](d^2 + e^2 \le r^2 \wedge d^2 + e^2 \ge r^2)}$$

Since the invariant $d^2 + e^2 \le r^2 \wedge d^2 + e^2 \ge r^2$ is easily proved to be equivalent to $d^2 + e^2 = r^2$, the above proof gives yet another proof of (2) when combined with a corresponding use of the generalization rule $[]gen'$.

8. Disjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a disjunction $F \vee G$. Lemma 8 takes care of how to handle differential substitution for the differential equations, if only we define the correct total derivative of $(F \vee G)'$. How?

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

The total derivative of a conjunction is the conjunction of the total derivatives. So, by analogy, it might stand to reason to define the total derivative of a disjunction as the disjunction of the total derivatives.

$$(F \vee G)' \stackrel{?}{\equiv} (F)' \vee (G)' \quad ???$$

Let's try it:

$$\lightning\ \mathbb{R}\ \frac{\dfrac{\dfrac{}{\vdash 2de + 2e(-d) = 0 \vee 5d + re \geq 0}\ \text{unsound}}{\vdash (2dd' + 2ee' = 0 \vee r'd + rd' \geq 0)^{e\ -d}_{d'\ e'}}}{d^2 + e^2 = r^2 \vee rd \geq 0 \vdash [d' = e, e' = -d, r' = 5](d^2 + e^2 = r^2 \vee rd \geq 0)}$$

That would be spectacularly wrong, however, because the formula at the bottom is not actually valid, so it does not deserve a proof. We have no business of 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 induction, it is crucial that Def. 1 defines the total derivative $(F \vee G)'$ of a disjunction conjunctively as $(F)' \wedge (G)'$ instead of as $(F)' \vee (G)'$. From an initial state ν which satisfies $\nu \models F$, and hence $\nu \models F \vee G$, the formula $F \vee G$ only is sustained differentially if F itself is a differential invariant, not if G is. For instance, $d^2 + e^2 = r^2 \vee rd \geq 0$ is no invariant of the above differential equation, because $rd \geq 0$ will be invalidated if we just follow the circle dynamics long enough. So if the disjunction was true because $rd \geq 0$ was true in the beginning, it does not stay invariant.

In practice, splitting differential induction proofs over disjunctions by $\vee$l can be useful if a direct proof with a single common differential invariant does not succeed:

$$\to\text{r}\ \frac{\vee\text{l}\ \dfrac{[]gen'\ \dfrac{\text{DI}\ \dfrac{\vdash A'^{\theta}_{x'}}{A \vdash [x' = \theta]A} \quad \vee\text{r}\ \dfrac{ax\ \dfrac{*}{A \vdash A, B}}{A \vdash A \vee B}}{A \vdash [x' = \theta](A \vee B)} \quad []gen'\ \dfrac{\text{DI}\ \dfrac{\vdash B'^{\theta}_{x'}}{B \vdash [x' = \theta]B} \quad \vee\text{r}\ \dfrac{ax\ \dfrac{*}{B \vdash A, B}}{B \vdash A \vee B}}{B \vdash [x' = \theta](A \vee B)}}{A \vee B \vdash [x' = \theta](A \vee B)}}{\vdash A \vee B \to [x' = \theta](A \vee B)}$$

9. Differential Invariants

Differential invariants are a general proof principles for proving invariants of formulas. Summarizing what this lecture has discovered so far leads to a single proof rule for differential invariants. That is why all previous proofs just indicated DI when using the various special cases of the differential invariant proof rule to be developed next.

All previous arguments remain valid when the differential equation has an evolution domain constraint H that it cannot leave by definition. In that case, the inductive proof step can even assume the evolution domain constraint to hold, because the system, by definition, is not allowed to leave it.

Definition 11 (Derivation)**.** The operator $(\cdot)'$ that is defined as follows on first-order real-arithmetic formulas is called *syntactic (total) derivation*:

$$(F \wedge G)' \equiv (F)' \wedge (G)' \tag{4a}$$
$$(F \vee G)' \equiv (F)' \wedge (G)' \tag{4b}$$
$$(\forall x\, F)' \equiv \forall x\, (F)' \tag{4c}$$
$$(\exists x\, F)' \equiv \forall x\, (F)' \tag{4d}$$
$$(a \geq b)' \equiv (a)' \geq (b)' \qquad \text{accordingly for } <, >, \leq, =, \text{ but not } \neq \tag{4e}$$

Furthermore, $F'^{\theta}_{x'}$ is defined to be the result of substituting θ for x' in F'. The operation mapping F to $(F)'^{\theta}_{x'}$ is called *Lie-derivative* of F with respect to $x' = \theta$.

By (4e), the derivation $(F)'$ on formulas F uses the derivation $(a)'$ on terms a that occur within F.

That is, to replace the left-hand side of a differential equation by the right-hand side.

Lemma 12 (Differential invariants)**.** *The differential invariant rule is sound:*

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

The version DI′ can be derived easily from the more fundamental, essential form DI similar to how the most useful loop induction rule ind′ derives from the essential form ind.[a]

[a] The proof rule DI′ is not implemented in KeYmaera, because a differential cut DC with F and a subsequent DI will lead to the same proof (Sect. 12).

The basic idea behind rule DI is that the premise of DI shows that the total derivative F' holds within evolution domain H when substituting the differential equations $x' = \theta$ 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 H, the total derivative F' along the differential constraints is pointing inwards or transversally to F but never outwards to $\neg F$; see Fig. 4 for an illustration. Hence,

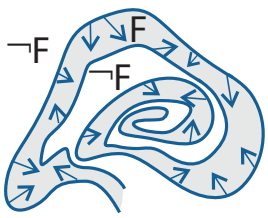


Figure 4: Differential invariant F for safety

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 that, unlike F', the premise of DI is a well-formed formula, because all differential expressions are replaced by non-differential terms when forming $F'^{\theta}_{x'}$.

Proof. Assume the premise $F'^{\theta}_{x'} = 0$ to be valid, i.e. true in all states. In order to prove that the conclusion $F \vdash [x' = \theta]F$ is valid, consider any state ν. Assume that $\nu \models F$, as there is otherwise nothing to show (sequent is trivially *true* since antecedent evaluates to *false*). If $\zeta \in [0, r]$ is any time during any solution $\varphi : [0, r] \to \mathcal{S}$ of any duration $r \in \mathbb{R}$ of $x' = \theta$ beginning in initial state $\varphi(0) = \nu$, then it remains to be shown that $\varphi(r) \models F$. By antecedent, $\nu \models F$, in the initial state $\nu = \varphi(0)$.

If the duration of φ is $r = 0$, we have $\varphi(0) \models F$ immediately, because $\nu \models F$. For duration $r > 0$, we show that F holds all along φ, i.e., $\varphi(\zeta) \models F$ for all $\zeta \in [0, r]$.

We have to show that $\nu \models F \to [x' = \theta \,\&\, H]F$ for all states ν. Let ν satisfy $\nu \models F$ as, otherwise, there is nothing to show. We can assume F to be in disjunctive normal form and consider any disjunct G of F that is true at ν. In order to show that F remains true during the continuous evolution, it is sufficient to show that each conjunct of G is. We can assume these conjuncts to be of the form $\eta \geq 0$ (or $\eta > 0$ where the proof is accordingly). Finally, using vectorial notation, we write $x' = \theta$ for the differential equation system. Now let $\varphi : [0, r] \to (V \to \mathbb{R})$ be any solution of $x' = \theta \,\&\, H$ beginning in $\varphi(0) = \nu$. If the duration of φ is $r = 0$, we have $\varphi(0) \models \eta \geq 0$ immediately, because $\nu \models \eta \geq 0$. For duration $r > 0$, we show that $\eta \geq 0$ holds all along the solution φ, i.e., $\varphi(\zeta) \models \eta \geq 0$ for all $\zeta \in [0, r]$.

Suppose there was a $\zeta \in [0, r]$ with $\varphi(\zeta) \models \eta < 0$, which will lead to a contradiction. The function $h : [0, r] \to \mathbb{R}$ defined as $h(t) = [\![\eta]\!]_{\varphi(\zeta)}$ satisfies the relation $h(0) \geq 0 > h(\zeta)$, because $h(0) = [\![\eta]\!]_{\varphi(0)} = [\![\eta]\!]_{\nu}$ and $\nu \models \eta \geq 0$ by antecedent of the conclusion. By Lemma 3, h is continuous on $[0, r]$ and differentiable at every $\xi \in (0, r)$. By mean value theorem, there is a $\xi \in (0, \zeta)$ such that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) \cdot (\zeta - 0) = h(\zeta) - h(0) < 0$. In particular, since $\zeta \geq 0$, we can conclude that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) < 0$. Now Lemma 3 implies that $\frac{\mathsf{d}h(t)}{\mathsf{d}t}(\xi) = [\![(\eta)']\!]_{\varphi(\xi)} < 0$. This, however, is a contradiction, because the premise implies that the formula $H \to (\eta \geq 0)'$ is true in all states along φ, including $\varphi(\xi) \models H \to (\eta \geq 0)'$. In particular, as φ is a solution for $x' = \theta \,\&\, H$, we know that $\varphi(\xi) \models H$ holds, and we have $\varphi(\xi) \models (\eta \geq 0)'$, which contradicts $[\![(\eta)']\!] < 0$. □

This proof rule enables us to easily prove (3) and all previous proofs as well:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 2de + 2e(-d) \leq 0}\,\mathbb{R}}{\vdash (2dd' + 2ee' \leq 2rr')^{\,e\ -d\ -0}_{\,d'\ e'\ r'}}}{d^2 + e^2 \leq r^2 \vdash [d' = e, e' = -d]d^2 + e^2 \leq r^2}\,\mathrm{DI}}{\vdash d^2 + e^2 \leq r^2 \to [d' = e, e' = -d]d^2 + e^2 \leq r^2}\,{\to}\mathrm{r}$$

10. Example Proofs

Example 13 (Quartic dynamics). The following simple dℒ proof uses DI to prove an invariant of a quartic dynamics.

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

Observe that 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 14. Consider the dynamics $x' = y, y' = -\omega^2 x - 2d\omega y$ of the damped oscillator with the undamped angular frequency ω and the damping ratio d. See Fig. 5 for one example of an evolution along this continuous dynamics. Figure 5 shows a trajectory

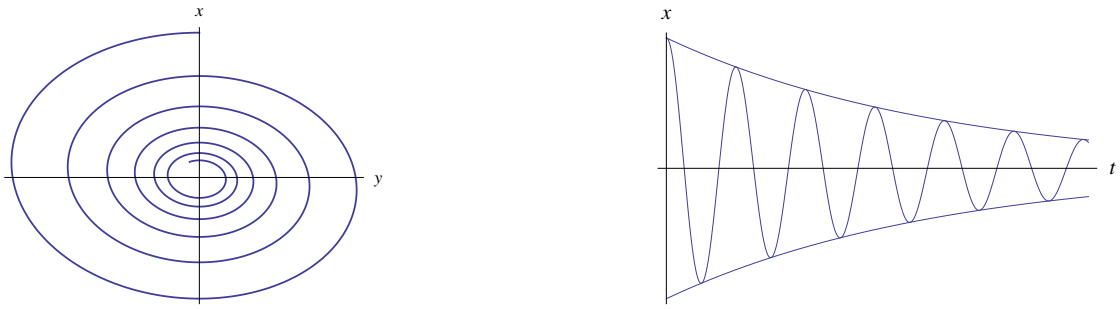


Figure 5: Trajectory and evolution of a damped oscillator

in the x, y space on the left, and an evolution of x over time t on the right. General symbolic solutions of symbolic initial-value problems for this differential equation can become surprisingly difficult. Mathematica, for instance, produces a long equation of exponentials that spans 6 lines of terms just for one solution. A differential invariant proof, instead, is very simple:

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

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

11. 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 (d, e). Suppose the robot moves with constant (linear) velocity into direction (d, e), which is rotating as before. Then the corresponding dynamics is:

$$x' = d, y' = e, d' = \omega e, e' = -\omega d$$

because the derivative of the x coordinate is the component d of the direction and the derivative of the y coordinate is the component e of the direction. If the rotation of the direction (d, e) is faster or slower, the differential equation would be formed correspondingly. Consider the following conjecture:

$$(x-1)^2+(y-2)^2 \geq p^2 \rightarrow [x' = d, y' = e, d' = \omega e, e' = -\omega d](x-1)^2+(y-2)^2 \geq p^2 \quad (5)$$

This conjecture expresses that the robot at position (x, y) will always stay at distance p from the point $(1, 2)$ if it started there. Let's try to prove conjecture (5):

$$\dfrac{\dfrac{\vdash 2(x-1)d+2(y-2)e \geq 0}{\vdash (2(x-1)x'+2(y-2)y' \geq 0)^{d\ e}_{x'\ y'}}}{(x-1)^2+(y-2)^2 \geq p^2 \vdash [x' = d, y' = e, d' = \omega e, e' = -\omega d](x-1)^2+(y-2)^2 \geq p^2}\ \text{DI}$$

Unfortunately, this differential invariant proof does not work. As a matter of fact, *fortunately* it does not work out, because conjecture (5) is not valid, so we will, fortunately, not be able to prove it with a sound proof technique. Conjecture (5) is too optimistic. Starting from some directions far far away, the robot will most certainly get too close to the point (1,2). Other directions may be fine.

Inspecting the above failed proof attempt, we could prove (5) if we knew something about the directions (d, e) that would make the remaining premise prove. What could that be?

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

Certainly, if we knew $d = e = 0$, the resulting premise would prove. 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 prove is if we knew $x - 1 = -e$ and $y - 2 = d$. In what sense could we "know" $x - 1 = -e \land y - 2 = d$? 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 (5) to include this assumption:

$$x - 1 = -e \land y - 2 = d \land (x-1)^2 + (y-2)^2 \geq p^2 \rightarrow \\ [x' = d, y' = e, d' = \omega e, e' = -\omega d](x-1)^2 + (y-2)^2 \geq p^2 \quad (6)$$

Yet, the place in the proof where we need to know $x - 1 = -e \land y - 2 = d$ for the above sequent prove to continue is in the middle of the inductive step. How could 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 $x-1=-e \wedge y-2=d$ is a differential invariant of the dynamics, so it stays true forever if it was true initially:

$$\text{DI}\dfrac{\dfrac{\dfrac{\text{not valid}}{\vdash d=-(-\omega d) \wedge e=\omega e}}{\vdash (x'=-e' \wedge y'=d')^{d\ e\ \omega e\ -\omega d}_{x'\ y'\ d'\ e'}}}{x-1=-e \wedge y-2=d \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d](x-1=-e \wedge y-2=d)}$$

This prove does not quite work out, because both sides of the equations are off by a factor of ω and, indeed, $x-1=-e \wedge y-2=d$ is not an invariant unless $\omega=1$. On second thought, that makes sense, because the angular velocity ω determines how quickly the robot turns, so if there is any relation between position and direction, 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 $\omega(x-1)=-e \wedge \omega(y-2)=d$ instead. That knowledge would still help the proof of (5), just with the same extra factor on both terms. So let's modify (6) to use this assumption on the initial state:

$$\omega(x-1)=-e \wedge \omega(y-2)=d \wedge (x-1)^2+(y-2)^2 \geq p^2 \rightarrow [x'=d,y'=e,d'=\omega e,e'=-\omega d](x-1)^2+(y-2)^2 \geq p^2 \quad (7)$$

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

$$\text{DI}\dfrac{\mathbb{R}\dfrac{\dfrac{*}{\vdash \omega d=-(-\omega d) \wedge \omega e=\omega e}}{\vdash (\omega x'=-e' \wedge \omega y'=d')^{d\ e\ \omega e\ -\omega d}_{x'\ y'\ d'\ e'}}}{\omega(x-1)=-e \wedge \omega(y-2)=d \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d](\omega(x-1)=-e \wedge \omega(y-2)=d)}$$

Now, how can this freshly proved invariant $\omega(x-1)=-e \wedge \omega(y-2)=d$ be made available in the previous proof? Perhaps we could prove (7) using the conjunction of the invariant we want with the additional invariant we need:

$$(x-1)^2+(y-2)^2 \geq p^2 \wedge \omega(x-1)=-e \wedge \omega(y-2)=d$$

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

$$\text{DI}\dfrac{\dfrac{\vdash 2(x-1)d+2(y-2)e \geq 0 \wedge \omega d=-(-\omega d) \wedge \omega e=\omega e}{\vdash (2(x-1)x'+2(y-2)y' \geq 0 \wedge \omega x'=-e' \wedge \omega y'=d')^{d\ e\ \omega e\ -\omega d}_{x'\ y'\ d'\ e'}}}{(x-1)^2 \ldots \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d]((x-1)^2+(y-2)^2 \geq p^2 \wedge \omega(x-1)=-e \wedge \omega(y-2)=d)}$$

because the right conjunct in the premise still proves beautifully but the left conjunct in the premise needs to know the invariant, which 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:

$$(ind)\ \frac{F \vdash [\alpha]F}{F \vdash [\alpha^*]F}$$

By analogy, we could augment the differential invariant proof rule DI similarly to include F 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:

$$(DI_{??})\ \frac{H \land F \vdash F'^{\theta}_{x'}}{F \vdash [x' = \theta \,\&\, H]F} \quad \text{sound?}$$

After all, we really only care about staying safe when we are still safe. And that would indeed easily prove the formula (7), which might make us cheer. But implicit properties of differential equations are a subtle business. Assuming F like in rule $DI_{??}$ would, in fact, be *unsound*, as the following simple counterexample shows, which "proves" an invalid property using the unsound proof rule $DI_{??}$:

$$\cfrac{\cfrac{\cfrac{\text{(unsound)}}{d^2 - 2d + 1 = 0 \vdash 2de - 2e = 0}}{d^2 - 2d + 1 = 0 \vdash (2dd' - 2d' = 0)^{e\ -d}_{d'\ e'}}}{\lightning\ d^2 - 2d + 1 = 0 \vdash [d' = e, e' = -d]d^2 - 2d + 1 = 0}$$

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

$$\cfrac{\cfrac{\cfrac{\text{(unsound)}}{\vdash -(x-y)^2 \geq 0 \to -2(x-y)(1-y) \geq 0}}{\vdash -(x-y)^2 \geq 0 \to (-2(x-y)(x'-y') \geq 0)^{1\ y}_{x'\ y'}}}{\lightning\ -(x-y)^2 \geq 0 \vdash [x' = 1, y' = y](-(x-y)^2 \geq 0)}$$

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 would be sound, but these are nontrivial [Pla10a, Pla12d, Pla12b, GP14, GSP14].

The reason why assuming invariants for their own proof is problematic for the case of differential equations is somewhat subtle [Pla10a, Pla12d]. In a nutshell, the proof rule $DI_{??}$ assumes more than it knows, so that the argument becomes cyclic. The antecedent only provides the invariant in a single point and Lecture 10 already explained that derivatives are not particularly well-defined in a single point.

12. Differential Cuts

Instead of these ill-guided attempts of assuming invariants for their own proof, there is a complementary proof rule for *differential cuts* [Pla10a, Pla08, Pla12d, Pla12b] that can be used to strengthen assumptions about differential equations in a sound way:

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

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

$$(cut)\ \frac{\Gamma \vdash C, \Delta \quad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta}$$

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. In the right premise, rule DC restricts the system evolution to the subdomain $H \wedge C$ of H, 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. 6

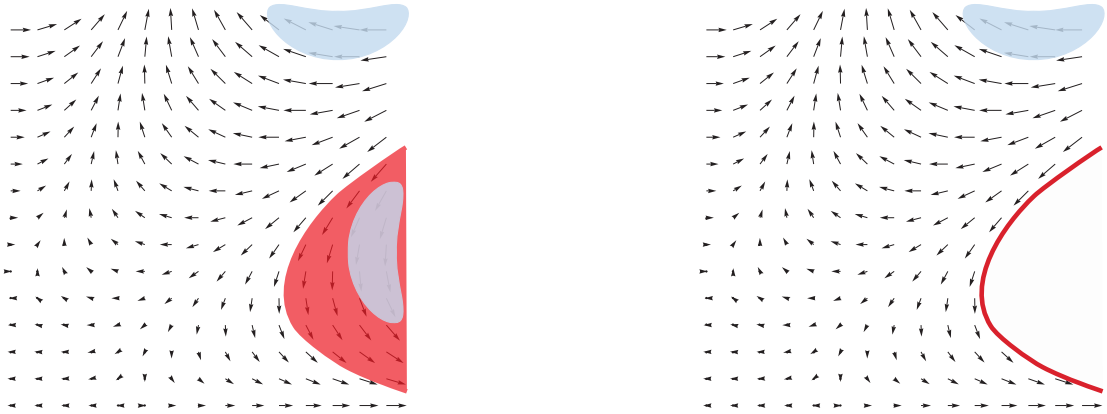


Figure 6: If the solution of the differential equation can never leave region C and enter the red region $\neg C$ (**left**), then this unreachable region $\neg C$ can be cut out of the state space without changing the dynamics of the system (**right**)

The benefit of rule DC is that C will (soundly) be available as an extra assumption for all subsequent DI uses on the right premise (see, e.g., the use of the evolution domain constraint in Example 14). 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 on the right premise, once they have been proven to be differential invariants in the left premise.

Proving the robot formula (7) in a sound way is now easy using a differential cut DC by $\omega(x-1) = -e \wedge \omega(y-2) = d$:

$$\dfrac{\dfrac{*}{\vdash \omega d = -(-\omega d) \wedge \omega e = \omega e}\,\mathbb{R}}{\dfrac{\vdash (\omega x' = -e' \wedge \omega y' = d')^{\frac{d}{x'}\,\frac{e}{y'}\,\frac{\omega e}{d'}\,\frac{-\omega d}{e'}}}{\omega(x-1)=-e\wedge\omega(y-2)=d \vdash [x'=d\,..](\omega(x-1)=-e\wedge\omega(y-2)=d)}\,\text{DI}}\qquad \dfrac{*}{\omega(x-1)=-e\wedge\omega(y-2)=d \vdash 2(x-1)d+2(y-2)e \geq 0}\,\mathbb{R}$$

$$\dfrac{\omega(x-1)=-e\wedge\omega(y-2)=d \vdash (2(x-1)x'+2(y-2)y' \geq 0)^{\frac{d}{x'}\,\frac{e}{y'}}}{(x-1)^2+(y-2)^2\geq p^2 \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d\,\&\,\omega(x-1)=-e\wedge\omega(y-2)=d](x-1)^2+(y-2)^2\geq p^2}\,\text{DI}$$

$$(x-1)^2+(y-2)^2\geq p^2, \omega(x-1)=-e\wedge\omega(y-2)=d \vdash [x'=d,y'=e,d'=\omega e,e'=-\omega d](x-1)^2+(y-2)^2\geq p^2\,\text{DC}$$

Amazing. Now we have a proper sound proof of the quite nontrivial robot motion property (7). And it even is a surprisingly short proof.

See ≪Curved motion model≫

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. 7. For example, we could also have gotten a proof of (7) by first doing a differential cut with $\omega(x-1) = -e$, then continue with a differential cut with $\omega(y-2) = d$, and then finally use both to prove the postcondition (Exercise 3). 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 [PC08, PC09, Pla10b].

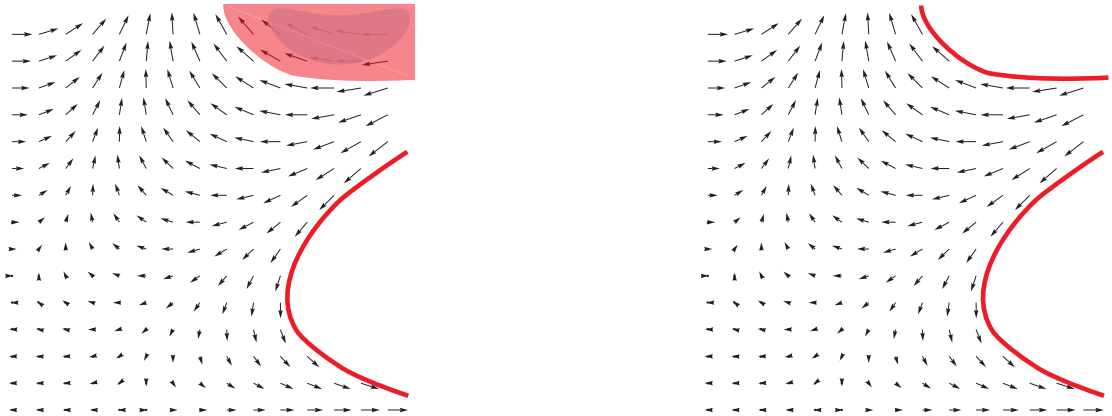


Figure 7: If the solution of the differential equation can never leave region D and enter the top red region $\neg D$ (**left**), then this unreachable region $\neg D$ can also be cut out of the state space without changing the dynamics of the system (**right**)

Proof of Soundness of DC. For simplicity, consider only the case where $H \equiv true$ here. Rule DC is sound using the fact that the left premise implies that every solution φ that satisfies $x' = \theta$ also satisfies C *all along* the solution. Thus, if solution φ satisfies $x' = \theta$, it also satisfies $x' = \theta \,\&\, C$, so that the right premise entails the conclusion. The proof is accordingly for the case □

See ≪ Tutorial Video on Differential Invariants, Differential Cuts≫

13. Differential Weakening

One simple but computable proof rule is *differential weakening*:

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

This rule is obviously sound, because the system $x' = \theta \,\&\, H$, by definition, will stop before it leaves H, hence, if H implies F (i.e. the region H is contained in the region F), then F is an invariant, no matter what the actual differential equation $x' = \theta$ does. Unfortunately, this simple proof rule cannot prove very interesting properties, because it only works when H is very informative. It can, however, be useful in combination with stronger proof rules (e.g., differential cuts).

For example, after having performed the differential cut illustrated in Fig. 6 and, then, subsequently, performing the differential cut illustrated in Fig. 7, all unsafe blue regions have been cut out of the state space, so that the system in Fig. 7(right) is trivially safe by differential weakening, because there are no more unsafe blue regions. That is, the ultimate evolution domain constraint $H \wedge C \wedge D$ after the two differential cuts with C and with D trivially implies the safety condition F, i.e. $H \wedge C \wedge D \vdash F$ is valid. But notice that it took the two differential cuts to make differential weakening useful. The original evolution domain constraint H was not strong enough to imply safety, since there were still unsafe blue regions in the original system in Fig. 6(left) and even still in the intermediate system in Fig. 7(left) obtained after one differential cut with C.

14. Summary

This lecture 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 also require some smarts (or good automatic procedures) to be found. Yet, once differential invariants have been identified, the proof follows easily.

Note 9 (Proof rules for differential equations)**.** *The following are sound proof rules for differential equations:*

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

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

A. Proving Aerodynamic Bouncing Balls

This section studies a hybrid system with differential invariants. Remember the bouncing ball that was proved in Lecture 7 on Loops & Invariants?

The little acrophobic bouncing ball graduated from its study of loops and control and yearningly thinks back of its joyful time when it was studying continuous behavior. Caught up in nostalgia, 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 into 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 which direction the ball is flying. If the ball is hurrying up, 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 could 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 $v = 0$:

$$x' = v, v' = -g - (\operatorname{sign} v) r v^2 \,\&\, x \geq 0 \tag{8}$$

That, however, gives a differential equation with a difficult right-hand side. Instead, the little bouncing ball 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 is 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]

$$\begin{array}{l} x \leq H \wedge v = 0 \wedge x \geq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge r \geq 0 \rightarrow \\ \big[\big(\texttt{if}(x = 0)\, v := -cv; \\ \quad (x' = v, v' = -g - rv^2 \,\&\, x \geq 0 \wedge v \geq 0 \cup x' = v, v' = -g + rv^2 \,\&\, x \geq 0 \wedge v \leq 0)\big)^* \\ \big]\,(0 \leq x \leq H) \end{array} \tag{9}$$

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 (9). 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

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

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 was what differential invariants were good at. And the ball was rather keen on trying them in the wild, anyhow.

Yet, first things first. The first step of the proof after →r is the search for an invariant for the loop induction proof rule ind'. Yet, since the proof of (9) 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.

Since we know the loop invariant for the ordinary bouncing ball from Lecture 7, 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 that invariant to work out for the aerodynamic ball (9) 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:

$$E_{x,v} \overset{\text{def}}{\equiv} 2gx \leq 2gH - v^2 \land x \geq 0 \tag{10}$$

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

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

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]

[2] Since this happens so frequently, KeYmaera implements a proof rule that, similar to the local version of loop invariants, keeps context assumptions around, which is fine as long as they are constant.

The differential invariant proof for the other differential equation in (9) works as well:

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

After this preparation, the rest of the proof of (9) is a matter of checking whether (10) is also a loop invariant. Except that the above two sequent proofs do not actually quite prove that (10) 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 DI would lead to $(x'\geq 0)^{v}_{x'}\equiv v\geq 0$, 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 invariants, 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.

$$\text{DC}\,\frac{\frac{*}{\ldots\vdash [x'=v,v'=-g+rv^2\,\&\,x\geq 0\land v\leq 0]\,2gx\leq 2gH-v^2}\quad \text{DW}\,\frac{\frac{*}{x\geq 0\land v\leq 0\land 2gx\leq 2gH-v^2\vdash 2gx\leq 2gH-v^2\land x\geq 0}\,ax}{2gx\leq 2gH-v^2\vdash [x'=v,v'=-g+rv^2\,\&\,x\geq 0\land v\leq 0\land 2gx\leq 2gH-v^2](2gx\leq 2gH-v^2\land x\geq 0)}}{\ldots 2gx\leq 2gH-v^2\vdash [x'=v,v'=-g+rv^2\,\&\,x\geq 0\land v\leq 0](2gx\leq 2gH-v^2\land x\geq 0)}$$

Now, what is left to do is a matter of proving (10) to be a loop invariant of (9).

Without the usual abbreviations this proof is hopeless to fit on a page:

$$\begin{aligned}
A_{x,v} &\overset{\text{def}}{\equiv} x\leq H\land v=0\land x\geq 0\land g>0\land 1\geq c\geq 0\land r\geq 0\\
B_{x,v} &\overset{\text{def}}{\equiv} 0\leq x\land x\leq H\\
(x''\ldots v\geq 0) &\overset{\text{def}}{\equiv} (x'=v,v'=-g-rv^2\,\&\,x\geq 0\land v\geq 0)\\
(x''\ldots v\leq 0) &\overset{\text{def}}{\equiv} (x'=v,v'=-g+rv^2\,\&\,x\geq 0\land v\leq 0)\\
E_{x,v} &\overset{\text{def}}{\equiv} 2gx\leq 2gH-v^2\land x\geq 0
\end{aligned}$$

$$ind'\,\frac{A_{x,v}\vdash E_{x,v}\quad [;]\text{r}\,\frac{[]gen'\,\frac{E_{x,v}\vdash [\texttt{if}(x=0)\,v:=-cv]E_{x,v}\quad [\cup]\text{r}\,\frac{\wedge\text{r}\,\frac{E_{x,v}\vdash [x''\ldots v\geq 0]E_{x,v}\quad E_{x,v}\vdash [x''\ldots v\leq 0]E_{x,v}}{E_{x,v}\vdash [x''\ldots v\geq 0]E_{x,v}\land [x''\ldots v\leq 0]E_{x,v}}}{E_{x,v}\vdash [x''\ldots v\geq 0\cup x''\ldots v\leq 0]E_{x,v}}}{E_{x,v}\vdash [\texttt{if}(x=0)\,v:=-cv][x''\ldots v\geq 0\cup x''\ldots v\leq 0]E_{x,v}}}{E_{x,v}\vdash [\texttt{if}(x=0)\,v:=-cv;(x''\ldots v\geq 0\cup x''\ldots v\leq 0)]E_{x,v}}\quad E_{x,v}\vdash B_{x,v}}{A_{x,v}\vdash [(\texttt{if}(x=0)\,v:=-cv;(x''\ldots v\geq 0\cup x''\ldots v\leq 0))^*]B_{x,v}}$$

The first and last premise prove 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 proves as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{E_{x,v}, x=0 \vdash E_{x,-cv}}{E_{x,v}, x=0 \vdash [v:=-cv]E_{x,v}}\,[:=]\mathrm{r}}{E_{x,v} \vdash x=0 \to [v:=-cv]E_{x,v}}\,{\to}\mathrm{r}}{E_{x,v} \vdash [?x=0][v:=-cv]E_{x,v}}\,[?]\mathrm{r}}{E_{x,v} \vdash [?x=0;v:=-cv]E_{x,v}}\,[;]\mathrm{r} \qquad \dfrac{\dfrac{*}{E_{x,v}, x\neq 0 \vdash E_{x,v}}\,ax}{E_{x,v} \vdash x\neq 0 \to E_{x,v}}\,{\to}\mathrm{r}}{E_{x,v} \vdash [?x\neq 0]E_{x,v}}\,[?]\mathrm{r}}{E_{x,v} \vdash [?x=0;v:=-cv]E_{x,v} \wedge [?x\neq 0]E_{x,v}}\,{\wedge}\mathrm{r}$$
$$\dfrac{E_{x,v} \vdash [?x=0;v:=-cv \cup ?x\neq 0]E_{x,v}}{E_{x,v} \vdash [\mathtt{if}(x=0)\, v:=-cv]E_{x,v}}\,[\cup]\mathrm{r}$$

This sequent proof first expands the $\mathtt{if}()$, recalling that it is an abbreviation for a choice with tests. The right resulting premise proves trivially by axiom (there was no state change in the corresponding part of the execution), the left premise proves 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 (9). That is pretty neat!

See ≪Aerodynamic bouncing ball model≫

It is about time for the newly upgraded aerodynamic acrophobic bouncing ball to notice a subtlety in its (provably safe) model. The bouncing ball had innocently split the differential equation (8) into two modes, one for $v \geq 0$ and one for $v \leq 0$ when developing the model (9). This seemingly innocuous step would have required more thought than the little bouncing ball had put in at the time. Of course, the single differential equation (8) 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 (9) that split the mode, however, enforces that the ground controller $\mathtt{if}(x=0)\, v:=-cv$ 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 over and pull the ball back down again, that is of no consequence, because the trigger condition $x = 0$ will not be the case then anyhow, unless the ball really started the day without much energy ($x = v = 0$). On its way down, the condition will 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 much 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 without enforcing a discrete ground controller action to happen. This leads to the following dL formula

with a systematical mode split, which is provably safe just the same (Exercise 4):

$$\begin{array}{l} x \leq H \wedge v = 0 \wedge x \geq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge r \geq 0 \rightarrow \\ \big[\big(\texttt{if}(x = 0)\, v := -cv; \\ \quad (x' = v, v' = -g - rv^2 \,\&\, x \geq 0 \wedge v \geq 0 \cup x' = v, v' = -g + rv^2 \,\&\, x \geq 0 \wedge v \leq 0)^{\textbf{*}}\big)^* \\ \big]\, (0 \leq x \leq H) \end{array} \tag{11}$$

Exercises

Exercise 1. We have chosen to define

$$(\theta < \eta)' \equiv ((\theta)' < (\eta)')$$

Prove that the following slightly relaxed definition would also give a sound proof rule for differential invariants:

$$(\theta < \eta)' \equiv ((\theta)' \leq (\eta)')$$

Exercise 2. We have defined

$$(\theta \neq \eta)' \equiv ((\theta)' = (\eta)')$$

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?

Exercise 3. Prove $\mathsf{d}\mathcal{L}$ formula(7) by first doing a differential cut with $\omega(x-1) = -e$, then continue with a differential cut with $\omega(y-2) = d$, and then finally use both to prove the original postcondition. Compare this proof to the proof in Sect. 12.

Exercise 4. 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) with its extra loop regardless. Compare the resulting proof to the sequent proof for (9).

Exercise 5. The least that the proof rules for differential equations get to assume is the evolution domain constraint H, because the system does not evolve outside it. Prove the following slightly stronger formulation of DI that assumes H to hold initially:

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

Exercise 6. Prove the following definitions to be sound for the differential invariant proof rule:

$$\begin{aligned} true' &\equiv true \\ false' &\equiv true \end{aligned}$$

Show how you can use those to prove the formula

$$A \to [x' = \theta \,\&\, H]B$$

in the case where $A \to \neg H$ is provable, i.e. where the system initially starts outside the evolution domain constraint H.

References

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

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

[LIC12] *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012*. IEEE, 2012.

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

[PC09] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. *Form. Methods Syst. Des.*, 35(1):98–120, 2009. Special issue for selected papers from CAV'08. doi:10.1007/s10703-009-0079-8.

[Pla08] André Platzer. *Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems*. PhD thesis, Department of Computing Science, University of Oldenburg, Dec 2008. Appeared with Springer.

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

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

[Pla12a] André Platzer. The complete proof theory of hybrid systems. In LICS [LIC12], pages 541–550. doi:10.1109/LICS.2012.64.

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

[Pla12c] André Platzer. Logics of dynamical systems. In LICS [LIC12], pages 13–24. doi:10.1109/LICS.2012.13.

[Pla12d] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012. doi:10.2168/LMCS-8(4:16)2012.