On the Coalgebra of Partial Differential Equations

Michele Boreale
Università di Firenze, Dipartimento di Statistica, Informatica, Applicazioni (DiSIA) "G. Parenti", Viale Morgagni 65, I-50134 Firenze, Italy
michele.boreale@unifi.it

Abstract

We note that the coalgebra of formal power series in commutative variables is final in a certain subclass of coalgebras. Moreover, a system Σ of polynomial PDEs, under a coherence condition, naturally induces such a coalgebra over differential polynomial expressions. As a result, we obtain a clean coinductive proof of existence and uniqueness of solutions of initial value problems for PDEs. Based on this characterization, we give complete algorithms for checking equivalence of differential polynomial expressions, given Σ.

2012 ACM Subject Classification Theory of computation → Invariants; Theory of computation → Operational semantics

Keywords and phrases coalgebra, partial differential equations, polynomials

Digital Object Identifier 10.4230/LIPIcs.MFCS.2019.24

Acknowledgements Three anonymous reviewers have provided valuable comments.

1 Introduction

The last two decades have seen an impressive growth of formal methods and tools for continuous and hybrid systems, centered around techniques for reasoning on ordinary differential equations (ODEs), see e.g. [29, 28, 21, 11, 15, 6] and references therein. On the other hand, formal methods for systems defined by *partial* differential equations (PDEs) have not undergone a comparable development. The present paper is meant as an initial contribution towards this development.

Like in our previous works on ODEs [5, 7], our starting point is a simple operational view of differential equations as programs for calculating the Taylor coefficients of a function. Taking a transition in such a program corresponds to taking a function's derivative. An output is returned as the result of evaluating the current state (function) at a fixed expansion point, for example the origin. This idea is certainly not new: it is for example at the root of classical methods to numerically solve ODEs.

We focus here on polynomial PDEs, which are expressive enough for the vast majority of problems arising in applications, and systematically pursue the above operational view in the framework of coalgebras. We first introduce a subclass of coalgebras that enjoy a commutativity property of transitions, then note that formal power series in commutative variables (CFPSs) are final for this subclass (Section 2). A system Σ of PDEs and a specification of initial data together form an initial value problem. Under a coherence condition (Section 3), an initial value problem induces a coalgebra structure over the set of differential polynomials. The solution of the initial value problem is therefore obtained as the unique coalgebra morphism from the set of such polynomials to the final coalgebra of CFPSs. This way, we obtain an elementary and clean proof of existence and uniqueness of solutions as CFPSs (Section 4). We also show that coherence is an essential requirement for this result. From a pragmatical point of view, we note that as solutions of PDEs, CFPSs may be viewed as a conservative extension of analytic functions: *if* an analytic solution of Σ exists, *then* its Taylor expansion from 0, seen as a formal power series, coincides with the unique solution in our sense.

44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019).
Editors: Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen; Article No. 24; pp. 24:1–24:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

$\begin{cases} \partial f = g \\ \partial g = -f \end{cases}$ verify $f^2+g^2=1$: $y^2+z^2=1$, $\underbrace{2yy'+2zz'}_{2yz-2zy=0}=0$ ✓

This characterization is the basis of an algorithm to automatically check polynomial equalities – e.g. conservation laws – valid among the functions defined by given system Σ and a specification of initial data (Section 5). Just like in certain on-the-fly algorithms for bisimulation checking, the underlying idea is, based on the introduced transition structure, to incrementally build a relation until it "closes up", but working here modulo sum and product of polynomials. Concepts from algebraic geometry, notably Gröbner bases, are used to prove the termination and correctness of this algorithm. In fact, we are more general than this, and also give a method to automatically compute the weakest precondition (= set of initial data specifications) under which a given equality is valid in Σ. These algorithms are complete, under a certain finite-parameter condition. This way one can, for example, automatically check conservation laws of a given physical system. Relationship with our previous work on ODEs [5, 7], as well as with related work by other authors, is discussed in the concluding section (Section 6). Proofs omitted from the present version will appear in a forthcoming online version of the paper.

2 Commutative coalgebras

Let X be a finite nonempty set of *actions (or variables)*, ranged over by $x, y, \ldots$ and O a nonempty set. We recall that a *(Moore) coalgebra*[1] with actions in X and outputs in O is a triple $C = (\mathcal{S}, \delta, o)$ where: $\mathcal{S}$ is a set of *states*, $\delta : \mathcal{S} \times X \to \mathcal{S}$ is a *transition* function, and $o : \mathcal{S} \to O$ is an *output* function (see e.g. [27]). A *bisimulation* in C is a binary relation $R \subseteq \mathcal{S} \times \mathcal{S}$ such that whenever $s\,R\,t$ then: (a) $o(s) = o(t)$, and (b) for each x, $\delta(s,x)\,R\,\delta(t,x)$. It is an (easy) consequence of the general theory of bisimulation that a largest bisimulation over C, called bisimilarity and denoted by $\sim_C$, exists, is the union of all bisimulation relations, and is an equivalence relation over $\mathcal{S}$. Given two coalgebras with actions in X and outputs in O, C_1 and C_2, a *morphism* from C_1 to C_2 is a function $\mu : \mathcal{S}_1 \to \mathcal{S}_2$ that: (1) preserves outputs ($o_1(s) = o_2(\mu(s))$), and (2) preserves transitions ($\mu(\delta_1(s,x)) = \delta_2(\mu(s), x)$), for each state s and action x). It is an easy consequence of this definition that a morphism preserves bisimulation in both directions, that is: $s \sim_{C_1} t$ if and only if $\mu(s) \sim_{C_2} \mu(t)$.

We introduce now the subclass of Moore coalgebras we will focus on. We say a coalgebra C has *commutative actions* (or just that is *commutative*) if for each state s and actions x, y, it holds that $\delta(\delta(s,x),y) \sim_C \delta(\delta(s,y),x)$. We will introduce below an example of commutative coalgebra. In what follows, we let σ range over X^*, and, for any state s, let $s(\sigma)$ be defined inductively as: $s(\epsilon) \triangleq s$ and $s(x\sigma) \triangleq \delta(s,x)(\sigma)$.

▶ **Lemma 2.1.** *Let C be a commutative coalgebra. If $\sigma, \sigma' \in X^*$ are permutations of one another then for any state $s \in \mathcal{S}$, $s(\sigma) \sim_C s(\sigma')$.*

We now introduce the coalgebra of formal power series in commutative variables with outputs in $O = \mathbb{R}$. Let $X^{\otimes}$, ranged over by $\tau, \tau', \ldots$, be the set of *monomials*[2] that can be formed from $X = \{x_1, \ldots, x_n\}$, in other words, the commutative monoid freely generated by X.

▶ **Definition 2.2** (commutative formal power series). *Let X be a finite nonempty alphabet. A* commutative formal power series *(CFPS) with indeterminates in X and coefficients in $\mathbb{R}$ is a total function $f : X^{\otimes} \to \mathbb{R}$. The set of these CFPSs will be denoted by $\mathcal{F}(X)$, or simply $\mathcal{F}$ if X is understood from the context.*

[1] In the paper, we only consider Moore coalgebras. For brevity, we shall omit the qualification "Moore".
[2] In general, we shall adopt for monomials the same notation we use for strings, as the context is sufficient to disambiguate. In particular, we overload the symbol ϵ to denote both the empty string and the empty monomial.

In the rest of the section, we fix an arbitrary X. We will sometimes use the suggestive notation

$$\sum_{\tau} f(\tau) \cdot \tau$$

to denote a CFPS $f = \lambda\tau.f(\tau)$. By slight abuse of notation, for each $r \in \mathbb{R}$, we will denote the CFPS that maps ϵ to r and anything else to 0 simply as r; while x_i will denote the i-th identity, the CFPS that maps x_i to 1 and anything else to 0. In the sequel, $\delta(f, x) \triangleq \frac{\partial f}{\partial x}$ denotes the CFPS obtained by the usual (formal) partial derivative of f along x. For a more workable formulation of this definition, let us introduce the following notation. Let us fix any total order $\mathbf{x} = (x_1, ..., x_n)$ of the variables in X. Given a vector $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n)$ of nonnegative integers (a *multi-index*), we let $\mathbf{x}^{\boldsymbol{\alpha}}$ denote the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Then $\frac{\partial f}{\partial x_i}$ is defined by the following, for each $\tau = \mathbf{x}^{(\alpha_1,...,\alpha_n)}$

$$\frac{\partial f}{\partial x_i}(\tau) \quad \triangleq \quad (\alpha_i + 1) f(x_i \tau) \,. \tag{1}$$

Finally, we define the coalgebra of CFPSs, $C_{\mathcal{F}}$

$$C_{\mathcal{F}} \quad \triangleq \quad (\mathcal{F}, \delta_{\mathcal{F}}, o_{\mathcal{F}})$$

where $\delta_{\mathcal{F}}(f, x) = \frac{\partial f}{\partial x}$ and $o_{\mathcal{F}}(f) = f(\epsilon)$ (the constant term of f). Bisimilarity in $C_{\mathcal{F}}$, denoted by $\sim_{\mathcal{F}}$, coincides with equality. It is easily seen that for each x, y, $\frac{\partial}{\partial y}\frac{\partial f}{\partial x} = \frac{\partial}{\partial x}\frac{\partial f}{\partial y}$, so that $C_{\mathcal{F}}$ is a commutative coalgebra. Now fix any commutative coalgebra $C = (\mathcal{S}, \delta, o)$. We define the function $\mu : \mathcal{S} \to \mathcal{F}$ as follows. For each $\tau = \mathbf{x}^{\boldsymbol{\alpha}}$

$$\mu(s)(\tau) \quad \triangleq \quad \frac{o(s(\tau))}{\boldsymbol{\alpha}!} \tag{2}$$

where $\boldsymbol{\alpha}! \triangleq \alpha_1! \cdots \alpha_n!$. Here, abusing slightly notation, we let $o(s(\tau))$ denote $o(s(\sigma))$, for some string σ obtained by arbitrarily ordering the elements in τ: the specific order does not matter, in view of Lemma 2.1 and of condition (a) in the definition of bisimulation.

▶ **Lemma 2.3.** *Let C be a commutative coalgebra and $f = \mu(s)$. For each x, $\frac{\partial f}{\partial x} = \mu(\delta(s, x))$.*

Based on the above lemma and the fact that $\sim_{\mathcal{F}}$ is equality, we can prove the following corollary, saying that $C_{\mathcal{F}}$ is *final* in the class of *commutative* coalgebras.

▶ **Corollary 2.4** (coinduction and finality of $C_{\mathcal{F}}$)**.** *Let C be a commutative coalgebra. The function μ in* (2) *is the unique coalgebra morphism from C to $C_{\mathcal{F}}$. Moreover, the following* coinduction *principle is valid: $s \sim_C t$ if and only if $\mu(s) = \mu(t)$ in $\mathcal{F}$.*

Proof. We have: (1) $o(s) = \mu(s)(\epsilon)$ by the definition of μ, and (2) $\mu(\delta(s, x)) = \delta_{\mathcal{F}}(\mu(s), x)$, by Lemma 2.3. This proves that μ is a coalgebra morphism. Next, we prove that $\sim_{\mathcal{F}}$ coincides with equality in $\mathcal{F}$. More precisely, we prove that for each τ and for each f, g: $f \sim_{\mathcal{F}} g$ implies $f(\tau) = g(\tau)$. Proceeding by induction on the length of τ, we see that the base case is trivial, while for the induction step $\tau = x_i\tau'$ we have: $f \sim_{\mathcal{F}} g$ implies $\frac{\partial f}{\partial x_i} \sim_{\mathcal{F}} \frac{\partial g}{\partial x_i}$ (bisimilarity), which in turn implies $\frac{\partial f}{\partial x_i}(\tau') = \frac{\partial g}{\partial x_i}(\tau')$ (induction hypothesis); but by (1), $f(x_i\tau') = (\frac{\partial f}{\partial x_i}(\tau'))/(\alpha_i + 1)$ and $g(x_i\tau') = (\frac{\partial g}{\partial x_i}(\tau'))/(\alpha_i + 1)$, and this completes the induction step. From the coincidence of $\sim_{\mathcal{F}}$ with equality in $\mathcal{F}$, and the fact that any morphism preserves bisimilarity in both directions, the last part of the statement (coinduction) follows immediately. Finally, let ν be any morphism from C to $C_{\mathcal{F}}$. From the definitions of bisimulation and morphism it is easy to see that for each s, $\mu(s) \sim_{\mathcal{F}} \nu(s)$: this implies $\mu(s) = \nu(s)$ by coinduction, and proves uniqueness of μ. ◀

We end this section by recalling the sum and product operations on $\mathcal{F}$. For any $\xi = \mathbf{x}^{\boldsymbol{\alpha}}$ and $\tau = \mathbf{x}^{\boldsymbol{\beta}}$, let $\xi \leq \tau$ if for each $i = 1, ..., n$, $\alpha_i \leq \beta_i$; in this case τ/ξ denotes the monomial $\mathbf{x}^{(\beta_1-\alpha_1,...,\beta_n-\alpha_n)}$. We have the following definitions of sum and product. For each $\tau \in X^{\otimes}$:

$$(f+g)(\tau) \triangleq f(\tau)+g(\tau) \qquad\qquad (f \cdot g)(\tau) \triangleq \sum_{\xi \leq \tau} f(\xi) \cdot g(\tau/\xi)\,. \tag{3}$$

These operations correspond to the usual sum and product of functions, when (convergent) CFPS are interpreted as analytic functions. These operations enjoy associativity, commutativity and distributivity. Moreover, if $f(\epsilon) \neq 0$ there exists a unique CFPS $f^{-1} \in \mathcal{F}$ that is a multiplicative inverse of f, that is $f \cdot f^{-1} = 1$. Finally, the following familiar rules of differentiation are satisfied:

$$\frac{\partial(f+g)}{\partial x} \triangleq \frac{\partial f}{\partial x} + \frac{\partial g}{\partial x} \qquad\qquad \frac{\partial(f \cdot g)}{\partial x} \triangleq \frac{\partial f}{\partial x} \cdot g + f \cdot \frac{\partial g}{\partial x}\,. \tag{4}$$

If the *support* of f, $\mathrm{supp}(f) \triangleq \{\tau : f(\tau) \neq 0\}$, is finite, we will call f a *polynomial*. The set of polynomials, denoted by $\mathbb{R}[X]$, is closed under the above defined operations of partial derivative, sum and product (but in general not inverse). Moreover, note that, when confining to polynomials, these operations are well defined even in case the cardinality of the set X of indeterminates is infinite.

3 Coherent systems of PDEs

We first review some notation and terminology from the formal theory of PDEs; these are standard notions, see e.g. [23, 18]. Like in the previous section, assume we are given a finite nonempty set X, which we will call here the *independent variables*. Another nonempty, finite set U of *dependent variables*, disjoint from X, is given; U is ranged over by $u, v, ...$. $\mathcal{D} \triangleq \{u_\tau : u \in U, \tau \in X^{\otimes}\}$ is the set of the *derivatives*; here u_ϵ will be identified with u. $E, F, ...$ range over $\mathcal{P} \triangleq \mathbb{R}[X \cup \mathcal{D}]$, the set of *(differential, multivariate) polynomials* with coefficients in $\mathbb{R}$ and indeterminates in $X \cup \mathcal{D}$. Considered as formal objects, polynomials are just finite-support CFPSs in $\mathcal{F}(X \cup \mathcal{D})$ (see Section 2). As such, they inherit from CFPSs the operations of sum, product and partial derivative, along with the corresponding properties. Syntactically, we shall write polynomials as expressions of the form $\sum_{\alpha \in M} \lambda_\alpha \cdot \alpha$, for $0 \neq \lambda_\alpha \in \mathbb{R}$ and $M \subseteq_{\mathrm{fin}} (X \cup \mathcal{D})^{\otimes}$. For example, $E = v_z u_{xy} + v_y^2 + u + 5x$ is a polynomial[3]. For an independent variable $x \in X$, the *total derivative of $E \in \mathcal{P}$ along x* is just the derivative of E along x, taking into account that $\frac{\partial u_\tau}{\partial x} = u_{x\tau}$. Formally, we have the following.

differential structure

▶ **Definition 3.1** (total derivative). *The operator $D_x : \mathcal{P} \to \mathcal{P}$ is defined by (note $\sum$ below has only finitely many nonzero terms)*

$$D_x E \triangleq \frac{\partial E}{\partial x} + \sum_{u,\tau} u_{x\tau} \cdot \frac{\partial E}{\partial u_\tau}$$

chain rule for differential polynomials

where $\frac{\partial E}{\partial a}$ denotes the partial derivative of polynomial E along $a \in X \cup \mathcal{D}$.

D_x inherits from partial derivatives rules for sum and product that are the analog of (4). As an example, for the polynomial E above, we have $D_x E = v_{xz} u_{xy} + v_z u_{xxy} + 2v_y v_{xy} + u_x + 5$.

[3] Real arithmetic expressions will be used as a meta-notation for polynomials: e.g. $(u+u_x+1)\cdot(x+u_y)$ denotes the polynomial $xu + uu_y + xu_x + u_x u_y + x + u_y$.

In particular, $D_x u_\tau = u_{x\tau}$ and $D_x x^k = kx^{k-1}$. Just as partial derivatives, total derivatives commute with each other, that is $D_x D_y F = D_y D_x F$. This suggests to extend the notation to monomials: for any monomial $\tau = x_1 \cdots x_m$, we let $D_\tau F$ be $D_{x_1} \cdots D_{x_m} F$, where the order of the variables is irrelevant.

quite general

▶ **Definition 3.2** (system of PDEs). *A system of PDEs is a nonempty set Σ of equations (pairs) of the form $u_\tau = E$, with $E \in \mathcal{P}$. The set of derivatives u_τ that appear as left-hand sides of equations in Σ is denoted $\mathrm{dom}(\Sigma)$. Based on Σ, the set $\mathcal{D}$ can be partitioned into two sets as follows:*

- $\mathcal{P}\mathrm{r}(\Sigma) \stackrel{\triangle}{=} \{u_\xi : \tau \leq \xi$ *for some* τ *s.t.* $u_\tau \in \mathrm{dom}(\Sigma)\}$ *is the set of principal derivatives of* Σ*;*
- $\mathcal{P}\mathrm{a}(\Sigma) \stackrel{\triangle}{=} \mathcal{D} \setminus \mathcal{P}\mathrm{r}(\Sigma)$ *is the set of parametric derivatives of* Σ.

We let $\mathcal{P}_0(\Sigma) \stackrel{\triangle}{=} \mathbb{R}[X \cup \mathcal{P}\mathrm{a}(\Sigma)]$.

if it exists!

The intuition of $\mathcal{P}\mathrm{a}(\Sigma)$ is that, once we fix the corresponding values, the rest of the solution, hence $\mathcal{P}\mathrm{r}(\Sigma)$, will be uniquely determined (see Example 3.4 below). Note that we do not require that each derivative occurs at most once as left-hand side in Σ. The *infinite prolongation* of a system Σ, denoted Σ^∞, is the system of PDEs of the form $u_{\xi\tau} = D_\xi F$, where $u_\tau = F$ is in Σ and $\xi \in X^\otimes$. Of course, $\Sigma^\infty \supseteq \Sigma$. Moreover, Σ and Σ^∞ induce the *same* sets of principal and parametric derivatives.

A *ranking* is a total order $\prec$ of $\mathcal{D}$ such that: (a) $u_\tau \prec u_{x\tau}$, and (b) $u_\tau \prec v_\xi$ implies $u_{x\tau} \prec v_{x\xi}$, for each $x \in X$, $\tau, \xi \in X^\otimes$ and $u, v \in U$. Dickson's lemma [10] implies that $\mathcal{D}$ with $\prec$ is a well-order, and in particular that there is no infinite descending chain in it. The system Σ is $\prec$-*normal* if, for each equation $u_\tau = E$ in Σ, $u_\tau \succ v_\xi$, for each v_ξ appearing in E. An easy but important consequence of condition (b) above is that if Σ is normal then also its prolongation Σ^∞ is normal.

Now, consider the equational theory over $\mathcal{P}$ induced by the equations in Σ^∞. More precisely, write $E \to_\Sigma F$ if F is the polynomial that is obtained from E by replacing one occurrence of u_τ with G, for some equation $u_\tau = G \in \Sigma^\infty$. Note, in particular, that $E \in \mathcal{P}$ cannot be rewritten if and only if $E \in \mathcal{P}_0(\Sigma)$. We let $=_\Sigma$ denote the reflexive, symmetric and transitive closure of $\to_\Sigma$. The following definition formalizes the key concepts of consistency and coherence of Σ. Basically, as we will show, under the syntactic requirement of normality, which is natural from an algorithmic point of view, consistency is a necessary and sufficient condition for Σ to admit a unique solution under *all* initial data specifications.

▶ **Definition 3.3** (consistency and coherence). *Let Σ be a system of PDEs.*

- *We say Σ is* consistent *if for each $E \in \mathcal{P}$ there is a unique $F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$.*
- *Let $\prec$ be a ranking. A system Σ is $\prec$-*coherent *if it is $\prec$-normal and consistent.*

For a consistent system, we can define a *normal form function*

$$S_\Sigma : \mathcal{P} \to \mathcal{P}_0(\Sigma)$$

by letting $S_\Sigma E = F$, for the unique $F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$. The term $S_\Sigma E$ will be often abbreviated as SE, if Σ is understood from the context. Deciding if a (finite) system Σ is coherent, for a suitable ranking $\prec$, is of course a nontrivial problem. In a *normal* system, since $\prec$ is a well-order, there are no infinite sequences of rewrites $E_1 \to_\Sigma E_2 \to_\Sigma E_3 \to_\Sigma \cdots$: therefore it is possible to rewrite any E into some $F \in \mathcal{P}_0(\Sigma)$ in a finite number of steps. Proving coherence in this case reduces basically to ensure that Σ contains "enough equations" to make $\to_\Sigma$ confluent. In fact, an even more general problem than checking coherence is completing a normal, non coherent system by new equations so as to make it coherent; or

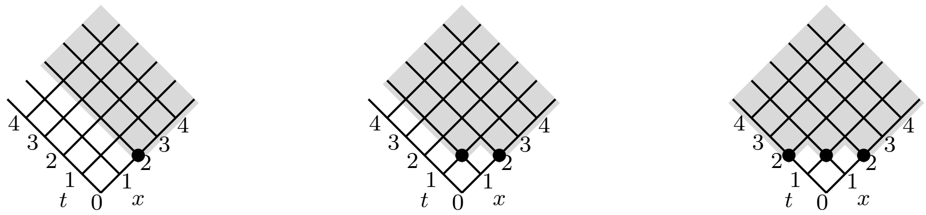

Figure 1 Lattices of u-derivatives, partially ordered by $u_\xi \leq u_\tau$ if and only if $\xi \leq \tau$. With reference to Example 3.4, black circles correspond to left-hand sides of equations, shaded regions to principal derivatives, and non-shaded regions to parametric derivatives.

deciding if this is impossible at all, because the system is intrinsically inconsistent. There is a rich literature on these problems, which we briefly review in the concluding section. The following simple example is enough to demonstrate these concepts for our purposes.

▶ **Example 3.4** (coherence)**.** Consider the heat equation in one spatial dimension, where $X = \{x, t\}$, $U = \{u\}$ and Σ is given by the single equation (for a real parameter $a \neq 0$)

$$\bullet \quad u_{xx} \ = \ au_t \,. \tag{5}$$

Here, the principal derivatives are $\mathcal{P}\mathrm{r}(\Sigma) = \{u_{xx\tau} : \tau \in X^{\otimes}\}$, and the parametric ones are $\mathcal{P}\mathrm{a}(\Sigma) = \{u_{t^j} : j \geq 0\} \cup \{u_{xt^j} : j \geq 0\}$ (see Figure 1, left). Since the system has just one equation, it is clearly consistent: indeed, its prolongation Σ^∞ has precisely one equation $u_{xx\tau} = D_\tau\,(au_t)$ for each principal derivative $u_{xx\tau}$. Concerning coherence, we consider the following ranking. Ordering the independent variables as $t < x$ induces a *graded* lexicographic order $\prec_{\mathrm{grlex}}$ over $X^{\otimes}$: that is, monomials are compared first by their total degree, and then lexicographically. We lift $\prec_{\mathrm{grlex}}$ to $\mathcal{D}$ as expected: explicitly, $u_\xi \prec u_\tau$ if, for $\xi = t^i x^j$ and $\tau = t^{i'} x^{j'}$, it holds that either $i + j < i' + j'$ or $(i + j = i' + j'$ and $j' > j)$. Σ is clearly $\prec$-normal.

Next, suppose we build a new system Σ_1 by adding the new equation (with no physical significance)

$$u_{tx} \ = \ u \,.$$

Now the parametric derivatives are u_{t^j} for $j \geq 0$ and u_x, while the remaining derivatives are principal (see Figure 1, center). The prolongation of the new system, Σ_1^∞, has both $u_{txx} = u_x$ and $u_{txx} = au_{tt}$ as equations, which implies $u_x =_{\Sigma_1} au_{tt}$. As $u_x, u_{tt} \in \mathcal{P}\mathrm{a}(\Sigma_1) \subseteq \mathcal{P}_0(\Sigma_1)$, we conclude that Σ_1 is *not* consistent, hence not coherent: indeed, there are two distinct but equivalent normal forms. This suggests that we can complete Σ_1 by inserting a third equation, a so-called *integrability condition*

$$u_{tt} \ = \ \frac{u_x}{a} \,.$$

In the resulting system Σ_2 the set of parametric derivatives has changed to $\{u, u_t, u_x\}$ (see Figure 1, right), and u_{txx} has the (only) normal form u_x. The system Σ_2 can be indeed checked to be consistent, hence coherent. Finally, consider adding to the original system Σ the two equations below, thus obtaining Σ_3

$$u_{tx} \ = \ t \qquad\qquad u_{tt} \ = \ 1 \,.$$

Together with (5) these two equations imply $a =_{\Sigma_3} 0$: Σ_3 is not consistent, moreover there is no way of completing it so as to get a consistent system. That is, Σ_3 is (informally speaking) intrinsically inconsistent.

Complexity?

For our purposes, it is enough to know that completing a given system of equations to make it coherent, or deciding that this is impossible, can be achieved by one of many existing computer algebra algorithms. For example, there is a completion procedure by Marvan [18], for which a Maple implementation is also available. See also Reid et al.'s method of reduction to *reduced involutive form* [23], implemented in the Maple rif package. An alternative to these methods is applying a procedure similar to the Knuth-Bendix completion algorithm [13] to the given system. Further references are discussed in the concluding section. In practice, in many cases arising from applications (e.g. mathematical physics), transforming the system into a coherent form for an appropriate ranking can be accomplished manually, without much difficulty. We shall not further dwell on algorithms for coherence checking in the rest of the paper. We end the section with a technical result about normal forms in coherent systems that will be used in the next section.

▶ **Lemma 3.5.** *Let Σ be coherent. For each $x \in X$ and $F \in \mathcal{P}$, $SD_x SF = SD_x F$.*

4 Coalgebraic semantics of initial value problems

We will provide differential polynomials with a coalgebra structure depending on Σ: from this, existence and uniqueness of solutions of initial value problems will follow almost immediately by coinduction (Corollary 2.4). The essential point is that coherence allows for the definition of a transition function based on total derivatives. In the definition below, it is useful to bear in mind that, informally, for a parametric derivative u_τ, the initial data value $\rho(u_\tau)$ specifies the value of $\frac{\partial u}{\partial \tau}$ at the origin.

▶ **Definition 4.1** (initial value problem)**.** *Let Σ be a system of PDEs. A* specification of initial data *for Σ is a mapping $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$. An* initial value problem *is a pair $\mathbf{B} = (\Sigma, \rho)$.*

In what follows, for any function $\psi : U \to \mathcal{F}$, we can consider its homomorphic extension $\mathcal{P} \to \mathcal{F}$, obtained by interpreting each expression E in the obvious way: replace u_τ by $\frac{\partial \psi(u)}{\partial \tau}$, and sum and product by the corresponding operations in $\mathcal{F}$ (see Section 2); an independent variable $x_i \in X$ is interpreted as the i-th identity CFPS. By slight abuse of notation, we will still denote by "ψ" the homomorphic extension of ψ. In part (a) below, recall that for a CFPS f, $f(\epsilon)$ represents, informally, the value of function f at the origin.

▶ **Definition 4.2** (solution of $\mathbf{B}$)**.** *A* solution *of a initial value problem $\mathbf{B} = (\Sigma, \rho)$ is a mapping $\psi : U \to \mathcal{F}$ such that: (a) the initial data specifications are satisfied, that is $\psi(u_\tau)(\epsilon) = \rho(u_\tau)$ for each $u_\tau \in \mathcal{P}\mathrm{a}(\Sigma)$; and (b) all equations are satisfied, that is $\psi(u_\tau) = \psi(F)$ for each $u_\tau = F$ in Σ^∞.*

The following lemma about solutions will be used to prove uniqueness of the solution of $\mathbf{B}$.

▶ **Lemma 4.3.** *Let $\mathbf{B} = (\Sigma, \rho)$ and ψ a solution of $\mathbf{B}$. For each $E, F \in \mathcal{P}$, $E =_\Sigma F$ implies $\psi(E) = \psi(F)$.*

With any coherent (w.r.t. some ranking) Σ and initial data specification ρ, $\mathbf{B} = (\Sigma, \rho)$, we can associate a coalgebra as follows. The initial data specification $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$ can be extended homomorphically to $\mathcal{P}_0(\Sigma) \to \mathbb{R}$, by interpreting $+$ and $\cdot$ as the usual sum and product over $\mathbb{R}$, respectively, and by letting $\rho(x) \triangleq 0$ for each independent variable $x \in X$. Now we define a coalgebra depending on $\mathbf{B}$:

$$C_{\mathbf{B}} \triangleq (\mathcal{P}, \delta_\Sigma, o_\rho)$$

where $\delta_\Sigma(E,x) \triangleq SD_xE$ and $o_\rho(E) \triangleq \rho(SE)$. We will denote by $\sim_{\mathbf{B}}$ bisimilarity in $C_{\mathbf{B}}$. As an example of transition, for the heat equation $\Sigma = \{u_{xx} = au_t\}$, one has $\delta_\Sigma(u_{xx}, t) = au_{tt}$.

▶ Remark 4.4. An obvious alternative to the above definition of transition function of $C_{\mathbf{B}}$ would be just letting $\delta_\Sigma(E,x) = D_xE$: this definition in fact would work as well, but it has the computational disadvantage of making the order of the derivatives higher at each step, which would be inconvenient for the algorithms to be developed later on (Section 5).

As expected, $C_{\mathbf{B}}$ is a commutative coalgebra. Moreover, each expression is bisimilar to its normal form. This is the content of the following lemma.

▶ **Lemma 4.5.** *Let $\mathbf{B} = (\Sigma, \rho)$, with Σ coherent. Then: (1) $C_{\mathbf{B}}$ is commutative; and (2) For each $E \in \mathcal{P}$, $E \sim_{\mathbf{B}} SE$.*

Note that since $\delta_\Sigma(\delta_\Sigma(E,x),y) = \delta_\Sigma(\delta_\Sigma(E,y),x)$, for any monomial τ, the notation $\delta_\Sigma(E,\tau)$ is well defined. As a consequence of the previous lemma, part 1, and of Corollary 2.4, there exists a unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. This morphism is the unique solution of $\mathbf{B}$ we are after. We need a lemma, saying that the unique morphism ϕ from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$ is compositional.

▶ **Lemma 4.6.** *Let $\mathbf{B} = (\Sigma, \rho)$, with Σ coherent, and let $\phi_{\mathbf{B}}$ be the unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. Then $\phi_{\mathbf{B}}$ is a homomorphism over $\mathcal{P}$.*

▶ **Theorem 4.7** (coalgebraic semantics of PDEs)**.** *Let $\mathbf{B} = (\Sigma, \rho)$, with Σ coherent. Let $\phi_{\mathbf{B}}$ denote the unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. Then $\phi_{\mathbf{B}}$ (restricted to U) is the unique solution of $\mathbf{B}$.*

Proof. By virtue of Lemma 4.6, $\phi_{\mathbf{B}}$ coincides with the homomorphic extension of $(\phi_{\mathbf{B}})_{|U}$. We first prove that that $\phi_{\mathbf{B}}$ respects the initial data specification. Let u_τ be parametric. By the definition of coalgebra morphism and of output functions in $C_{\mathcal{F}}$ and $C_{\mathbf{B}}$, we have

$$\phi_{\mathbf{B}}(u_\tau)(\epsilon) \quad = \quad o_{\mathcal{F}}(\phi_{\mathbf{B}}(u_\tau)) \quad = \quad o_\rho(u_\tau) \quad = \quad \rho(Su_\tau) \quad = \quad \rho(u_\tau)$$

which proves the wanted condition. Next, we have to prove that $\phi_{\mathbf{B}}$ satisfies the equations in Σ^∞. But for each such equation, say $u_\tau = F$, we have $Su_\tau =_\Sigma SF$ by the definition of $=_\Sigma$, hence $u_\tau \sim_{\mathbf{B}} F$ by Lemma 4.5(2), hence the thesis by coinduction (Corollary 2.4). We finally prove uniqueness of the solution. Assume ψ is a solution of $\mathbf{B}$, and consider the homomorphic extension of ψ to $\mathcal{P}$, still denoted by ψ. We prove that ψ is a coalgebra morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$, hence $\psi = \phi_{\mathbf{B}}$ will follow by coinduction (Corollary 2.4). Let $E \in \mathcal{P}$. There are two steps in the proof.

- $\psi(E)(\epsilon) = \rho(SE) = o_\rho(E)$. This follows directly from Lemma 4.3, since $\psi(E) = \psi(SE)$.
- For each x, $\frac{\partial\psi(E)}{\partial x} = \psi(\delta_\Sigma(E,x))$. First, we note that $\frac{\partial\psi(E)}{\partial x} = \psi(D_xE)$. This is proven by induction on the size of E: in the base case when $E = u_\tau$, just use the fact that, by the definition of solution, $\frac{\partial\psi(u_\tau)}{\partial x} = \frac{\partial}{\partial x}\frac{\partial\psi(u)}{\partial\tau} = \frac{\partial\psi(u)}{\partial\tau x} = \psi(u_{\tau x}) = \psi(D_xu_\tau)$; in the induction step, use the fact that ψ is an homomorphism over $\mathcal{P}$, and the derivation rules of D_x and $\frac{\partial}{\partial x}$ for sum and product. Now applying Lemma 4.3, we get $\psi(D_xE) = \psi(SD_xE) = \psi(\delta_\Sigma(E,x))$, which is the wanted equality. ◀

▶ Remark 4.8 (analyticity). The previous theorem guarantees that formal power series solutions of a coherent system of PDEs always exist and are unique. In general, there is no guarantee of analyticity for such solutions. However, *if* a solution ψ of Σ in the usual sense exists that is analytic around the origin, *then* its Taylor expansion from the origin, seen as a CFPS, coincides with our solution $\phi_{\mathbf{B}}$: for each u and $f = \psi(u)$, we have that $f = \sum_{\boldsymbol{\alpha}} (\frac{\partial f}{\partial\tau})(0) \cdot \frac{\mathbf{x}^{\boldsymbol{\alpha}}}{\boldsymbol{\alpha}!} = \phi_{\mathbf{B}}(u)$. Riquier's theorem [24] gives sufficient syntactic conditions for the existence of analytic solutions; see [26, 16, 17] for further discussion of this point.

example?

The computational content of Theorem 4.7 is twofold. One one hand, we can use coinduction as a technique to prove semantically valid identities $E = F$ for the initial value problem at hand, as bisimulations $E \sim_{\mathbf{B}} F$ (via Corollary 2.4). On the other hand, we can calculate mechanically the coefficients of the Taylor expansion of the solution. This will also be key to the algorithms presented in Section 5.

▶ **Corollary 4.9** (Taylor coefficients). *Let Σ be coherent, let ρ be an initial data specification and let $\phi_{\mathbf{B}}$ be the unique solution of $\mathbf{B} = (\Sigma, \rho)$. Then, for each $E \in \mathcal{P}$, $\phi_{\mathbf{B}}(E) = \sum_{\tau=\mathbf{x}^{\boldsymbol{\alpha}}} c_\tau \cdot \tau$ where*

$$c_\tau = \frac{\rho(\delta_\Sigma(E, \tau))}{\boldsymbol{\alpha}!} . \tag{6}$$

Proof. This follows immediately from Theorem 4.7 and from the definitions of unique morphism (2) and of the coalgebra $C_{\mathbf{B}}$. ◀

The terms $\frac{\delta_\Sigma(E,\tau)}{\boldsymbol{\alpha}!} \in \mathcal{P}_0(\Sigma)$ appearing in (6) provide a "symbolic" representation of the Taylor coefficients of solutions, independent of ρ.

▶ **Example 4.10.** Consider $U = \{f, g, i, j, h, k\}$, $X = \{x, y\}$ and $\Sigma = \{\, f_x = -g\, , f_y = -g\, , g_x = f\, , g_y = f\, , i_x = -j\, , i_y = 0\, , j_x = i\, , j_y = 0\, , h_x = 0\, , h_y = -k\, , k_x = 0\, , k_y = h\,\}$. Note that $\mathcal{P}\mathrm{a}(\Sigma) = U$. The system is consistent because Σ^∞ has just one equation for each $u_\tau \in \mathcal{P}\mathrm{r}(\Sigma)$. Moreover, it is normal, hence coherent, with respect to any graded ranking. Consider now the initial value problem $\mathbf{B} = (\Sigma, \rho)$ where ρ is defined by $\rho(f) = \rho(i) = \rho(h) = 1$ and $\rho(g) = \rho(j) = \rho(k) = 0$. Let $E \stackrel{\triangle}{=} ih - jk$, $F \stackrel{\triangle}{=} ik + jh$ and $R \subseteq \mathcal{P} \times \mathcal{P}$, $R \stackrel{\triangle}{=} \{(f, E), (g, F), (-f, -E), (-g, -F)\}$: it is immediate to check that R is a bisimulation in $C_{\mathbf{B}}$. By coinduction and Theorem 4.7, we have therefore $\phi_{\mathbf{B}}(f) = \phi_{\mathbf{B}}(E)$ and $\phi_{\mathbf{B}}(g) = \phi_{\mathbf{B}}(F)$. Note that, in the given $\mathbf{B}$, the variables in U encode $\cos(x + y), \sin(x + y), \cos(x), \sin(x), \cos(y), \sin(y)$, respectively. Therefore e.g. $\phi_{\mathbf{B}}(f) = \phi_{\mathbf{B}}(E)$ actually proves that $\cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y)$, a well-known trigonometric identity.

Finally, a more refined argument leads to a precise characterization of the systems that admit (unique) solutions for every initial data specification, under normality.

▶ **Theorem 4.11** (consistency, existence and uniqueness). *Let Σ be a normal system. Σ is coherent if and only if for each ρ, $\mathbf{B} = (\Sigma, \rho)$ has a solution. Moreover, for each such $\mathbf{B}$ the solution is unique.*

5 Equivalence checking

no complexity is given

In this section, based on Theorem 4.7 and on an algebraic characterization of bisimilarity we shall discuss below, we will provide a decision algorithm for the equivalence problem $\phi_{\mathbf{B}}(E) = \phi_{\mathbf{B}}(F)$, limited to the following subclass of PDE systems.

▶ **Definition 5.1** (finite-parameter systems). *A system Σ is finite-parameter if $\mathcal{P}\mathrm{a}(\Sigma)$ is finite.*

For instance, with reference to Example 3.4, Σ_2 is finite-parameter, while Σ and Σ_1 are not. We need to introduce now some additional, mostly standard notation about polynomials. According to (6), the calculation of the Taylor coefficients of a solution of an initial value problem $\mathbf{B} = (\Sigma, \rho)$ involves evaluating expressions in $\mathcal{P}_0(\Sigma) = \mathbb{R}[X \cup \mathcal{P}\mathrm{a}(\Sigma)]$. As $k \stackrel{\triangle}{=} |X \cup \mathcal{P}\mathrm{a}(\Sigma)| < +\infty$, elements of $\mathcal{P}_0(\Sigma)$ can be treated as usual multivariate polynomials in a finite number of indeterminates. In particular, we can identify initial data specifications

ρ with points in $\mathbb{R}^k$ that vanish in the x-coordinates ($x \in X$). In this section we will let ρ range over $\mathbb{R}^k$. Moreover, we let $\mathbb{R}^k_0 \triangleq \{\rho \in \mathbb{R}^k \,:\, \rho(x) = 0 \text{ for each } x \in X\}$ and, for polynomials $E \in \mathcal{P}_0(\Sigma)$ and initial data specifications $\rho \in \mathbb{R}^k_0$, write $\rho(E)$ as $E(\rho)$ – that is the value in $\mathbb{R}$ obtained by evaluating E at point ρ.

In what follows, we shall also make use a few elementary notions from algebraic geometry [10]. In particular, an *ideal* $J \subseteq \mathcal{P}_0(\Sigma)$ is a nonempty set of polynomials closed under addition, and under multiplication by polynomials in $\mathcal{P}_0(\Sigma)$. For $P \subseteq \mathcal{P}_0(\Sigma)$, $\langle\, P \,\rangle \triangleq \{\sum_{i=1}^m G_i \cdot E_i \,:\, m \geq 0,\, G_i \in \mathcal{P}_0(\Sigma),\, E_i \in P\}$ denotes the smallest ideal which includes P, and $V(P) \subseteq \mathbb{R}^k$ the *(affine) variety* induced by P: $V(P) \triangleq \{\rho \in \mathbb{R}^k \,:\, E(\rho) = 0 \text{ for each } E \in P\} \subseteq \mathbb{R}^k$. For $W \subseteq \mathbb{R}^k$, $I(W) \triangleq \{E \in \mathcal{P}_0(\Sigma) \,:\, E(\rho) = 0 \text{ for each } \rho \in V\}$. We will use a few basic facts about ideals and varieties: (a) both $I(\cdot)$ and $V(\cdot)$ are inclusion reversing: $P_1 \subseteq P_2$ implies $V(P_1) \supseteq V(P_2)$ and $W_1 \subseteq W_2$ implies $I(W_1) \supseteq I(W_2)$; (b) any ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ stabilizes in a finite number of steps (Hilbert's basis theorem); (c) for finite $P \subseteq \mathcal{P}_0(\Sigma)$, the problem of deciding if $E \in \langle\, P \,\rangle$ is decidable, by computing a Gröbner basis (a set of generators with special properties) of $\langle\, P \,\rangle$. See [10] for a comprehensive treatment.

Given a coherent, finite-parameter Σ and an initial data specification $\rho \in \mathbb{R}^k_0$, let us denote by $\phi_{\mathbf{B}}$ the unique solution of the initial value problem $\mathbf{B} = (\Sigma, \rho)$ (Theorem 4.7). Since by definition $\phi_{\mathbf{B}}$ is a homomorphism, for any given $E, F \in \mathcal{P}$, establishing that $\phi_{\mathbf{B}}(E) = \phi_{\mathbf{B}}(F)$ is equivalent to establish that $\phi_{\mathbf{B}}(E - F) = 0$. In other words, we can identify polynomial equations with polynomials, and valid polynomial equations under ρ with polynomials $E \in \mathcal{Z}_{\mathbf{B}} \subseteq \mathcal{P}$, where (below, 0 denotes the zero CFPS in $\mathcal{F}(X)$)

$$\mathcal{Z}_{\mathbf{B}} \triangleq \phi_{\mathbf{B}}^{-1}(0)\,.$$

The equality problem reduces therefore to the *membership* problem for $\mathcal{Z}_{\mathbf{B}}$, for which we will now give an algorithm. In general terms, given $E \in \mathcal{P}$, suppose we want to decide if $E \in \mathcal{Z}_{\mathbf{B}}$. Note that, by virtue of Lemma 4.3, we can assume w.l.o.g. that $E \in \mathcal{P}_0(\Sigma)$. We shall rely mainly on Corollary 4.9. Consider now the chain of sets $A_0 \subseteq A_1 \subseteq \cdots \subseteq \mathcal{P}_0(\Sigma)$ defined as:

$$A_0 \triangleq \{E\} \qquad\qquad A_{i+1} \triangleq A_i \cup \{\delta_\Sigma(F, x) \,:\, F \in A_i,\, x \in X\}\,. \tag{7}$$

Let $m \geq 0$ be the least integer such that either: (a) there exists $F \in A_m$ s.t. $F(\rho) \neq 0$; or (b) no such $F \in A_m$ exists, but $A_{m+1} \subseteq I_m$, where, for each $i \geq 0$, $I_i \triangleq \langle\, A_i \,\rangle$ is the ideal in $\mathcal{P}_0(\Sigma)$ generated by A_i. The algorithm returns "No" if (a) occurs, and "Yes" if (b) occurs. Note that the I_i's, $i \geq 0$, form an ascending chain of ideals in $\mathcal{P}_0(\Sigma)$, which must stabilize in a finite numbers of steps (by Hilbert's basis theorem). Moreover, the inclusion $A_{m+1} \subseteq I_m$ is decidable (by Gröbner basis construction). This ensures termination and effectiveness of the outlined algorithm. Concerning its correctness, we premise the following lemma, which implies that we can effectively detect stabilization of the sequence of the ideals I_i s.

▶ **Lemma 5.2.** *Let Σ be coherent and finite-parameter. Suppose $A_{m+1} \subseteq I_m$. Then $I_m = I_{m+j}$ for each $j \geq 1$.*

▶ **Corollary 5.3** (membership checking)**.** *Let Σ be coherent and finite-parameter, ρ an initial data specification for Σ and $E \in \mathcal{P}_0(\Sigma)$. Then $\phi_{\mathbf{B}}(E) = 0$ if and only if the above algorithm returns "Yes".*

Proof. "No" is returned in case (a) occurs: as A_m consists precisely of all $\delta_\Sigma(E, \tau)$ such that $|\tau| \leq m$, this implies that $\phi_{\mathbf{B}}(E) \neq 0$, by virtue of (6). Assume on the other hand "Yes" is returned, that is case (b) of the algorithm occurs. Then by Lemma 5.2, $I_0 \subseteq \cdots \subseteq I_m =$

$I_{m+1} = I_{m+2} = \cdots$: therefore I_m contains in effect *every* $\delta_\Sigma(E, \tau)$ such that $\tau \in X^{\otimes}$. As ρ makes all polynomials in A_m vanish, by the definition of ideal ρ also makes all polynomials in $I_m = \langle\ A_m\ \rangle$ vanish. As a consequence, $(\delta_\Sigma(E, \tau))(\rho) = 0$ for all $\tau \in X^{\otimes}$, which, from Corollary 4.9, implies that $\phi_{\mathbf{B}}(E) = 0$. ◀

▶ **Example 5.4** (Burgers' equation)**.** Consider the following system, which is a special case of Burgers' equation [1, 9]

$$u_t \ = \ -u \cdot u_x \qquad\qquad u_x \ = \ \frac{1}{t+1}\,.$$

To code up this system, we fix $X = \{t, x\}$ and $U = \{u, v\}$, where v represents $1/(t+1)$, and let

$$\Sigma \ = \ \{u_t = -u \cdot u_x,\ u_x = v,\ v_t = -v^2,\ v_x = 0\}\,. \tag{8}$$

As $\mathcal{P}\mathrm{a}(\Sigma) = \{u, v\}$, the system is finite-parameter. Σ can be checked to be consistent – in particular there is a unique equation in Σ^∞ for u_{tx}, that is $u_{tx} = -v^2$. Moreover, with the lexicographic order induced by $u > v$ and $t > x$, Σ is coherent. Now fix $\rho(u) = \rho(v) = 1$ as an initial data specification and let $E \stackrel{\triangle}{=} u - (x+1)v$. We check that $E = 0$ is a valid equation for the initial value problem $\mathbf{B} = (\Sigma, \rho)$, that is $E \in \mathcal{Z}_{\mathbf{B}}$, applying the above algorithm. We have: $A_0 = \{E\}$ and $A_1 = \{E\} \cup \{\delta_\Sigma(E, t), \delta_\Sigma(E, x)\} = \{E\} \cup \{-v \cdot E, 0\}$. As trivially $\{0, -v \cdot E\} \subseteq \langle\ \{E\}\ \rangle = I_0$, and $E(\rho) = (-v \cdot E)(\rho) = 0$, the algorithm returns "Yes". Note that the validity of $E = 0$ implies that $u = (x+1)v = \frac{x+1}{t+1}$, $v = \frac{1}{t+1}$ yield a solution of $\mathbf{B}$.

Finally, relying on the ascending chain (7), we devise a complete algorithm to compute the set of initial data specifications under which a given equation E is valid in Σ – so to speak, the weakest precondition of E.

▶ **Corollary 5.5** (weakest precondition)**.** *Let Σ be coherent and finite-parameter, $E \in \mathcal{P}_0(\Sigma)$. Let $I_{m+1} = I_m$. Then $\{\rho \in \mathbb{R}_0^k \,:\, \phi_{(\Sigma,\rho)}(E) = 0\} = V(X \cup A_m)$.*

▶ **Example 5.6** (Burgers' equation, continued)**.** Consider again the system Σ in (8) and $E = u - v \cdot (x+1)$. As $I_1 = I_0 = \langle\ \{E\}\ \rangle$, we see that the set of ρ's under which E is valid is $V(X \cup \{E\})$; that is, those ρ's such that $\rho(t) = \rho(x) = 0$ and $\rho(u) = \rho(v)$.

▶ Remark 5.7 (complexity). Procedures for computing Gröbner bases, such as Buchberger's algorithm, have a very high *worst*-case time and space complexity – exponential in the number of variables and the degree of the involved polynomials, see [10]. The number of steps m before the chain (7) stabilizes can also depend super-exponentially on the number of variables and their degrees, see [19]. This theoretical complexity is of course inherited by our algorithms. On the other hand, Gröbner basis algorithms have shown to behave well in many practical cases: this suggests that an assessment of our algorithms based on concrete case studies might be more informative than a purely complexity theoretical one. We leave a systematic exploration of this more pragmatical aspect for future work.

6 Conclusion, further and related work

We have put forward a coalgebraic framework for PDEs, that yields a clean proof of existence and uniqueness of solutions of initial value problems, and complete algorithms for checking equivalence of differential polynomial expressions, under a finite-parameters assumption. To the best of our knowledge, no such characterization and completeness results for PDEs exist in the literature. As for future work, we plan to explore extensions of the present results to *postconditions*: computing at once the most general, in a precise sense, consequences of a given algebraic set of initial data specifications. This would also permit to automatically discover valid equations, rather than just check given ones.

Conceptually, the present development parallels in part our previous work on polynomial ODEs [5, 7]. Technically, the case of PDEs is by far more challenging, for the following reasons. (a) Existence of solutions, and of the transition structure itself, depends now on coherence, which is trivial in ODEs. (b) In PDEs, differential polynomials live in the infinite-indeterminates space $\mathcal{P}$, which requires reduction to $\mathcal{P}_0(\Sigma)$ via S and a finiteness assumption on parametric derivatives; in ODEs, $\mathcal{P} = \mathcal{P}_0(\Sigma)$ always has finitely many indeterminates.

An operational view of functions and differential equations similar to ours has been considered elsewhere in the literature on coalgebras [20, 27]. In particular, it is at the basis of Rutten's calculus of *behavioural differential equations* [27]. In this calculus, neither PDEs nor equivalence algorithms are considered, though. Algorithms for equivalence checking are presented in [4, 3], limited to linear *weighted automata*: in terms of differential equations, these basically correspond to linear ODEs.

In the field of formal methods, we are aware of the work by Boldo et al. [2], who apply theorem proving to the formal verification of a numerical PDE integrator written in C. Platzer, in his work on differential hybrid games [22], relies on certain Hamilton-Jacobi type PDEs in order to define a solution concept for differential games. These works pursue goals rather different from ours, though.

Our work is also related to the field of Differential Algebra. In the classical exposition, coherent systems correspond to Riquier-Janet's *orthonomic passive* systems [24, 12], further developed by Thomas [30]. A modern presentation of orthonomic passive systems is in Marvan's [18]. A more geometrical approach is followed by Reid et al. [23, 26]. The work of Riquier, Janet and Thomas is the root of what is nowadays known as Ritt-Kolchin's Differential Algebra (DA) [25, 14]. Recent developments of DA include the work by the French school, especially Boulier et al., see e.g. [8, 16]. The relationship of our coalgebraic framework with DA is not yet entirely clear and deserves further investigation.

References

1 H. Bateman. Some recent researches on the motion of fluids. *Monthly Weather Review*, 43(4):163–170, 1915.

2 S. Boldo, F. Clément, J.-C. Filliâtre, M. Mayero, G. Melquiond, and P. Weis. Trusting Computations: a Mechanized Proof from Partial Differential Equations to Actual Program. *Computers and Mathematics with Applications*, 68(3):325–352, 2014.

3 F. Bonchi, M. M. Bonsangue, M. Boreale, J. J. M. M. Rutten, and A. Silva. A coalgebraic perspective on linear weighted automata. *Inf. Comput.*, 211:77–105, 2012.

4 M. Boreale. Weighted Bisimulation in Linear Algebraic Form. In *CONCUR 2009*, volume 5710 of *LNCS*, pages 163–177. Springer, 2009.

5 M. Boreale. Algebra, coalgebra, and minimization in polynomial differential equations. In *FoSSACS 2017*, volume 10203 of *LNCS*, pages 71–87. Springer, 2017. Full version in *Logical Methods in Computer Science* 15(1) arXiv.org:1710.08350, 2019.

6 M. Boreale. Algorithms for exact and approximate linear abstractions of polynomial continuous systems. In *HSCC 2018*, pages 207–216. ACM, 2018.

7 M. Boreale. Complete algorithms for algebraic strongest postconditions and weakest preconditions in polynomial ODE's. In SOFSEM 2018: Theory and Practice of Computer Science - 44th International Conference on Current Trends in Theory and Practice of Computer Science, volume 10706 of *LNCS*, pages 442–455. Springer, 2018.

8 F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. *Appl. Algebra Engrg. Comm. Comput.*, 20(1):73–121, 2009.

9 J. M. Burgers. A mathematical model illustrating the theory of turbulence. In *Advances in applied mechanics*, volume 1, pages 171–199. Elsevier, 1948.

10 D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer, 2007.

11 K. Ghorbal and A. Platzer. Characterizing Algebraic Invariants by Differential Radical Invariants. In *TACAS 2014*, volume 8413 of *LNCS*, pages 279–294. Springer, 2014. URL: `http://reports-archive.adm.cs.cmu.edu/anon/2013/CMU-CS-13-129.pdf`.

12 M. Janet. *Sur les systèmes d'équations aux dérivées partielles.* Thèses françaises de l'entre-deux-guerres. Gauthiers-Villars, Paris, 1920. URL: `http://www.numdam.org/item?id=THESE_1920__19__1_0`.

13 D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. W. Leech, editor, *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970.

14 E. R. Kolchin. *Differential algebra and algebraic groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1973.

15 H. Kong, S. Bogomolov, Ch. Schilling, Yu Jiang, and Th.A. Henzinger. Safety Verification of Nonlinear Hybrid Systems Based on Invariant Clusters. In *HSCC 2017*, pages 163–172. ACM, 2017.

16 F. Lemaire. *Contribution à l'algorithmique en algèbre différentielle.* Génie logiciel [cs.SE]. Université des Sciences et Technologie de Lille - Lille, 2002. URL: `https://tel.archives-ouvertes.fr/tel-00001363/document`.

17 F. Lemaire. An Orderly Linear PDE System with Analytic Initial Conditions with a Non-analytic Solution. *J. Symb. Comput.*, 35(5):487–498, May 2003. `doi:10.1016/S0747-7171(03)00017-8`.

18 M. Marvan. Sufficient Set of Integrability Conditions of an Orthonomic System. *Foundations of Computational Mathematics*, 9(6):651–674, 2009.

19 D. Novikov and S. Yakovenko. Trajectories of polynomial vector fields and ascending chains of polynomial ideals. *Annales de l'Institut Fourier*, 49(2):563–609, 1999. `doi:10.5802/aif.1683`.

20 D. Pavlovic and M.H. Escardó. Calculus in Coinductive Form. In *LICS 1998*, pages 408–417. IEEE, 1998.

21 A. Platzer. Logics of dynamical systems. In *LICS 2012*, pages 13–24. IEEE, 2012.

22 A. Platzer. Differential hybrid games. *ACM Trans. Comput. Log.*, 18(3):19–44, 2017.

23 G. Reid, A. Wittkopf, and A. Boulton. Reduction of systems of nonlinear partial differential equations to simplified involutive forms. *European Journal of Applied Mathematics*, 7(6):635–666, 1996.

24 C. Riquier. *Les systèmes d'équations aux dérivèes partielles.* Gauthiers-Villars, Paris, 1910.

25 J. F. Ritt. *Differential Algebra*, volume XXXIII. American Mathematical Society Colloquium Publications, American Mathematical Society, New York, N. Y, 1950.

26 C. J. Rust, G. J. Reid, and A. D. Wittkopf. Existence and Uniqueness Theorems for Formal Power Series Solutions of Analytic Differential Systems. In *ISSAC 1999*, pages 105–112, 1999.

27 J. J. M. M. Rutten. Behavioural differential equations: a coinductive calculus of streams, automata, and power series. *Theoretical Computer Science*, 308(1–3):1–53, 2003.

28 S. Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In *HSCC 2010*, pages 221–230. ACM, 2010.

29 S. Sankaranarayanan, H. Sipma, and Z. Manna. Non-linear loop invariant generation using Gröbner bases. In *POPL 2004*. ACM, 2004.

30 J. M. Thomas. *Differential Systems*, volume XXI. American Mathematical Society Colloquium Publications, American Mathematical Society, New York, N. Y, 1937.