Coalgebras, partial differential equations and boundary problems

Michele Boreale[1]
Università di 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 of polynomial PDEs, under a coherence condition, induces a natural coalgebra over differential polynomial expressions. As a result, we obtain by coinduction existence and uniqueness of solutions of *boundary value* problems, the PDEs analog of ODEs initial value problems. We then lift this result to *stratified* systems, that is boundary problems in their full generality, where function definitions can be decomposed into distinct subsystems, focusing on different subsets of independent variables. For these systems, we then give a - in a precise sense, complete - algorithm to compute weakest preconditions and strongest postconditions. To some extent, this result algebraicizes and automates equational reasoning on polynomial boundary problems. We illustrate some experiments conducted with a proof-of-concept implementation of the method.

2012 ACM Subject Classification Theory of computation → Pre- and post-conditions; Theory of computation → Invariants; Theory of computation → Operational semantics

Keywords and phrases coalgebra, partial differential equations, polynomials

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. [27, 28, 18, 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 a contribution to this development.

Like in our previous works on ODEs [4, 5], 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). Under a coherence condition (Section 3), a system of PDEs and a boundary condition together induce a coalgebra structure over the set of differential polynomials. The solution of a boundary value problem is therefore given by the unique coalgebra morphism from the set of 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. Next, we consider *stratified* systems, where there can be distinct sets of equations for the same function, each assuming that a different subset of independent variables has been fixed to zero (Section 5). This way, the system's solution, say $f(x,y)$, can be made dependent on constraints involving not only $f(x,y)$ and its derivatives, but also $f(x,0)$, $f(0,y)$ and their derivatives, which is how general boundary problems are formulated. Under an acyclicity condition among subsystems, the existence and uniqueness result is lifted to such systems.

This is the basis for algorithms to automatically check polynomial equalities - e.g. conservation laws - valid among the functions defined by a system (Section 6). Just like in on-the-fly algorithms for bisimulation checking, the underlying idea is, based on the transition structure, to incrementally build a relation until it "closes up", but working modulo sum and product of polynomials. Concepts from algebraic geometry are used to prove the termination and correctness of this algorithm. In fact, we are more general than this, and give a method to automatically compute both weakest *preconditions* (= sets of boundary conditions) and and strongest *postconditions* (= valid polynomial equalities). The method is complete,

* Author's address: Michele Boreale, Università di Firenze, Dipartimento di Statistica, Informatica, Applicazioni (DiSIA) "G. Parenti", Viale Morgagni 65, I-50134 Firenze, Italy.

subject to certain assumptions. This way one can, for example, automatically *discover* all the polynomial equalities up to a given degree, valid under a set of boundary conditions. The original boundary problem is therefore reduced to a purely algebraic system, which can be used for reasoning and, in some cases, to find explicit solutions. We illustrate this point on two well-known examples drawn from mathematical physics, using a proof-of-concept implementation of our method (Section 7). Relations with our previous work on ODEs [4, 5], as well as with work by other authors, is discussed in the concluding section (Section 8). Proofs and additional technical material are reported in a separate appendix (Appendix A).

2 Commutative coalgebras

Let X be a finite nonempty set of *actions (or variables)*, ranged over by $x, y, ...$ and O a nonempty set. We recall that a *(Moore) coalgebra* with actions in X and outputs in O is a triple $C = (S, \delta, o)$ where: S is a set of *states*, $\delta : S \times X \to S$ is a *transition* function, and $o : S \to O$ is an *output* function (see e.g. [26]). A *bisimulation* in C is a binary relation $R \subseteq S \times S$ such that whenever sRt 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 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 $\mu : S_1 \to S_2$ 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 permutation of one another then for any state $s \in S$, $s(\sigma) \sim_C s(\sigma')$.*

We now assume $O = \mathbb{K}$ is a field, and introduce the coalgebra of formal power series in commutative variables over $\mathbb{K}$. Let $X^{\otimes}$, ranged over by $\tau, \tau', ...$, be the set of *monomials*[2] that can be formed from $X = \{x_1, ..., x_n\}$, in other words, the commutative monoid freely generated by X. We are particularly interested in the case when $\mathbb{K} = \mathbb{R}$.

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

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 definition, let us introduce the following notation. Let us fix any total order $x_1, ..., x_n$ of the variables in X. Given a vector $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n)$ of nonnegative integers (a *multi-index*) and the vector of variables $\mathbf{x} = (x_1, ..., x_n)$, 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 CFPS's, $C_{\mathcal{F}}$

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

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

[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.

$C = (S, \delta, o)$. We define the function $\mu : S \to \mathcal{F}$ as follows. For each $\tau = \mathbf{x}^{\boldsymbol{\alpha}}$

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

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 $\mathcal{F}$.*

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 $\mathbf{x}^{(\alpha_1 - \beta_1, ..., \alpha_n - \beta_n)}$. We have the following definitions of sum and product. For each $\tau \in X^{\otimes}$:

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

These operations correspond to the usual sum and product of functions, when (convergent) CFPS are interpreted as analytical 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 derivation are satisfied:

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

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 indeterminates set X is infinite.

3 Coherent systems of PDE's

We first review some notation and terminology from the formal theory of PDEs; these are standard notions, see e.g. [19, 17]. Like in the previous section, assume we are given a finite nonempty set X, which we will call here the *independent* variables. Another nonempty, not necessarily finite set U of *dependent* variables, disjoint from X, is given; U is ranged over by $u, v, ...$, possibly with superscripts $u^i, v^i, ...$ $\mathcal{D} \triangleq \{u_\tau : u \in U, \tau \in X^{\otimes}\}$ 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 CFPS's in $\mathcal{F}(X \cup \mathcal{D})$ (see Section 2). As such, they inherit from CFPS's 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.

▶ **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)*

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

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

[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 $xu + uu_y + xu_x + u_x u_y + x + u_y$.

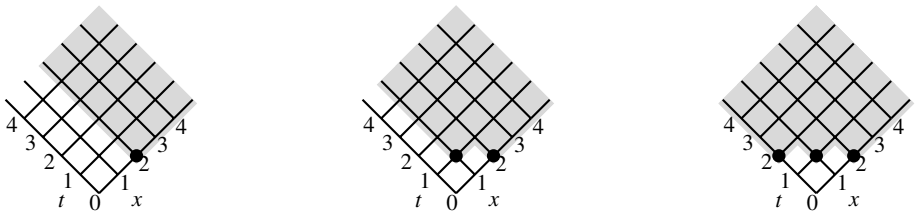

Figure 1 Lattices of u-derivatives, partially ordered by $u_\xi \le u_\tau$ if and only if $\xi \le \tau$. With reference to Example 3.4, black circles correspond to left-hand sides of equations, shaded regions to principal derivatives.

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 $D_x E = v_{xz}u_{xy} + v_z u_{xxy} + 2v_y v_{xy} + u_x + 5$. 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.

▸ **Definition 3.2** (system of PDE)**.** *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:*

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

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

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. 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 natural requirement of normality, consistency is a necessary and sufficient condition for Σ to admit a unique solution under *all* boundary conditions.

▸ **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 $S\,E$, 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 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 of systems)**.** 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 $a \neq 0$)

$$u_{xx} = au_t . \tag{5}$$

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 joining the 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 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.

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 [17], for which a Maple implementation is also available. See also Reid et al.'s method of reduction to *reduced involutive form* [19], 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. This is all the more true for the stratified systems we shall introduce later on (Section 5), where, in each subsystem, one finds often no more than one equation per dependent variables. 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 later on (Section 4).

▸ **Lemma 3.5.** *Let Σ be coherent. For each $x \in X$ and $F \in \mathcal{P}$, $S\,D_x S\,F = S\,D_x F$.*

4 Coalgebraic semantics of boundary value problems

Boundary value problems are the analog for PDEs of initial value problems for ODEs. In this section we provide differential polynomials with a coalgebra structure, depending on Σ: from this existence and uniqueness of solutions of boundary 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.

▸ **Definition 4.1** (boundary value problem)**.** *Let Σ be a system of PDE's and let $\mathcal{P}\mathrm{a}(\Sigma)$ be the set of its parametric variables. A* boundary condition *is a mapping $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$. A* boundary 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.

▶ **Definition 4.2** (solution of **B**). *A* solution *of* $\mathbf{B} = (\Sigma, \rho)$ *is a mapping* $\psi : U \to \mathcal{F}$ *such that: (a) the boundary conditions 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 **B**.

▶ **Lemma 4.3.** *Let* $\mathbf{B} = (\Sigma, \rho)$ *and* ψ *a solution of* **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 boundary condition ρ, $\mathbf{B} = (\Sigma, \rho)$, we can associate a coalgebra as follows. The boundary condition $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$ can be extended homomorphically $\mathcal{P}_0(\Sigma) \to \mathbb{R}$, interpreting + and $\cdot$ as the usual sum and product over $\mathbb{R}$, and letting $\rho(x) \triangleq 0$ for each independent variable $x \in X$. Now we define a coalgebra depending on **B**:

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

where $\delta_\Sigma(E, x) \triangleq S D_x E$ and $o_\rho(E) \triangleq \rho(S E)$. We will denote by $\sim_{\mathbf{B}}$ bisimilarity in $C_{\mathbf{B}}$. As a consequence of Lemma 3.5, $\delta_\Sigma(\delta_\Sigma(E, x), y) = \delta_\Sigma(\delta_\Sigma(E, y), x)$, so that for any monomial τ, the notation $\delta_\Sigma(E, \tau)$ is well defined. As an example of transition, for the heat equation $\Sigma = \{u_{xx} = a u_t\}$, one has $\delta_\Sigma(u_{xx}, t) = a u_{tt}$.

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

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* $E \in \mathcal{P}$, $E \sim_{\mathbf{B}} S E$.

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 **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* $\phi_{\mathbf{B}}$ *be the unique morphism from* $C_{\mathbf{B}}$ *to* $C_{\mathcal{F}}$. *Then* $\phi_{\mathbf{B}}$ *coincides with the homomorphic extension of* $(\phi_{\mathbf{B}})_{|U}$ *to* $\mathcal{P}$.

▶ **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* **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 boundary conditions. Let u_τ be parametric. By definition of morphism and of output functions in $C_{\mathcal{F}}$ and $C_{\mathbf{B}}$, we have

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

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 $S u_\tau =_\Sigma S F$ by definition of $=_\Sigma$, hence $u_\tau \sim_{\mathbf{B}} F$ by Lemma 4.5(2), hence the thesis by coinduction. We finally prove uniqueness of the solution. Assume ψ is a solution of **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.

- $\psi(E)(\epsilon) = \rho(S E) = o_\rho(E)$. This follows directly from Lemma 4.3, since $\psi(E) = \psi(S E)$.
- For each x, $\frac{\partial \psi(E)}{\partial x} = \psi(\delta_\Sigma(E, x))$. First, we note that $\frac{\partial \psi(E)}{\partial x} = \psi(D_x E)$. This is proven by induction on the size of E: in the base case when $E = u_\tau$, just use the fact that, by definition of solution, $\frac{\partial \psi(u_\tau)}{\partial x} = \frac{\partial}{\partial x}\frac{\partial \psi(u)}{\partial \tau} = \frac{\partial \psi(u)}{\partial \tau x} = \psi(u_{\tau x}) = \psi(D_x u_\tau)$; 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 $\psi(D_x E) = \psi(S D_x E) = \psi(\delta_\Sigma(E, x))$, which is the wanted equality.

◀

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 boundary problem at hand, as bisimulations $E \sim_{\mathbf{B}} F$ (via Corollary 2.4). On the other hand, we can calculate mechanically the coefficients c_τ of the Taylor expansion of $\phi(E) = \sum_{\tau = \mathbf{x}^\alpha} c_\tau \tau$ as

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

This follows from the definitions of the unique morphism (2) and of the coalgebra $C_{\mathbf{B}}$. The terms $\frac{\delta_\Sigma(E,\tau)}{\alpha!} \in \mathcal{P}_0(\Sigma)$ provide for a "symbolic" representation of such coefficients, independent of ρ. Also note that there is no guarantee of analyticity for the CFPSs of the solution $\phi_{\mathbf{B}}$. However, if a solution ψ of Σ in the usual sense exists that is analytical around the origin, then it coincides with $\phi_{\mathbf{B}}$, as a CFPS expanded from the origin: for $f = \psi(u)$, $f = \sum_{\tau=\mathbf{x}^\alpha} \frac{\tau}{\alpha!}(\frac{\partial f}{\partial \tau})(0) = \phi_{\mathbf{B}}(u)$. We omit the simple proof of this fact.

▶ **Example 4.8.** 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 boundary 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 $E \triangleq ih - jk$, $F \triangleq ik + jh$ and $R \subseteq \mathcal{P}\times\mathcal{P}$, $R \triangleq \{(f, E), (g, F), (-f, -E), (-g, -F)\}$: it is immediate to check that R is a bisimulation in $C_{\mathbf{B}}$. By coinduction and Theorem 4.7, we have therefore $\phi_{\mathbf{B}}(f) = \phi_{\mathbf{B}}(ih - jk)$ and $\phi_{\mathbf{B}}(g) = \phi_{\mathbf{B}}(ik + jh)$. 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. $\phi_{\mathbf{B}}(f) = \phi_{\mathbf{B}}(ih - jk)$ actually proves that $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$, a well-known trigonometric identity.

A more refined argument leads to a precise characterization of systems that admit (unique) solutions for every boundary condition, under normality.

▶ **Theorem 4.9** (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 Stratified systems

An individual system Σ alone cannot express general boundary problems, where one wants to specify constraints on the functions obtained by keeping the value of certain independent variables fixed. This difficulty is overcome by stratified systems. We first introduce *subsystems*. We fix a nonempty set of dependent variables U and a finite nonempty set of independent variables X. For $Y \subseteq X$, a Y-subsystem defines, informally, functions where variables outside Y have been zeroed. In particular, derivatives are taken only along variables in Y.

▶ **Definition 5.1** (subsystems). *Let Σ a set of equations and $Y \subseteq X$. For any pair $\Gamma = (\Sigma, Y)$, written $\Sigma(Y)$, we define:*

- $\mathcal{P}\mathrm{r}(\Gamma) \triangleq \{u_{\tau\xi} : u_\tau \in \mathrm{dom}(\Sigma)$ *and* $\xi \in Y^\otimes\}$*;*
- $\mathcal{P}\mathrm{a}(\Gamma) \triangleq \{u_\tau : u_\tau \notin \mathcal{P}\mathrm{r}(\Gamma)$ *and* $u_{\tau\xi} \in \mathcal{P}\mathrm{r}(\Gamma)$ *for some* $\xi \in Y^\otimes\}$*;*
- $\mathcal{D}(\Gamma) \triangleq \mathcal{P}\mathrm{a}(\Gamma) \cup \mathcal{P}\mathrm{r}(\Gamma)$.

*We finally let $U(\Gamma)$ be the set of derivatives that are $\preceq$-minimal in $\mathcal{D}(\Gamma)$, that is: $U(\Gamma) \triangleq \{u_\tau \in \mathcal{D}(\Gamma) :$ for all $u_{\tau'} \in \mathcal{D}(\Gamma)$, $\tau \not\succeq \tau'\}$. We call Γ a Y-*subsystem *if for each equation $u_\tau = G$ in Σ, $G \in \mathcal{P}(\Gamma) \triangleq \mathbb{R}[Y \cup \mathcal{D}(\Gamma)]$. We call Γ a* main *subsystem if $Y = X$ and $U(\Gamma) = U$.*

Looking at the definition of $\mathcal{P}\mathrm{a}(\Gamma)$ and $\mathcal{P}\mathrm{r}(\Gamma)$, we see that a Y-subsystem $\Gamma = \Sigma(Y)$ can be equivalently defined as a system of PDEs, in the sense of Def. 3.2, with independent variables Y and dependent variables $U(\Gamma)$, provided we identify each derivative $u_{\xi\tau} \in \mathcal{D}(\Gamma)$ with $(u_\xi)_\tau$ ($u_\xi \in U(\Gamma)$, $\tau \in Y^\otimes$; note that $\mathcal{D}(\Gamma) = \{u_{\xi\tau} : u_\xi \in U(\Gamma), \tau \in Y^\otimes\}$). With this convention, subsystems inherit all the definitions and results relative to systems, seen in Section 3. In particular, the infinite prolongation of Γ is the set of equations $\Gamma^\infty \triangleq \{u_{\tau\xi} = D_\xi G : u_\tau = G \in \Sigma$ and $\xi \in Y^\otimes\}$. Of course, the original and the inherited notion coincide for a main subsystem. We introduce the concept of stratified system, that is, a set of subsystems organized hierarchically. Stratified systems can encode boundary problems in their general form.

▶ **Definition 5.2** (stratified system). *A* stratified system *is a finite set of subsystems $H = \{\Gamma_1, ..., \Gamma_m\}$ ($m \geq 1$, $\Gamma_i = \Sigma_i(X_i)$, $X_i \subseteq X$) such that:*

(a) for some $1 \leq j \leq m$, Γ_j is a main subsystem; we will conventionally take $j = 1$;
(b) for any $i \neq j$, $\mathcal{P}\mathrm{r}(\Gamma_i) \cap \mathcal{P}\mathrm{r}(\Gamma_j) = \emptyset$;
(c) the binary relation over $\{1, ..., m\}$ defined as $i \prec j$ iff $\mathcal{P}\mathrm{a}(\Gamma_j) \cap \mathcal{P}\mathrm{r}(\Gamma_i) \neq \emptyset$, is acyclic.

The set of parametric derivatives of H, written $\mathcal{P}\mathrm{a}(H)$, is the set of derivatives that are not principal for any subsystem in H. We define $\mathcal{P}_0(H) \triangleq \mathbb{R}[X \cup \mathcal{P}\mathrm{a}(H)]$. We say H is normal *(resp.* consistent, coherent*) if all of its subsystems are normal (resp. consistent, coherent), for one and the same ranking on $\mathcal{D}$.*

Note that each H features a unique main subsystem.

▸ **Example 5.3** (heat equation with uniform initial temperature)**.** This is the boundary problem problem given by $u_t(t,x) = u_{xx}(t,x)/a$ $(0 \neq a \in \mathbb{R})$ and $u_x(0,x) = 0$. The corresponding stratified system is $H = \{\Sigma_1(X_1), \Sigma_2(X_2)\}$ with $\Sigma_1 = \{u_t = u_{xx}/a\}$, $X_1 = X = \{t,x\}$ and $\Sigma_2 = \{u_x = 0\}$, $X_2 = \{x\}$. Clearly $2 \prec 1$. Looking at the non-main subsystem, we see that $\mathcal{D}(\Gamma_2) = \{u_{x^j} : j \geq 0\}$, $U(\Gamma_2) = \{u\}$, $\mathcal{P}\mathrm{r}(\Gamma_2) = \{u_{x^j} : j \geq 2\}$ and $\mathcal{P}\mathrm{a}(\Gamma_2) = \{u, u_x\}$. Therefore $\mathcal{P}\mathrm{a}(H) = \{u, u_x\}$. Fixing the lexicographic order induced bt $t > x$, H is trivially seen to be coherent.

In order to define solutions of stratified systems, let us introduce some additional notation about CFPS's. For a CFPS $f \in \mathcal{F}(X)$ and $Y \subseteq X$, we can consider the CFPS $f_{|Y^\otimes} \in \mathcal{F}(Y)$. For an intuitive explanation of this concept, assume e.g. f represents $f(x_1, x_2)$ and $Y = \{x_2\}$: recalling that we take the origin as the expansion point, $f_{|Y^\otimes}$ represents $f(0, x_2)$, that is, f where the variables not in Y have been replaced by 0. Formally, for $\psi : \mathcal{P} \to \mathcal{F}(X)$ and a subsystem $\Gamma = \Sigma(Y)$, we let $\psi_\Gamma : U(\Gamma) \to \mathcal{F}(Y)$ be defined as $\psi_\Gamma(u_\tau) = \psi(u_\tau)_{|Y^\otimes}$. Note that ψ_Γ can be extended homomorphically to the whole $\mathcal{P}(\Gamma)$ as expected; we will still denote by ψ_Γ such an extension.

▸ **Definition 5.4** (solutions of H)**.** *Let H be a stratified system.*

1. *A* solution *of H is function $\psi : \mathcal{P} \to \mathcal{F}(X)$ such that for each $\Gamma \in H$, ψ_Γ respects all the equations in Γ^∞.*
2. *Let $\rho : \mathcal{P}\mathrm{a}(H) \to \mathbb{R}$ be a boundary condition. Let $\Sigma_0 = \{u_\tau = \rho(u_\tau) : u_\tau \in \mathcal{P}\mathrm{a}(H)\}$ and $\Gamma_0 = \Sigma_0(\emptyset)$. A* solution of the boundary problem $\mathbf{B} = (H, \rho)$ *is solution of the stratified system $H \cup \{\Gamma_0\}$.*

We can linearly order the subsystems of H according to a topological order compatible with $\prec$ and then lift inductively existence and uniqueness (Theorem 4.9) to H.

▸ **Theorem 5.5** (uniqueness of solutions of H)**.** *Let H be a coherent stratified system. For any boundary condition ρ for H, there is a unique solution of $\mathbf{B} = (H, \rho)$.*

In view of the subsequent algorithmic developments, the next step is to obtain a formula for the Taylor coefficients of the solutions of H, in analogy with the formula (6) for simple systems of Section 4. A pivotal role here is played by the reduction function S_H introduced below, by which any polynomial in $\mathcal{P}$ can be rewritten to a form in $\mathcal{P}_0(H)$, where it can be evaluated for any given boundary condition ρ. We need a technical lemma.

▸ **Lemma 5.6.** *Let $H = \{\Gamma_1, ..., \Gamma_m\}$ be a coherent stratified system. Let $=_H$ denote the reflexive, symmetric and transitive closure over $\mathcal{P}$ of $\to_{\Sigma_1} \cup \cdots \cup \to_{\Sigma_m}$. For each $E, F \in \mathcal{P}_0(H)$, $E =_H F$ implies $E = F$.*

Due to normality, each $E \in \mathcal{P}$ must have an $=_H$-equivalent term in $\mathcal{P}_0$. Based on this fact and the above lemma, we can define S_H as follows.

▸ **Definition 5.7** (reduction S_H)**.** *Let H be a coherent stratified system. We let the function $S_H : \mathcal{P} \to \mathcal{P}_0(H)$ be defined as $S_H E \triangleq F$, where F is the unique element in $\mathcal{P}_0(H)$ s.t. $E =_H F$.*

Let ϕ be a solution of H. If $E =_H F$, it is *not* true in general that $\phi(E) =_H \phi(F)$. It is true, however, that $\phi(E)(\epsilon) =_H \phi(F)(\epsilon)$. This is the basis for the following formula, giving the Taylor coefficients of $\phi(E)$. This is also key to the algorithms of the next section.

▸ **Corollary 5.8** (Taylor coefficients)**.** *Let H be a coherent stratified system. Denote by δ_{Σ_1} the transition function of the main subsystem of H. For any boundary condition ρ for H, the unique solution ϕ of (H, ρ) enjoys the following, for every $E \in \mathcal{P}$ and $\tau = \mathbf{x}^\alpha \in X^\otimes$.*

$$\phi(E)(\tau) = \frac{\rho(S_H(\delta_{\Sigma_1}(E, \tau)))}{\alpha!}\,. \tag{7}$$

6 Algorithms for pre- and postconditions

We first discuss the equality problem, which reduces to a membership check. Then introduce pre- and post-conditions, and finally give the DC algorithm to compute them. From now on, it will be necessary to restrict our attention to the following type of systems.

▸ **Definition 6.1** (finite parameters)**.** *A stratified system H is* finite parameter *if $\mathcal{P}\mathrm{a}(H)$ is finite.*

Let us now introduce some additional notation and terminology about polynomials. According to (7), the calculation of the Taylor coefficients of a solution of a boundary problem $\mathbf{B} = (H, \rho)$ involves evaluating expressions in $\mathcal{P}_0(H) =$

$\mathbb{R}[X \cup \mathcal{P}\mathrm{a}(H)]$. We let $p, q, \ldots$ range over $\mathcal{P}_0(H)$. As $k \triangleq |X \cup \mathcal{P}\mathrm{a}(H)| < +\infty$, elements of $\mathcal{P}_0(H)$ can be treated as usual multivariate polynomials in a finite number of indeterminates. In particular, we can identify boundary conditions ρ for H with points in $\mathbb{R}^k$. Accordingly, for polynomials $p \in \mathcal{P}_0(H)$ and boundary conditions $\rho \in \mathbb{R}^k$, it is notationally convenient to write $\rho(p)$ as $p(\rho)$, that is the value in $\mathbb{R}$ obtained by evaluating p at point ρ. In fact, as we shall confine ourselves to the case $\rho(x) = 0$ for $x \in X$, we will have $\rho \in \mathbb{R}^k_0 \triangleq \{\rho \in \mathbb{R}^k : \rho(x) = 0 \text{ for each } x \in X\}$.

In what follows, we shall use a few elementary notions from algebraic geometry. In particular, an *ideal* $J \subseteq \mathcal{P}_0(H)$ is a nonempty set of polynomials closed under addition, and under multiplication by polynomials in $\mathcal{P}_0(H)$. For $P \subseteq \mathcal{P}_0(H)$, $\langle\, P \,\rangle \triangleq \{\sum_{i=1}^m h_i \cdot p_i : m \geq 0, h_i \in \mathcal{P}_0(H), p_i \in P\}$ denotes the smallest ideal which includes P, and $V(P) \subseteq \mathbb{R}^k$ the *(affine) variety* induced by P: $V(P) \triangleq \{\rho \in \mathbb{R}^k : p(\rho) = 0 \text{ for each } p \in P\} \subseteq \mathbb{R}^k$. For $W \subseteq \mathbb{R}^k$, $I(W) \triangleq \{p \in \mathcal{P}_0(H) : p(\rho) = 0 \text{ for each } \rho \in V\}$. 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 (Hilber's basis theorem); (c) for finite $P \subseteq \mathcal{P}_0(H)$, the problem of deciding if $p \in \langle\, P \,\rangle$ is decidable, by computing a Gröbner basis (a set of generators with special properties) of $\langle\, P \,\rangle$. See [10] for a comprehensive treatment.

The membership problem. Given a coherent, finite parameter H and a boundary condition $\rho \in \mathbb{R}^k_0$, let us denote by $\phi_{\mathbf{B}}$ the unique solution of the boundary value problem $\mathbf{B} = (H, \rho)$ (Theorem 5.5). Since $\phi_{\mathbf{B}}$ is a homomorphism by definition, for any given $E, F \in \mathcal{P}$, establishing that $\phi_{\mathbf{B}}(E) = \phi_{\mathbf{B}}(F)$ is equivalent to establishing 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 $\mathcal{F}(X)$)

$$\mathcal{Z}_{\mathbf{B}} \triangleq \phi_{\mathbf{B}}^{-1}(0). \tag{8}$$

The equality problem reduces therefore to the *membership* problem for $\mathcal{Z}_{\mathbf{B}}$, for which we will now give an algorithm. Note that, as $\mathcal{Z}_{\mathbf{B}}$ is a subset of $\mathcal{P}$, where indeterminates are drawn from an *infinite* set, algebraic geometry techniques cannot be applied directly to $\mathcal{Z}_{\mathbf{B}}$. We get round this difficulty by working instead in $\mathcal{P}_0(H)$, via S_H and Corollary 5.8.

In general terms, given $E \in \mathcal{P}$, suppose we want to decide if $E \in \mathcal{Z}_{\mathbf{B}}$. Let us abbreviate $\delta_{\Sigma_1}(E, \tau)$ as E_τ in the sequel, where Σ_1 is understood from the context. Note that $E \in \mathcal{Z}_{\mathbf{B}}$ means, in view of (7), that for each τ, $(S_H E_\tau)(\rho) = 0$. Consider now the chain of sets $A_0 \subseteq A_1 \subseteq \cdots \subseteq \mathcal{P}$ defined as:

$$A_0 = \{E\} \qquad\qquad A_{i+1} = A_i \cup \{F_x : F \in A_i, x \in X\}.$$

For each $i \geq 0$, define $B_i \triangleq S_H(A_i) = \{S_H E : E \in A_i\} \subseteq \mathcal{P}_0(H)$. Let $m \geq 0$ be the least integer such that either: (a) there exists $q \in B_m$ s.t. $q(\rho) \neq 0$; or (b) no such $q \in B_m$ exists, but $B_{m+1} \subseteq I_m$, where, for each $i \geq 0$, $I_i \triangleq \langle\, B_i \,\rangle$ is the ideal in $\mathcal{P}_0(H)$ generated by B_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 $\mathcal{P}_0(H)$, which must stabilize in a finite numbers of steps (by Hilbert's basis theorem). Moreover, the inclusion $B_{m+1} \subseteq I_m$ is decidable (by Gröbner basis construction). This ensures termination and effectiveness of the outlined algorithm. Concerning its correctness, this is obvious in case (a). As to case (b), we premise the following lemma, which implies that we can effectively detect stabilization of the sequence of the ideals I_i s.

▶ **Lemma 6.2.** *Let H be coherent and finite parameter. Suppose $B_{m+1} \subseteq I_m$. Then $I_m = I_{m+j}$ for each $j \geq 1$.*

Now, assume case (b) of the algorithm arises. We note the following: (i) it holds that $I_0 \subseteq \cdots \subseteq I_m = I_{m+1} = I_{m+2} = \cdots$; since for each $i \geq 0$, $B_i = S_H(A_i) \subseteq I_i$, I_m contains in effect all $S_H E_\tau$, for each τ; (ii) as ρ makes all polynomials in $B_m = S_H(A_m)$ vanish, it also makes all polynomials in $I_m = \langle\, B_m \,\rangle$ vanish. As a consequence, $(S_H E_\tau)(\rho) = 0$ for all $\tau \in X^\otimes$.

Preconditions and postconditions. Going beyond the simple equality problem, one can be interested in computing *preconditions*: find all the boundary conditions $\rho \in \mathbb{R}^k_0$ under which all the equations in a given set $Q \subseteq \mathcal{P}$ are valid. Or, dually, *postconditions*: find the set $Q \subseteq \mathcal{P}$ of all valid equations, given a set of boundary conditions $W \subseteq \mathbb{R}^k_0$. Here, we shall confine ourselves to *algebraic* sets W, that is, varieties induced sets of polynomials $P \subseteq \mathcal{P}_0(H)$. This leads to the following definition. Note that requiring $P \supseteq X$ is equivalent to requiring that $V(P) \subseteq \mathbb{R}^k_0$. Recall the definition of $\mathcal{Z}_{(H,\rho)}$ from (8).

▶ **Definition 6.3** (pre- and postconditions)**.** *Let H be coherent and parameter finite. Let $P \subseteq \mathcal{P}_0(H)$ s.t. $X \subseteq P$ and $Q \subseteq \mathcal{P}$. We define the sets $\mathrm{wp}_H(Q) \subseteq \mathbb{R}^k_0$ and $\mathrm{sp}_H(P) \subseteq \mathcal{P}$ as follows.*

$$\mathrm{wp}_H(Q) \triangleq \bigcup \{V(R) : X \subseteq R \subseteq \mathcal{P}_0(H) \text{ and for each } \rho \in V(R),\ Q \subseteq \mathcal{Z}_{(H,\rho)}\}$$

$$\mathrm{sp}_H(P) \triangleq \bigcup \{R : R \subseteq \mathcal{P} \text{ and for each } \rho \in V(P),\ R \subseteq \mathcal{Z}_{(H,\rho)}\}.$$

Any $W \subseteq \mathrm{wp}_H(Q)$ will be called an (algebraic) precondition for Q, any $R \subseteq \mathrm{sp}_H(P)$ an (algebraic) postcondition for P. We focus here on computing strongest postconditions, which, as we shall see, can be used to compute preconditions as well. Actually, it is computationally convenient to introduce a *relativized* version of this problem:

Given user-specified sets P and R ($X \subseteq P \subseteq_{\mathrm{fin}} \mathcal{P}_0(H)$, $R \subseteq \mathcal{P}$), find a finite characterization of $\mathrm{sp}_H(P) \cap R$. (9)

By 'finding a finite characterization', we mean effectively computing a finite set of generators, of an appropriate algebraic type, for the set in question (see next paragraph). Note that the membership problem of the preceding subsection reduces to checking if $E \in \mathrm{sp}_H(P) \cap R$, where, for given boundary condition ρ and $E \in \mathcal{P}$, we pose $P \triangleq X \cup \{d - \rho(d) : d \in \mathcal{P}\mathrm{a}(H)\}$ (so that $V(P) = \{\rho\}$) and $R \triangleq \{E\}$. In the more general treatment, R will be represented by means of a polynomial template, to be introduced shortly.

A double chain algorithm. We first introduce *polynomial templates* [27], that is, polynomials in $\mathrm{Lin}(\mathbf{a})[X \cup \mathcal{D}]$, where $\mathrm{Lin}(\mathbf{a})$ are (formal) linear combinations of the parameters $\mathbf{a} = \{a_1, ..., a_s\}$ ($s \geq 1$) with real coefficients. For instance, $\ell = 5a_1 + 42a_2 - 3a_3$ is one such expression[4]. In other words, a polynomial template has the form $\pi = \sum_i \ell_i \alpha_i$ for distinct monomials $\alpha_i \in (X \cup \mathcal{D})^{\otimes}$, and ℓ_i linear expressions in the parameters a_i's. For example, the following is a template: $\pi = (5a_1 + (3/4)a_3)u_x y^2 + (7a_1 + (1/5)a_2)uz + (a_2 + 42a_3)$. For $v \in \mathbb{R}^s$, we denote by $\pi[v] \in \mathcal{P}$ the polynomial obtained from π by replacing each occurrence of a_i with v_i in the linear expressions of π and evaluating them. For $V \subseteq \mathbb{R}^s$, $\pi[V] \triangleq \{\pi[v] : v \in V\} \subseteq \mathcal{P}$. In particular, for a user specified π, we will set $R \triangleq \pi[\mathbb{R}^s]$ in the relativized strongest postcondition problem (9). We extend δ_{Σ_1} and S_H to templates as expected: for $\pi = \sum_i \ell_i \alpha_i$, $\delta_{\Sigma_1}(\pi, x) \triangleq \sum_i \ell_i \delta_{\Sigma_1}(\alpha_i, x)$ and $S_H \pi \triangleq \sum_i \ell_i S_H \alpha_i$, seen as a polynomials in $\mathrm{Lin}(\mathbf{a})[X \cup \mathcal{D}]$ and $\mathrm{Lin}(\mathbf{a})[X \cup \mathcal{P}\mathrm{a}(H)]$, respectively. We use π_τ as an abbreviation of $\delta_{\Sigma_1}(\pi, \tau)$.

We are now set to introduce the algorithm. Given $P \subseteq \mathcal{P}_0(H)$, with $X \subseteq P$, and a template π, fix $P_0 \supseteq X$ s.t. $I_0 \triangleq \langle\, P_0 \,\rangle \subseteq I(V(P))$ ($P_0 = P$ is a possible choice). The algorithm consists in generating two sequences of sets, $V_i \subseteq \mathbb{R}^s$ and $J_i \subseteq \mathcal{P}_0(H)$, for $i \geq 0$, defined as follows. The idea is that, at step i, V_i collects those $v \in \mathbb{R}^s$ such that $S_H(\pi[v])$ together with its derivatives up to order i vanish on $V(P)$. The J_i's are used to detect stabilization.

$$\begin{aligned} V_i &\triangleq \bigcap_{\tau : |\tau| \leq i} \{v \in \mathbb{R}^s : (S_H \pi_\tau)[v] \in I_0\} \\ J_i &\triangleq \langle\, \bigcup_{\tau : |\tau| \leq i} (S_H \pi_\tau)[V_i] \,\rangle . \end{aligned} \tag{10}$$

Consider the least m such that *both* $V_m = V_{m+1}$ and $J_m = J_{m+1}$: we let $\mathrm{DC}_H(P_0, \pi) \triangleq (V_m, J_m)$. Note that m is well defined. Indeed, $V_0 \supseteq V_1 \supseteq \cdots$ forms a descending chain of finite-dimensional vector spaces in $\mathbb{R}^s$, which must stabilize at some m'; then $J_{m'} \subseteq J_{m'+1} \subseteq \cdots$ forms an ascending chain of ideals in $\mathcal{P}_0(H)$, which must stabilize at some $m \geq m'$. We remark that the condition $V_{m+1} = V_m$ alone does *not* imply stabilization in general. The following theorem states correctness and relative completeness of DC.

▶ **Theorem 6.4** (relative completeness of DC)**.** *Let H be coherent and finite parameter. Let $X \subseteq P \subseteq \mathcal{P}_0$ and π be a template. Fix $P_0 \supseteq X$ s.t. $I_0 \triangleq \langle\, P_0 \,\rangle \subseteq I(V(P))$. Let $\mathrm{DC}_H(P_0, \pi) = (V_m, J_m)$. Then*

(a) $\pi[V_m] \subseteq \pi[\mathbb{R}^s] \cap \mathrm{sp}_H(P)$*, with equality if $I_0 = I(V(P))$;*

(b) $V(J_m) = \mathrm{wp}_H(\pi[V_m])$.

A few computational considerations about this theorem are in order. First, the sets V_i can be effectively represented by the successive linear constraints imposed on the parameters $a_1, ..., a_s$ in (10): these constraints can be be made explicit by reducing the $S_H \pi_\tau$'s modulo a suitable Gröbner basis for I_0 (details in the Appendix; see also [5]). Second, the halting condition involves detecting both $V_{m+1} = V_m$, which is relatively easy, and $J_{m+1} = J_m$: the latter reduces to checking if $\pi_{\tau x}[v] \in J_m$ for all $|\tau| = m$, $x \in X$ and v in a basis of V_m. Again, this can be carried out using a suitable Gröbner basis for J_m. Third, completeness (equality) in part (a) of the theorem is only guaranteed if P_0 is chosen such that $I_0 = I(V(P))$, otherwise $\pi[V_m]$ is just a postcondition. When $I_0 = I(V(P))$, I_0 is said to be a *real radical* of P. Computing real radicals is a computationally hard problem in general; in a number of special cases of interest, fortunately, the real radical is trivial. For instance, if P only contains elements of the form $d - e$, for d an indeterminate and e an indeterminate or a constant, then $\langle\, P \,\rangle = I(V(P))$, so that $\langle\, P \,\rangle$ is a real radical. Also note that the completeness in part (b) does *not* depend on having a real radical at hand. Examples of applications of this theorem will be illustrated in the next section.

[4] Linear expressions with a constant term, such as $2 + 5a_1 + 42a_2 - 3a_3$ are not allowed.

7 Examples

We have put a proof-of-concept implementation[5] of the DC algorithm of Section 6 at work on some boundary problems drawn from mathematical physics. We illustrate two cases below.

▸ **Example 7.1** (Burgers' equation)**.** We consider the inviscid case of Burgers' equation [1, 8] with a linear boundary condition at $t = 0$ ($b, c \in \mathbb{R}$)

$$u_t(t,x) \;=\; u(t,x)\cdot u_x(t,x) \qquad\qquad u(0,x) \;=\; bx + c\,.$$

We fix $U = \{u, b, c\}$ and $X = \{t, x\}$. The above boundary problem corresponds to the the stratified system $H_1 = \{\Gamma_1, \Gamma_2\}$, where

$$\Gamma_1 \;=\; (\{u_t = uu_x\} \cup \Sigma_0,\ \{t,x\}) \qquad\qquad \Gamma_2 \;=\; (\{u_x = b\},\ \{x\})\,.$$

The auxiliary equations $\Sigma_0 = \{b_t = 0, b_x = 0, c_t = 0, c_x = 0\}$ just encode that b, c are constants. As $\mathcal{P}\mathrm{a}(H_1) = \{u, b, c\}$, the system is finite parameter. Moreover, H_1 is trivially consistent, and, with the lexicographic order induced by $u > b > c$ and $t > x$, is coherent. We fix the set of possible boundary conditions to $V(P)$ where $P = X \cup \{u - c\}$: this just encodes $u(0,0) = c$. In order to discover interesting postconditions of $V(P)$, we consider a complete polynomial template of total degree 3 over the indeterminates $Z \triangleq X \cup \mathcal{P}\mathrm{a}(H_1)$, $\pi = \sum_{\tau_i \in Z^{\otimes}, |\tau_i| \le 3} a_i \tau_i$, which consists of $s = 56$ terms. Letting $P_0 = P$, we run $\mathrm{DC}_{H_1}(P, \pi)$, which halts at the iteration $m = 5$, returning (V_5, J_5) (this took about 6.5s in our experiment). The algorithm returns V_m in the form of a result template π', such that $\pi'[\mathbb{R}^s] = \pi[V_m]$, so that the set of all instances of π' forms a valid postcondition of P. As in this case $I_0 = \langle\, P \,\rangle$ is a real radical, Theorem 6.4(a) implies that $\pi'[V_5] = \mathrm{sp}_{H_1}(P) \cap \pi[\mathbb{R}^s]$. Specifically, we find, for a_1 a parameter:

$$\pi' \;=\; a_1 \cdot (ctu + u - b - cx)\,.$$

In other words, up to the multiplicative constant a_1, $ctu + u = b + cx$ is the only equation of degree ≤ 3 satisfied by the solutions of H_1, for boundary conditions $\rho \in V(P)$. This equation can be easily solved algebraically for u - note that we are actually manipulating CFPS's- and yields the unique solution of the boundary problem:

$$u \;=\; \frac{cx + b}{ct + 1}\,.$$

Interestingly, this solution was only found many years after Burgers' equation was introduced [9].

▸ **Example 7.2** (Heat equation)**.** We consider a boundary problem for the heat equation in one spatial dimension, with a (generic) sinusoidal boundary condition at $t = 0$ ($b, c \in \mathbb{R}$)

$$u_t(t,x) \;=\; b \cdot u_{xx}(t,x) \qquad\qquad u(0,x) \;=\; \sin(cx)\,. \tag{11}$$

We seek for solutions u of this boundary problem that can be expressed as products of a sinusoidal function of x and of an exponential function of t. Let us code the problem into a stratified system. We fix $U = \{u, f, g, h, a, b, c, d, i, j\}$ and $X = \{t, x\}$. Here, f, g, h will code $\cos(cx)$, $\sin(cx)$ and $\exp(-dt)$, respectively, while a, b, c, d, i, j will act as a supply of generic constants. We let $H_2 = \{\Gamma_1, \Gamma_2, \Gamma_3\}$, where

$$\Gamma_1 = (\{u_t = bu_{xx}\} \cup \Sigma_0,\ \{t,x\}) \quad \Gamma_2 = (\{u_x = g,\ f_x = -cg,\ g_x = cf\},\ \{x\}) \quad \Gamma_3 = (\{h_t = -dh\},\ \{t\})\,.$$

The auxiliary equations in Σ_0 encode that a, b, c, d, i, j are constants, like in the previous example, and moreover that $f_t = g_t = h_x = 0$. It can be checked that $2 \prec 1$ and $3 \prec 1$, which ensures that H is stratified, and that $\mathcal{P}\mathrm{a}(H_2) = U$ is finite. Moreover, the system is consistent: apart from the trivial case of constants, each subsystem features at most one equation for dependent variable. As for normality, hence coherence, we order the independent variables as $t > x$ and consider a ranking $\prec$ such that: (a) $v_\xi \prec u_\tau$ if either $v \neq u$ or ($v = u$ and $\xi \prec_{\mathrm{lex}} \tau$); (b) the remaining pairs, not involving u, are ordered according to an arbitrary graded ranking. To search for solutions of the wanted form, we consider an "ansatz" represented by the following polynomial[6]

$$E \triangleq a \cdot (u + igh + jfh) \tag{12}$$

and look for the weakest precondition $\mathrm{wp}_{H_2}(\{E\})$, that is, the largest algebraic set of boundary conditions under which the solutions of H_2 satisfy $E = 0$. We will then solve algebraically for a, d, i, j (considering b, c as given), replace the

[5] Code and examples available at `https://github.com/micheleatunifi/PDEPY/blob/master/PDE.py`. Execution times reported here are for a Python Anaconda distribution running under Windows 10 on a Surface Pro laptop.

[6] In this example we make use of some hindsight about the possible form of the solution. In principle, this could be reduced or avoided by using a richer ansatz.

corresponding values in E and find u. To compute $\mathrm{wp}_{H_2}(\{E\})$, we use the DC algorithm. We consider $P = X \cup \{a\}$ and $\pi = a_1 \cdot E$, for a dummy parameter a_1: then $\mathrm{sp}_{H_2}(P) \cap \pi[\mathbb{R}]$ is nonempty, as of course $E = 0$ is valid if $a = 0$, and consists in fact of all scalar multiples of E. We then run $\mathrm{DC}_{H_1}(P,\pi)$, which halts at iteration $m = 3$, returning (V_3, J_3) (this took about 4s in our experiment). Theorem 6.4 ensures that $V(J_3) = \mathrm{wp}_{H_2}(\pi[V_3]) = \mathrm{wp}_{H_2}(\{E\})$. A Gröbener basis of $J_3 \subseteq \mathcal{P}_0(H_2)$ consists of 22 polynomials. To pick up a specific solution, we impose further conditions on some variables in $\mathcal{P}\mathrm{a}(H_2)$: $a = 1$ (as E is defined up to a multiplicative constant), $f = 1$, $g = 0$, $h = 1$ (initial values of cos, sin and exp) and $c \neq 0$ (rules out trivial solutions), we solve the resulting algebraic equations for d, i, j and find: $d = bc^2$, $i = -1$ and $j = 0$. We replace these values in (12) and, recalling that f, g, h encode $\cos(cx)$, $\sin(cx)$ and $\exp(-dt)$, we find

$$u = \sin(cx) \cdot \exp(-bc^2 t)$$

which is the classical solution obtained when applying the separation of variables method.

8 Conclusion, further and related work

We have put forward a coalgebra based framework for PDEs, that yields clean proofs of existence and uniqueness of solutions of boundary problems, and complete algorithms for pre- and postconditions. To the best of our knowledge, no such completeness result for PDEs boundary problems exists in the literature.

An operational view of differential equations similar to ours has been considered elsewhere in the literature on coalgebras. For example, it is at the basis of Rutten's calculs of *behavioural differential equations* [26]. In this calculus, neither boundary problems nor equivalence algorithms are considered, though. Algorithms for equivalence checking are presented in [3, 2], limited to linear weighted automata, basically corresponding to linear ODEs.

Conceptually, the present development parallels our previous work on polynomial ODEs [4, 5]. 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 boundary problems, a prominent role is played by their (acyclic) hierarchical structure, which is again trivial in ODEs. (c) In PDEs, differential polynomials live in the infinite-indeterminates space $\mathcal{P}$, which requires reduction to $\mathcal{P}_0(H)$ via S_H, *and* a finiteness assumption on parametric derivatives; in ODEs, $\mathcal{P} = \mathcal{P}_0(\Sigma)$ has always finitely many indeterminates.

Our work is of course related to the field of Differential Algebra. In the classical exposition, coherent systems correspond to Riquier-Janet's *orthonomic passive* systems [20, 12], further developed by Thomas [29]. A modern presentation of orthonomic passive systems is in Marvan's [17]. A more geometrical approach is followed by Reid et al. [19, 25]. The work of Riquier, Janet and Thomas is the root of what is nowadays known as Ritt-Kolchin's Differential Algebra (DA) [21, 14]. A comprehensive exposition of DA, with an emphasis on the Riquier-Janet approach, is in Roberz's [22]. Recent developments of DA include the work by the French school, especially Boulier et al., see e.g. [7, 16]. Specifically, their RosenfeldGröbner algorithm computes the ideal of the differential and polynomial consequences of a system Σ: in our notation, this is related to $\mathrm{sp}_{\{\Sigma\}}(\emptyset)$. While any one of the above mentioned DA techniques can be used to reduce a system to a coherent form, which is required by our approach, none of them seems to focus on boundary problems as such. To the best of author's understanding, existing DA results on boundary problems are mostly confined to linear ODEs, see e.g. [23, 24].

References

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

2 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.

3 M. Boreale. Weighted Bisimulation in Linear Algebraic Form. *CONCUR 2009*, LNCS 5710: 163-177, Springer, 2009.

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

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

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

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

8 J.M. Burgers. A mathematical model illustrating the theory of turbulence. In *Advances in applied mechanics*, Vol. 1, pp. 171-199, Elsevier, 1948.

9 S. Chandrasekhar. On the decay of plane shock waves. *Ballistic Research Laboratories* 423, 1943.

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, A. Platzer. Characterizing Algebraic Invariants by Differential Radical Invariants. *TACAS 2014*, LNCS 8413: 279-294, 2014. Extended version available from `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. `http://www.numdam.org/item?id=THESE_1920__19__1_0`

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

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

15 H. Kong, S. Bogomolov, Ch. Schilling, Yu Jiang, Th.A. Henzinger. Safety Verification of Nonlinear Hybrid Systems Based on Invariant Clusters. *HSCC 2017*: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. `https://tel.archives-ouvertes.fr/tel-00001363/document`

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

18 A. Platzer. Logics of dynamical systems. *LICS 2012*: 13-24, IEEE, 2012.

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

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

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

22 D. Robertz. *Formal Algorithmic Elimination for PDEs*. Lectures Notes in Mathematics, Springer, 2014.

23 M. Rosenkranz, G. Regensburger. Solving and factoring boundary problems for linear ordinary differential equations in differential algebras. *J. Symb. Comput.* 43(8): 515-544, 2008.

24 M. Rosenkranz, G. Regensburger, L. Tec, B. Buchberger. Symbolic Analysis for Boundary Problems: From Rewriting to Parametrized Gröbner Bases. *CoRR abs/1210.2950*, 2012.

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

26 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.

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

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

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

A Proofs and additional technical material

A.1 Proofs of Section 2

Proof of Lemma 2.3. Let $x = x_i$. For each $\tau = \mathbf{x}^{\alpha}$ in $X^{\otimes}$ we have

$$\begin{aligned}\frac{\partial f}{\partial x_i}(\tau) &= (\alpha_i+1)f(x_i\tau)\\ &= (\alpha_i+1)\frac{o(s(x_i\tau))}{\boldsymbol{\alpha}!(\alpha_i+1)}\\ &= \frac{o(\delta(s,x_i)(\tau))}{\boldsymbol{\alpha}!}\\ &= \mu(\delta(s,x_i))(\tau)\end{aligned}$$

where the first and second equality follow from (1) and (2), respectively, and the third one from the definition of $s(x_i\tau)$. This proves the wanted statement. ◂

Proof of Corollary 2.4. We have: (1) $o(s) = \mu(s)(\epsilon)$ by 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 Γ 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. ◂

A.2 Proofs of Section 3

Proof of Lemma 3.5. The *leading derivative* of an expression $E \in \mathcal{P} \setminus \mathcal{P}_0(\Sigma)$ is the principal derivative u_τ of highest ranking occurring in E. Let us define the *rank* of F, $\mathrm{rk}(F)$, as 0 if $F \in \mathcal{P}_0(\Sigma)$, and as the leading derivative of F otherwise. The set of ranks is well ordered according to $\prec$, augmented with the rule $0 \prec u_\tau$. The proof goes by induction on the rank.

The base case $F \in \mathcal{P}_0(\Sigma)$ and is trivial, as $SF = F$ by consistency. Assume now that $\mathrm{rk}(F) = u_\tau$, where u_τ is the leading derivative of F: then F has the form $\sum_j c_j \cdot u_\tau^{k_j}\gamma_j + F'$, where $0 \neq c_j \in \mathbb{R}$, $k_j \geq 1$ and u_τ does not occur in the monomials γ_j and in the expression F'. Let $u_\tau = G \in \Sigma^{\infty}$, so that $u_{x\tau} = D_xG \in \Sigma^{\infty}$ as well. We have the following.

- Applying (repeatedly) $u_\tau = G$ from left to right, we have by equational reasoning $F =_\Sigma E \triangleq \sum_j c_j \cdot G^{k_j}\gamma_j + F'$. Hence $SF = SE$, where, by normality, $\mathrm{rk}(E) \prec \mathrm{rk}(F)$. Then, using the induction hypothesis in the second equality below, and then the rules for total derivation, which imply $D_xE = \sum_j c_j k_j G^{k_j-1}D_xG\gamma_j + c_jG_j^kD_x\gamma_j + D_xF'$, we have
$$\begin{aligned}SD_xSF &= SD_xSE\\ &= SD_xE\\ &= S(\sum_j c_jk_jG^{k_j-1}D_xG\gamma_j + c_jG_j^kD_x\gamma_j + D_xF').\end{aligned} \tag{13}$$
- On the other hand, by total derivation and then by applying (repeatedly) both $u_\tau = G$ and $u_{x\tau} = D_xG$, we have
$$\begin{aligned}SD_xF &= S(\sum_j c_jk_ju_\tau^{k_j-1}u_{x\tau}\gamma_j + c_ju_\tau^{k_j}D_x\gamma_j + D_xF')\\ &= S(\sum_j c_jk_jG^{k_j-1}D_xG\gamma_j + c_jG_j^kD_x\gamma_j + D_xF')\end{aligned}$$
where the last term above is the same as (13).

◂

A.3 Proofs of Section 4

Proof of Lemma 4.3. If $E \to_\Sigma F$, the thesis is a consequence of property (b) of the definition of solution, and the fact that ψ is a homomorphic extension from U to $\mathcal{P}$. The proof for the general case follows from this fact and from the definition of $=_\Sigma$. ◂

Proof of Lemma 4.5. For what concerns part 1, for each x, y and F, we have

$$\begin{aligned}\delta_\Sigma(\delta_\Sigma(F,x),y) &= S\,D_x S\,D_y F\\ &= S\,D_x D_y F\\ &= S\,D_y D_x F\\ &= S\,D_y S\,D_x F\\ &= \delta_\Sigma(\delta_\Sigma(F,y),x) \qquad (14)\end{aligned}$$

where the second equality and fourth follow from Lemma 3.5, and the third one is a property of total derivation.

For what concerns part 2, it is sufficient to show that the relation $R = \{(E, S\,E) : E \in \mathcal{P}\} \cup Id$, where Id is the identity relation, is a bisimulation. Condition (a) of the definition holds trivially; concerning condition (b), for any x we have that $\delta_\Sigma(E,x) = S\,D_x E = S\,D_x S\,E = \delta_\Sigma(S\,E,x)$, where the second equality follows again from Lemma 3.5. ◂

We need now a technical lemma, saying essentially that polynomial expressions in $\mathcal{P}_0(\Sigma)$ equated under all boundary conditions, are equal.

▸ **Lemma A.1.** *Let $E, F \in \mathcal{P}_0(\Sigma)$. Suppose that, for each boundary condition ρ and $\mathbf{B} = (\Sigma, \rho)$, $\phi_{\mathbf{B}}(E)(\epsilon) = \phi_{\mathbf{B}}(F)(\epsilon)$. Then $E = F$.*

Proof. We can write $E = \sum_{i=1}^{k} p_i \tau_i$ and $F = \sum_{i=1}^{k} q_i \tau_i$, for some $k \geq 0$, $p_i, q_i \in \mathbb{R}[\mathcal{P}\mathrm{a}(\Sigma)]$ and distinct $\tau_i \in X^{\otimes}$, for $1 \leq i \leq k$; possibly, either p_i or q_i are 0 for some i. We can assume the monomials $\tau_1, \tau_2, \ldots$ are numbered in such a way that $i < j$ implies that the total total degree of τ_i is less or equal than τ_j's. We shall prove that $p_j = q_j$ for all $1 \leq j \leq k$, by induction on j.

Let us first consider the base case, $j = 1$. Note that, by the rules of total derivative, $D_{\tau_1} E = p_1 + E'$ and $D_{\tau_1} F = q_1 + F'$, for some $E', F' \in \mathcal{P}$ such both E' and F' are divisible by some variable, say $E' = x \cdot E''$ and $F' = y \cdot F''$: this stems from the fact that, for $j > 1$, the monomials τ_j have a total degree $\geq$ than τ_1's, hence $D_{\tau_1}(\tau_j p_j)$ and $D_{\tau_1}(\tau_j q_j)$ must necessarily be divisible by some variable in X. Now, for an arbitrary ρ and the corresponding $\mathbf{B} = (\Sigma, \rho)$, $\phi_{\mathbf{B}}(E) = \phi_{\mathbf{B}}(F)$ implies $\phi_{\mathbf{B}}(D_{\tau_1} E) = \phi_{\mathbf{B}}(D_{\tau_1} F)$: this follows from the fact that, for any solution ψ, $\psi(D_\tau E) = \frac{\partial \psi(E)}{\partial \tau}$ (see the second part of the proof of Theorem 4.7). Then by homomorphism, $\phi_{\mathbf{B}}(D_{\tau_1} E)(\epsilon) = \phi_{\mathbf{B}}(p_1)(\epsilon) + \phi_{\mathbf{B}}(E')(\epsilon) = \rho(p_1) + 0$ (indeed, by definition, $\rho(x) = 0$ for each $x \in X$, hence $\phi_{\mathbf{B}}(E')(\epsilon) = \phi_{\mathbf{B}}(x)(\epsilon) \cdot \phi_{\mathbf{B}}(E'')(\epsilon) = 0$); similarly $\phi_{\mathbf{B}}(D_{\tau_1} F)(\epsilon) = \rho(q_1)$, which, together with $\phi_{\mathbf{B}}(E) = \phi_{\mathbf{B}}(F)$, implies $p_1(\rho) = q_1(\rho)$. Since this holds for an arbitrary boundary condition ρ, and $p_1, q_1 \in \mathbb{R}[\mathcal{P}\mathrm{a}(\Sigma)]$, we deduce $p_1 = q_1$. For the inductive step $j > 1$, consider $E_j \triangleq \sum_{i \geq j} p_i \tau_i$ and $F_j \triangleq \sum_{i \geq j} q_i \tau_i$ and proceed similarly to show $E_j = F_j$, then use the induction hypothesis to conclude $E = F$. ◂

Proof of Lemma 4.6. Let us denote by ψ the homomorphic extension of $(\phi_{\mathbf{B}})_{|U}$ to $\mathcal{P}$. One checks that $\psi(E) \sim_{\mathcal{F}} \phi_{\mathbf{B}}(E)$, by induction on E. The proof also exploits the fact that, by Lemma 3.5, $\delta_\Sigma(u, \tau) = S\,u_\tau$, hence $u_\tau \sim_{\mathbf{B}} \delta_\Sigma(u, \tau)$ by virtue of Lemma 4.5(2), therefore $\phi_{\mathbf{B}}(u_\tau) = \phi_{\mathbf{B}}(\delta_\Sigma(u, \tau))$ by coinduction. ◂

Proof of Theorem 4.9. Assume that Σ is consistent. We define a coalgebra $C = (\mathcal{P}, \delta, o)$ over $\mathcal{P}$ by letting: $\delta(E, x) \triangleq D_x E$ and $o(E) \triangleq \rho(S\,E)$. We note that the analog of Lemma 4.5 carries over to this coalgebra; in particular, one can easily show that $=_\Sigma$ is a C-bisimulation. As a consequence, the proof of existence of a solution of Theorem 4.7 carries over essentially unchanged to Σ. Conversely, assume that for each ρ, $\mathbf{B} = (\Sigma, \rho)$ has a solution ψ. Consider any $E, F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$: by Lemma 4.3, $\psi(E) = \psi(F)$, hence $\psi(E)(\epsilon) = \psi(F)(\epsilon)$. Since this holds for an arbitrary ρ, Lemma A.1 tells us that $E = F$. On the other hand, by normality for each G there must exist $E \in \mathcal{P}_0(\Sigma)$ such that $G =_\Sigma E$. This shows that Σ is consistent (hence coherent).

Finally, suppose that, for a given ρ, a solution of $\mathbf{B} = (\Sigma, \rho)$ exists. Consider any such solution ψ: for any $E, F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$, one has $\psi(E) = \psi(F)$ (Lemma 4.3) hence $\rho(E) = \rho(F)$. Now we define a coalgebra $C' = (\mathcal{P}, \delta', o')$ over $\mathcal{P}$ by letting: $\delta'(E, x) \triangleq D_x E$ and $o'(E) \triangleq \rho(F)$ for any $F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$. Note that such a F must exist by normality. Also note that the definition of C', and in particular that of of $o'(\cdot)$, does not depend on the specific choice of F, *nor it depends on the specific solution ψ* of $\mathbf{B}$. The proof of the second part of Theorem 4.7 shows[7] that ψ is a morphism from C' to the final coalgebra, hence the unique such morphism. Since the construction of C' does not depend on the specific solution ψ, this shows uniqueness of the solution ψ of $\mathbf{B}$. ◂

[7] In particular, this part of the proof of Theorem 4.7 does not rely on coherence.

A.4 Proofs of Section 5

We need a property of solutions of boundary problems. The simple proof relies on the fact that ψ is a coalgebra morphism, and is omitted.

▸ **Lemma A.2.** *Let ψ be the solution of a consistent boundary problem $\mathbf{B}$. Then for each expression E and $\xi = \mathbf{x}^{\boldsymbol{\alpha}}$, $\psi(E)(\xi) = \frac{\psi(D_\xi E)(\epsilon)}{\boldsymbol{\alpha}!}$.*

Proof of Theorem 5.5. Consider the stratified system $\overline{H} \triangleq H \cup \{\Gamma_0\}$. Note that $\mathcal{P}\mathrm{a}(\overline{H}) = \emptyset$, so that each derivative is principal for exactly one subsystem. We define a set of boundary problems $\mathbf{B}_i$ (Def. 4.1) and the corresponding solutions ψ_i (Def. 4.2), one for each subsystem Γ_i of $\overline{H}$ seen a system of PDEs, with X_i as independent variables and $U(\Gamma_i)$ as dependent variables. We proceed by induction on the relation over subsystem indices ($i \prec j$), which is by definition acyclic.

- The base case is when $\mathcal{P}\mathrm{a}(\Gamma_i) = \emptyset$. Then we let $\mathbf{B}_i \triangleq (\Sigma_i(X_i), \emptyset)$, where $\emptyset$ denotes here the empty function, and let ψ_i be the corresponding unique solution (Theorem 4.9).
- Assume $\mathcal{P}\mathrm{a}(\Gamma_i) \neq \emptyset$. Then we let $\mathbf{B}_i \triangleq (\Sigma_i(X_i), \rho_i)$, where $\rho_i : \mathcal{P}\mathrm{a}(\Gamma_i) \to \mathbb{R}$ is the boundary condition defined as $\rho_i(u_\tau) \triangleq \psi_j(u_\tau)(\epsilon)$, for each $u_\tau \in \mathcal{P}\mathrm{a}(\Gamma_i)$, where Γ_j, with $j \prec i$ is the unique subsystem such that $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_j)$, and ψ_j is the unique solution of $\mathbf{B}_j$ (Theorem 4.9).

Now we show that $\psi \triangleq \psi_1$ is a solution of $\overline{H}$ (recall that $X_1 = X$ by convention). In fact, we show that for each i, $\psi_{\Gamma_i} = \psi_i$ from which the wanted claim follows. We first show that for each subsystem Γ_i and $u_\tau \in \mathcal{D}(\Gamma_i)$

$$\psi_{\Gamma_i}(u_\tau)(\epsilon) \quad = \quad \psi_i(u_\tau)(\epsilon)\,. \tag{15}$$

This is obvious if $i = 1$, hence assume $i \neq 1$. We distinguish the case $u_\tau \in \mathcal{P}\mathrm{a}(\Gamma_i)$ and the case $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_i)$. In the first case, let j be the unique index such that $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_j)$ (note that $j \neq 1$, otherwise we would have $u_{\tau\xi} \in \mathcal{P}\mathrm{r}(\Gamma_i) \cap \mathcal{P}\mathrm{r}(\Gamma_1)$ for some $\xi \in X_i^{\otimes}$, which is absurd; hence $u_\tau \in \mathcal{P}\mathrm{a}(\Gamma_1)$ as well). Then the following equalities follow from the definitions of $\psi_{\Gamma_k}, \psi_k, \rho_k$ ($0 \leq k \leq m$).

$$\begin{aligned}
\psi_{\Gamma_i}(u_\tau)(\epsilon) &= \psi_1(u_\tau)(\epsilon) \\
&= \rho_1(u_\tau) \\
&= \psi_j(u_\tau)(\epsilon) \\
&= \rho_i(u_\tau) \\
&= \psi_i(u_\tau)(\epsilon)\,.
\end{aligned}$$

In the second case, $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_i)$, we have the following.

$$\begin{aligned}
\psi_{\Gamma_i}(u_\tau)(\epsilon) &= \psi_1(u_\tau)(\epsilon) \\
&= \rho_1(u_\tau) \\
&= \psi_i(u_\tau)(\epsilon)\,.
\end{aligned}$$

This proves (15). Now in order to show that $\psi_{\Gamma_i} = \psi_i$, consider the following, for arbitrary $u_\tau \in \mathcal{D}(\Gamma_i)$ and $\xi \in X_i^{\otimes}$, $\xi = \mathbf{x}^{\boldsymbol{\alpha}}$.

$$\begin{aligned}
\psi_{\Gamma_i}(u_\tau)(\xi) &= \psi_{\Gamma_i}(u_{\tau\xi})(\epsilon)/\boldsymbol{\alpha}! && (16)\\
&= \psi_i(u_{\tau\xi})(\epsilon)/\boldsymbol{\alpha}! && (17)\\
&= \psi_i(u_\tau)(\xi) && (18)
\end{aligned}$$

where (16) and (18) follow from Lemma A.2, and (17) from (15).

Next, we prove that ψ is the unique solution. Suppose ϕ is a solution of $\overline{H}$. Then it easily follows by induction on $\prec$ that for each i, ϕ_{Γ_i} is a solution of $\mathbf{B}_i$ as defined above. By uniqueness (Theorem 4.9), ϕ_{Γ_i} is the unique solution of $\mathbf{B}_i$, hence $\phi_{\Gamma_i} = \psi_i$ as defined above. Moreover, clearly $\phi = \phi_{\Gamma_1}$. Hence $\phi = \phi_{\Gamma_1} = \psi_1 = \psi$. ◂

▸ **Lemma A.3.** *Let H be coherent. Let ρ be a boundary condition for H, and let ϕ be the unique solution of (H,ρ). For each $E, F \in \mathcal{P}$, $E =_H F$ implies $\phi(E)(\epsilon) = \phi(F)(\epsilon)$.*

Proof. Let ϕ be the unique solution of (H,ρ). Therefore, for each i, $\phi(\cdot)_{|X_i^\otimes}$ is the unique solution of $\mathbf{B}_i = (\Gamma_i,\rho_i)$ with $\Gamma_i = \Sigma_i(X_i)$ the i-th subsystem (as per proof of Theorem 5.5). By definition of solution and Lemma 4.3, for each $u_\tau = G \in \Sigma_i^\infty(X_i)$, $\phi(u_\tau)_{|X_i^\otimes} = \phi(G)_{|X_i^\otimes}$. Now, since $\phi(\cdot)$ acts as a homomorphism on $\mathcal{P}$ (Lemma 4.6), the same does $\phi(\cdot)_{|X_i^\otimes}$. As a consequence, for any polynomial $E \in \mathcal{P}$, $\phi(E)_{|X_i^\otimes} = \phi(E[G/u_\tau])_{|X_i^\otimes}$. This in turn implies that whenever $E \to_H F$ (with $\to_H \stackrel{\triangle}{=} \cup_i \to_{\Sigma_i}$), where $F = E[G/u_\tau]$, one has $\phi_{|X_i^\otimes}(E) = \phi_{|X_i^\otimes}(F)$; in particular, $\phi(E)(\epsilon) = \phi(F)(\epsilon)$, as of course $\epsilon \in X_i^\otimes$. This also implies that whenever $E =_H F$ one has $\phi(E)(\epsilon) = \phi(F)(\epsilon)$, as required. ◂

▸ **Lemma A.4.** *Let H be coherent. Let ρ be a boundary condition for H, and let ϕ be the unique solution of (H,ρ). For any $E \in \mathcal{P}$, $\phi(E)(\epsilon) = \phi(S_H E)(\epsilon)$.*

Proof. This is an immediate consequence of Lemma A.3. ◂

▸ **Lemma A.5.** *Let H be a stratified system. Let $E, F \in \mathcal{P}_0(H)$. Suppose that, for each boundary condition ρ and $\mathbf{B} = (H,\rho)$, $\phi_{\mathbf{B}}(E)(\epsilon) = \phi_{\mathbf{B}}(F)(\epsilon)$. Then $E = F$.*

Proof. This is essentially identical to the proof of Lemma A.1, just change "Σ" in that proof with "H". ◂

Proof of Lemma 5.6. For an arbitrary boundary condition $\rho : \mathcal{P}\mathrm{a}(H) \to \mathbb{R}$, consider the unique solution ϕ of the corresponding problem (H,ρ). For any $E, F \in \mathcal{P}_0(H)$, Lemma A.3 says that $\rho(E) = \phi(E)(\epsilon) = \phi(F)(\epsilon) = \rho(F)$. Lemma A.5 allows us to conclude that $E = F$. ◂

Proof of Corollary 5.8. We use the characterizations of ϕ as the unique solution of the boundary problem $\mathbf{B}_1 = (\Sigma_1(X),\rho_1)$ (as per proof of Theorem 5.5) and as a coalgebra morphism (Theorem 4.7). First, we observe that by Lemma A.2, $\phi(E)(\tau) = \phi(D_\tau E)(\epsilon)/\alpha! = \phi(\delta_{\Sigma_1}(E,\tau))(\epsilon)/\alpha!$, where the last equality stems from the definition of δ_{Σ_1} and Lemma 3.5. Second, by Lemma A.4, we have that $\phi(\delta_{\Sigma_1}(E,\tau))(\epsilon) = \phi(S_H(\delta_{\Sigma_1}(E,\tau)))(\epsilon)$. For brevity, let $F = S_H(\delta_{\Sigma_1}(E,\tau))$. Since $F \in \mathcal{P}_0(H)$, we have that $\phi(F)(\epsilon) = \phi_0(F)(\epsilon)$, where ϕ_0 is the unique solution of $\mathbf{B}_0 = (\Gamma_0,\emptyset)$ (Definition 5.4(2)). But ϕ_0 just assigns to each $u_\tau \in \mathcal{P}\mathrm{a}(H)$ the *constant* CFPS $\rho(u_\tau) \in \mathbb{R}$, and to each variable $x_i \in X$ the i-th identity: hence $\phi_0(F)(\epsilon) = \rho(F)$, which completes the proof of (7). ◂

A.5 Proofs of Section 6

▸ **Lemma A.6.** *Let H be coherent. Then for each $E, F \in \mathcal{P}$, we have $S_H(E+F) = S_H E + S_H F$ and $S_H(E \cdot F) = (S_H E)\cdot(S_H F)$. The same holds true for S_1.*

Proof. Let us consider the statement for S_H. We only consider the sum, as the product is similar. Fix an arbitrary boundary condition ρ for H and denote by $\phi_{\mathbf{B}}$ the unique solution of $\mathbf{B} = (H,\rho)$ (Theorem 5.5). We have: $\phi_{\mathbf{B}}(S_H(E+F))(\epsilon) = \phi_{\mathbf{B}}(E+F)(\epsilon) = \phi(E)_{\mathbf{B}}(\epsilon) + \phi(F)_{\mathbf{B}}(\epsilon) = \phi_{\mathbf{B}}(S_H E)(\epsilon) + \phi_{\mathbf{B}}(S_H F)(\epsilon) = \phi_{\mathbf{B}}(S_H E + S_H F)(\epsilon)$, where: the first equality follows from Lemma A.4, the second one because ϕ is a homomorphism, the third one again from Lemma A.4, the last one by definition of homomorphic extension of ρ to $\mathcal{P}_0(H)$. Since this equality holds for an arbitrary ρ, and $S_H(E+F) \in \mathcal{P}_0(H)$, $(S_H E + S_H F) \in \mathcal{P}_0(H)$, Lemma A.5 allows us to conclude that $S_H(E+F) = S_H E + S_H F$. The proof for $S_1 = S_{\Sigma_1}$ is similar. ◂

Proof of Lemma 6.2. In the proof, we shall make use of the following equalities satisfied by S_H. For each $E \in \mathcal{P}$ and $x \in X$

$$S_H D_x S_H E = S_H D_x E \tag{19}$$

$$S_H S_1 E = S_H E. \tag{20}$$

The proof of (19) is essentially identical to that of Lemma 3.5 (induction on the rank of the leading derivative in E) and is omitted. Concerning (20), note that $E =_{\Sigma_1} S_1 E$ implies $E =_H S_1 E$, which in turn implies $E =_H S_H S_1 E$, that is $S_H E = S_H S_1 E$.

Now we are ready to show that $I_m = I_{m+j}$ by induction on j. In what follows, we abbreviate δ_{Σ_1} as δ_1. For $j = 1$, $I_{m+1} = I_m$ follows from the hypothesis that $B_{m+1} \subseteq I_m$. Consider now any $p \in I_{m+j+1}$, we show that $p \in I_m$. By definition, $p = \sum_i h_i S_H E_i$, where for each i, $h_i \in \mathcal{P}_0(H)$, and either: (i) $E_i \in A_{j+m}$; or (ii) $E_i = \delta_1(F_i, x_i)$ for some $F_i \in A_{j+m}$ and $x_i \in X$.

We will show that for each i, $S_H E_i \in I_m$, from which the thesis will follow. In fact, in case (i) this follows from the induction hypothesis, as $S_H E_i \in B_{j+m} \subseteq I_m$. We consider case (ii). We have

$$\begin{aligned}
S_H E_i &= S_H \delta_1(F_i, x_i) \\
&= S_H S_1 D_{x_i} F_i \\
&= S_H D_{x_i} F_i && (21)\\
&= S_H D_{x_i} S_H F_i && (22)\\
&= S_H D_{x_i} \sum_\ell g_\ell q_\ell && (23)\\
&= S_H D_{x_i} \sum_\ell g_\ell S_H G_\ell && (24)\\
&= \sum_\ell S_H(D_{x_i} g_\ell) S_H G_\ell \; + \; g_\ell S_H D_{x_i} S_H G_\ell && (25)\\
&= \sum_\ell S_H(D_{x_i} g_\ell) S_H G_\ell \; + \; g_\ell S_H D_{x_i} G_\ell && (26)\\
&= \sum_\ell S_H(D_{x_i} g_\ell) S_H G_\ell \; + \; g_\ell S_H S_1 D_{x_i} G_\ell && (27)\\
&= \sum_\ell S_H(D_{x_i} g_\ell) S_H G_\ell \; + \; g_\ell S_H \delta_1(G_\ell, x_i) && (28)
\end{aligned}$$

where:

- (21) follows from (20);
- (22) follows from (19);
- (23), for some $g_\ell \in \mathcal{P}_0(H)$ and $q_\ell \in B_m = S_H(A_m)$, follows from the fact that $F_i \in A_{j+m}$ and the induction hypothesis $I_{m+j} = I_m$;
- (24), for some $G_\ell \in A_m$, follows from the previous point;
- (25) follows by first distributing D_{x_i} and then S_H (Lemma A.6) over sums and products, and further noting that $S_H g_\ell = g_\ell$, as $g_\ell \in \mathcal{P}_0(H)$;
- (26) follows again from (19);
- (27) follows again from (20);
- (28) follows by definition of δ_1.

Finally note that, as $S_H G_\ell \in I_m$ and $S_H \delta_1(G_\ell, x_i) \in I_{m+1} = I_m$, the term in (28) is by definition in I_m, which completes the proof. ◀

We need need a few 'substitution lemmas' for templates, also to effectively compute (10).

▶ **Lemma A.7.** *Let H be a coherent stratified system. Let π a polynomial template, $v \in \mathbb{R}^s$.*

1. $\delta_{\Sigma_1}(\pi[v], x) = \delta_{\Sigma_1}(\pi, x)[v]$ *for any $x \in X$;*
2. $S_H(\pi[v]) = (S_H \pi)[v]$.

Proof. Let $\pi = \sum_i \ell_i \alpha_i$, for distinct monomials $\alpha_i \in (X \cup \mathcal{D})^\otimes$. Facts (1) and (2) easily follow from the distributivity properties of S_H and S_1 (Lemma A.6). As an example, for (1) we have

$$\begin{aligned}
\delta_{\Sigma_1}(\pi[v], x) &= \delta_{\Sigma_1}(\sum_i \ell_i[v]\alpha_i, x) \\
&= S_1 \sum_i \ell_i[v] D_x \alpha_i \\
&= \sum_i \ell_i[v] S_1 D_x \alpha_i \\
&= \sum_i \ell_i[v] \delta_{\Sigma_1}(\alpha_i, x) \\
&= (\sum_i \ell_i \delta_{\Sigma_1}(\alpha_i, x))[v] \\
&= \delta_{\Sigma_1}(\pi, x)[v] && (29)
\end{aligned}$$

The proof for (2) is similar. ◀

▶ **Lemma A.8.** *Let* $\mathrm{DC}_H(P_0,\pi) = (V_m, J_m)$*, under the hypotheses of Theorem 6.4. Then for each* $j \geq 1$*, one has* $V_m = V_{m+j}$ *and* $J_m = J_{m+j}$*.*

Proof. We proceed by induction on j. The base case $j = 1$ follows from the definition of m. Assuming by induction hypothesis that $V_m = \cdots = V_{m+j}$ and that $J_m = \cdots = J_{m+j}$, we prove now that $V_m = V_{m+j+1}$ and that $J_m = J_{m+j+1}$. The key to the proof is the following fact

$$(S_H\pi_{\tau x})[v] \quad \in \quad J_m \quad \text{for each } |\tau| = m+j,\ x \in X \text{ and } v \in V_m\,. \tag{30}$$

From this fact the thesis will follow, as we show below.

1. $V_m = V_{m+j+1}$. To see this, observe that for each $v \in V_{m+j} = V_m$ (the equality here follows from the induction hypothesis), it follows from (30) and the definition of J_m that $(S_H\pi_{\tau x})[v]$ can be written as a finite sum of the form $\sum_l h_l \cdot (S_H\pi_{\tau_l})[w_l]$, with $0 \leq |\tau_l| \leq m$ and $w_l \in V_m$. For each $0 \leq |\tau_l| \leq m$, $(S_H\pi_{\tau_l})[w_l] \in I_0$ by assumption, from which it easily follows that also $(S_H\pi_{\tau x})[v] = \sum_l h_l \cdot (S_H\pi_{\tau_l})[w_l] \in I_0$. Since fact holds for each τ of size m and $x \in X$, hence for each τ of size $m+1$, it shows that $v \in V_{m+j+1}$, proving that $V_{m+j+1} \supseteq V_{m+j} = V_m$. The reverse inclusion is obvious.
2. $J_m = J_{m+j+1}$. As a consequence of $V_{m+j+1} = V_{m+j} (= V_m)$ (the previous point), we can write

$$\begin{aligned} J_{m+j+1} &= \langle \bigcup_{|\tau|\leq m+j} (S_H\pi_\tau)[V_{m+j}] \cup \bigcup_{|\xi|=m+j+1} (S_H\pi_\xi)[V_{m+j}] \rangle \\ &= \langle J_{m+j} \cup \bigcup_{|\xi|=m+j+1} (S_H\pi_\xi)[V_{m+j}] \rangle \\ &= \langle J_m \cup \bigcup_{|\xi|=m+j+1} (S_H\pi_\xi)[V_m] \rangle \end{aligned}$$

where the last step follows by induction hypothesis. From (30), we have that for $|\xi| = m+j+1$, $(S_H\pi_\xi)[V_m] \subseteq J_m$, which implies the thesis for this case, as $\langle J_m \rangle = J_m$.

We prove now (30). Fix any $v \in V_m$. First, note that for $|\tau| = m+j$ and $x \in X$, by definition $\pi_{\tau x}[v] = \delta_{\Sigma_1}(\pi_\tau[v], x) = S_1 D_x(\pi_\tau[v])$ (where in the first step we have used Lemma A.7; here $S_1 = S_{\Sigma_1}$). Now consider $S_H\pi_\tau$: by induction hypothesis, $(S_H\pi_\tau)[V_m] = (S_H\pi_\tau)[V_{m+j}] \subseteq J_{m+j} = J_m$, hence $(S_H\pi_\tau)[v]$ can be written as a finite sum $\sum_l h_l \cdot (S_H\pi_{\tau_l}[w_l])$, with $0 \leq |\tau_l| \leq m$ and $w_l \in V_m$ and $h_l \in \mathcal{P}_0(H)$. Summing up, we have

$$\begin{aligned} (S_H\pi_{\tau x})[v] &= S_H S_1 D_x(\pi_\tau[v]) \\ &= S_H D_x(\pi_\tau[v]) && (31)\\ &= S_H D_x S_H(\pi_\tau[v]) && (32)\\ &= S_H D_x \sum_l h_l \cdot S_H\pi_{\tau_l}[w_l] && (33)\\ &= S_H \sum_l (D_x h_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot D_x S_H(\pi_{\tau_l}[w_l]) && (34)\\ &= \sum_l S_H(D_x h_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H D_x S_H(\pi_{\tau_l}[w_l]) && (35)\\ &= \sum_l S_H(D_x h_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H D_x(\pi_{\tau_l}[w_l]) && (36)\\ &= \sum_l S_H(D_x h_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H S_1 D_x(\pi_{\tau_l}[w_l]) && (37)\\ &= \sum_l S_H(D_x h_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H\delta_1(\pi_{\tau_l}[w_l], x) && (38)\\ &= \sum_l S_H(D_x h_l) \cdot S_H\pi_{\tau_l x}[w_l] + h_l \cdot S_H\pi_{\tau_l x}[w_l] && (39) \end{aligned}$$

where:

- (31) follows from (20);
- (32) follows from (19);
- (33) follows from the equality for $S_H(\pi_\tau[v]) = (S_H\pi)[v]$ (here we use Lemma A.7) proven above;
- (34) follows from distributing D_x over sum and products, and applying the rules for total derivation;
- (35) follows from distributing S_H (Lemma A.6) over sums and products, and further noting that $S_H h_l = h_l$, as $h_l \in \mathcal{P}_0(H)$;

- (36) follows again from (19);
- (37) follows again from (20);
- (38) follows from the definition of δ_1;
- (39) follows from Lemma A.7.

Now, for each $w_l \in V_m = V_{m+1}$, the term $S_H\pi_{\tau_l x}[w_l]$, with $0 \leq |\tau_l x| \leq m+1$, is by definition in $J_{m+1} = J_m$. Thus (39) proves that $S_H\pi_{\tau x}[v] \in J_m$, as required. ◂

Proof of Theorem 6.4. Let us consider part (a). Fix any $v \in V_m$, we must prove that $\pi[v] \in \mathrm{sp}_H(P)$, that is $\phi_{(H,\rho)}(\pi[v]) = 0$ for each $\rho \in V(P)$. By Corollary 5.8, our task reduces to showing that, for each τ, $(S_H(\pi[v]_\tau))(\rho) = (S_H\pi_\tau)[v](\rho) = 0$ (here we have used Lemma A.7), for each $\rho \in V(P)$. That is, for each τ, $(S_H\pi_\tau)[v] \in I(V(P))$. The latter is implied by $(S_H\pi_\tau)[v] \in I_0 \subseteq I(V(P))$. By definition (10), this holds for each τ such that $v \in V_{|\tau|}$. Hence for each τ, as $v \in V_0 \supseteq \cdots \supseteq V_m = V_{m+1} = \cdots$ (Lemma A.8). Assume now that $I_0 = I(V(P))$ and consider $v \in \mathbb{R}^s$ such that $\pi[v] \in \mathrm{sp}_H(P)$: we show that $v \in V_m$. Our task is showing that for each τ with $|\tau| \leq m$, $(S_H\pi_\tau)[v] \in I(V(P))$. The latter means precisely that $(S_H\pi_\tau)[v](\rho) = 0$ for each $\rho \in V(P)$. But this holds by definition of $\pi[v] \in \mathrm{sp}_H(P)$ and Corollary 5.8: indeed, for each τ, $(S_H(\pi[v]_\tau))(\rho) = (S_H\pi_\tau)[v](\rho) = 0$ (here we have used Lemma A.7), for each $\rho \in V(P)$.

Let us consider part (b). First, consider any $\rho \in \mathrm{wp}_H(\pi[V_m])$. By definition and Corollary 5.8 (and using Lemma A.7), this is equivalent to $(S_H\pi_\tau)[v](\rho) = 0$ for each $v \in V_m$ and τ. By definition of ideal J_m, this implies $q(\rho) = 0$ for each $q \in J_m$, that is $\rho \in V(J_m)$. On the other hand, consider any $\rho \in V(J_m)$ and any $v \in V_m$. Showing that $\rho \in \mathrm{wp}_H(\pi[V_m])$, that is $\phi_{(H,\rho)}(\pi[v]) = 0$, is equivalent, via Corollary 5.8 (and again Lemma A.7), to showing that $(S_H\pi_\tau)[v](\rho) = 0$, for each τ. Consider any such τ: for $k \geq m$ large enough, by definition of J_k and the fact that $V_m = V_k$, we have $J_k \supseteq (S_H\pi_\tau)[V_m]$, hence $J_m = J_k \supseteq (S_H\pi_\tau)[V_m]$ (Lemma A.8), therefore $(S_H\pi_\tau)[v](\rho) = 0$, as required. ◂

A.6 Computational details of the DC algorithm in Section 6

For each $i \geq 0$, the conditions $(S_H\pi_\tau)[v] \in I_0$ in the definition of V_i (eq. (10)) impose certain constraints on $v \in \mathbb{R}^s$. These constraints can be represented as linear equalities on the parameters $a_1, ..., a_s$. In order to make them explicit, we rely on the following lemma. We refer the reader to [10, Ch.3,§1,Th.2] for the definitions of reduced Gröbner basis G, of p mod G, as well as of the technical notion of elimination order (the lexicographic order is one such order). See [5, Lemma 3] for a proof.

▸ **Lemma A.9.** *Let* $\mathbf{z} = \{z_1, ..., z_k\}$ *and* $\mathbf{a} = \{a_1, ..., a_s\}$ *be disjoint sets of indeterminates. Fix for* $\mathbb{R}[\mathbf{a}, \mathbf{z}]$ *an elimination order for the indeterminates* a_i*'s. Let* $G \subseteq \mathbb{R}[\mathbf{z}]$ *be a reduced Gröbner basis w.r.t. to this order. Let* $\gamma \in \mathrm{Lin}(\mathbf{a})[\mathbf{z}]$*, seen as a polynomial in* $\mathbb{R}[\mathbf{a}, \mathbf{z}]$ *and* $r = \gamma$ mod G*. Then* r *is linear in* $\mathbf{a}$*. Moreover, for each* $v \in \mathbb{R}^s$*,* $\gamma[v]$ mod $G = r[v]$.

Fix a reduced Gröbner basis $G \subseteq \mathcal{P}_0(H)$ of I_0, w.r.t. an elimination order for the parameters a_i's. Letting $\mathbf{z} = X \cup \mathcal{P}\mathrm{a}(H)$ and $\gamma = S_H\pi_\tau$ in the above lemma, we have that for each τ and v, $(S_H\pi_\tau[v]) = (S_H\pi_\tau)[v] \in I_0$ exactly if $r[v] = 0$, where $r \triangleq S_H\pi_\tau$ mod G. By seeing r as a polynomial in $\mathrm{Lin}(\mathbf{a})[X \cup \mathcal{P}\mathrm{a}(H)]$, the condition on v in (10) is equivalent to

$$r[v] = 0. \tag{40}$$

This can be represented as a set of *linear* constraints on the parameters $\mathbf{a}$: indeed, a polynomial is zero exactly when all of its coefficients - in the present case, linear expressions in $\mathbf{a}$ - are zero. For instance, if $r = (a_1 + a_2)x_1 + a_3x_2$ then $r[v] = 0$ corresponds to the constraints $\{a_1 = -a_2, a_3 = 0\}$. We can now be more explicit on the finite representation of the sets V_i, J_i. In particular, each subspace V_i can be represented by a finite basis B_i, which can be computed from the linear constraints on $\mathbf{a} = (a_1, ..., a_s)$ in (40), as outlined above. From (10) it is then easy to check that $P_i \triangleq \cup_{\tau:|\tau|\leq i}(S_H\pi_\tau)[B_i]$ generates J_i. The termination conditions $V_m = V_{m+1}$ and $J_m = J_{m+1}$ can also be checked effectively. In particular, the condition $J_m = J_{m+1}$ involves computing a Gröbner basis of J_m starting from the set of generators P_m, a potentially expensive operation. Fortunately, this need not be done at each step, but only if actually $V_m = V_{m+1}$, the latter a relatively inexpensive check. Suppose $\mathrm{DC}_H(P_0, \pi) = (V_m, J_m)$. Given a template $v \in \mathbb{R}^s$, checking if $\pi[v] \in \pi[V_m]$ is equivalent to checking if $v \in V_m$: this can be effectively done knowing a basis B of the vector space V_m. In practice, it is sometimes more convenient to represent the whole set $\pi[V_m]$ returned by DC_H compactly in terms of a *new* s'-parameters result template, say π', such that $\pi'[\mathbb{R}^{s'}] = \pi[V_m]$. The result template π' can in fact be built directly from π, by propagating the linear constraints on $\mathbf{a}$ (40) as they are generated. In general, the techniques illustrated in [4, 5] for the manipulation of V_i, J_i's apply in the present context.