Automatic pre- and postconditions for partial differential equations

Michele Boreale*
Università di Firenze, Italy

October 25, 2019

Abstract

Based on a simple automata-theoretic and algebraic framework, we study reasoning techniques for polynomial PDEs. We first introduce *stratified* systems, representing PDE initial value problems in their full generality, where function definitions can be decomposed into distinct subsystems, focusing on different subsets of independent variables. For such systems, we prove uniqueness of the solution under a certain coherence condition. We then give a — in a precise sense, complete — algorithm to compute weakest preconditions and strongest postconditions for such systems. To some extent, this result reduces equational reasoning on PDE initial value (and boundary) problems to algebraic reasoning. We illustrate some experiments conducted with a proof-of-concept implementation of the method.

1 Introduction

Techniques for reasoning on ordinary differential equations (ODEs) are at the heart of current formal methods and tools for continuous and hybrid systems, which form an active research area, see e.g. [23, 24, 17, 12, 14, 4] and references therein. Although examples of hybrid systems whose continuous dynamics is described by *partial* differential equations (PDEs) abund, formal techniques for reasoning on PDEs have comparably received much less attention. Existing proposals mostly focus on specific types of equations, such as the Hamilton-Jacobi equations [9, 18]. The present paper, continuing the work started in [5], is meant as a further contribution to developing formal methods for reasoning on PDEs. Our approach is *formal*, in the sense of being entirely based on simple coalgebra (automata theory) and algebra (polynomials), rather than on calculus like most of the previous proposals. Nevertheless, the resulting notion of PDE solution conservatively extends the classical analytic one, in a sense made precise below.

In our previous work [5] we have shown that, under a certain coherence condition, a system Σ of polynomial PDEs admits a unique solution in a set of commutative formal power series (CFPSs; Section 2). Most important, this solution can be expressed operationally, in terms of the transition function of a suitable automaton. This lays the basis for mechanical checking of equations: that is, that a given (polynomial) expression involving the PDE variables becomes identically 0 when the solution is plugged into it. The corresponding procedure is similar in spirit to an on-the-fly bisimulation checking algorithm. Pragmatically, our CFPS solutions conservatively extend classical ones: if an analytic solution of Σ in the classical sense exists, then its Taylor expansion from 0, seen as a formal power series, coincides with the unique solution in our sense.

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

In the present paper, we make two substantial steps forward. First, we introduce *stratified systems*, by which one can represent fairly complicated initial value problems — and, through changes of coordinates, also boundary problems. Second and most crucial, we give a complete algorithm to automatically compute *pre-* and *postconditions* of a given system. In particular, this allows one to automatically compute *all* valid equations that fit a user-specified format, rather than just checking the validity of given ones.

More in detail, in a stratified system we have distinct sets of equations (subsystems): in each of them, a distinct subset of the independent variables is fixed to zero. This way, in a system with, say, two independent variables x and y, the solution, $f(x,y)$, can be made dependent on constraints involving not only $f(x,y)$ and its derivatives, but also $f(x,0)$ and its x-derivatives, and $f(0,y)$ and its y-derivatives. This is how initial value problems are formulated in their generality. Under a syntactic acyclicity condition among subsystems, we prove existence and uniqueness of solutions for stratified systems (Section 3), and an automata-theoretic representation of the corresponding Taylor coefficients.

This result lays the basis of an algorithm to automatically compute both weakest *preconditions* (= sets of initial conditions) and and strongest *postconditions* (= valid polynomial equations). The method is complete, subject to certain assumptions (Section 4). This way one can, for example, automatically *discover* all polynomial equations up to a given degree, valid under a given set of initial value conditions. Or vice-versa, compute the largest set of initial conditions for given equations to be valid. The original initial value problem is therefore reduced to a purely algebraic system, which can be used for reasoning and, in some cases, to find explicit solutions. Concepts from algebraic geometry are used to prove the termination and correctness of this algorithm. Using a proof-of-concept implementation (Section 5), we illustrate this algorithm on well-known examples drawn from mathematical physics, including an application to a boundary problem. Relations with our previous work on ODEs [2, 3], as well as with work by other authors, is discussed in the concluding section (Section 6). For the sake of readability, most proofs and additional technical material are reported in a separate Appendix (Appendix A).

2 Background

We review some notation and terminology from the theory of formal power series and from the formal theory of PDEs, including the main result of [5].

2.1 Commutative formal power series and polynomials

Assume a finite, nonempty set $X = \{x_1, ..., x_n\}$ of *independent variables* is given. The set X, ranged over by $t, x, ...$, will be kept fixed for the rest of the paper. Let $X^{\otimes}$, ranged over by $\tau, \xi, ...$, be the set of *monomials*[1] that can be formed from the elements of X, in other words, the commutative monoid freely generated by X. A *commutative formal power series* (CFPS) with indeterminates in X and coefficients in $\mathbb{R}$ is a total function $f : X^{\otimes} \to \mathbb{R}$. The set of these CFPSs will be denoted by $\mathcal{F}(X)$, or simply $\mathcal{F}$ if X is understood from the context. 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 $\lambda \in \mathbb{R}$, we will denote the CFPS that maps ε to λ and anything else to 0 simply as λ; 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, $\delta(f,x) \stackrel{\triangle}{=} \frac{\partial f}{\partial x}$ denotes the CFPS obtained by the usual (formal) partial derivative of f along x. For a more workable formulation of this definition, let us introduce

[1] 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. When $X = \emptyset$, $X^{\otimes} \stackrel{\triangle}{=} \{\varepsilon\}$.

the following notation. Let us fix any total order $\mathbf{x} = (x_1, ..., x_n)$ of the variables in X. Given a vector $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_n)$ of nonnegative integers (a *multi-index*), we let $\mathbf{x}^{\boldsymbol{\alpha}}$ denote the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Then $\frac{\partial f}{\partial x_i}$ is defined by the following, for each $\tau = \mathbf{x}^{(\alpha_1, ..., \alpha_n)}$

$$\frac{\partial f}{\partial x_i}(\tau) \quad \stackrel{\triangle}{=} \quad (\alpha_i + 1) f(x_i \tau). \tag{1}$$

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

$$(f+g)(\tau) \stackrel{\triangle}{=} f(\tau) + g(\tau) \qquad\qquad (f \cdot g)(\tau) \stackrel{\triangle}{=} \sum_{\xi \leq \tau} f(\xi) \cdot g(\tau/\xi). \tag{2}$$

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

$$\frac{\partial(f+g)}{\partial x} \stackrel{\triangle}{=} \frac{\partial f}{\partial x} + \frac{\partial g}{\partial x} \qquad\qquad \frac{\partial(f \cdot g)}{\partial x} \stackrel{\triangle}{=} \frac{\partial f}{\partial x} \cdot g + f \cdot \frac{\partial g}{\partial x}. \tag{3}$$

If the *support* of f, $\mathrm{supp}(f) \stackrel{\triangle}{=} \{\tau : f(\tau) \neq 0\}$, 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). It is important to note that, when confining to polynomials, these operations are well defined even in case the cardinality of the set X of indeterminates is infinite.

2.2 Partial differential equations

The definitions in this paragraph are standard, or slight variations of the standard ones; see e.g. [19, 16]. A finite, nonempty set U of *dependent variables*, disjoint from X and ranged over by $u, v, ...$, is given. We let $\mathcal{D} \stackrel{\triangle}{=} \{u_\tau : u \in U, \tau \in X^{\otimes}\}$ be the set of the *derivatives*. Informally, a symbol $u \in U$ represents a function, and u_τ its partial derivative $\frac{\partial u}{\partial \tau}$; u_ε will be identified with u. We let $\mathcal{P} \stackrel{\triangle}{=} \mathbb{R}[X \cup \mathcal{D}]$, ranged over by $E, F, ...$, denote the set of *(differential, multivariate) polynomials* with coefficients in $\mathbb{R}$ and indeterminates in $X \cup \mathcal{D}$. Considered as formal objects, polynomials are just finite-support CFPSs in $\mathcal{F}(X \cup \mathcal{D})$, as per previous subsection.As such, they inherit from $\mathcal{F}(X \cup \mathcal{D})$ the operations of sum, product and partial derivative, along with the corresponding properties. Syntactically, we shall write polynomials as expressions of the form $\sum_{\gamma \in M} \lambda_\gamma \cdot \gamma$, for $0 \neq \lambda_\gamma \in \mathbb{R}$ and $M \subseteq_{\mathrm{fin}} (X \cup \mathcal{D})^{\otimes}$. Note that this notation is consistent with the sum and product operations introduced in (2). For example, $E = v_z u_{xy} + v_y^2 + u + 5x$ is a polynomial[2]. 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, the operator $D_x : \mathcal{P} \to \mathcal{P}$ is defined by (note $\sum$ below has only finitely many nonzero terms)

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

where $\frac{\partial E}{\partial a}$ denotes the partial derivative of polynomial E along $a \in X \cup \mathcal{D}$. D_x inherits differentiation rules for sum and product that are the analog of (3). As an example, for the polynomial E above, we have $D_x E = v_{xz} u_{xy} + v_z u_{xxy} + 2 v_y v_{xy} + u_x + 5$. In particular, $D_x u_\tau = u_{x\tau}$ and $D_x x^k = k x^{k-1}$. 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 $D_{x_1} \cdots D_{x_m} F$,

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

where the order of the variables is irrelevant. We formally introduce systems of PDEs below, along with the key notions of *parametric* and *principal* derivatives. Here, the intuition is that parametric derivatives play a role similar to the lower order derivatives in ODEs initial value problems: once we fix the values of those functions at the origin, the solution will be uniquely determined. On the other hand, the definition of the principal derivatives depends on the parametric ones, just like higher order derivatives in ODEs depend on the lower order ones.

Definition 1 (system of PDEs) *A* system of PDEs *is a nonempty set Σ of equations (pairs) of the form $u_\tau = E$, with $E \in \mathcal{P}$. The set of derivatives u_τ that appear as left-hand sides of equations in Σ is denoted by* $\mathrm{dom}(\Sigma)$*. Based on Σ, the set $\mathcal{D}$ is partitioned into the sets of* principal *and* parametric *derivatives, defined as*

$$\mathcal{P}\mathrm{r}(\Sigma) \quad \stackrel{\triangle}{=} \quad \{u_{\tau\xi} : u_\tau \in \mathrm{dom}(\Sigma) \text{ and } \xi \in X^{\otimes}\} \qquad \mathcal{P}\mathrm{a}(\Sigma) \quad \stackrel{\triangle}{=} \quad \mathcal{D} \setminus \mathcal{P}\mathrm{r}(\Sigma)\,.$$

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

Note that we do *not* insist 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.

We can now introduce the concept of *solution* of PDEs, which is based on a PDE's analog of initial value problems (IVPs). In what follows, we say a function $\psi : \mathcal{P} \to \mathcal{F}(X)$ is a *homomorphism* if it preserves sum and product of polynomials, as expected, and additionally: preserves derivatives, that is $\psi(u_\tau) = \frac{\partial}{\partial\tau}\psi(u)$, and maps each $x_i \in X$ to the i-th identity CFPS. For any function $\psi : U \to \mathcal{F}(X)$, its homomorphic extension $\mathcal{P} \to \mathcal{F}(X)$, is defined as expected; by slight abuse of notation, we will still denote by "ψ" the homomorphic extension of ψ over $\mathcal{P}$. In the definition below, it is useful to bear in mind that, informally, for a parametric derivative u_τ, the initial data value $\rho(u_\tau)$ specifies the value of $\frac{\partial u}{\partial \tau}$ at the origin.

Definition 2 (initial value problem) *Let Σ be a system of PDEs. An* initial data specification *is a mapping $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$. An* initial value problem (IVP) *is a pair $\mathbf{B} = (\Sigma, \rho)$.*

A solution *of* $\mathbf{B}$ *is a homomorphism $\psi : \mathcal{P} \to \mathcal{F}(X)$ such that: (a) the initial value conditions are satisfied, that is $\psi(u_\tau)(\varepsilon) = \rho(u_\tau)$ 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^∞.*

For Σ to have a solution, a few syntactic conditions must be imposed, whose purpose is to avoid inconsistencies in the equational theory generated by Σ. 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 shown in [5], under the natural requirement of normality, consistency is a necessary and sufficient condition for Σ to admit a unique solution under *all* initial conditions.

Definition 3 (coherence) *Let Σ be a system of PDEs.*

- Σ *is* consistent *if for each $E \in \mathcal{P}$ there is a unique $F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$.*

- *Let $\prec$ be a ranking. A system Σ is $\prec$-*coherent *if it is $\prec$-normal and consistent.*

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

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

by letting $S_\Sigma E = F$, for the unique $F \in \mathcal{P}_0(\Sigma)$ such that $E =_\Sigma F$. The term $S_\Sigma E$ will be often abbreviated as SE, if Σ is understood from the context. Deciding if a (finite) system Σ is coherent, for a suitable ranking $\prec$, is of course a nontrivial problem. 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 reduces then to showing that $\to_\Sigma$ confluent. 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, like those in [19, 16]; see the discussion and the references in [5]. In many cases arising from applications, say mathematical physics, transforming the system into a coherent form for an appropriate ranking can be accomplished manually, without much difficulty: see the examples in Section 5.

We can now characterize explicitly the (unique) solution of a coherent Σ. Intuitively, the CFPS associated with $E \in \mathcal{P}$ takes each monomial $\tau \in X^{\otimes}$ to a real that depends on evaluating the τ-derivative of E under ρ, once this derivative is put in normal form. Formally, the characterization is based on a transition function, $\delta_\Sigma : \mathcal{P} \times X \to \mathcal{P}_0(\Sigma)$, defined as

$$\delta_\Sigma(E,x) \quad \stackrel{\triangle}{=} \quad S_\Sigma D_x E\,. \tag{4}$$

It can be shown (see [5]) that δ_Σ satisfies the following commutation property: $\delta_\Sigma(\delta_\Sigma(E,x),y) = \delta_\Sigma(\delta_\Sigma(E,y),x)$ for all $x,y \in X$. This justifies the notation $\delta_\Sigma(E,\tau)$ for $\tau \in X^{\otimes}$, with $\delta_\Sigma(E,\varepsilon) \stackrel{\triangle}{=} S_\Sigma E$. Next, an initial data specification $\rho : \mathcal{P}\mathrm{a}(\Sigma) \to \mathbb{R}$ can be extended homomorphically to a function $\mathcal{P}_0(\Sigma) \to \mathbb{R}$, interpreting $+$ and $\cdot$ as the usual sum and product over $\mathbb{R}$, and defining $\rho(x) \stackrel{\triangle}{=} 0$ for each independent variable $x \in X$. The following theorem of existence and uniqueness of solutions is the main result of [5]. For the sake of completeness, the proof is also reproduced in the Appendix. Below, for $\boldsymbol{\alpha} = (\alpha_1,...,\alpha_n) \in \mathbb{N}^n$, we define $\boldsymbol{\alpha}! \stackrel{\triangle}{=} \alpha_1! \cdots \alpha_n!$.

Theorem 1 (existence and uniqueness of solution, [5]) *Let Σ be coherent. For any initial data specification ρ, there is a unique solution $\phi_{\mathbf{B}} : \mathcal{P} \to \mathcal{F}(X)$ of the IVP $\mathbf{B} = (\Sigma,\rho)$. Moreover, $\phi_{\mathbf{B}}$ satisfies the following formula, for each $E \in \mathcal{P}$ and $\tau = \mathbf{x}^{\boldsymbol{\alpha}} \in X^{\otimes}$.*

$$\phi_{\mathbf{B}}(E)(\tau) \quad = \quad \frac{\rho(\delta_\Sigma(E,\tau))}{\boldsymbol{\alpha}!}\,. \tag{5}$$

We remark that our concept of solution of a PDE IVP conservatively extends the classical solution concept, in the following sense: if a classical solution exists that is analytic around the origin, then its Taylor expansion, seen as a formal power series, coincides our CFPS solution. See the Appendix.

3 Stratified systems

A system Σ alone cannot express general initial value 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 can be

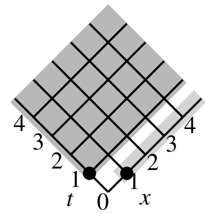

Figure 1: Lattice of derivatives for the stratified system of Example 1. Dark-shaded region = $\mathcal{P}\mathrm{r}(\Gamma_1)$, light-shaded region = $\mathcal{P}\mathrm{r}(\Gamma_2)$.

taken only along variables in Y. We introduce some standard notation on partial orders. For a partial order $\preceq$ defined over some universe A and for $B \subseteq A$, we will let $\uparrow_{\preceq}(B) \stackrel{\triangle}{=} \{a \in A : a \succeq b$ for some $b \in B\}$ denote the upward closure of B w.r.t $\preceq$; similarly, we will let $\downarrow_{\preceq}(B)$ denote the downward closure of B. Moreover, we will let $\min_{\preceq}(B) \stackrel{\triangle}{=} \{b \in B :$ whenever $b' \in B$ and $b' \preceq b$ then $b' = b\}$ denote the set of $\preceq$-minimal element of B. Additionally, we define the following partial order $\leq_Y$ on the set of derivatives $\mathcal{D}$ depending on $Y \subseteq X$: $u_\tau \leq_Y u_{\tau'}$ if and only if $\tau' = \tau\xi$ for some $\xi \in Y^{\otimes}$. In the definition of subsystem given below, the intuition is that the $\leq_Y$-minimal derivatives, the set U_Γ, act as the dependent variables of a new system of PDEs with independent variables in Y and derivatives in $\mathcal{D}_\Gamma$.

Definition 4 (subsystem) *Let Σ a set of equations and $Y \subseteq X$. For $\Gamma = (\Sigma, Y)$, we define the following subsets of $\mathcal{D}$.*

$$\begin{array}{rclcrcl} U_\Gamma & \stackrel{\triangle}{=} & \min_{\leq_Y}(\downarrow_{\leq_Y}\{u_\tau : u_\tau \textit{ occurs in } \Sigma\}) & \qquad & \mathcal{D}_\Gamma & \stackrel{\triangle}{=} & \uparrow_{\leq_Y}(U_\Gamma) \\ \mathcal{P}\mathrm{r}(\Gamma) & \stackrel{\triangle}{=} & \uparrow_{\leq_Y}(\mathrm{dom}(\Sigma)) & & \mathcal{P}\mathrm{a}(\Gamma) & \stackrel{\triangle}{=} & \mathcal{D}_\Gamma \setminus \mathcal{P}\mathrm{r}(\Gamma)\,. \end{array}$$

*We let $\mathcal{P}_\Gamma \stackrel{\triangle}{=} \mathbb{R}[Y \cup \mathcal{D}_\Gamma]$. We say Γ is a Y-*subsystem*, written $\Gamma = \Sigma(Y)$, if for each polynomial E appearing in Σ, $E \in \mathcal{P}_\Gamma$. We call Γ a* main *subsystem if $Y = X$ and $U_\Gamma = U$. Finally, $\Gamma^\infty \stackrel{\triangle}{=} \{u_{\tau\xi} = D_\xi G : u_\tau = G \in \Sigma$ and $\xi \in Y^{\otimes}\}$.*

Stratified systems can encode initial value problems in their general form.

Definition 5 (stratified system) *A* stratified system *is a finite set of subsystems $H = \{\Gamma_1, ..., \Gamma_m\}$ ($m \geq 1$, $\Gamma_i = \Sigma_i(X_i)$, $\Sigma_i \neq \emptyset$, $X_i \subseteq X$) 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 $\mathcal{P}\mathrm{r}(\Gamma_i) \cap \mathcal{P}\mathrm{a}(\Gamma_j) \neq \emptyset$, 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 $\mathcal{P}_0(H) \stackrel{\triangle}{=} \mathbb{R}[X \cup \mathcal{P}\mathrm{a}(H)]$. We say H is coherent *if all of its subsystems are coherent, w.r.t. one and the same ranking on $\mathcal{D}$.*

Note that each H features a unique main subsystem.

Example 1 (Heat equation with initial temperature) Consider the heat equation in one spatial dimension $u_t(t,x) = u_{xx}(t,x)/a$ ($0 \neq a \in \mathbb{R}$), with an initial temperature exponentially decaying from the origin, $u_x(0,x) = -u(0,x)$. The corresponding stratified system is $H = \{\Gamma_1, \Gamma_2\} = \{\Sigma_1(X_1), \Sigma_2(X_2)\}$ with $\Sigma_1 = \{u_t = u_{xx}/a\}$, $X_1 = X = \{t,x\}$ and $\Sigma_2 = \{u_x = -u\}$, $X_2 = \{x\}$. We have (see Fig. 1):

$$\begin{array}{llllllllllll} U_{\Gamma_1} & = & \{u\} & \mathcal{D}_{\Gamma_1} & = & \{u_\tau : \tau \in X^{\otimes}\} & \mathcal{P}\mathrm{r}(\Gamma_1) & = & \{u_{t\tau} : \tau \in X^{\otimes}\} & \mathcal{P}\mathrm{a}(\Gamma_1) & = & \{u_{x^j} : j \geq 0\} \\ U_{\Gamma_2} & = & \{u\} & \mathcal{D}_{\Gamma_2} & = & \{u_{x^j} : j \geq 0\} & \mathcal{P}\mathrm{r}(\Gamma_2) & = & \{u_{x^j} : j \geq 1\} & \mathcal{P}\mathrm{a}(\Gamma_2) & = & \{u\}. \end{array}$$

Note that $\mathcal{D}_{\Gamma_1} = \mathcal{D}$, so Γ_1 is the main subsystem, and that $\mathcal{P}\mathrm{a}(H) = \{u\}$. Clearly, $2 \prec 1$, as $\mathcal{P}\mathrm{r}(\Gamma_2) \cap \mathcal{P}\mathrm{a}(\Gamma_1) \neq \emptyset$; on the other hand, $1 \not\prec 2$, as $\mathcal{P}\mathrm{r}(\Gamma_1) \cap \mathcal{P}\mathrm{a}(\Gamma_2) = \emptyset$; so the relation $\prec$ is acyclic. Finally, fixing the lexicographic order induced by $t > x$, H is trivially seen to be coherent.

Example 2 (Euler-Tricomi) Consider $H = \{\Gamma_1, \Gamma_2\} = \{(\Sigma_1, \{x,y\}), (\Sigma_2, \{y\})\}$, with $\Sigma_1 = \{u_{xx} = -xu_{yy}\}$ and $\Sigma_2 = \{u_{xy} = a\,,\, u_y = b\}$ ($a, b \in \mathbb{R}$), a special case of the Euler-Tricomi equation. Proceeding in fashion similar to the previous example, we can check that: (1) $U_{\Gamma_1} = \{u\}$, $\mathcal{D}_{\Gamma_1} = \mathcal{D}$ and $\mathcal{P}\mathrm{a}(\Gamma_1) = \{u_{y^j}, u_{xy^j} \,:\, j \geq 0\}$; (2) $U_{\Gamma_2} = \{u, u_x\}$, $\mathcal{D}_{\Gamma_2} = \mathcal{P}\mathrm{a}(\Gamma_1)$ and $\mathcal{P}\mathrm{a}(\Gamma_2) = U_{\Gamma_2}$. Clearly $2 \prec 1$ and $1 \not\prec 2$. The lexicographic order induced by $x > y$ makes H 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: $\psi_\Gamma(u_\tau) \stackrel{\triangle}{=} \psi(u_\tau)_{|Y^{\otimes}}$. 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 6 (solutions of H) *Let H be a stratified system.*

1. *A* solution *of H is homomorphism $\psi : \mathcal{P} \to \mathcal{F}(X)$ 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 an initial data specification. 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 initial value 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 1) to H.

Theorem 2 (existence and uniqueness for H) *Let H be a coherent stratified system. For any initial data specification 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 solution of H, in analogy with the formula (5) for simple systems. This formula will be based on the transition function of the main subsystem, δ_{Σ_1}. However, a pivotal role now will be also played by the reduction function S_H introduced below: it allows one to rewrite any polynomial in $\mathcal{P}$ to a form in $\mathcal{P}_0(H)$, where it can be evaluated for any given initial data specification ρ. Below, recall that $\to_{\Sigma_i}$ denotes the rewrite relation over $\mathcal{P}$ induced by the equations in Σ_i.

Definition 7 (reduction S_H) *Let $H = \{\Gamma_1, \ldots, \Gamma_m\}$ 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 $E \in \mathcal{P}$, we let $S_H E$ denote an arbitrarily fixed $F \in \mathcal{P}_0(H)$ such that $E =_H F$.*

In the definition above, note that, due to normality, each $E \in \mathcal{P}$ must have an $=_H$-equivalent term in $\mathcal{P}_0(H)$, so $S_H E$ is well defined. Now, 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 $\phi(E)(\varepsilon) =_H \phi(F)(\varepsilon)$; moreover if $F \in \mathcal{P}_0(H)$ then $\phi(F)(\varepsilon) = \rho(F)$. These facts are the basis of the following formula, giving the Taylor coefficients of $\phi(E)$. This is also key to the algorithm in the next section.

Corollary 1 (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 initial data specification ρ for H, the unique solution ϕ of (H,ρ) enjoys the following, for every $E \in \mathcal{P}$ and $\tau = \mathbf{x}^{\boldsymbol{\alpha}} \in X^{\otimes}$.*

$$\phi(E)(\tau) = \frac{\rho(S_H(\delta_{\Sigma_1}(E,\tau)))}{\boldsymbol{\alpha}!}\,. \tag{6}$$

Example 3 (Example 1, cont.) For simplicity, we let $a = 1$. Consider any initial data specification $\rho(u) = u_0 \in \mathbb{R}$ for H, let ϕ be the solution of (H,ρ) and $f = \phi(u)$. We compute the first few coefficients of f by applying (6) with $E = u$. Let us first compute a few $S_H(\delta_{\Sigma_1}(u,\tau))$ s. Recall that the definition of $=_{\Sigma_i}$ is based on Γ_i^∞ $(i = 1,2)$.

$$\begin{array}{rclrcl}
S_H(\delta_{\Sigma_1}(u,\varepsilon)) & = & S_H u = u & S_H(\delta_{\Sigma_1}(u,t)) & = & S_H u_{xx} = S_H(-u_x) = u \\
S_H(\delta_{\Sigma_1}(u,x)) & = & S_H u_x = -u & S_H(\delta_{\Sigma_1}(u,tt)) & = & S_H u_{x^4} = u \\
S_H(\delta_{\Sigma_1}(u,tx)) & = & S_H u_{x^3} = -u & S_H(\delta_{\Sigma_1}(u,xx)) & = & S_H u_{xx} = u\,.
\end{array}$$

In general, one can check that for $\tau = (t,x)^{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha} = (\alpha_1,\alpha_2)$, $S_H(\delta_{\Sigma_1}(u,\tau)) = (-1)^{\alpha_2}u$. Hence, by (6), we have the CFPS: $f = u_0 + u_0 t - u_0 x + (u_0/2)t^2 - u_0 tx + (u_0/2)x^2 \cdots = \sum_{\tau=\mathbf{x}^{\boldsymbol{\alpha}}} (-1)^{\alpha_2}(u_0/\boldsymbol{\alpha}!)\tau$.

4 Algorithms for pre- and postconditions

We will first recall some terminology and some basic facts from algebraic geometry, then introduce pre- and postconditions and finally the POST algorithm to compute them.

4.1 Preliminaries

From now on, it will be necessary to restrict our attention to the following subclass of stratified systems.

Definition 8 (finite parameters) *A stratified system H is* finite-parameter *if $\mathcal{P}\mathrm{a}(H)$ is finite.*

For instance, the systems in both Example 1 and 2 are finite-parameter, while the systems consisting of only the subsystem Γ_1, in either examples, are not. In applications, one would expect that most systems are parameter-finite. Let us now introduce some additional notation and terminology about polynomials. According to (6), the calculation of the Taylor coefficients of a solution of an IVP $\mathbf{B} = (H,\rho)$ involves evaluating expressions in $\mathcal{P}_0(H) = \mathbb{R}[X \cup \mathcal{P}\mathrm{a}(H)]$. As $k \stackrel{\triangle}{=} |X \cup \mathcal{P}\mathrm{a}(H)| < +\infty$, elements of $\mathcal{P}_0(H)$ can be treated as usual multivariate polynomials in a *finite* number of indeterminates. In particular, we can identify initial data specifications ρ for H with points in $\mathbb{R}^k$. Accordingly, for polynomials $E \in \mathcal{P}_0(H)$ and initial data specification $\rho \in \mathbb{R}^k$, it is notationally convenient to write $\rho(E)$ as $E(\rho)$, that is the value in $\mathbb{R}$ obtained by evaluating E at point ρ. In fact, as we shall confine ourselves to the case $\rho(x) = 0$ for $x \in X$, we will have $\rho \in \mathbb{R}^k_0 \stackrel{\triangle}{=} \{\rho \in \mathbb{R}^k : \rho(x) = 0 \text{ for each } x \in X\}$.

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 $P \subseteq \mathcal{P}_0(H)$, $\langle\, P \,\rangle \stackrel{\triangle}{=} \{\sum_{i=1}^m h_i \cdot p_i : m \geq 0, h_i \in \mathcal{P}_0(H), p_i \in P\}$ denotes the smallest ideal which includes P, and $\mathbf{V}(P) \subseteq \mathbb{R}^k$ the *(affine) variety* induced by P: $\mathbf{V}(P) \stackrel{\triangle}{=} \{\rho \in \mathbb{R}^k : p(\rho) = 0 \text{ for each } p \in P\} \subseteq \mathbb{R}^k$. For $W \subseteq \mathbb{R}^k$, $\mathbf{I}(W) \stackrel{\triangle}{=} \{E \in \mathcal{P}_0(H) : p(\rho) = 0 \text{ for each } \rho \in V\}$. We will use a few basic facts about ideals and varieties: (a) both $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$ are inclusion reversing: $P_1 \subseteq P_2$ implies $\mathbf{V}(P_1) \supseteq \mathbf{V}(P_2)$ and $W_1 \subseteq W_2$ implies $\mathbf{I}(W_1) \supseteq \mathbf{I}(W_2)$; (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.

4.2 Preconditions and postconditions.

Computing the *preconditions* of a given set $Q \subseteq \mathcal{P}$ means finding all the initial data specifications $\rho \in \mathbb{R}^k_0$ under which all the polynomials in Q represent valid equations for the system H — that is, they are identically zero when one plugs the solution of H into them. Dually, computing the *postconditions* of given a set of initial data specifications $W \subseteq \mathbb{R}^k_0$ means finding the set $Q \subseteq \mathcal{P}$ of all polynomial equations that are valid under all initial data $\rho \in W$. Here, we shall confine ourselves to *algebraic* sets W, that is $W = \mathbf{V}(P)$ for some $P \subseteq \mathcal{P}_0(H)$. This leads to the following definition. Note that $P \supseteq X$ just means that $\mathbf{V}(P) \subseteq \mathbb{R}^k_0$. Recall that, for a coherent H and an initial data specification $\rho \in \mathbb{R}^k_0$, we let $\phi_{(H,\rho)}$ denote the unique solution of the IVP (H,ρ).

Definition 9 (pre- and postconditions) *Let H be coherent and finite-parameter. Let P and Q be sets of polynomials such that $X \subseteq P \subseteq \mathcal{P}_0(H)$ and $Q \subseteq \mathcal{P}$. We define the sets of* weakest preconditions $\mathrm{wp}_H(Q) \subseteq \mathbb{R}^k_0$ *and of the* strongest postconditions $\mathrm{sp}_H(P) \subseteq \mathcal{P}$ *as follows.*

$$
\begin{aligned}
\mathrm{wp}_H(Q) &\stackrel{\triangle}{=} \{\rho \in \mathbb{R}^k_0 : \phi_{(H,\rho)}(E) = 0 \ \textit{for each}\ E \in Q\} \\
\mathrm{sp}_H(P) &\stackrel{\triangle}{=} \{E \in \mathcal{P} : \phi_{(H,\rho)}(E) = 0 \ \textit{for each}\ \rho \in \mathbf{V}(P)\}\,.
\end{aligned}
$$

Any $W \subseteq \mathrm{wp}_H(Q)$ will be called an (algebraic) precondition for Q, any $R \subseteq \mathrm{sp}_H(P)$ a postcondition for $\mathbf{V}(P)$. 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 ($X \subseteq P \subseteq_{\text{fin}} \mathcal{P}_0(H)$ and $R \subseteq \mathcal{P}$), find a finite characterization of $\mathrm{sp}_H(P) \cap R$. (7)

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). Following a well-established tradition in the field of continuous and hybrid system, the set R will be represented by means of a polynomial template, to be introduced shortly.

4.3 A double chain algorithm.

We first introduce *polynomial templates* [23], that is, polynomials in $\mathrm{Lin}(\mathbf{a})[X \cup \mathcal{D}]$, where $\mathrm{Lin}(\mathbf{a})$ are (formal) linear combinations of the parameters in $\mathbf{a} = (a_1, \ldots, a_s)$ (for fixed $s \geq 1$) with real coefficients. For instance, $\ell = 5a_1 + 42a_2 - 3a_3$ is one such expression[3]. In other words, a polynomial template has the form $\pi = \sum_i \ell_i \gamma_i$ for distinct monomials $\gamma_i \in (X \cup \mathcal{D})^{\otimes}$, 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 $V \subseteq \mathbb{R}^s$, $\pi[V] \stackrel{\triangle}{=} \{\pi[v] : v \in V\} \subseteq \mathcal{P}$.

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

In particular, for a user specified π, we will set $R \stackrel{\triangle}{=} \pi[\mathbb{R}^s]$ in the relativized strongest postcondition problem (7). We extend δ_{Σ_1} and S_H to templates as expected: for $\pi = \sum_i \ell_i \gamma_i$, $\delta_{\Sigma_1}(\pi, x) \stackrel{\triangle}{=} \sum_i \ell_i \delta_{\Sigma_1}(\gamma_i, x)$ and $S_H \pi \stackrel{\triangle}{=} \sum_i \ell_i S_H \gamma_i$, 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 shall make use of the following substitution properties of templates, which hold true in coherent systems (see Lemma A.13 in in the Appendix).

$$\begin{aligned} \delta_{\Sigma_1}(\pi[v], x) &= \delta_{\Sigma_1}(\pi, x)[v] \text{ for each } x \in X & (8) \\ S_H(\pi[v]) &= (S_H \pi)[v] \text{ for each } v \in \mathbb{R}^s. & (9) \end{aligned}$$

We are now set to introduce the POST algorithm. Given $P \subseteq \mathcal{P}_0(H)$, with $P \supseteq X$, and a template π, fix $P_0 \supseteq X$ s.t. $I_0 \stackrel{\triangle}{=} \langle P_0 \rangle \subseteq \mathbf{I}(\mathbf{V}(P))$ ($P_0 = P$ 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 $S_H(\pi[v])$, and its derivatives up to order i, vanish on $\mathbf{V}(P)$, that is belong to $\mathbf{I}(\mathbf{V}(P))$. The J_i's are used to detect stabilization. We use π_τ as an abbreviation of $\delta_{\Sigma_1}(\pi, \tau)$.

$$\begin{aligned} V_i &\stackrel{\triangle}{=} \bigcap_{\tau : |\tau| \leq i} \{ v \in \mathbb{R}^s : (S_H \pi_\tau)[v] \in I_0 \} & (10) \\ J_i &\stackrel{\triangle}{=} \Big\langle \bigcup_{\tau : |\tau| \leq i} (S_H \pi_\tau)[V_i] \Big\rangle. & (11) \end{aligned}$$

Consider the least m such that *both* $V_m = V_{m+1}$ and $J_m = J_{m+1}$: we let $\mathrm{POST}_H(P_0, \pi) \stackrel{\triangle}{=} (V_m, J_m)$. 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 next theorem states correctness and relative completeness of POST.

Theorem 3 (relative completeness of POST) *Let H be coherent and finite-parameter. Let $X \subseteq P \subseteq \mathcal{P}_0(H)$ and π be a template. Fix $P_0 \supseteq X$ s.t. $I_0 \stackrel{\triangle}{=} \langle P_0 \rangle \subseteq \mathbf{I}(\mathbf{V}(P))$. Let $\mathrm{POST}_H(P_0, \pi) = (V_m, J_m)$. Then*

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

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

PROOF In the proof we shall make use of the following stabilization property of the sequence of the (V_i, J_i)s (see Lemma A.14 in the Appendix).

$$\mathrm{POST}_H(P_0, \pi) = (V_m, J_m) \text{ implies that for each } j \geq 1,\ V_m = V_{m+j} \text{ and } J_m = J_{m+j}. \qquad (12)$$

Let us consider part (a) of the theorem. 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 $\rho \in \mathbf{V}(P)$. By Corollary 1, 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 (8) and (9)), for each $\rho \in \mathbf{V}(P)$. That is, for each τ, $(S_H \pi_\tau)[v] \in \mathbf{I}(\mathbf{V}(P))$. The latter is implied by $(S_H \pi_\tau)[v] \in I_0 \subseteq \mathbf{I}(\mathbf{V}(P))$. By definition (10), this holds for each τ such that $v \in V_{|\tau|}$. Hence for each τ, as $v \in V_0 \supseteq \cdots \supseteq V_m = V_{m+1} = \cdots$ (by (12)). Assume now that $I_0 = \mathbf{I}(\mathbf{V}(P))$ 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 $|\tau| \leq m$, $(S_H \pi_\tau)[v] \in \mathbf{I}(\mathbf{V}(P))$. The latter means precisely that $(S_H \pi_\tau)[v](\rho) = 0$ for each $\rho \in \mathbf{V}(P)$. But this holds by definition of $\pi[v] \in \mathrm{sp}_H(P)$ and Corollary 1: indeed, for each τ, $(S_H(\pi[v]_\tau))(\rho) = (S_H \pi_\tau)[v](\rho) = 0$ (here we have used (8) and (9)), for each $\rho \in \mathbf{V}(P)$.

Let us consider part (b). First, consider any $\rho \in \mathrm{wp}_H(\pi[V_m])$. By definition and Corollary 1 (and using (8) and (9)), 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 $F(\rho) = 0$ for each $F \in J_m$, that is $\rho \in \mathbf{V}(J_m)$. On the other hand, consider any

$\rho \in \mathbf{V}(J_m)$ 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 1 (and again (8) and (9)), 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 $J_m = J_k \supseteq (S_H\pi_\tau)[V_m]$ (by (12)), therefore $(S_H\pi_\tau)[v](\rho) = 0$, as required. $\square$

The vector spaces V_i s in (10) can be effectively represented by the successive linear constraints imposed on the parameters in $\mathbf{a} = (a_1, \ldots, a_s)$ by (10). In turn, this leads to computing finite sets of generators for the ideals J_i s in (11). This is made explicit below. For a set of linear expressions $L \subseteq \mathrm{Lin}(\mathbf{a})$, let $\mathrm{span}(L) \stackrel{\triangle}{=} \{v \in \mathbb{R}^s : \ell[v] = 0 \text{ for each } \ell \in L\} \subseteq \mathbb{R}^s$ be the vector space of parameter evaluations that annihilate all expressions in L. For $\pi \in \mathrm{Lin}[\mathbf{a}][\mathbb{R}]$, let $\mathrm{coeff}(\pi)$ be the set of coefficients (linear expressions) of π. Recall that for a Gröbner basis G and a polynomial E, E mod G denotes the remainder of the division[4] of E by G.

Lemma 1 *Under the hypotheses of Theorem 3, let $G \subseteq \mathcal{P}_0(H)$ be a Gröbner basis of I_0. Then $V_i = \mathrm{span}\big(\cup_{|\tau| \leq i}\mathrm{coeff}((S_H\pi_\tau) \bmod G)\big)$. As a consequence $J_i = \big\langle\ \cup_{|\tau| \leq i} (S_H\pi_\tau)[B_i]\ \big\rangle$, where B_i is a basis of V_i.*

Example 4 (Example 1, cont.) Fix $P = P_0 = X$, that is $\mathbf{V}(P) = \mathbb{R}^k_0$, with $k = |\{t,x,u\}| = 3$: here we impose no constraints on the initial data. We seek for linear relations between u and u_x, considering the template $\pi \stackrel{\triangle}{=} a_1 u + a_2 u_x$. We compute $\mathrm{POST}_H(P_0, \pi) = (V_m, J_m)$ as follows. Below we reuse the equalities for $S_H(\delta_{\Sigma_1}(u,\tau))$ already computed in Example 3.

- ($i = 0$). $S_H\pi = (a_1 - a_2)u$. Therefore $V_0 = \mathrm{span}(\{a_1 - a_2\}) = \{(\lambda, \lambda) : \lambda \in \mathbb{R}\}$ and $J_0 = \{0\}$.
- ($i = 1$). $S_H\pi_x = S_H(a_1 u_x + a_2 u_{xx}) = (a_2 - a_1)u$ and $S_H\pi_t = S_H(a_1 u_{xx} + a_2 u_{x^3}) = (a_1 - a_2)u$. Therefore $V_1 = \mathrm{span}(\{a_2 - a_1, a_1 - a_2\}) = V_0$ and similarly $J_1 = J_0$.

Hence the algorithm stabilizes already at $m = 0$, returning $V_0 = \{(\lambda, \lambda) : \lambda \in \mathbb{R}\}$ and $J_0 = \{0\}$. This means that the valid instances of π are of the form $\lambda(u + u_x)$, for all $\lambda \in \mathbb{R}$. Or, equivalently, that $u_x = -u$ is a valid equation, under any initial data specification.

Suppose $\mathrm{POST}_H(P_0, \pi) = (V_m, J_m)$. Given a parameter evaluation $v \in \mathbb{R}^s$, 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_m of the vector space V_m. In practice, it is more convenient to represent the whole set $\pi[V_m]$ returned by POST_H compactly in terms of a new *result template*, say π', such that $\pi'[\mathbb{R}^s] = \pi[V_m]$. In the example above, $\pi' = a_1(u + u_x)$. The result template π' can in fact be computed directly from π, by propagating, via substitutions, the linear constraints on $\mathbf{a}$ given by $\mathrm{coeff}((S_H\pi_\tau) \bmod G)$ as they are generated (Lemma 1).

Remark 1 (on completeness) Completeness (equality) in part (a) of Theorem 3 is only guaranteed if P_0 is chosen such that $I_0 = \mathbf{I}(\mathbf{V}(P))$, otherwise $\pi[V_m]$ is just a postcondition. When $I_0 = \mathbf{I}(\mathbf{V}(P))$, I_0 is said to be a *real radical* of P. Computing real radicals is a computationally hard problem, in the general case. For a number of special cases relevant to our goals, 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 $\langle\ P\ \rangle = \mathbf{I}(\mathbf{V}(P))$, so that $\langle\ P\ \rangle$ is a real radical. Also note that the completeness in part (b) of Theorem 3 does *not* depend on having a real radical at hand. See [3] for further discussion on the real radical problem.

[4] Here we use the fact that $G \subseteq \mathcal{P}_0(H)$ is also a Gröbner over the larger polynomial ring $\mathbb{R}[X \cup \mathcal{P}\mathrm{a}(H) \cup \{a_1, \ldots, a_s\}]$, which includes also templates, once an elimination monomial order (e.g. lexicographic) for the a_i s is fixed. Additional details can be found in the Appendix.

5 Experiments

We have put a proof-of-concept implementation[5] of the POST algorithm of Section 4 at work on some IVPs drawn from mathematical physics. We illustrate three cases below.

Example 5 (Burgers' equation) We consider the inviscid case of the Burgers' equation [1, 7], with a linear initial condition at $t=0$ (for generic $b,c\in\mathbb{R}$)

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

We fix $U=\{u,b,c\}$ and $X=\{t,x\}$. The above IVP is encoded by the the stratified system $H_1 = \{\Gamma_1,\Gamma_2\}$, where

$$\Gamma_1 \,=\, (\{u_t=-uu_x\}\cup\Sigma_{aux1},\ \{t,x\}) \qquad\qquad \Gamma_2 \,=\, (\{u_x=b\}\cup\Sigma_{aux2},\ \{x\})\,.$$

The auxiliary equations $\Sigma_{aux1}=\{b_t=0,c_t=0,c_x=0\}$ and $\Sigma_{aux2}=\{b_x=0\}$ 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, with the lexicographic order induced by $u>b>c$ and $t>x$, is coherent. We fix the set of possible initial data specifications to $\mathbf{V}(P)$ where $P=X\cup\{u-c\}$: this just encodes $u(0,0)=c$. In order to discover interesting postconditions of $\mathbf{V}(P)$, we consider a complete polynomial template of total degree 3 over the indeterminates $Z\stackrel{\triangle}{=}X\cup\mathcal{P}\mathrm{a}(H_1)$, $\pi=\sum_{\tau_i\in Z^{\otimes},|\gamma_i|\le 3}a_i\gamma_i$, which consists of $s=56$ terms. Letting $P_0=P$, we run $\mathrm{POST}_{H_1}(P,\pi)$, 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 $I_0=\left\langle\, P \,\right\rangle$ is a real radical, Theorem 3(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 initial data specifications $\rho\in\mathbf{V}(P)$. This equation can be easily solved algebraically for u - note that we are actually manipulating CFPS's- and yields the unique solution of the IVP:

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

We note that for Burgers' equation also weak, non classical solutions with discontinuities, representing shock waves, are interesting [8]: at present, we do not know how to represent these solutions in our framework.

Example 6 (Heat equation) We consider an IVP for the heat equation in one spatial dimension, with a (generic) sinusoidal spatial initial condition at $t=0$ ($b,c\in\mathbb{R}$)

$$u_t \;=\; b\cdot u_{xx} \qquad\qquad u(0,x) \;=\; \sin(cx)\,. \tag{13}$$

We seek for solutions u of this IVP that can be expressed as a product of a sinusoidal function of x and of an exponential function of t. Let us code this 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

$$\Gamma_1=(\,\{u_t=bu_{xx}\}\cup\Sigma_{aux1},\ \{t,x\}\,) \quad \Gamma_2=(\{u_x=g,\ f_x=-cg,\ g_x=cf\}\cup\Sigma_{aux2},\ \{x\}\,)$$
$$\Gamma_3=(\,\{h_t=-dh\}\cup\Sigma_{aux3},\ \{t\}\,)\,.$$

The auxiliary equations in Σ_{auxi} encode that a,b,c,d,i,j are constants, like in the previous example, and moreover that $f_t=g_t=h_x=0$:

[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.

$$\Sigma_{aux1} = \{f_t = 0, g_t = 0, h_x = 0, c_t = 0, d_x = 0, a_t = 0, a_x = 0, i_t = 0, i_x = 0, j_t = 0, j_x = 0\}$$
$$\Sigma_{aux2} = \{c_x = 0\} \quad \Sigma_{aux3} = \{d_t = 0\}\,.$$

By inspection, $2 \prec 1$, $3 \prec 1$ and $1 \not\prec 2,3$, which ensures that H is stratified; also $\mathcal{P}\mathrm{a}(H_2) = U$ is finite. Moreover, the system is consistent: apart from the trivial case of constants, each subsystem features at most one equation per 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 $\xi \prec_{\text{lex}} \tau$); (b) the remaining pairs, not involving u, are ordered according to an arbitrary graded ranking. To search for solutions of the wanted form[6], we consider an "ansatz" represented by the following polynomial.

$$E \stackrel{\triangle}{=} a \cdot (u + igh + jfh) \tag{14}$$

and look for the weakest precondition $\mathrm{wp}_{H_2}(\{E\})$, that is, the largest algebraic set of initial data specification 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 corresponding values in E and find u. To compute $\mathrm{wp}_{H_2}(\{E\})$, we use the POST 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 $\mathrm{POST}_{H_1}(P, \pi)$, which halts at iteration $m = 3$, returning (V_3, J_3) (this took about 4s in our experiment). Theorem 3 ensures that $\mathbf{V}(J_3) = \mathrm{wp}_{H_2}(\pi[V_3]) = \mathrm{wp}_{H_2}(\{E\})$. 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 (14) 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.

A *boundary problem* prescribes the form of the solution at some specified curve, rather than an initial condition like an IVP. A boundary problem can often be transformed into an IVP via a suitable change of coordinates, hence becoming amenable to analysis with our algorithm. One can exploit the *method of characteristics* [11, Ch.3] as a systematic recipe for carrying out this transformation. The resulting technique is illustrated in the following example.

Example 7 (A boundary problem) Consider the PDE $u_x^2 + u_y^2 = 1$, with the boundary condition $u_{|C} = 0$, where C is the unit circle centered at the origin. According to the method of characteristics, one can transform a boundary problem into a *family* of (hopefully simpler) ODE IVPs. In the present case, letting s denote the only independent variable, and x, y, z, p, q denote dependent variables, one gets the following IVPs, depending on a parameter $r \in \mathbb{R}$ (see [15, Ch.2] for a detailed derivation).

$$\begin{array}{lllll} \frac{dx}{ds}(s;r) = 2p & \frac{dy}{ds}(s;r) = 2q & \frac{dz}{ds}(s;r) = 2p^2 + 2q^2 & \frac{dp}{ds}(s;r) = 0 & \frac{dq}{ds}(s;r) = 0 \\ x(0;r) = \cos(r) & y(0;r) = \sin(r) & z(0;r) = 0 & p(0;r) = \cos(r) & q(0;r) = \sin(r)\,. \end{array}$$

The union of the trajectories $(x(s;r), y(s;r), z(s;r))$ determined by these IVPs represents the solution u of the original problem, in the sense that for each r and s, $z(s;r) = u(x(s;r), y(s;r))$. Note that $(x(0;r), y(0;r))$ represents a parametrization of the circle C depending on $r \in \mathbb{R}$, and that $z(0;r) = 0$ as required by the boundary condition. To obtain an explicit formula for u, at this stage the method of characteristics prescribes to try the following: (1) solve the given IVPs, obtaining formulae for x, y, z as functions of (s, r); (2) invert the functions x and y, that is express (s, r) in terms of (x, y). This way one can rewrite $z(s;r) = u(x(s;r), y(s;r))$ as a function of x and y alone.

[6] That is, (sinusoid of x) $\times$ (exponential of t)

One can avoid to carry out steps (1) and (2) explicitly by exploiting the POST algorithm. In fact, seeing r as an independent *variable*, rather than a parameter, one can turn the above family of IVPs into a coherent stratified system H_3 of PDEs for the functions $x(s,r), y(s,r), \ldots$: say $H_3 = \{(\Sigma_1, \{s,r\}), (\Sigma_2, \{r\})\}$, for the obvious choices of Σ_1 and Σ_2. Now, one can use POST to systematically search for all valid polynomial relations linking x,y,z. If the resulting polynomial system can be solved for z, obtaining say $z = f(x,y)$, one can deduce $u(x,y) = f(x,y)$, at least for (x,y) sufficiently near to the boundary[7] C. In the present case, we run $\mathrm{POST}_{H_3}(P,\pi)$ with $P = \{s, r, x-1, y-1, z, p-1, q\}$ (encoding initial values for x,y,z,p,q) and π the complete template of total degree 2 over the variables $\{x,y,z\}$, which has 10 parameters. We get stabilization at $m = 5$ (after about 5s), obtaining a 1-parameter result template π', where $\pi'[1] = x^2+y^2-z^2-2z-1 = x^2+y^2-(z+1)^2$. Therefore $x^2+y^2 = (z+1)^2$ is the only valid polynomial relation of degree ≤ 2 for this system. Solving for z, we obtain $z = \pm\sqrt{x^2+y^2}-1$. The function involving the negative square root does not satisfy the boundary condition, so we deduce that $u = z = \sqrt{x^2+y^2}-1$ is the solution of the original problem.

6 Conclusion, further and related work

We have put forward a framework for PDEs, based on simple algebra and coalgebra, that yields a complete algorithm for pre- and postconditions of IVPs. To the best of our knowledge, no such completeness result for PDEs exists in the literature.

Conceptually, the present development parallels our previous work on polynomial ODEs, especially [2, 3]. 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 stratified systems and the related IVPs, 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 related to the field of Differential Algebra (DA), see [6, 16, 20, 19, 21] and references therein. See also the discussion in [5]. In particular, Boulier et al.'s RosenfeldGröbner algorithm [6], computes the ideal of the differential and polynomial consequences of a system Σ. While this ideal is clearly related to our $\mathrm{sp}_{\{\Sigma\}}(\emptyset)$, how to encode general pre- or postconditions in their format is far from trivial, if possible at all. More generally, while DA techniques can be used to reduce systems to a coherent form, which is required by our approach, none of them seems to focus on IVPs or boundary problems as such.

At present, we can only capture classical solutions of PDEs: but in practice, *weak* solutions [11, Ch.1], admitting discontinuities, are often considered. We leave a possible extension of our approach to weak solutions for future work.

References

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

[2] 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

[7] Technically, under mild conditions [15, Ch.2] that are satisfied in the present example, the function $G(s,r) \stackrel{\triangle}{=} (x(s,r), y(s,r))$ is locally invertible around $s = 0$. Therefore, for each (x_0,y_0) sufficiently near to the boundary C and for $(s_0,r_0) = G^{-1}(x_0,y_0)$, we have: $u(x_0,y_0) = u(G(s_0,r_0)) = z(s_0,r_0) = f(G(s_0,r_0)) = f(G(G^{-1}(x_0,y_0))) = f(x_0,y_0)$.

[3] 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.

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

[5] M. Boreale. On the Coalgebra of Partial Differential Equations. *MFCS 2019*, LIPIcs 138: 24:1-24:13, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. `http://www.dagstuhl.de/dagpub/978-3-95977-117-7`

[6] 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.

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

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

[9] Ch.G. Claudel, A.M. Bayen. Solutions to Switched Hamilton-Jacobi Equations and Conservation Laws Using Hybrid Components. *HSCC 2008*:101-115, ACM, 2008.

[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] C. Evans. *Partial Differential Equations*. American Mathematical Society. 2nd edition, 2010.

[12] 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`.

[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] 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.

[15] J. Levandosky. *Lecture Notes for Partial Differential Equations of Applied Mathematics (Math 220A)*. Stanford University, 2002. `https://web.stanford.edu/class/math220a/lecturenotes.html`.

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

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

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

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

[21] 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.

[22] 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.

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

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

A Proofs and additional technical material

A.1 Proofs of Section 2

We give here a self-contained proof of Theorem 1. This result is reproduced from [5]. The proof is based on a simple coalgebraic concepts, which are recalled below.

A.1.1 Commutative coalgebras

Let X be a finite nonempty set of *actions (or variables)*, ranged over by $x, y, \ldots$ and O a nonempty set. We recall that a *(Moore) coalgebra*[8] with actions in X and outputs in O is a triple $C = (\mathcal{S}, \delta, o)$ where: $\mathcal{S}$ is a set of *states*, $\delta : \mathcal{S} \times X \to \mathcal{S}$ is a *transition* function, and $o : \mathcal{S} \to O$ is an *output* function (see e.g. [22]). A *bisimulation* in C is a binary relation $R \subseteq \mathcal{S} \times \mathcal{S}$ such that whenever $s R t$ then: (a) $o(s) = o(t)$, and (b) for each x, $\delta(s,x) R \delta(t,x)$. It is an (easy) consequence of the general theory of bisimulation that a largest bisimulation over C, called bisimilarity and denoted by $\sim_C$, exists, is the union of all bisimulation relations, and is an equivalence relation over $\mathcal{S}$. Given two coalgebras with actions in X and outputs in O, C_1 and C_2, a *morphism* from C_1 to C_2 is a function $\mu : \mathcal{S}_1 \to \mathcal{S}_2$ that: (1) preserves outputs ($o_1(s) = o_2(\mu(s))$, and (2) preserves transitions ($\mu(\delta_1(s,x)) = \delta_2(\mu(s), x)$), for each state s and action x). It is an easy consequence of this definition that a morphism preserves bisimulation in both directions, that is: $s \sim_{C_1} t$ if and only if $\mu(s) \sim_{C_2} \mu(t)$.

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

Lemma A.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 define the coalgebra of CFPSs, $C_{\mathcal{F}}$

$$C_{\mathcal{F}} \quad \stackrel{\triangle}{=} \quad (\mathcal{F}, \delta_{\mathcal{F}}, o_{\mathcal{F}})$$

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

$$\mu(s)(\tau) \quad \stackrel{\triangle}{=} \quad \frac{o(s(\tau))}{\boldsymbol{\alpha}!} \tag{15}$$

where $\boldsymbol{\alpha}! \stackrel{\triangle}{=} \alpha_1! \cdots \alpha_n!$. 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 A.1 and of condition (a) in the definition of bisimulation.

Lemma A.2 *Let C be a commutative coalgebra and $f = \mu(s)$. For each x, $\frac{\partial f}{\partial x} = \mu(\delta(s,x))$.*

[8] In the paper, we only consider Moore coalgebras. For brevity, we shall omit the qualification "Moore".

PROOF Let $x = x_i$. For each $\tau = \mathbf{x}^{\boldsymbol{\alpha}}$ in $X^{\otimes}$ we have

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

where the first and second equality follow from (1) and (15), respectively, and the third one from the definition of $s(x_i\tau)$. This proves the wanted statement. □

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 A.1 (coinduction and finality of $C_{\mathcal{F}}$) *Let C be a commutative coalgebra. The function μ in* (15) *is the unique coalgebra morphism from C to $C_{\mathcal{F}}$. Moreover, the following* coinduction *principle is valid: $s \sim_C t$ if and only if $\mu(s) = \mu(t)$ in $\mathcal{F}$.*

PROOF We have: (1) $o(s) = \mu(s)(\varepsilon)$ by definition of μ, and (2) $\mu(\delta(s,x)) = \delta_{\mathcal{F}}(\mu(s),x)$, by Lemma A.2. 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.1.2 Proof of Theorem 1

We need a few technical lemmas. First, a result about normal forms in coherent systems.

Lemma A.3 *Let Σ be coherent. For each $x \in X$ and $F \in \mathcal{P}$, $SD_xSF = SD_xF$.*

PROOF 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 $F =_\Sigma E \stackrel{\triangle}{=} \sum_j c_j \cdot G^{k_j}\gamma_j + F'$. 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 differentiation, which imply $D_x E = \sum_j c_j k_j G^{k_j-1} D_x G \gamma_j + c_j G_j^k D_x \gamma_j + D_x F'$, we have

$$\begin{aligned} SD_xSF &= SD_xSE \\ &= SD_xE \\ &= S\big(\sum_j c_j k_j G^{k_j-1} D_x G \gamma_j + c_j G_j^k D_x \gamma_j + D_x F'\big)\,. \end{aligned} \tag{16}$$

- On the other hand, by total differentiation and then by applying (repeatedly) both $u_\tau = G$ and $u_{x\tau} = D_x G$, we have

$$\begin{aligned} SD_xF &= S\big(\sum_j c_j k_j u_\tau^{k_j-1} u_{x\tau} \gamma_j + c_j u_\tau^{k_j} D_x \gamma_j + D_x F'\big) \\ &= S\big(\sum_j c_j k_j G^{k_j-1} D_x G \gamma_j + c_j G_j^k D_x \gamma_j + D_x F'\big) \end{aligned}$$

  where the last term above is the same as (16).

□

Next, a result about solutions.

Lemma A.4 *Let $\mathbf{B} = (\Sigma, \rho)$ and ψ a solution of $\mathbf{B}$. For each $E, F \in \mathcal{P}$, $E =_\Sigma F$ implies $\psi(E) = \psi(F)$.*

PROOF 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 homomorphism over $\mathcal{P}$. The proof for the general case follows from this fact and from the definition of $=_\Sigma$. □

With any coherent (w.r.t. some ranking) Σ and initial data specification ρ, $\mathbf{B} = (\Sigma, \rho)$, we can now associate a coalgebra as follows.

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

where δ_Σ is defined in (4) and $o_\rho(E) \stackrel{\triangle}{=} \rho(SE)$. We will denote by $\sim_{\mathbf{B}}$ bisimilarity in $C_{\mathbf{B}}$. As a consequence of Lemma A.3, $\delta_\Sigma(\delta_\Sigma(E,x),y) = \delta_\Sigma(\delta_\Sigma(E,y),x)$, so that for any monomial τ, the notation $\delta_\Sigma(E,\tau)$ is well defined. As an example of transition, for the heat equation $\Sigma = \{u_{xx} = au_t\}$, one has $\delta_\Sigma(u_{xx},t) = au_{tt}$.

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 A.5 *Let $\mathbf{B} = (\Sigma, \rho)$, with Σ coherent. Then: (1) $C_{\mathbf{B}}$ is commutative; and (2) For each $E \in \mathcal{P}$, $E \sim_{\mathbf{B}} SE$.*

PROOF For what concerns part 1, for each x, y and F, we have

$$\begin{aligned} \delta_\Sigma(\delta_\Sigma(F,x),y) &= SD_xSD_yF \\ &= SD_xD_yF \\ &= SD_yD_xF \\ &= SD_ySD_xF \\ &= \delta_\Sigma(\delta_\Sigma(F,y),x) \end{aligned} \tag{17}$$

where the second equality and fourth follow from Lemma A.3, and the third one is a property of total derivatives.

For what concerns part 2, it is sufficient to show that the relation $R = \{(E, SE) : E \in \mathcal{P}\} \cup Id$, 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 $\delta_\Sigma(E,x) = SD_xE = SD_xSE = \delta_\Sigma(SE,x)$, where the second equality follows again from Lemma A.3. □

As a consequence of the previous lemma, part 1, and of Corollary A.1, there exists a unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. This morphism is the unique solution of $\mathbf{B}$ we are after. We need a lemma, saying that the unique morphism ϕ from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$ is compositional.

Lemma A.6 *Let $\mathbf{B} = (\Sigma, \rho)$, with Σ coherent, and let $\phi_{\mathbf{B}}$ be the unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. Then $\phi_{\mathbf{B}}$ is a homomorphism over $\mathcal{P}$.*

PROOF 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 A.3, $\delta_\Sigma(u,\tau) = Su_\tau$, hence $u_\tau \sim_{\mathbf{B}} \delta_\Sigma(u,\tau)$ by virtue of Lemma A.5(2), therefore $\phi_{\mathbf{B}}(u_\tau) = \phi_{\mathbf{B}}(\delta_\Sigma(u,\tau))$ by coinduction. □

PROOF OF THEOREM 1: Let $\phi_{\mathbf{B}}$ denote the unique morphism from $C_{\mathbf{B}}$ to $C_{\mathcal{F}}$. We prove that $\phi_{\mathbf{B}}$ is the unique solution of $\mathbf{B}$. By virtue of Lemma A.6, $\phi_{\mathbf{B}}$ coincides with the homomorphic extension of $(\phi_{\mathbf{B}})_{|U}$. We first prove that that $\phi_{\mathbf{B}}$ respects the initial data specification. Let u_τ be parametric. By the definition of coalgebra morphism and of output functions in $C_{\mathcal{F}}$ and $C_{\mathbf{B}}$, we have

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

which proves the wanted condition. Next, we have to prove that $\phi_{\mathbf{B}}$ satisfies the equations in Σ^∞. But for each such equation, say $u_\tau = F$, we have $Su_\tau =_\Sigma SF$ by the definition of $=_\Sigma$, hence $u_\tau \sim_{\mathbf{B}} F$ by Lemma A.5(2), hence the thesis by coinduction (Corollary A.1). We finally prove uniqueness of the solution. Assume ψ is a solution of $\mathbf{B}$. 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 A.1). Let $E \in \mathcal{P}$. There are two steps in the proof.

- $\psi(E)(\varepsilon) = \rho(SE) = o_\rho(E)$. This follows directly from Lemma A.4, since $\psi(E) = \psi(SE)$.
- For each x, $\frac{\partial\psi(E)}{\partial x} = \psi(\delta_\Sigma(E,x))$. First, we note that $\frac{\partial\psi(E)}{\partial x} = \psi(D_x E)$. This is proven by induction on the size of E: in the base case when $E = u_\tau$, just use the fact that, by the definition of solution, $\frac{\partial\psi(u_\tau)}{\partial x} = \frac{\partial}{\partial x}\frac{\partial\psi(u)}{\partial\tau} = \frac{\partial\psi(u)}{\partial\tau x} = \psi(u_{\tau x}) = \psi(D_x u_\tau)$; in the induction step, use the fact that ψ is an homomorphism over $\mathcal{P}$, and the differentiation rules of D_x and $\frac{\partial}{\partial x}$ for sum and product. Now applying Lemma A.4, we get $\psi(D_x E) = \psi(SD_x E) = \psi(\delta_\Sigma(E,x))$, which is the wanted equality.

Finally, formula (5) is an immediate consequence of the definition of coalgebra $C_{\mathbf{B}}$ and of the final morphism $\phi_{\mathbf{B}} = \mu$ in (15). □

A.1.3 Proof of conservative extension

We show that CFPSs are a conservative extension of classical, analytic solutions in the usual sense. Let $\mathcal{A}$ denote the set of real functions f that are analytic — admit a Taylor expansion — in a neighborhood of $0 \in \mathbb{R}^n$; for definiteness, we take each such function defined over the largest possible open set containing the origin. $\mathcal{A}$ induces a commutative coalgebra $C_{\mathcal{A}} = (\mathcal{A}, \delta_{\mathcal{A}}, o_{\mathcal{A}})$, where $\delta_{\mathcal{A}}(f,x) = \frac{\partial f}{\partial x}$ (conventional partial derivative along x) and $o_{\mathcal{A}}(f) = f(0)$. The unique morphism $\mu_{\mathcal{A}} : C_{\mathcal{A}} \to C_{\mathcal{F}}$ (Corollary A.1) is given by (15), that is, for $\tau = \mathbf{x}^{\boldsymbol{\alpha}}$, $\mu_{\mathcal{A}}(f)(\tau) = \frac{1}{\boldsymbol{\alpha}!}\frac{\partial f}{\partial\tau}(0)$. In other words, $\mu_{\mathcal{A}}$ maps the analytic function f into the CFPS obtained from the Taylor expansion of f from 0. Now fix a coherent Σ. Let $\psi : U \to \mathcal{A}$ be a solution of $\mathbf{B} = (\Sigma, \rho)$, in the classical sense, and assume it analytic. This means, letting the homomorphic extension $\mathcal{P} \to \mathcal{A}$ of ψ be still be denoted by ψ, that

(a) $\psi(u_\tau)(0) = \rho(u_\tau)$ for each $u_\tau \in \mathcal{P}\mathrm{a}(\Sigma)$; and,

(b) $\psi(u_\tau) = \psi(F)$ for each $u_\tau = F$ in Σ^∞.

We want to show that for each $E \in \mathcal{P}$ the Taylor expansion of $\psi(E)$, seen as a CFPS, coincides with $\phi_{\mathbf{B}}(E)$, the unique solution obtained from Theorem 1: formally, that $\mu_{\mathcal{A}}(\psi(E)) = \phi_{\mathbf{B}}(E)$. This is a consequence of the following lemma.

Lemma A.7 *Let Σ be coherent. Then ψ is a coalgebra morphism $C_{\mathbf{B}} \to C_{\mathcal{A}}$.*

PROOF First, by repeating verbatim the proof of Lemma A.4, we check that

$$\text{whenever } E =_{\Sigma} F \text{ then } \psi(E) = \psi(F). \tag{18}$$

Indeed, if $E \to_{\Sigma} F$, this is a consequence of property (b) above of the definition of solution (in the classical sense), 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 $=_{\Sigma}$. Second, we will exploit the following fact:

$$\text{whenever } F \in \mathcal{P}_0(\Sigma) \text{ then } \psi(F)(0) = \rho(F). \tag{19}$$

This is shown by an induction on F, where the base case $F = u_{\tau}$ relies on the above definition of solution, part (a). We can now repeat basically the same arguments of the uniqueness part of Theorem 1, as follows. Let $E \in \mathcal{P}$. There are two steps in the proof.

- $\psi(E)(0) = \psi(SE)(0) = \rho(SE) = o_{\rho}(E)$, where the first equality follows from (18) and the second one from (19).
- 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 the above definition of solution (in the analytic sense), part (b), $\frac{\partial \psi(u_{\tau})}{\partial x} = \frac{\partial}{\partial x}\frac{\partial \psi(u)}{\partial \tau} = \frac{\partial \psi(u)}{\partial \tau x} = \psi(u_{\tau x}) = \psi(D_x u_{\tau})$; in the induction step, use the fact that ψ is a homomorphism over $\mathcal{P}$, and the differentiation rules of D_x and $\frac{\partial}{\partial x}$ for sum and product. Now applying (18), we get $\psi(D_x E) = \psi(SD_x E) = \psi(\delta_{\Sigma}(E,x))$, which is the wanted equality.

$\square$

From the lemma just proven, and since the composition of two coalgebra morphisms is a coalgebra morphism, we have that $\mu_{\mathcal{A}} \circ \psi : C_{\mathbf{B}} \to C_{\mathcal{F}}$ is a coalgebra morphism. By the uniqueness of such morphism (Corollary A.1), we have $\mu_{\mathcal{A}} \circ \psi = \phi_{\mathbf{B}}$, which is the wanted claim.

A.2 Proofs of Section 3

We first state a simple property of solutions of simple IVPs (Σ, ρ)

Lemma A.8 *Let ψ be the solution of a coherent IVP $\mathbf{B} = (\Sigma, \rho)$. For each expression E and $\xi = \mathbf{x}^{\boldsymbol{\alpha}}$, $\psi(E)(\xi) = \frac{\psi(D_{\xi}E)(\varepsilon)}{\boldsymbol{\alpha}!}$.*

PROOF An immediate application of formula (5) and of the definition of δ_{Σ} in (4). Note in particular that $\psi(D_{\xi}E)(\varepsilon) = \rho(S_{\Sigma}D_{\xi}E) = \rho(\delta_{\Sigma}(E,\xi))$. $\square$

The next lemma basically says that each subsystem $\Gamma_i = \Sigma_i(X_i)$ in a coherent stratified system can be interpreted as a coherent system in the dependent variables U_{Γ_i} and the independent variables X_i.

Lemma A.9 *Let $H = \{\Gamma_1, ..., \Gamma_k\}$ be a coherent stratified system. Then, for each i, (Σ_i, X_i), seen as a system of PDEs with dependent variables in U_{Γ_i}, independent variables in X_i and derivatives in $\mathcal{D}_i \stackrel{\triangle}{=} \{\upsilon_{\xi} : \upsilon \in U_{\Gamma_i}, \xi \in X_i^{\otimes}\}$, is coherent in the sense of Definition 3.*

PROOF By assumption each Σ_i is $\prec$-normal, for one and the same ranking $\prec$ defined on $\mathcal{D}$. The ranking $\prec$ induces a total order $\prec'$ over $\mathcal{D}_i$ defined as: $(u_\tau)_\xi \prec' (v_{\tau'})_{\xi'}$ iff $u_{\tau\xi} \prec v_{\tau'\xi'}$. The total order $\prec'$ is a ranking over $\mathcal{D}_i$: this immediately stems from $\prec$ being a ranking over $\mathcal{D}$. By the same reasoning, Σ_i is $\prec'$-normal when elements of $\mathcal{D}_{\Gamma_i}$ are interpreted as elements of $\mathcal{D}_i$. $\square$

We next prove Theorem 2. In fact, it is technically convenient for the subsequent development to prove a slightly more detailed statement, which also provides us with some information about the form of the solution.

Theorem A.1 (Theorem 2) *Let H be a coherent stratified system. For any initial data specification ρ for H, there is a unique solution $\phi_{\mathbf{B}}$ of $\mathbf{B} = (H, \rho)$. Moreover, for each i, $(\phi_{\mathbf{B}})_{\Gamma_i}$ is also the solution of (Σ_i, ρ_i), for some ρ_i whose restriction to $\mathcal{P}\mathrm{a}(H)$ coincides with ρ.*

PROOF Consider the stratified system $\overline{H} \stackrel{\triangle}{=} H \cup \{\Gamma_0\}$. We will define below a set of initial value problems $\mathbf{B}_i = (\Gamma_i, \rho_i)$ (Definition 2), $i = 0, \ldots, k$, where each Γ_i is seen as a system of PDEs with independent variables X_i and dependent variables U_{Γ_i}. By Lemma A.9, each Γ_i is coherent, hence $\mathbf{B}_i$ will have a unique solution ψ_i in the sense of Definition 2 (Theorem 1). Note that, under the identification $\mathcal{D}_i = \mathcal{D}_{\Gamma_i}$, ψ_i induces a function $\mathcal{P}_{\Gamma_i} \to \mathcal{F}(X_i)$: this function, still denoted by ψ_i, respects the equations in Σ_i. Similarly, ρ_i induces a function $\mathcal{P}\mathrm{a}(\Gamma_i) \to \mathbb{R}$.

We proceed now to the actual definition of the $\mathbf{B}_i$s by induction on the relation over subsystem indices ($i \prec j$), which is by definition acyclic. Note that $\mathcal{P}\mathrm{a}(\overline{H}) = \emptyset$, so that each $u_\tau \in \mathcal{D}$ is principal for exactly one subsystem.

- The base case is when $\mathcal{P}\mathrm{a}(\Gamma_i) = \emptyset$. Then we let $\mathbf{B}_i \stackrel{\triangle}{=} (\Sigma_i(X_i), \emptyset)$, where $\emptyset$ denotes here the empty function, and let ψ_i be the corresponding unique solution (Theorem 1).
- Assume $\mathcal{P}\mathrm{a}(\Gamma_i) \neq \emptyset$. Then we let $\mathbf{B}_i \stackrel{\triangle}{=} (\Sigma_i(X_i), \rho_i)$, where $\rho_i : \mathcal{P}\mathrm{a}(\Gamma_i) \to \mathbb{R}$ is the initial data specification defined by $\rho_i(u_\tau) \stackrel{\triangle}{=} \psi_j(u_\tau)(\varepsilon)$, for each $u_\tau \in \mathcal{P}\mathrm{a}(\Gamma_i)$; here j is the unique index such that $j \prec i$ and $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_j)$, and ψ_j is the unique solution of $\mathbf{B}_j$.

Now we show that $\psi \stackrel{\triangle}{=} \psi_1$ 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 $u_\tau \in \mathcal{D}_{\Gamma_i}$

$$\psi_{\Gamma_i}(u_\tau)(\varepsilon) \quad = \quad \psi_i(u_\tau)(\varepsilon)\,. \tag{20}$$

This is obvious if $i = 1$, hence assume $i \neq 1$. We distinguish the case $u_\tau \in \mathcal{P}\mathrm{a}(\Gamma_i)$ from the case $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_i)$. In the first case, let j be the unique index such that $u_\tau \in \mathcal{P}\mathrm{r}(\Gamma_j)$, so that $j \prec i$. Note that $j \neq 1$: otherwise, one would have $1 \prec i$, which is impossible, due to acyclicity and $i \prec 1$ (as to the latter, note that there must exist $u_{\tau'} \in \mathcal{P}\mathrm{r}(\Gamma_i) \cap \mathcal{P}\mathrm{a}(\Gamma_1)$; in fact $\mathcal{P}\mathrm{r}(\Gamma_i) \neq \emptyset$, as $\Sigma_i \neq \emptyset$). Then the following equalities follow from the definitions of $\psi_{\Gamma_k}, \psi_k, \rho_k$ ($0 \leq k \leq m$).

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

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

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

This proves (20). Now in order to show that $\psi_{\Gamma_i} = \psi_i$, consider the following, for arbitrary $u_\tau \in \mathcal{D}_{\Gamma_i}$ and $\xi \in X_i^{\otimes}$, $\xi = \mathbf{x}^{\boldsymbol{\alpha}}$.

$$\begin{aligned} \psi_{\Gamma_i}(u_\tau)(\xi) &= \psi_{\Gamma_i}(u_{\tau\xi})(\varepsilon)/\boldsymbol{\alpha}! && (21)\\ &= \psi_i(u_{\tau\xi})(\varepsilon)/\boldsymbol{\alpha}! && (22)\\ &= \psi_i(u_\tau)(\xi) && (23)\end{aligned}$$

where (21) and (23) follow from Lemma A.8 applied to ψ_1 and ψ_i respectively, and (22) from (20).

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 (under the identification $\mathcal{D}_{\Gamma_1} = \mathcal{D}_i$). By uniqueness (Theorem 1), 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 $\phi = \phi_{\Gamma_1} = \psi_1 = \psi$.

The last part of the statement follows by construction of $\phi_{\mathbf{B}}$. □

Lemma A.10 *Let H be coherent and let ρ be an initial data specification for H. Let ϕ be the unique solution of (H,ρ). For each $E,F \in \mathcal{P}$, $E =_H F$ implies $\phi(E)(\varepsilon) = \phi(F)(\varepsilon)$.*

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 2). By definition of solution and Lemma A.4, for each $u_\tau = G \in \Sigma_i^{\infty}(X_i)$, $\phi(u_\tau)_{|X_i^{\otimes}} = \phi(G)_{|X_i^{\otimes}}$. Now, since ϕ acts as a homomorphism on $\mathcal{P}$ (Lemma A.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 $\phi(E)_{|X_i^{\otimes}} = \phi(F)_{|X_i^{\otimes}}$ for some X_i; in particular, $\phi(E)(\varepsilon) = \phi(F)(\varepsilon)$, as of course $\varepsilon \in X_i^{\otimes}$. This finally implies that whenever $E =_H F$ one has $\phi(E)(\varepsilon) = \phi(F)(\varepsilon)$, as required. □

PROOF OF COROLLARY 1: We use the characterizations of ϕ as the unique solution of the IVP $\mathbf{B}_1 = (\Sigma_1(X), \rho_1)$ (Theorem A.1) and as a coalgebra morphism (Theorem 1). First, we observe that by Lemma A.8, $\phi(E)(\tau) = \phi(D_\tau E)(\varepsilon)/\boldsymbol{\alpha}! = \phi(\delta_{\Sigma_1}(E,\tau))(\varepsilon)/\boldsymbol{\alpha}!$, where the last equality stems from the definition of δ_{Σ_1} and Lemma A.3. Second, by Lemma A.10 , we have that $\phi(\delta_{\Sigma_1}(E,\tau))(\varepsilon) = \phi(S_H(\delta_{\Sigma_1}(E,\tau)))(\varepsilon)$. For brevity, let $F = S_H(\delta_{\Sigma_1}(E,\tau))$. As $F \in \mathcal{P}_0(H) \subseteq \mathcal{P}_0(\Sigma_1)$, we have $\phi(F)(\varepsilon) = \rho_1(F)$ by definition of coalgebra morphism (15). But, by Theorem A.1, ρ_1 coincides with ρ on elements of $\mathcal{P}_0(H)$, hence $\phi(F)(\varepsilon) = \rho_1(F) = \rho(F)$, which completes the proof of (6). □

A.3 Proofs of Section 4

We first need a technical result, saying basically that if two polynomials in normal forms are mapped to the same solution under all initial data specifications, then they coincide syntactically.

Lemma A.11 *Let H be a coherent. Let $E,F \in \mathcal{P}_0(H)$. Suppose that, for each initial data specification ρ and $\mathbf{B} = (H,\rho)$, $\phi_{\mathbf{B}}(E)(\varepsilon) = \phi_{\mathbf{B}}(F)(\varepsilon)$. Then $E = F$.*

PROOF Let us write $E = \sum_{i=1}^{k} \tau_i p_i$ and $F = \sum_{i=1}^{k} \tau_i q_i$, for some $k \geq 0$, $p_i, q_i \in \mathbb{R}[\mathcal{P}\mathrm{a}(H)]$ and *distinct* monomials $\tau_i \in X^{\otimes}$, 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 consider the unique solution ϕ of (H,ρ). Since ϕ is also the unique solution of $\mathbf{B}_1 = (\Sigma_1, \rho_1)$ for a suitable ρ_1 (Theorem A.1), hence a $C_{\mathbf{B}_1}$-coalgebra morphism, we have, applying Lemma A.4 and (repeadetly) Lemma A.3: $\phi(D_{\tau_1}E) = \phi(\delta_{\Sigma_1}(E,\tau_1)) = \phi(\delta_{\Sigma_1}(F,\tau_1)) = \phi(D_{\tau_1}F)$. Moreover, by homomorphism and (6) (note that $S_H p_1 = p_1$, being $p_1 \in \mathbb{R}[\mathcal{P}\mathrm{a}(H)]$), $\phi(D_{\tau_1}E)(\varepsilon) = \phi(p_1)(\varepsilon) + \phi(E')(\varepsilon) = \rho(p_1) + 0$: indeed, by definition, $\rho(x) = 0$ for each $x \in X$, hence $\phi(E')(\varepsilon) = \phi(x)(\varepsilon) \cdot \phi(E'')(\varepsilon) = 0$. Similarly, $\phi(D_{\tau_1}F)(\varepsilon) = \rho(q_1)$. Since this equality holds for an arbitrary ρ, and p_1, q_1 are polynomials with indeterminates in $\mathcal{P}\mathrm{a}(H)$, we deduce that indeed $p_1 = q_1$. For the inductive step $j > 1$, consider $E_j \stackrel{\triangle}{=} \sum_{i \geq j} \tau_i p_i$ and $F_j \stackrel{\triangle}{=} \sum_{i \geq j} \tau_i q_i$ and proceed similarly to show $E_j = F_j$, then use the induction hypothesis to conclude $E = F$. $\square$

The next lemma says that the normal form functions S_1 and S_H preserve the sum and product operations on polynomials defined in (3). In what follows, we shall abbreviate S_{Σ_1} as S_1.

Lemma A.12 *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 initial data specification ρ for H and denote by $\phi_{\mathbf{B}}$ the unique solution of $\mathbf{B} = (H,\rho)$ (Theorem 2). We have:

$$\begin{aligned}
\phi_{\mathbf{B}}(S_H(E+F))(\varepsilon) &= \phi_{\mathbf{B}}(E+F)(\varepsilon) && (24)\\
&= \phi_{\mathbf{B}}(E)(\varepsilon) + \phi_{\mathbf{B}}(F)(\varepsilon) && (25)\\
&= \phi_{\mathbf{B}}(S_H E)(\varepsilon) + \phi_{\mathbf{B}}(S_H F)(\varepsilon) && (26)\\
&= \rho(S_H E) + \rho(S_H F) && (27)\\
&= \rho(S_H E + S_H F) && (28)\\
&= \phi_{\mathbf{B}}(S_H E + S_H F)(\varepsilon) && (29)
\end{aligned}$$

where: (24) and (26) follow from Lemma A.10; (25) follows because ϕ is a homomorphism; (27) and (27) follow from (6); (28) follows by definition of homomorphic extension of ρ to $\mathcal{P}_0(H)$. Since $\phi_{\mathbf{B}}(S_H(E+F))(\varepsilon) = \phi_{\mathbf{B}}(S_H E + S_H F)(\varepsilon)$ holds for an arbitrary ρ, and $S_H(E+F)$ and $S_H E + S_H F$ are both polynomials in $\mathcal{P}_0(H)$, Lemma A.11 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. $\square$

We need need two 'substitution lemmas' for templates, also to effectively compute (10). These prove the equalities (8) and (9).

Lemma A.13 *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 $\pi = \sum_i \ell_i \gamma_i$, for distinct monomials $\gamma_i \in (X \cup \mathcal{D})^{\otimes}$. Facts (1) and (2) easily follow from the distributivity properties of S_H and S_1 (Lemma A.12). As an example, for (1) we have

$$\begin{aligned}
\delta_{\Sigma_1}(\pi[v],x) &= \delta_{\Sigma_1}\big(\sum_i \ell_i[v]\gamma_i, x\big)\\
&= S_1\sum_i \ell_i[v]D_x\gamma_i\\
&= \sum_i \ell_i[v]S_1D_x\gamma_i\\
&= \sum_i \ell_i[v]\delta_{\Sigma_1}(\gamma_i,x)\\
&= \big(\sum_i \ell_i\delta_{\Sigma_1}(\gamma_i,x)\big)[v]\\
&= \delta_{\Sigma_1}(\pi,x)[v] \qquad (30)
\end{aligned}$$

The proof for (2) is similar. □

We finally arrive at the proof of the stabilization property stated in (12).

Lemma A.14 (property (12)**)** *Let* $\mathrm{POST}_H(P_0,\pi) = (V_m, J_m)$*, under the hypotheses of Theorem 3. 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

$$(S_H\pi_{\tau x})[v] \quad \in \quad J_m \quad \text{for each } |\tau| = m+j,\, x\in X \text{ and } v \in V_m\,. \qquad (31)$$

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 (31) 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

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

   where the last step follows by induction hypothesis. From (31), 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 (31). In this proof, we shall make use of the following equalities satisfied by S_H. For each $E \in \mathcal{P}$ and $x \in X$

$$S_H D_x S_H E \quad = \quad S_H D_x E \qquad (32)$$

$$S_H S_1 E \quad = \quad S_H E\,. \qquad (33)$$

The proof of (32) is essentially identical to that of Lemma A.3 (induction on the rank of the leading derivative in E) and is omitted. Concerning (33), note that $E =_{\Sigma_1} S_1E$ implies $E =_H S_1E$, which in turn implies $E =_H S_HS_1E$, that is $S_HE = S_HS_1E$. Let us now proceed to the proof of (31). Fix any $v \in V_m$. First, note that for $|\tau| = m+j$ and $x \in X$, by definition $\pi_{\tau x}[v] = \delta_{\Sigma_1}(\pi_\tau[v], x) = S_1D_x(\pi_\tau[v])$ (where in the first step we have used Lemma A.13; 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

$$\begin{aligned}
(S_H\pi_{\tau x})[v] &= S_HS_1D_x(\pi_\tau[v]) \\
&= S_HD_x(\pi_\tau[v]) && (34)\\
&= S_HD_xS_H(\pi_\tau[v]) && (35)\\
&= S_HD_x\sum_l h_l \cdot S_H\pi_{\tau_l}[w_l] && (36)\\
&= S_H\sum_l (D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot D_xS_H(\pi_{\tau_l}[w_l]) && (37)\\
&= \sum_l S_H(D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_HD_xS_H(\pi_{\tau_l}[w_l]) && (38)\\
&= \sum_l S_H(D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_HD_x(\pi_{\tau_l}[w_l]) && (39)\\
&= \sum_l S_H(D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_HS_1D_x(\pi_{\tau_l}[w_l]) && (40)\\
&= \sum_l S_H(D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H\delta_1(\pi_{\tau_l}[w_l], x) && (41)\\
&= \sum_l S_H(D_xh_l) \cdot S_H\pi_{\tau_l}[w_l] + h_l \cdot S_H\pi_{\tau_l x}[w_l] && (42)
\end{aligned}$$

where:

- (34) follows from (33);
- (35) follows from (32);
- (36) follows from the equality for $S_H(\pi_\tau[v]) = (S_H\pi)[v]$ (here we use Lemma A.13) proven above;
- (37) follows from distributing D_x over sum and products, and applying the rules for total derivatives;
- (38) follows from distributing S_H (Lemma A.12) over sums and products, and further noting that $S_Hh_l = h_l$, as $h_l \in \mathcal{P}_0(H)$;
- (39) follows again from (32);
- (40) follows again from (33);
- (41) follows from the definition of δ_1;
- (42) follows from Lemma A.13.

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 (42) proves that $S_H\pi_{\tau x}[v] \in J_m$, as required. □

A.4 Proofs of Section 4

We refer the reader to [10, Ch.3,§1,Th.2] for the definitions of Gröbner basis G, of reduction $\bmod G$, as well as of the technical notion of elimination order; the lexicographic order is one such order. See [3, Lemma 3] for a proof of the following lemma.

Lemma A.15 *Let $\mathbf{z} = \{z_1, ..., z_k\}$ and $\mathbf{a} = \{a_1, ..., a_s\}$ be disjoint sets of indeterminates. Let $G \subseteq \mathbb{R}[\mathbf{z}]$ be a Gröbner basis in $\mathbb{R}[\mathbf{a} \cup \mathbf{z}]$ w.r.t. a monomial elimination order for the a_i s in $\mathbf{a}$. Consider $p \in \mathrm{Lin}(\mathbf{a})[\mathbf{z}]$, seen as a polynomial in $\mathbb{R}[\mathbf{a} \cup \mathbf{z}]$, and $r = p \bmod G$. Then r is linear in $\mathbf{a}$. Moreover, for each $v \in \mathbb{R}^s$, $p[v] \bmod G = r[v]$.*

PROOF OF LEMMA 1: Let $\mathbf{z} = X \cup \mathcal{P}\mathrm{a}(H)$. Let $G \subseteq \mathcal{P}_0(H)$ be the given Gröbner basis of I_0: G can be seen as a Gröbner in the larger ring $\mathbb{R}[\mathbf{a} \cup \mathbf{z}]$, w.r.t. some elimination order for the parameters a_i s in $\mathbf{a}$. Fix any $\tau \in X^{\otimes}$. Applying Lemma A.15 with $p = S_H \pi_\tau$, we have that for each $v \in \mathbb{R}^s$: $(S_H \pi_\tau)[v] \in I_0$ iff $r^{(\tau)}[v] = 0$, where $r^{(\tau)} \triangleq S_H \pi_\tau \bmod G$; this is true iff $v \in \mathrm{span}(\mathrm{coeff}(r^{(\tau)}))$. Hence, by definition (10), $v \in V_i$ iff $v \in \mathrm{span}(\mathrm{coeff}(r^{(\tau)}))$ for each $|\tau| \leq i$. This is in turn equivalent to $v \in \mathrm{span}(\cup_{|\tau| \leq i} \mathrm{coeff}(r^{(\tau)}))$, which is the first part of the statement. The last part follows because, for any template π, vector space $V \subseteq \mathbb{R}^s$ and basis B of V, one has $\langle\, \pi[V] \,\rangle = \langle\, \pi[B] \,\rangle$. $\square$