

CIRCUITS, BLOCKS, AND GALOIS GROUPS IN STRUCTURAL IDENTIFIABILITY

SANAY SEHGAL AND DAVI KLITZ

Specht Labs, New York, NY

ABSTRACT. The input–output relations of a rational ODE model are the polynomial relations among its parameters and the derivatives of its inputs and outputs that hold on every trajectory, and structural identifiability is read from their coefficients. We compute these relations, decide when the structure of a model makes their elimination unnecessary, and study the group that permutes the parameter values they cannot tell apart. The relations are the circuit polynomials of an algebraic matroid on the parameters and the output jets: a greedy basis in jet order gives each output’s relation of least order, these relations form a characteristic set of the input–output ideal exactly when they generate a prime ideal, and they are computed by evaluation and interpolation, without differential elimination. When the ideal is not prime, identifiability is decided on each of its minimal primes, and the rank of a Wronskian decides whether a single experiment fixes the coefficients; a measured corank of one settles this outright. For linear cycles coupled through one common denominator affine in their states, the input–output relation is a single resultant in one auxiliary unknown, and for two cycles it is inverted in closed form from three of its coefficient slices without ever being formed. For parameter-disjoint linear blocks observed through their sum, the indistinguishable values are indexed, outside a thin set, by the cycle covers of an imitation digraph. Finally, when the unknowns are locally identifiable, the indistinguishable values are permuted by the Galois group of the map to the coefficients. Point counts over finite fields determine its degree and cycle-type statistics, and a single prime can certify that it is not regular; loops around the branch points on one line generate its geometric part and complete the preimage; and a computed preimage is complete when, and generically only when, its trace along a line in the space of outputs is a rational function of degree bounded by Bézout’s theorem.

1. INTRODUCTION

Let Σ be the model

$$(1.1) \quad \dot{x} = f(x, \theta, u), \quad y = g(x, \theta),$$

with f and g rational over $\mathbb{Q}$. Two values of its unknowns are *indistinguishable* if they produce the same output, and a parameter is *structurally identifiable* if it takes one value on the set of values indistinguishable from a generic one. The *input–output relations* of Σ are the polynomial relations among its parameters and the derivatives of its inputs and outputs that hold on every trajectory, and identifiability is read from their coefficients. This paper asks three questions of them: how to compute them, what the structure of a model buys, and how the values they cannot tell apart are organised.

The standard route to identifiability eliminates the states. Ljung and Glad decide global identifiability with Ritt’s algorithm [23]; Bellu, Saccomani, Audoly and D’Angiò compute the input–output relations by characteristic sets in DAISY [2]; Boulier, Lazard, Ollivier and Petitot decompose differential ideals by the Rosenfeld–Gröbner algorithm [5]; and Dong, Goodbrake, Harrington and Pogudin compute the relations by projections in StructuralIdentifiability.jl [9]. Ovchinnikov, Pogudin and Thompson show that the coefficients of the relations generate the field of identifiable functions under standard hypotheses [29], and Ovchinnikov, Pillay, Pogudin and Scanlon that in general these coefficients are identifiable only from several experiments [28]. Hong, Ovchinnikov, Pogudin and Yap avoid the relations in SIAN by working with truncated Taylor series [18], and Sedoglavic’s rank test on the jet map decides local identifiability without them [34]. On large models, the elimination is where input–output methods stop. For the benchmark model *Pharm* of Demignot and Domurado [7], two linear cycles coupled through one saturable term, the relation has 1,062,556 terms.

When the unknowns are locally but not globally identifiable, the values indistinguishable from a given one form a finite set. Bates, Hauenstein and Meshkat introduced its size as the identifiability degree, and computed it by homotopy continuation, monodromy and the trace test [1]; COMBOS, of Meshkat, Kuo and DiStefano, reports the number of local solutions of a locally identifiable model [25]. Hauenstein, Rodriguez and Sottile compute Galois and monodromy groups of parametrised polynomial systems numerically [15], Duff, Korotynskiy, Pajdla and Regan recover the symmetries of a polynomial system by monodromy [10], and Hauenstein and Sherman estimate its number of solutions statistically [16]. Trace tests go back to Sommese, Verschelde and Wampler [36], with the linear trace test of Leykin, Rodriguez and Sottile [21] and its multiprojective version by Hauenstein and Rodriguez [14]. Rey Barreiro and coauthors study discrete symmetries as a source of local, non-global identifiability [31], and recovering a Galois group from the distribution of Frobenius elements is classical in number theory [37].

Two combinatorial threads also run through the paper. Algebraic matroids, surveyed by Rosen, Sidman and Theran [33], have been used by Meshkat, Rosen and Sullivant to test observability [26] and by Hollering and Sullivant for identifiability in phylogenetics [17], and Malić and Streinu compute circuits of the rigidity matroid by combinatorial resultants [24]. For linear compartmental models, indistinguishability was studied by Godfrey and Chapman [12], and Bortner and Meshkat give graph-based sufficient conditions for it [4].

Our first question is how to compute the input–output relations, whether they generate the right ideal, and which experiment a verdict drawn from them concerns. For the first, the relations are the circuit polynomials of an algebraic matroid on the parameters and the output jets, read off the Jacobian of the jet map, which exists for every model. A greedy basis in jet order gives each output’s relation of least order, and these relations form a characteristic set of the input–output ideal exactly when they generate a prime ideal. They are computed by evaluation and interpolation over finite fields or, when the degree is too large, by resultants taken one variable at a time. For the second, relations with one leader each can generate a non-prime ideal, only one of whose minimal primes carries the trajectories, and a membership test run over the coefficients of the relations themselves can then undercount identifiable parameters. On a primality failure, `StructuralIdentifiability.jl` adjoins an extra projection [9]; we decompose the ideal and decide field membership on each minimal prime. For the third, a verdict read from input–output coefficients is in general a multi-experiment verdict [28, 29], and the rank of a Wronskian of a relation’s terms along one trajectory decides whether a single experiment fixes the coefficients. `StructuralIdentifiability.jl` computes this Wronskian and warns when its corank exceeds one; since specialisation can only lower rank, a measured corank of one settles the single-experiment case outright.

Our second question is what structure buys. Models in applications are often assembled from linear blocks, such as compartments exchanging material at constant rates, joined either through one shared nonlinear term or through one shared output. For the first joint we take k linear cycles coupled only through a common denominator that is affine in their states, as in competitive Michaelis–Menten kinetics. Collapsing the linear states leaves one scalar Lur’e relation per cycle, and the input–output relation becomes a single resultant in one auxiliary unknown, whatever k is. One scaling is lost for each unobserved cycle, and at $k = 2$ and 3 nothing else is. For two cycles the resultant can be inverted without being formed: three of its coefficient slices return every parameter in closed form. For the second joint we take linear blocks with disjoint parameters, observed only through their sum. The output then no longer factors over the blocks, and the obstruction is that one block may imitate another, a pointwise form of the indistinguishability of Godfrey and Chapman. For parameter values outside a thin set, every indistinguishable value permutes the blocks along a cycle cover of an imitation digraph, so that the model is identifiable exactly as its blocks are when the digraph has no cycles.

Our third question is how the indistinguishable values are organised when the unknowns are locally identifiable. They then form the preimage of a point under a generically finite map, and they are permuted by one group, the Galois group of the map, whose geometric part is its monodromy group. By Galois theory the group is regular exactly when every indistinguishable value is the image of a given one under a rational symmetry of the parameters. We read the group in three ways. Arithmetically, the numbers of points of one preimage over finite fields, at a base point with no rational preimage, give the degree and the cycle-type

statistics of the group, need no elimination when the map is taken to the Taylor coefficients of the output, and at a single prime can certify that the group is not regular. Topologically, the loops of Hauenstein, Rodriguez and Sottile, used the other way round, become a stopping rule that completes the preimage; they see the geometric part of the group, which is all of it when the Galois closure adds no constants. Analytically, when the preimage is sliced by a line in the space of outputs, where the linear trace test does not apply, completeness is detected by the rationality of the trace.

We are not aware of prior use of jet-matroid circuits to compute input–output relations, of composition over the minimal primes of a non-prime ideal, of the corank-one rule, or of finite-field point counts in structural identifiability.

Section 2 collects the background. Section 3 computes the relations, Section 4 decides identifiability when they generate a non-prime ideal, and Section 5 decides which experiment a verdict concerns. Section 6 treats blocks joined through a shared nonlinear term, and Section 7 blocks joined through a shared output. Section 8 reads the Galois group of the map arithmetically, Section 9 topologically, and Section 10 analytically. The algorithms are probabilistic in the usual sense, and each correctness statement is proved.

2. PRELIMINARIES

This section fixes notation and collects the background used later: models and identifiability (Section 2.1), differential algebra (Section 2.2), input–output relations and the maps they define (Section 2.3), algebraic matroids (Section 2.4), fields of definition (Section 2.5), finite-dimensional algebras and resultants (Section 2.6), linear differential operators (Section 2.7), the transfer function of a linear model (Section 2.8), Galois groups of polynomials and thin sets (Section 2.9), cycle covers of digraphs (Section 2.10), Wronskians and experiments (Section 2.11), evaluation and interpolation (Section 2.12), reduction modulo primes and the Chebotarev density theorem (Section 2.13), and continuation, traces and Bézout’s theorem (Section 2.14). One small model runs through the section. Throughout, fields have characteristic zero unless a prime is named, and a property holds for a *generic* point if it holds outside a proper Zariski-closed set.

2.1. Models and identifiability. A *model* Σ is a system (1.1) with states $x = (x_1, \dots, x_n) \in \mathbb{C}^n$, inputs u , outputs $y_1, \dots, y_m$ and parameters $\theta \in \mathbb{C}^r$, in which f and g are rational over $\mathbb{Q}$. The initial state $x_0 = x(0)$ may be known or unknown; when it is unknown we count it among the unknowns. The *Lie derivative* along Σ ,

$$\mathcal{D}h = \sum_{i=1}^n f_i \frac{\partial h}{\partial x_i} + \sum_{j \geq 0} u^{(j+1)} \frac{\partial h}{\partial u^{(j)}},$$

gives the output derivatives as $y_i^{(j)} = \mathcal{D}^j g_i$ along every trajectory. At $t = 0$, each $y_i^{(j)}$ is therefore a rational function of the unknowns and finitely many input derivatives, and we regard it as such; we call it a *jet* of y_i , of order j . For a model with one output we write $y_j = y^{(j)}$, and ∂ for the derivation d/dt .

Two values of the unknowns are *indistinguishable* if they produce the same output, for generic inputs. For a value θ^* of the unknowns, let $\mathcal{F}(\theta^*)$ be the set of values indistinguishable from it. A function $h(\theta)$, and in particular a parameter θ_i , is *globally identifiable* if it takes one value on $\mathcal{F}(\theta^*)$ for generic θ^* , and *locally identifiable* if it takes finitely many. The number of values is its *identifiability degree* [1]. The identifiable functions form a subfield of $\mathbb{Q}(\theta)$.

Local identifiability has a rank test. Let $\mathcal{J}_N$ be the Jacobian of the jets of order at most N with respect to (θ, x_0) , at a generic point, with the input jets set to generic values. Its rank increases with N up to the first order at which it does not, and is constant from then on, by the argument of Lemma 3.4 below. Since the rank is at most $n + r$, it stabilises at an order $N_0 \leq n + r$. A parameter θ_i is locally identifiable exactly when it is algebraic over the field generated by the jets, that is, when the unit vector e_i lies in the row space of $\mathcal{J}_{N_0}$ [34].

Hypotheses of this kind are checked at random points. By the Schwartz–Zippel lemma, a nonzero polynomial of degree D vanishes at a point drawn uniformly from $S \times \dots \times S$, for a finite set $S \subset \mathbb{Q}$, with

probability at most $D/|S|$. An algorithm *verifies a statement at a random point* if it evaluates it, in exact arithmetic, at a rational point drawn from a large box.

Example 2.1. Let $\dot{x} = -\theta x$ and $y = x$, so that $n = r = 1$. The jets are $y^{(j)} = (-\theta)^j x_0$. The Jacobian of $(y, \dot{y})$ with respect to (θ, x_0) is

$$\begin{pmatrix} 0 & 1 \\ -x_0 & -\theta \end{pmatrix},$$

of rank two, so the rank stabilises at order one and θ is locally identifiable. Indeed $\theta = -\dot{y}/y$ is globally identifiable.

2.2. Differential algebra. Let $\mathbb{Q}(\theta)\{y\}$ be the ring of polynomials over $\mathbb{Q}(\theta)$ in the symbols $y_i^{(j)}$, with the derivation that sends each symbol to the next and is zero on $\mathbb{Q}(\theta)$; the rings $\mathbb{Q}(\theta)\{x, y\}$ and so on are defined in the same way. Inputs, when present, are adjoined with their derivatives to the coefficient field, so that rankings, leaders and characteristic sets concern the outputs only.

A *ranking* is a total order on the symbols $y_i^{(j)}$ in which every symbol lies below its derivative and $v < w$ implies $v' < w'$, where $'$ denotes the derivative. We use the *orderly* ranking, which orders by j and then by i . For a differential polynomial p , its *leader* is the highest-ranked symbol in it, its *initial* is its leading coefficient in the leader, and its *separant* is its partial derivative by the leader. A polynomial q is *reduced* with respect to p if q involves no proper derivative of the leader of p and has lower degree than p in that leader. A finite set A of differential polynomials is *autoreduced* if each element is reduced with respect to the others. The leaders of an autoreduced set are derivatives of distinct outputs, since of two derivatives of one output, one is a derivative of the other. By Ritt's reduction, for an autoreduced set A and a differential polynomial q there are a product h of powers of the initials and separants of A and a differential polynomial ρ , reduced with respect to every element of A , such that $hq - \rho$ lies in the differential ideal $[A]$ generated by A [32, 20].

A *characteristic set* of a differential ideal P is an autoreduced subset of P of least rank, in the order of Ritt [32, 20]. An autoreduced subset $A \subseteq P$ is a characteristic set exactly when P contains no nonzero element reduced with respect to every element of A [20]. If P is prime and A is a characteristic set, let H_A be the product of the initials and separants of A . Then P is the saturation $[A] : H_A^\infty$, and by Rosenfeld's lemma, the elements of P involving no proper derivative of a leader form the ideal $(A) : H_A^\infty$ of the polynomial ring they live in [20, 5].

Write $f = F/Q$ and $g = G/Q$ with F and G polynomial and Q a common denominator. The differential ideal

$$I_\Sigma = [Q\dot{x} - F, Qy - G] : Q^\infty \subseteq \mathbb{Q}(\theta)\{x, y\}$$

is prime, and it consists of the differential polynomials that vanish on every trajectory [18, 29]. Its elimination ideal $P = I_\Sigma \cap \mathbb{Q}(\theta)\{y\}$ is the *input-output ideal* of Σ , and its elements are the *input-output relations*. For fixed θ , the jets $y_i^{(0)}, \dots, y_i^{(n)}$ are $n+1$ functions of the n coordinates of x_0 , so P contains a nonzero element involving the jets of y_i alone. Such an element is reduced with respect to every autoreduced set whose leaders are derivatives of other outputs. By the criterion above, a characteristic set of P for the orderly ranking therefore has exactly one element whose leader is a derivative of y_i , for each i .

Ovchinnikov, Pogudin and Thompson show that the coefficients of a suitably normalised characteristic set of P , a *characteristic presentation*, generate a subfield of the field of identifiable functions, equal to it under standard hypotheses [29]. In Example 2.1, P is the differential ideal generated by $\dot{y} + \theta y$, and $\{\dot{y} + \theta y\}$ is a characteristic set, with leader $\dot{y}$ and with initial and separant equal to 1. Its normalised coefficient θ is identifiable, as the theorem predicts.

2.3. Input-output relations and the maps they define. For an autonomous model with one output, the input-output relation of least order has the form $R(\theta; y_0, \dots, y_j) = 0$, where j is the least index for which y_j is algebraic over $\mathbb{Q}(\theta)(y_0, \dots, y_{j-1})$, the y_i being regarded as functions of the initial states. It is irreducible, and unique up to a factor in $\mathbb{Q}(\theta)^\times$.

Normalising a relation by one of its coefficients makes its other coefficients rational functions of θ . Collecting them for a fixed set of relations gives a rational *coefficient map* $\gamma: \mathbb{C}^r \dashrightarrow \mathbb{C}^M$. For a characteristic presentation, these coefficients generate a subfield of the field of identifiable functions, equal to it under standard hypotheses [29]. Two indistinguishable values satisfy the same relations, so

$$\mathcal{F}(\theta^*) \subseteq \gamma^{-1}(\gamma(\theta^*)) = \{\theta \in \mathbb{C}^r : \gamma(\theta) = \gamma(\theta^*)\},$$

and a parameter that takes one value on the right-hand side for generic θ^* is globally identifiable. In Section 6, which decides identifiability from input–output relations, we work with the right-hand side and write $\mathcal{F}(\theta^*)$ for it.

A second map needs no relations. The *Taylor map* $T_N = (y^{(j)}(0))_{j \leq N}$ sends the unknowns to the output jets at $t = 0$, and is built by Lie differentiation alone; its preimages determine the same identifiable functions once N is at least the bound of [18, Thm. 3.16].

2.4. Algebraic matroids. For a finite set E of elements of a field extension of $\mathbb{Q}$, the *algebraic matroid* on E has as independent sets the subsets that are algebraically independent over $\mathbb{Q}$ [33, 30]. When the elements of E are rational functions of unknowns z , the rank of a subset is the rank of its Jacobian with respect to z at a generic point. An element e *depends* on a set S if e is algebraic over $\mathbb{Q}(S)$, that is, if adding e to S does not raise the rank; the elements that depend on S form its *closure*. In this language, the rank test of Section 2.1 says that θ_i is locally identifiable exactly when it lies in the closure of the set of jets.

A *circuit* is a minimal dependent set. For a circuit C , the ideal of polynomial relations among the elements of C is prime and principal, generated by an irreducible *circuit polynomial* p_C that involves every element of C and is unique up to scale [33]. If B is a basis and $e \notin B$, then $B \cup \{e\}$ contains a unique circuit, the *fundamental circuit* of e , and it contains e [30]. For any order on E , the *greedy* procedure, which takes each element in turn and keeps it when it does not depend on the elements already kept, produces a basis B , and every element outside B depends on the elements of B that precede it. For $S \subseteq E$, the *contraction* M/S is the algebraic matroid on $E \setminus S$ over the field $\mathbb{Q}(S)$; its circuits are the minimal nonempty sets of the form $C \setminus S$ with C a circuit of M [30].

In Example 2.1, the functions $\theta, y, \dot{y}, \ddot{y}$ of (θ, x_0) have rank two, and every three of them are dependent, so their matroid is uniform of rank two on four elements. The circuit polynomials are

$$\dot{y} + \theta y, \quad \ddot{y} - \theta^2 y, \quad \ddot{y} + \theta \dot{y}, \quad y\ddot{y} - \dot{y}^2.$$

The last involves no parameter. It is a relation among the jets alone, valid for every θ , and it is obtained by eliminating θ from the first two. Contracting θ gives the matroid of $y, \dot{y}, \ddot{y}$ over $\mathbb{Q}(\theta)$, which is uniform of rank one.

2.5. Fields of definition. Let $k \subseteq k'$ be fields and I an ideal of a polynomial ring $k'[z]$ in finitely many variables z . We say that I is *defined over* k if it is generated by polynomials with coefficients in k . For a fixed term order, I has a unique reduced Gröbner basis, and I is defined over k exactly when the coefficients of this basis lie in k , since Buchberger’s algorithm, run on generators with coefficients in k , never leaves k [6]. So I has a smallest field of definition, generated by these coefficients. If I is defined over k , then so is every elimination ideal $I \cap k'[z']$, for z' a subset of the variables, and so is every saturation $I : h^\infty$ with $h \in k[z]$, since both are computed by Gröbner bases from generators over k [6]. In particular, if a principal ideal (q) is defined over k , then q divided by any one of its nonzero coefficients has all its coefficients in k .

2.6. Finite-dimensional algebras and resultants. Let K be a field and J an ideal of $K[L_1, \dots, L_m]$ generated by $p_1, \dots, p_m$ with $p_i \in K[L_i]$ monic of positive degree δ_i . The leading monomials $L_i^{\delta_i}$ are pairwise coprime, so the p_i form a Gröbner basis of J for every term order, by Buchberger’s first criterion [6]. Consequently a polynomial of degree less than δ_i in each L_i lies in J only if it is zero, and $A = K[L_1, \dots, L_m]/J$ has dimension $\prod_i \delta_i$ over K . When each p_i is squarefree, $A = \bigotimes_i K[L_i]/(p_i)$ is reduced, since tensor products of reduced algebras over a perfect field are reduced. A reduced finite-dimensional K -algebra is the product of finite field extensions of K , one for each minimal prime, and in it every prime is maximal.

For polynomials $f = \sum_{i=0}^a \alpha_i u^i$ and $g = \sum_{i=0}^b \beta_i u^i$ over a commutative ring, the *Sylvester resultant* $\text{Res}_{a,b}(f, g)$ of formal degrees (a, b) is the determinant of the $(a + b) \times (a + b)$ Sylvester matrix of their coefficients [6]. It lies in the ideal generated by f and g , so it vanishes whenever they have a common root in a domain containing their coefficients. If $\alpha_a \neq 0$ and f has roots $\xi_1, \dots, \xi_a$, then

$$\text{Res}_{a,b}(f, g) = \alpha_a^b \prod_{i=1}^a g(\xi_i);$$

in particular $\text{Res}_u(f, g) = \prod_i g(\xi_i)$ when f is monic. If instead f has degree $a' < a$, the formal leading coefficients of f vanish, and $\text{Res}_{a,b}(f, g) = \pm \beta_b^{a-a'} \text{Res}_{a',b}(f, g)$.

Let $\ell = \sum_i \lambda_i L_i$ with $\lambda_i \in \mathbb{Q}$. Multiplication by L_i on $K[L_i]/(p_i)$ has characteristic polynomial p_i , so multiplication by ℓ on the tensor product A has characteristic polynomial

$$\chi_\ell(T) = \prod_{\xi} \left(T - \sum_i \lambda_i \xi_i \right),$$

the product over all tuples $\xi = (\xi_1, \dots, \xi_m)$ with $p_i(\xi_i) = 0$, counted with multiplicity. By the product formula, χ_ℓ is computed without factoring as an iterated resultant: set $h_m = T - \ell$ and $h_{i-1} = \text{Res}_{L_i}(p_i, h_i)$; then $h_0 = \chi_\ell$. When each p_i is squarefree, the tuples are distinct points, and for generic $\lambda = (\lambda_i)$ the values $\sum_i \lambda_i \xi_i$ at distinct points are distinct. Then ℓ generates each factor field of A , and its images in distinct factors have distinct minimal polynomials.

Irreducibility is tested at specialisations. Let F be a polynomial in T whose coefficients are polynomials in some variables w . If F is primitive and factors over the field $\mathbb{Q}(w)$, then by Gauss's lemma it factors into polynomials in T with coefficients in $\mathbb{Q}[w]$, and at a point where the leading coefficient of F does not vanish the factors keep their degrees. So irreducibility of the specialised polynomial implies irreducibility of F . The same holds for reduction modulo a prime not dividing the leading coefficient.

2.7. Linear differential operators. Over a field of constants, such as $\mathbb{Q}(\theta)$, the linear differential operators form a commutative polynomial ring in ∂ , so determinants and adjugates of matrices over it behave as usual: for a square matrix A over $\mathbb{Q}(\theta)$,

$$\text{adj}(\partial I - A) (\partial I - A) = \det(\partial I - A) I.$$

Over a differential field $(\mathcal{K}, \partial)$ whose derivation is not zero, the operators $\mathcal{K}[\partial]$ form a noncommutative ring with $\partial c = c\partial + \partial(c)$ for $c \in \mathcal{K}$. It has a left and a right division algorithm, so any operators $\mathcal{L}_1, \dots, \mathcal{L}_s$ have a *least common left multiple*: the monic operator of least order that is a left multiple of each [27, 38]. Its order is at most the sum of the orders of the $\mathcal{L}_i$, and it annihilates every element annihilated by some $\mathcal{L}_i$.

2.8. Linear models and transfer functions. Let $\dot{x} = Ax$ and $y = c^\top x$ be a linear, input-free model with one output, with A an $n \times n$ matrix and $x(0) = x_0$. Its output is $y(t) = c^\top e^{At} x_0$, with Laplace transform

$$Y(s) = c^\top (sI - A)^{-1} x_0 = \frac{N(s)}{D(s)}, \quad D = \det(sI - A), \quad N = c^\top \text{adj}(sI - A) x_0.$$

The polynomial D is monic of degree n , and since $\text{adj}(sI - A) = s^{n-1}I + \dots$, the polynomial N has degree less than n and coefficient $c^\top x_0$ at s^{n-1} . An analytic output is determined by its Laplace transform, so two values of the unknowns produce the same output if and only if they give the same Y . When A is block diagonal with blocks A_b , Y is the sum of the transfer functions N_b/D_b of the blocks.

Suppose D is squarefree. Then Y has the partial fraction decomposition

$$Y(s) = \sum_{D(\zeta)=0} \frac{\rho_\zeta}{s - \zeta}, \quad \rho_\zeta = \frac{N(\zeta)}{D'(\zeta)},$$

which is unique. So $N = \sum_\zeta \rho_\zeta \prod_{\zeta' \neq \zeta} (s - \zeta')$, the coefficient $c^\top x_0$ of s^{n-1} in N is $\sum_\zeta \rho_\zeta$, and N/D is in lowest terms exactly when every residue ρ_ζ is nonzero.

2.9. Galois groups of polynomials and thin sets. Let $\Delta \in \mathbb{Q}[s]$ be squarefree, with Galois group G_Δ acting on its roots. If $\Delta = \prod_c \Delta_c$ with each $\Delta_c \in \mathbb{Q}[s]$, then G_Δ preserves the root set Z_c of each factor, and so embeds in $\prod_c \text{Sym}(Z_c)$. If $h \in \mathbb{Q}(s)$ is defined at the roots, then $g(h(\zeta)) = h(g(\zeta))$ for every $g \in G_\Delta$ and every root ζ . For quadratic factors with discriminants δ_c , Kummer theory gives $G_\Delta = \prod_c S_2$ exactly when no nonempty product of the δ_c is a square in $\mathbb{Q}$.

A subset of $\mathbb{Q}^r$ is *thin* if it is contained in a finite union of proper Zariski-closed subsets and of sets $\pi(Y(\mathbb{Q}))$, where $\pi: Y \rightarrow \mathbb{A}^r$ is a dominant, generically finite map of degree at least two from an irreducible variety [35]. Hilbert's irreducibility theorem states that if a polynomial in s with coefficients in $\mathbb{Q}(\theta)$ has Galois group G over $\mathbb{Q}(\theta)$, then its specialisation at θ^* has Galois group G over $\mathbb{Q}$ for every $\theta^* \in \mathbb{Q}^r$ outside a thin set [35]. A thin set contains few integer points: of the $(2H + 1)^r$ points of $\mathbb{Z}^r$ with coordinates of absolute value at most H , it contains $O(H^{r-1/2} \log H)$ [35]. So a random integer point of a large box lies outside a given thin set with high probability.

2.10. Cycle covers. A digraph on the vertices $1, \dots, B$ may have loops. A *cycle cover* is a permutation σ of the vertices such that $b \rightarrow \sigma(b)$ is an edge for every b ; equivalently, a partition of the vertices into directed cycles, a loop counting as a cycle of length one. If every vertex has a loop, the identity is a cycle cover, and a cycle cover other than the identity exists if and only if the digraph has a directed cycle of length at least two: such a cover contains one, and such a cycle, completed by the loops at the other vertices, is one.

2.11. Wronskians and experiments. Along one trajectory with analytic inputs, the outputs are analytic near $t = 0$, and the functions of t generated by the outputs, the inputs and their derivatives lie in the differential field of meromorphic functions on a small disc. Its constants are the constant functions, and they include the parameter values. The Wronskian criterion compares linear dependence over the constants with a rank. It needs this setting: for merely smooth functions, a vanishing Wronskian does not imply linear dependence, as Peano's pair t^2 and $t|t|$ shows.

Theorem 2.2 ([3, 19]). *Let $\mathcal{K}$ be a differential field of characteristic zero with field of constants C , and let $t_1, \dots, t_s \in \mathcal{K}$. Then the rank of the Wronskian matrix $W = (t_j^{(i)})_{0 \leq i < s, 1 \leq j \leq s}$ equals the dimension of the C -span of $t_1, \dots, t_s$.*

Single-experiment identifiability asks what one generic trajectory determines, and *multi-experiment* identifiability what several independent trajectories with the same parameters determine. The latter can identify more, and the coefficients of the input–output relations are in general identifiable only in this weaker sense [28, 29]. In Example 2.1, the terms $\dot{y}$ and y of $\dot{y} + \theta y$ satisfy $\dot{y} = -\theta y$ along every trajectory, so their Wronskian matrix

$$\begin{pmatrix} \dot{y} & y \\ \ddot{y} & \dot{y} \end{pmatrix}$$

has rank one. Up to scale, the only constant relation between them is the one with coefficients $(1, \theta)$, so one trajectory determines θ .

2.12. Evaluation and interpolation. A polynomial relation of degree at most D among given functions is found as the kernel of the matrix of values of the monomials of degree at most D at sample points. Computations are done modulo primes p . A prime is *bad* for a computation if it divides a denominator that occurs, or a nonzero integer that the computation tests for zero; a computation involves finitely many such integers, so only finitely many primes are bad. A rational number a/b with $|a| \leq N$ and $0 < b \leq D'$ is determined by its residue modulo M whenever $2ND' < M$, and rational reconstruction recovers it by the extended Euclidean algorithm; residues modulo several primes are combined into one modulo their product by the Chinese remainder theorem [39]. A result obtained this way is certified by checking it at points not used to compute it.

2.13. Reduction modulo primes and the Chebotarev density theorem. Let Z be a finite set of points cut out by polynomials with rational coefficients, and let E be the field generated over $\mathbb{Q}$ by the coordinates of its points, a Galois extension whose group permutes $Z(\overline{\mathbb{Q}})$. We say that Z has *good reduction* at a prime p if the coefficients of its defining polynomials are p -integral, the points of $Z(\overline{\mathbb{Q}})$ are integral at the primes above p , and their reductions are distinct simple points of the reduced system, which has no other points over $\overline{\mathbb{F}}_p$. The reduction is then étale, and all but finitely many primes are good.

At a good prime, a *Frobenius element* $\text{Frob}_p \in \text{Gal}(E/\mathbb{Q})$ acts on $Z(\overline{\mathbb{Q}})$, and it is well defined up to conjugacy. The $\mathbb{F}_{p^v}$ -points of the reduction are exactly the points fixed by Frob_p^v . The *Chebotarev density theorem* states that for each conjugacy class C of $\text{Gal}(E/\mathbb{Q})$, the primes with $\text{Frob}_p \in C$ have natural density $|C|/|\text{Gal}(E/\mathbb{Q})|$ [37]. We also use *Burnside's lemma*: the average over a finite permutation group of the number of fixed points is the number of its orbits.

2.14. Continuation, traces and Bézout's theorem. Along a path in the base of a map that avoids its branch points, the points of a preimage continue as analytic functions of the path parameter; numerically, this is homotopy continuation, and the continued points are called *sheets*. The classical trace test [36, 21, 14] applies to a curve cut by a pencil of parallel hyperplanes in the space where its points live: the sum of the points of a set of sheets is affine-linear in the pencil parameter exactly when the set is the whole of the cut. We also use Bézout's theorem [11]: a system of polynomial equations of degrees $\delta_1, \dots, \delta_s$ has at most $\prod_i \delta_i$ isolated solutions, and the components of the set it cuts out have total degree at most $\prod_i \delta_i$.

3. INPUT–OUTPUT RELATIONS AS CIRCUIT POLYNOMIALS

In this section Σ is autonomous, without inputs; for models with inputs, the input jets are added to the ground set below as free coordinates, and the same arguments apply.

3.1. The jet matroid.

Definition 3.1. Let $N \geq 0$. The *jet matroid* of Σ at order N is the algebraic matroid on the ground set

$$E_N = \{\theta_1, \dots, \theta_r\} \cup \{y_i^{(j)} : 1 \leq i \leq m, 0 \leq j \leq N\},$$

each element viewed as a function of (θ, x_0) , so that θ_l is the l -th coordinate function. Its rank function is the rank of the matrix

$$\begin{pmatrix} I_r & 0 \\ \frac{\partial y^{(\leq N)}}{\partial \theta} & \frac{\partial y^{(\leq N)}}{\partial x_0} \end{pmatrix}.$$

The identity block is essential. Without it the matroid is that of the jets alone, and a relation among jets alone would have to hold for every value of θ , like the last circuit polynomial in Section 2.4. Contracting the parameters instead gives the algebraic matroid of the jets over $\mathbb{Q}(\theta)$, whose circuits are the minimal nonempty sets $C \setminus \Theta$, for C a circuit of the jet matroid and Θ the set of parameters.

Proposition 3.2. *Let $C \subseteq E_N$ be a circuit containing at least one jet. Then $p_C(\theta; y^{(\cdot)}) = 0$ holds on every trajectory of Σ at every time. Hence p_C is an input–output relation.*

Proof. By definition p_C vanishes identically as a function of (θ, x_0) when each jet is replaced by its expression at $t = 0$. Since Σ is autonomous, the jets at time t along the trajectory from x_0 are the jets at time 0 along the trajectory from $x(t)$. The identity at $(\theta, x(t))$ gives the relation at time t . $\square$

3.2. Leaders and fundamental circuits. Order E_N by listing the parameters first and then the jets by increasing order j , with the outputs in a fixed order within each j . On the jets this is the orderly ranking of Section 2.2. Build a basis B greedily: an element enters B when it is independent of the elements already in B .

Proposition 3.3. *For each output y_i , let $y_i^{(k_i)}$ be the first jet of y_i that does not enter B . Then $B \cup \{y_i^{(k_i)}\}$ contains a unique circuit C_i , and C_i contains $y_i^{(k_i)}$. Every other element of C_i precedes $y_i^{(k_i)}$ in the order, so C_i contains no leader $y_j^{(k_j)}$ with $j \neq i$ and no jet of order above k_i . The circuit polynomial p_{C_i} is an input–output relation in which y_i appears to order exactly k_i , the least order at which a jet of y_i is algebraic over the elements preceding it.*

Proof. The element $e = y_i^{(k_i)}$ depends on the elements of B that precede it, so $B \cup \{e\}$ is dependent. Its fundamental circuit C_i is unique and contains e (Section 2.4). The elements of B that follow e play no part in the dependency, since e already depends on the preceding ones; so every element of C_i other than e precedes it. A leader $y_j^{(k_j)}$ with $j \neq i$ is not in B , so it is not in C_i . Proposition 3.2 gives the relation. Every jet of y_i of order below k_i entered B , so each is algebraically independent of the elements preceding it, which gives the last statement. $\square$

We call $y_i^{(k_i)}$ the *leader* of y_i and write $p_i = p_{C_i}$.

Lemma 3.4. *If $y_i^{(k)}$ depends on the elements preceding it, then so does $y_i^{(j)}$ for every $j > k$. Hence the greedy basis contains exactly the jets $y_i^{(0)}, \dots, y_i^{(k_i-1)}$ of each output, and an order N with $N \geq \max_i k_i$ suffices.*

Proof. It suffices to treat $j = k + 1$. Let q be the minimal polynomial of $e = y_i^{(k)}$ over the field generated by the elements preceding it, cleared of denominators, and let $S = \partial q / \partial e$ be its separant. Differentiating $q = 0$ along trajectories gives $S y_i^{(k+1)} + Q = 0$, where Q involves only the derivatives of the other elements occurring in q . These are parameters, whose derivative is zero, and jets that precede e , whose derivatives precede $y_i^{(k+1)}$ because the order is a ranking. Since q is irreducible and S is nonzero of lower degree in e , S is not a multiple of q , so S does not vanish identically on the jets. Hence $y_i^{(k+1)} = -Q/S$ depends on the elements preceding it. $\square$

By Lemma 3.4, no jet $y_j^{(l)}$ with $l \geq k_j$ lies in B . So p_i involves no leader other than its own, and no derivative of one. This is the defining property of an autoreduced set, and we now show that more is true.

Example 3.5. Let $\dot{x}_1 = ax_1 - bx_1x_2$, $\dot{x}_2 = -cx_2 + dx_1x_2$ and $y = x_1$. The greedy basis is $\{a, b, c, d, y, \dot{y}\}$, and the leader is $\dot{y}$. The set $\{a, c, d, y, \dot{y}\}$ has rank 5, and adding $\dot{y}$ leaves the rank at 5, so the fundamental circuit is $C = \{a, c, d, y, \dot{y}\}$. Its circuit polynomial is

$$p_C = y\dot{y} - \dot{y}^2 + c y\dot{y} - d y^2\dot{y} - ac y^2 + ad y^3,$$

which vanishes identically on the jets of the model. The parameter b is not in C , so no coefficient of the relation involves it. This agrees with the scaling $x_2 \mapsto \lambda x_2$, $b \mapsto b/\lambda$, which leaves y unchanged.

3.3. A characteristic set. Let P be the input–output ideal of Σ , let K be the field generated over $\mathbb{Q}(\theta)$ by the jets $y_i^{(j)}$ with $j < k_i$, and write $L_i = y_i^{(k_i)}$. By Lemma 3.4 the generators of K are the jets in B , so they are algebraically independent over $\mathbb{Q}(\theta)$. Let J be the ideal of $K[L_1, \dots, L_m]$ generated by $p_1, \dots, p_m$.

Theorem 3.6. *The relations $p_1, \dots, p_m$ form an autoreduced subset of P for the orderly ranking. They form a characteristic set of P if and only if J is prime. In particular, for a single output, p_1 alone is a characteristic set of P .*

Proof. **Claim 1: autoreduced.** Each p_i lies in P by Proposition 3.2, and its leader is L_i , since every other element of C_i precedes L_i . By the remark after Lemma 3.4, p_i involves no L_j with $j \neq i$ and no derivative of one, so p_i is reduced with respect to p_j .

Claim 2: each p_i is an irreducible element of $K[L_i]$. The elements of C_i other than L_i lie in B , so they are parameters or generators of K , and $p_i \in K[L_i]$. The polynomial p_i is irreducible and involves L_i , so by Gauss’s lemma it is irreducible over the field generated by the other elements of C_i . The field K is obtained from that field by adjoining the remaining elements of B , which are algebraically independent over it, and irreducibility is preserved under such an extension.

Claim 3: the kernel of evaluation. Let $\varphi : K[L_1, \dots, L_m] \rightarrow \mathbb{Q}(\theta, x_0)$ send each jet to its expression as a function. It is well defined, because the generators of K are algebraically independent functions. Its kernel is a proper prime ideal containing J , and it is the localisation of the set of elements of P that involve only the jets $y_i^{(j)}$ with $j \leq k_i$.

Claim 4: if J is prime, the p_i form a characteristic set. The initials of the p_i are nonzero elements of K , so the p_i may be taken monic, and the algebra $K[L_1, \dots, L_m]/J$ is finite-dimensional (Section 2.6). So the prime J is maximal and equals $\ker \varphi$. Let $q \in P$ be reduced with respect to every p_i . Then q involves no jet of y_i above L_i and has degree less than $\deg_{L_i} p_i$ in each L_i , so $q \in \ker \varphi = J$. By Section 2.6, $q = 0$. So P contains no nonzero element reduced with respect to the p_i , and they form a characteristic set (Section 2.2).

Claim 5: if the p_i form a characteristic set, J is prime. By Rosenfeld's lemma, the elements of P involving no proper derivative of a leader form the ideal $(p_1, \dots, p_m) : H^\infty$, where H is the product of the initials and separants. None of the nonzero polynomials in the generators of K lies in P , so localising at them and using Claim 3 gives $\ker \varphi = J : H^\infty$ in $K[L_1, \dots, L_m]$. The initials are nonzero elements of K , hence units. The separant of p_i is a unit modulo p_i in $K[L_i]$, because p_i is irreducible by Claim 2 and so coprime to its derivative. Hence H is a unit modulo J , so $J : H^\infty = J$ and $J = \ker \varphi$ is prime. $\square$

Corollary 3.7. *Normalise each p_i by one of its coefficients. Then its coefficients are identifiable functions.*

Proof. Let $k_P \subseteq \mathbb{Q}(\theta)$ be the field generated by the normalised coefficients of a characteristic presentation A of P . It consists of identifiable functions [29]. Let $q \in P$ involve only jets of order at most N . Ritt's reduction (Section 2.2) gives $hq - \rho$ in the ideal generated by the derivatives of A of order at most N , with ρ reduced; then $\rho \in P$, so $\rho = 0$ by the criterion for characteristic sets. Hence the intersection of P with a polynomial ring in finitely many jets is obtained, from generators with coefficients in k_P , by a saturation and an elimination, and by Section 2.5 it is defined over k_P . So the ideal of relations over $\mathbb{Q}(\theta)$ among the jets in C_i is defined over k_P . This ideal is prime of height one, hence principal, and it is generated by p_i , which is irreducible over $\mathbb{Q}(\theta)$ by Gauss's lemma. By Section 2.5, the normalised p_i has its coefficients in k_P . $\square$

3.4. Computing the circuit. The matroid is read at a random point, modulo a prime p . Evaluation at a point and reduction modulo p can only lower the rank of a matrix. Hence an independence observed at the point holds generically, and a dependency observed at the point is generic unless the point lies in a proper Zariski-closed set, which a random point avoids with high probability (Section 2.1). The relation computed below is afterwards checked at points it has not seen, and this is what confirms the dependency. Interpolation. Fix θ^* and vary x_0 . The jets of C_i then satisfy the specialised relation $p_i(\theta^*, \cdot)$. Let M_D be the matrix of values of the monomials of degree at most D in these jets at sampled points.

Proposition 3.8. *Let θ^* be generic, and suppose $p_i(\theta^*, \cdot)$ is irreducible of degree D_0 in the jets. Then the least D with $\ker M_D \neq 0$ is D_0 , and at $D = D_0$ the kernel is spanned by the coefficient vector of $p_i(\theta^*, \cdot)$, provided the sample points avoid a proper Zariski-closed set.*

Proof. For generic θ^* , the values of the jets of C_i at θ^* fill a hypersurface, contained in the zero set of $p_i(\theta^*, \cdot)$. That zero set is irreducible by hypothesis, so the two are equal, and the relations among the jets at θ^* form the ideal generated by $p_i(\theta^*, \cdot)$. A polynomial of degree at most D in this ideal is a multiple of the generator, so none exists for $D < D_0$, and those of degree D_0 are its scalar multiples. For sample points outside a proper closed set, the kernel of M_D is exactly the space of such polynomials. $\square$

This fixes the monomial support of the relation. Normalising by a pivot monomial, each coefficient ratio $\kappa_\alpha(\theta) = c_\alpha/c_{\text{piv}}$ is a rational function of θ . The numerator polynomials P_α are fitted jointly from the linear conditions $P_\alpha(\theta) - \kappa_\alpha(\theta) P_{\text{piv}}(\theta) = 0$ over sampled θ . The degree is scanned upward to the first cell of nullity one, the coefficients are lifted from $\mathbb{F}_p$ to $\mathbb{Q}$ by the Chinese remainder theorem and rational reconstruction, and the result is verified at unseen points (Section 2.12). No division and no symbolic elimination occur, and the cost grows with the *support* of the relation, not with the number of variables.

Algorithm 1 Input–output relations from the jet matroid**Input:** Σ ; an order N at which the jet Jacobian’s rank has stabilised**Output:** one relation per output, verified at unseen points, or a named bound

- 1: evaluate the jet Jacobian of Definition 3.1 at a random point modulo p
- 2: build B greedily in jet order; for each output, record its leader and C_i (Proposition 3.3)
- 3: **for** each output y_i **do**
- 4: fix θ^* , vary x_0 , and find the support by the first nullity-one degree (Proposition 3.8)
- 5: fit the coefficients in θ jointly; lift by CRT and rational reconstruction
- 6: **if** a degree bound is hit **then** use resultants along a greedy order
- 7: verify at unseen points, and against the order from the rank test
- 8: **end for**

Resultants along an order. When the degree is too large for the sample budget, the relation is computed instead by eliminating one variable at a time with a Sylvester resultant. Each resultant lies in the ideal generated by its arguments (Section 2.6), so it vanishes when the jets are substituted and is an input–output relation. Since P is prime, one of its irreducible factors lies in P , and that factor is selected by testing membership at random points. The mechanism is that of combinatorial resultants in rigidity theory [24]. Their combinatorics, which rests on the inductive structure of rigidity circuits, does not transfer, and we choose the elimination order greedily by the least degree of the next resultant. The two routes fail differently: interpolation degrades with the degree, and resultants with the number of variables.

4. NON-PRIME INPUT–OUTPUT IDEALS

In this section $R_1, \dots, R_m$ are the relations $p_1, \dots, p_m$ of Section 3, or more generally elements of P with the same leaders L_i , each squarefree in its leader and involving no other leader and no derivative of one; K and $J = \langle R_1, \dots, R_m \rangle$ are as in Section 3.3. By Corollary 3.7, the coefficients of the p_i are identifiable, so a positive membership answer over the field they generate is sound. What is not automatic is that J is the right ideal: by Theorem 3.6, the p_i form a characteristic set exactly when J is prime. Each R_i is a norm over the branches of an inversion of the output map, and when two of them are quadratic over the same extension, J is the intersection of several prime ideals. Only one of these carries the trajectories of Σ .

Example 4.1. Let Σ have states x_1, x_2 , parameters b, e , outputs $y_1 = x_1 + 2x_2$ and $y_2 = x_1x_2$, and

$$\dot{x}_1 = bx_1 - 2y_1 - 2e(x_1 - 2x_2), \quad \dot{x}_2 = -bx_2 + y_1 + e(x_1 - 2x_2).$$

The output map has two branches, exchanged by the sign of $\tau = x_1 - 2x_2 = \pm\sqrt{y_1^2 - 8y_2}$. Then $\dot{y}_1 = b\tau$ and $\dot{y}_2 = y_1\tau + e\tau^2$. The leaders are $\dot{y}_1$ and $\dot{y}_2$, and the circuit polynomials are the norms over the two branches,

$$R_1 = \dot{y}_1^2 - b^2(y_1^2 - 8y_2), \quad R_2 = (\dot{y}_2 - e(y_1^2 - 8y_2))^2 - y_1^2(y_1^2 - 8y_2),$$

which involve b only through b^2 . Eliminating τ between the two equations instead gives $b(\dot{y}_2 - e(y_1^2 - 8y_2)) - y_1\dot{y}_1 = 0$, which records how the branches pair up and involves b itself. It is reduced with respect to R_1 and R_2 , so J is not prime. Hence b is globally identifiable, but membership over the coefficients of R_1 and R_2 leaves it undecided, and a count of the preimage of those coefficients gives it degree two.

4.1. Primality and components. The initials of the R_i are nonzero elements of K , so the R_i may be taken monic. Then the ring $A = K[L_1, \dots, L_m]/J$ is finite-dimensional over K , and the R_i form a Gröbner basis of J (Section 2.6).

Lemma 4.2. For a generic $\ell = \sum_i \lambda_i L_i$ with $\lambda_i \in \mathbb{Q}$, let χ_ℓ be the characteristic polynomial of multiplication by ℓ on A . Then J is prime if and only if χ_ℓ is irreducible over K . More precisely, if $\chi_\ell = \prod_j F_j$ with the F_j irreducible, then the minimal primes of J are $P_j = J + \langle F_j(\ell) \rangle$.

Proof. By Section 2.6, A is reduced and is a product $\prod_j A_j$ of finite field extensions of K , one for each minimal prime. By the same section, for generic ℓ the image of ℓ generates each A_j over K , and the images in distinct factors have distinct minimal polynomials. Hence $\chi_\ell = \prod_j \chi_{\ell,j}$, with $\chi_{\ell,j}$ the minimal polynomial of ℓ in A_j , irreducible and pairwise distinct. The element $\chi_{\ell,j}(\ell)$ vanishes in A_j and is a unit in every A_i with $i \neq j$, so it generates the kernel of $A \rightarrow A_j$. The number of factors is one exactly when J is prime. $\square$

In the algorithm, χ_ℓ is computed by iterated resultants (Section 2.6) at a random specialisation of K that preserves the leader degrees, and it is factored over $\mathbb{Z}$ and modulo two primes. Irreducibility at the specialisation implies irreducibility over K , by the last paragraph of Section 2.6. The algorithm adjoins $F_j(\ell)$ exactly as `StructuralIdentifiability.jl` adjoins an extra projection when primality fails [9]. It differs in what is done with the components.

For a minimal prime P_j of J , let $\mathcal{E}_j \subseteq \mathbb{Q}(\theta)$ be the field generated by the coefficients of its reduced Gröbner basis for a fixed term order, each basis element written as a quotient of polynomials in the jets over $\mathbb{Q}(\theta)$, in lowest terms, and normalised.

Proposition 4.3. *If $\theta_i \in \mathcal{E}_j$ for every minimal prime P_j of J , then θ_i is globally identifiable.*

Proof. Let φ be as in Claim 3 of the proof of Theorem 3.6. Its kernel is a proper prime ideal containing J . Since A is finite-dimensional, every prime containing J is maximal, and hence minimal over J , so $\ker \varphi = P_j$ for some j . As in the proof of Corollary 3.7, $\ker \varphi$ is the localisation of an elimination ideal of P , which is defined over the field k_P of that proof. By Section 2.5, its reduced Gröbner basis has coefficients in the field generated over k_P by the generators of K , and $\mathcal{E}_j \subseteq k_P$. The field k_P consists of identifiable functions [29], and $\theta_i \in \mathcal{E}_j$ by hypothesis. $\square$

A parameter that lies in $\mathcal{E}_j$ for some j and not for others is reported as a disagreement, not as a verdict. In Example 4.1, the two minimal primes contain $b(\dot{y}_2 - e(y_1^2 - 8y_2)) \mp y_1\dot{y}_1$, so both put b in their field, and b is globally identifiable.

5. WHICH QUESTION AN INPUT-OUTPUT VERDICT ANSWERS

Let $R = \sum_{j=1}^s c_j(\theta) \mu_j$ be an input-output relation, normalised, with μ_j monomials in the output and input jets. Along one trajectory, the functions $t_j = \mu_j(y(t), u(t))$ satisfy $\sum_j c_j(\theta) t_j = 0$, and the c_j are constants along it, in the sense of Section 2.11.

Definition 5.1. The *Wronskian corank* of R along a trajectory is $s - \text{rank } W$, where W is the Wronskian matrix of $t_1, \dots, t_s$. By Theorem 2.2, it is the dimension of the space of constant vectors a with $\sum_j a_j t_j = 0$ along the trajectory.

The corank is at least 1, since $(c_j(\theta))_j$ is such a vector. When it is 1 along a generic trajectory, one experiment determines the coefficient vector up to scale, and a verdict read from the coefficients concerns a single experiment. When it is larger, the terms satisfy further relations along each trajectory, whose coefficients depend on the initial condition. A verdict read from the coefficients then concerns several independent experiments [28, 29].

Proposition 5.2. *Let (θ^*, x_0^*) be a rational point, with rational input jets, at which the entries of W at $t = 0$ are defined, and let p be a prime at which their values are p -integral. Let W^* be these values reduced modulo p , and let W be the Wronskian along a generic trajectory. Then $\text{corank } W^* \geq \text{corank } W \geq 1$. In particular, if $\text{corank } W^* = 1$ then $\text{corank } W = 1$, and every verdict read from the coefficients of R is a single-experiment verdict.*

Proof. Every minor of W^* is the image of the corresponding minor of W under evaluation at (θ^*, x_0^*) followed by reduction modulo p . A nonzero minor can become zero under either operation, and a zero minor stays zero, so $\text{rank } W^* \leq \text{rank } W$. The bound $\text{corank } W \geq 1$ was noted above. $\square$

The converse direction carries no such guarantee: a measured corank of two or more may come from a special point or a bad prime. The algorithm therefore takes the minimum over several points and requires two primes to agree, and it treats a corank of two or more as probabilistic evidence. A measured corank of 0 contradicts Proposition 5.2 and is reported as a fault of the computation.

A relation that is a proper multiple of another always has a large corank.

Lemma 5.3. *Let R' be an input–output relation and f a polynomial in the jets with $q \geq 2$ monomials $v_1, \dots, v_q$. Suppose every product of some v_l with a monomial of R' occurs in $R = fR'$. Then the Wronskian corank of R along a generic trajectory is at least q . In particular, a relation of corank one is not such a multiple.*

Proof. Each $v_l R'$ vanishes along every trajectory, and by hypothesis its monomials are terms of R ; so its coefficient vector, whose entries lie in $\mathbb{Q}(\theta)$ and are constant along a trajectory, is a vector a as in Definition 5.1. The polynomials $v_1 R', \dots, v_q R'$ are linearly independent over $\mathbb{Q}(\theta)$, since $\sum_l \lambda_l v_l R' = (\sum_l \lambda_l v_l) R'$ vanishes only when every λ_l does. So their coefficient vectors are independent over $\mathbb{Q}(\theta)$, and they remain independent at a generic parameter value. $\square$

The square of a relation, when no two products of its terms cancel, is the case $f = R'$ of Lemma 5.3, and it gives a check on an implementation. For the relation $\dot{y} + \theta y$ of Example 2.1, the square $\dot{y}^2 + 2\theta y \dot{y} + \theta^2 y^2$ has three terms, all proportional to $e^{-2\theta t}$ along a trajectory, so its corank is two.

In the algorithm, the corank decides the route taken. With corank 1, every single-experiment test on the input–output coefficients is admitted. With corank 2 or more, those tests decline and a multi-experiment membership test is used instead. `StructuralIdentifiability.jl` computes the same Wronskian and warns when the corank exceeds one [9]. Proposition 5.2 is what allows the corank-one case to be treated as settled rather than probable.

6. LUR'E ELIMINATION

In this section we collapse a model of competing cycles to one scalar Lur'e relation per cycle, show that for every number of cycles the input–output relation is a single Sylvester resultant, determine what the relations cannot see, and, for two cycles, read the parameters off three coefficient slices of the resultant.

6.1. The class.

Definition 6.1. Let $k \geq 2$. A model is of *Lur'e type with k cycles* if its states are $x_1, \tilde{x}_1, \dots, x_k, \tilde{x}_k$, it is autonomous with output $y = x_1$, and

$$(6.1) \quad \dot{x}_b = \alpha_b(\tilde{x}_b - x_b) - \frac{V_b x_b}{D}, \quad \dot{\tilde{x}}_b = \beta_b(x_b - \tilde{x}_b), \quad D = 1 + \sum_{c=1}^k \frac{x_c}{K_c},$$

for $b = 1, \dots, k$, where $\alpha_b, \beta_b, V_b, K_b$ are nonzero rational functions of θ .

Each state x_b exchanges linearly with its partner $\tilde{x}_b$ and is removed through the one denominator D that all cycles share. Competitive Michaelis–Menten kinetics has this form: a removal rate $V_b^{\max} x_b / (K_b(1 + \sum_{c \neq b} x_c / K_c) + x_b)$ equals $V_b x_b / D$ with $V_b = V_b^{\max} / K_b$.

Example 6.2. The model *Pharm* of Demignot and Domurado [7], in the form of [22], is

$$\begin{aligned} \dot{x}_0 &= a_1(x_1 - x_0) - \frac{k_a n x_0}{D}, & \dot{x}_1 &= a_2(x_0 - x_1), \\ \dot{x}_2 &= b_1(x_3 - x_2) - \frac{k_c n x_2}{D}, & \dot{x}_3 &= b_2(x_2 - x_3), \end{aligned}$$

with $D = k_a k_c + k_a x_0 + k_c x_2$, output $y = x_0$, and unknown parameters $a_1, a_2, b_1, b_2, k_a, k_c, n$. Dividing D by $k_a k_c$ shows that it is of Lur'e type with two cycles, (x_0, x_1) and (x_2, x_3) , with $K_1 = k_c, K_2 = k_a, V_1 = n/k_c$ and $V_2 = n/k_a$.

The class is narrow in existing benchmarks. Of the 62 models in the suite of [9], only two have a common denominator that is affine in at least two states: *Pharm*, and SIR24, which has inputs and is not built from cycles.

6.2. Collapsing the linear states. Partition the states into $L = \{\tilde{x}_1, \dots, \tilde{x}_k\}$, whose equations are linear, and $N = \{x_1, \dots, x_k\}$. Write $\dot{x}_L = A_{LL}x_L + A_{LN}x_N$ and $\dot{x}_N = A_{NN}x_N + A_{NL}x_L + \psi(x_N)$, with ψ the nonlinear terms. The entries of the matrices A lie in $\mathbb{Q}(\theta)$ and do not depend on t , so they are constants for ∂ , and the adjugate identity of Section 2.7 applies over $\mathbb{Q}(\theta)[\partial]$.

Proposition 6.3. *Let $\chi(\partial) = \det(\partial I - A_{LL})$. Then*

$$[\chi(\partial)(\partial I - A_{NN}) - A_{NL} \operatorname{adj}(\partial I - A_{LL})A_{LN}] x_N = \chi(\partial) \psi(x_N).$$

Proof. The ring $\mathbb{Q}(\theta)[\partial]$ is commutative, and $\operatorname{adj}(\partial I - A_{LL})(\partial I - A_{LL}) = \chi(\partial)I$ over it. Applying $\operatorname{adj}(\partial I - A_{LL})$ to $(\partial I - A_{LL})x_L = A_{LN}x_N$ gives $\chi(\partial)x_L = \operatorname{adj}(\partial I - A_{LL})A_{LN}x_N$. Applying $\chi(\partial)$ to the equation for x_N and substituting gives the statement. $\square$

Hence the $|L|$ linear states are removed at the cost of one characteristic polynomial, where an elimination by resultants pays one elimination per state. The proof uses ψ only as a function of t , so the proposition also applies to a subsystem, with the remaining states entering through ψ . For the cycle (x_0, x_1) of *Pharm*, taken alone in this way, $\chi(\partial) = \partial + a_2$, and the operator acting on x_0 is $\partial + a_1 - a_1 a_2 / (\partial + a_2) = \partial(\partial + a_1 + a_2) / (\partial + a_2)$.

6.3. The collapsed relations. Set $E = K_1 D$, so that $E = K_1 + y + w_2 + \dots + w_k$ with $w_b = (K_1/K_b) x_b$, and let $u = y/E$ and $v_b = w_b/E$.

Proposition 6.4. *A model of Lur'e type with k cycles satisfies*

$$(6.2) \quad y_2 + s_1 y_1 + n_1(\dot{u} + t_1 u) = 0,$$

$$(6.3) \quad \ddot{w}_b + s_b \dot{w}_b + n_b(\dot{v}_b + t_b v_b) = 0, \quad b = 2, \dots, k,$$

with $s_b = \alpha_b + \beta_b$, $t_b = \beta_b$ and $n_b = K_1 V_b$. Write $c_0 = K_1$, and φ for the vector of the s_b, t_b, n_b and c_0 . For *Pharm*,

$$\varphi = (a_1 + a_2, a_2, n, b_1 + b_2, b_2, nk_c/k_a, k_c),$$

and the map $\theta \mapsto \varphi$ is birational where $n_2 \neq 0$.

Proof. By Proposition 6.3, applied to cycle b alone with $\chi = \partial + \beta_b$, the equations (6.1) give $(\partial^2 + (\alpha_b + \beta_b)\partial) x_b = -(\partial + \beta_b)(V_b x_b/D)$. For $b = 1$, $V_1 x_1/D = K_1 V_1 y/E$, which gives (6.2). For $b \geq 2$, multiply by K_1/K_b and use $x_b/D = K_b w_b/E$; the nonlinear term becomes $K_1 V_b w_b/E$, which gives (6.3). For *Pharm* the values follow from Example 6.2, and one inverts φ by $a_2 = t_1$, $a_1 = s_1 - t_1$, $b_2 = t_2$, $b_1 = s_2 - t_2$, $n = n_1$, $k_c = c_0$ and $k_a = n_1 c_0 / n_2$. $\square$

The rescaling $x_b \mapsto w_b$ is a reparametrisation, so verdicts about φ transfer to θ only through the pullback, and only where the pullback is one-to-one; the algorithm checks this.

6.4. What the relations cannot see.

Proposition 6.5. *The relations (6.2) and (6.3) involve the unknowns only through φ , which does not involve $K_2, \dots, K_k$. Moreover, for each $b \geq 2$ and $\lambda \neq 0$, the map $(x_b, \tilde{x}_b, K_b) \mapsto (\lambda x_b, \lambda \tilde{x}_b, \lambda K_b)$, with every other quantity fixed, carries solutions of (6.1) to solutions with the same output. Hence, when the initial states are unknown, K_b is not identifiable for $b \geq 2$, and the unknowns are identifiable at best up to one scaling for each unobserved cycle.*

Proof. The first statement is read off the definitions of s_b, t_b, n_b and c_0 . The map fixes x_b/K_b , hence D , hence the equations of every cycle $c \neq b$ and the output $y = x_1$. Once D is fixed, the equations of cycle b are homogeneous of degree one in $(x_b, \tilde{x}_b)$. The initial states are unknown, so the scaled initial condition is admissible. $\square$

Pharm escapes this scaling because its parametrisation ties V_2 to K_2 through the shared parameter n , so that $K_2 = k_a$ is recovered from φ . For generic models (6.1) with unknown initial states, a rank computation of the Jacobian of the jet map at random points gives rank 11 of 12 at $k = 2$ and 16 of 18 at $k = 3$. The missing directions are exactly the scalings of Proposition 6.5, with confounded sets $\{K_b, x_b(0), \tilde{x}_b(0)\}$ for $b \geq 2$, so every other unknown is locally identifiable at $k = 2$ and $k = 3$. We do not know whether φ is identifiable for every k .

6.5. One resultant for every number of cycles. By (6.2), $\dot{u} = -(y_2 + s_1 y_1)/n_1 - t_1 u$. Let $\mathcal{K}$ be the field of rational functions in u and $y_0, y_1, \dots$ over $\mathbb{Q}(\varphi)$, with the derivation $\partial y_i = y_{i+1}$ and $\partial u = -(y_2 + s_1 y_1)/n_1 - t_1 u$. Along a trajectory, evaluation at $(u(t), y(t), \dot{y}(t), \dots)$ respects ∂ wherever the denominators involved do not vanish. Since $v_b = (u/y_0) w_b$, relation (6.3) says that $\mathcal{L}_b w_b = 0$ for the linear differential operator

$$\mathcal{L}_b = \partial^2 + s_b \partial + n_b(\partial + t_b) \circ \frac{u}{y_0} \in \mathcal{K}[\partial].$$

Let M be the monic least common left multiple of $\mathcal{L}_2, \dots, \mathcal{L}_k$ (Section 2.7). Its order is at most the sum of the orders, $2(k-1)$.

Proposition 6.6. *Along every trajectory of a model of Lur'e type with k cycles, $W = y/u - c_0 - y$ satisfies $M(W) = 0$. Clearing denominators in $M(y_0/u - c_0 - y_0)$ gives a polynomial $P_k(u)$ whose coefficients are polynomials in φ and finitely many output jets. For $k = 2$, $M = \mathcal{L}_2$, and P_2 agrees up to a factor in $\mathbb{Q}(\varphi)$ with the polynomial obtained by substituting $E = y/u$ into (6.3).*

Proof. Since $E = y/u$ and $E = c_0 + y + w_2 + \dots + w_k$, we have $W = w_2 + \dots + w_k$. Each w_b satisfies $\mathcal{L}_b w_b = 0$ along the trajectory, and $M = Q_b \mathcal{L}_b$ for some $Q_b \in \mathcal{K}[\partial]$, so $M(w_b) = Q_b(\mathcal{L}_b w_b) = 0$. By linearity $M(W) = 0$. The coefficients of M lie in $\mathcal{K}$, and so does every derivative of u , so $M(y_0/u - c_0 - y_0)$ is a rational function of u and finitely many jets over $\mathbb{Q}(\varphi)$; its numerator is P_k . For $k = 2$ the operator $\mathcal{L}_2$ is already monic, so $M = \mathcal{L}_2$, and $M(W) = 0$ is (6.3) with $E = y/u$. $\square$

Let $Q_k = \partial P_k$ be the total derivative of P_k along (6.2), and set $R_k = \text{Res}_u(P_k, Q_k)$.

Proposition 6.7. *R_k vanishes on every output trajectory of a model of Lur'e type with k cycles.*

Proof. Along a trajectory, $u(t) = y(t)/E(t)$ is a common root of P_k and Q_k , which are polynomials in u whose coefficients are the output jets at time t . A resultant vanishes whenever its arguments have a common root. $\square$

The resultant is informative only if it does not vanish identically, that is, if P_k and Q_k have no common factor in u . For $k = 2$ this follows from Fact 6.9 below; for $k \geq 3$ it has to be checked. The order of the relation it carries is bounded by the number of states.

Proposition 6.8. *The input–output relation of least order of a model of Lur'e type with k cycles has order at most $2k$ in y , with equality if and only if $y_0, \dots, y_{2k-1}$ are algebraically independent over $\mathbb{Q}(\theta)$, that is, if and only if the Jacobian of $(y_0, \dots, y_{2k-1})$ with respect to the initial states has rank $2k$.*

Proof. Over $\mathbb{Q}(\theta)$, the jets $y_0, \dots, y_{2k}$ are $2k+1$ rational functions of the $2k$ initial states, so they are algebraically dependent, and a relation of order at most $2k$ exists. The least order is the least j with y_j algebraic over $\mathbb{Q}(\theta)(y_0, \dots, y_{j-1})$. If $y_0, \dots, y_{2k-1}$ are independent, no $j < 2k$ qualifies, so the least order is $2k$. If they are dependent, some y_j with $j < 2k$ is algebraic over the jets before it, and the least order is below $2k$. In characteristic zero, algebraic independence of rational functions is the full rank of their Jacobian. $\square$

For $k = 2$ equality holds, since the irreducible relation R_{true} below involves y_4 . At $k = 2$ and $k = 3$ it also follows from the rank computation above: its only missing directions involve some K_b , so the columns for the initial states are independent.

6.6. Two cycles. For $k = 2$ we write $P = P_2$, $Q = Q_2$ and $R = R_2$. Here P is quartic in u , so $P = \sum_{i=0}^4 p_i u^i \in \mathbb{Q}[\varphi][y_0, \dots, y_3][u]$ and $Q = \sum_{i=0}^4 q_i u^i$. Write $\varepsilon = s_1 y_1 + y_2$.

Fact 6.9. *We have*

$$\begin{aligned} p_0 &= 2y_0^3 \varepsilon^2, & p_3 &= n_1 y_0 G, & p_4 &= n_1^2 n_2 F, \\ p_2 &= n_1^2 y_0^2 B, & q_4 &= -n_1^2 n_2 H, \end{aligned}$$

where

$$\begin{aligned} F &= (t_1 - t_2)y_0(c_0 + y_0) + c_0 y_1, \\ G &= n_2(c_0 + y_0)\varepsilon + n_1 y_0(n_2 t_2 - s_2 y_1 - y_2), \\ B &= t_1(s_2 + t_1)y_0 + (s_2 + 2t_1)y_1 + y_2, \\ H &= 4c_0 t_1(t_1 - t_2)y_0 + c_0(3t_1 + t_2)y_1 - c_0 y_2 + 4t_1(t_1 - t_2)y_0^2 - 2(t_1 - t_2)y_0 y_1. \end{aligned}$$

Only q_1 involves y_4 , and $\partial q_1 / \partial y_4 = n_1 y_0^3$. Moreover $R = \lambda y_0^9 \varepsilon R_{\text{true}}$ with $\lambda \in \mathbb{Q}(\varphi)^\times$ and R_{true} irreducible, of total degree 20 with 3,536 monomials in the jets at specialised φ .

These are polynomial identities, checked symbolically. The factorisation also holds with φ symbolic. There R has 528,302 terms and total degree 57, and R_{true} has 427,432 terms in φ and the jets together, of which 3,536 are distinct jet monomials. Pulled back to the parameters of *Pharm* through Proposition 6.4, and multiplied by k_a^5 to clear the denominator of n_2 , R_{true} has 1,062,556 terms and total degree 46. That is the size of the input–output relation obtained by elimination, as it must be, since both are the irreducible relation of least order. The collapsed parameters compress the relation by a factor of about 2.5; they do not make it small. The gain of Algorithm 2 is that the relation is never formed at all. Only the shapes of p_0, p_2, p_3, p_4 and q_4 are used below.

Lemma 6.10. *Let $f = \sum_{i=0}^4 a_i u^i$ and $g = \sum_{i=0}^4 b_i u^i + zu$, with z an indeterminate. Then, in the Sylvester resultant of formal degrees $(4, 4)$,*

$$[z^4] \text{Res}(f, g) = a_4^3 a_0, \quad [z^3] \text{Res}(f, g)|_{a_4=0} = -b_4 a_3^3 a_0, \quad [z^2] \text{Res}(f, g)|_{a_4=a_3=0} = b_4^2 a_2^3 a_0.$$

Proof. If f has degree d with roots $\alpha_1, \dots, \alpha_d$ and leading coefficient a_d , then $\text{Res}_{d,4}(f, g) = a_d^4 \prod_i g(\alpha_i)$ by Section 2.6, and $g(\alpha_i) = g_0(\alpha_i) + z\alpha_i$ with $g_0 = g - zu$. The top coefficient in z is therefore $a_d^4 \prod_i \alpha_i = \pm a_d^3 a_0$. When the formal leading coefficients of f vanish, the Sylvester determinant of formal degrees $(4, 4)$ equals $b_4^{4-d} \text{Res}_{d,4}(f, g)$ up to sign, by the same section. This gives the three identities for $d = 4, 3, 2$. The signs were fixed by a symbolic computation in eleven free variables. $\square$

Theorem 6.11. *Let Σ be of Lur'e type with two cycles, and suppose $s_1 \neq 0$, $n_1 n_2 \neq 0$, $c_0 \neq 0$, $t_1 \neq t_2$ and $t_2 \neq 0$. Suppose moreover that the linear system (6.4) below has full rank at the chosen locus points, and that the polynomials (6.5) have greatest common divisor of degree one. Then φ is a function of the projective class of R . Hence $\mathcal{F}(\theta^*)$ is a single point, and every parameter determined by the pullback $\theta \mapsto \varphi$ is globally identifiable.*

Proof. By Fact 6.9, y_4 enters R only through q_1 , linearly, with coefficient $n_1 y_0^3$. We apply Lemma 6.10 with $z = n_1 y_0^3 y_4$. Since R is known only up to a factor μ constant in the jets, the three reads below use only roots, multiplicities and ratios.

Only the projective class of R_{true} is determined by the output, since $R = \lambda y_0^9 \varepsilon R_{\text{true}}$ and ε involves s_1 . By Fact 6.9, whose factorisation holds with φ symbolic, $[y_4^4] R_{\text{true}}$ is proportional to $y_0^6 \varepsilon F^3$. As a polynomial in y_1 , its factor of multiplicity one is ε , whose root $-y_2/s_1$ gives s_1 . Hence the factor $y_0^9 \varepsilon$, and with it the class of R , is determined by the class of R_{true} , and we may read from R .

Slice I1. We have $[y_4^4] R = \mu \cdot 2n_1^{10} n_2^3 y_0^{15} \varepsilon^2 F^3$. As a polynomial in y_1 , the factor of multiplicity two is ε , with root $-y_2/s_1$, which gives s_1 . The factor of multiplicity three is F , with root $y_1^*(y_0) = -\frac{t_1 - t_2}{c_0} y_0(c_0 + y_0)$. The values at two distinct y_0 determine $t_1 - t_2$ and $(t_1 - t_2)/c_0$, hence c_0 .

Slice I2. The locus $\{F = 0\}$ is now known, and on it $p_4 = 0$, so $[y_4^3] R = -\mu(n_1 y_0^3)^3 q_4 p_3^3 p_0$. Here $p_3^3 = n_1^3 y_0^3 G^3$, while q_4 is linear and p_0 quadratic in y_2 through ε , so the factor of multiplicity three is G , provided that G

Algorithm 2 Lur'e elimination**Input:** a model of Lur'e type with two cycles**Output:** *globally* for every parameter determined by the pullback, or the failing hypothesis

- 1: build $\theta \mapsto \varphi$; stop unless it is one-to-one
- 2: draw a rational θ^* satisfying the domain conditions of Theorem 6.11, and set $\varphi^* = \varphi(\theta^*)$
- 3: evaluate $R(\varphi^*; \cdot)$ at chosen jets, as $\text{Res}_u(P, Q)$ in exact arithmetic
- 4: read $s_1, t_1 - t_2, c_0$ (I1); ρ, v, s_2 (I2); t_1 (I3); test the rank and gcd hypotheses
- 5: recover θ from φ
- 6: **return** *globally* if the recovered θ equals θ^* and R vanishes on jets of Σ ; otherwise the failed read

involves y_2 at the locus point and that its root there differs from those of ε and H , which holds at a generic locus point. Its root in y_2 , at a locus point $(y_0, y_1^*(y_0))$, satisfies

$$(6.4) \quad y_2^*((c_0 + y_0) - \rho y_0) + (c_0 + y_0)s_1 y_1^* + v y_0 - \sigma y_0 y_1^* = 0,$$

which is linear in $\rho = n_1/n_2$, $v = n_1 t_2$ and $\sigma = \rho s_2$. Three locus points in general position determine ρ , v and $s_2 = \sigma/\rho$.

Slice I3. On $\{F = G = 0\}$, $p_4 = p_3 = 0$ and $[y_4^2]R = \mu(n_1 y_0^3)^2 q_4^2 p_2^3 p_0$. At a locus point i , dividing the value V_i of this slice by the known quantity $y_0^{15} H^2 \varepsilon^2$ leaves $U_i = \mu' B_i(t_1)^3$, where $\mu' = 2\mu n_1^{12} n_2^2$ is common to all i and B_i is the polynomial B of Fact 6.9 at the point, known except for t_1 because H is free of t_1 on $\{F = 0\}$. Hence t_1 is a common root of the polynomials

$$(6.5) \quad U_0 B_i(t_1)^3 - U_i B_0(t_1)^3, \quad i = 1, 2, \dots,$$

and by hypothesis their only common root. Then $t_2 = t_1 - (t_1 - t_2)$, $n_1 = v/t_2$ and $n_2 = n_1/\rho$.

Every read is a root, a multiplicity, or a ratio in which μ cancels, so it depends only on the projective class of R . The excluded loci are exactly where a read has nothing to read. The last statement follows from Proposition 6.4. $\square$

For $k \geq 3$ the slice identities, which are specific to two quartics in u , have not been derived, and both the degree of P_k in u and the order of the relation grow. The resultant R_k can then be read by a generic method, such as a rank test or a count of its preimages, at the cost of the explicit inverse.

STATUS: For $k \geq 3$, neither P_k nor the slices of its resultant have been derived.

7. PARALLEL SPLITS

In this section we give conditions under which a parallel linear model with one summed output is identifiable exactly when its blocks are, and an algorithm that checks them.

Let Σ be linear and input-free with one output, $\dot{x} = A(\theta)x$ and $y = c^\top x$ with c constant, and let its states split into blocks $b = 1, \dots, B$ such that A is block diagonal, the unknowns of distinct blocks are disjoint, and c reads every block. The initial states are known. As in Section 2.8, set

$$D_b = \det(sI - A_b), \quad N_b = c_b^\top \text{adj}(sI - A_b) x_{0,b}, \quad Y = \sum_{b=1}^B \frac{N_b}{D_b},$$

so that D_b is monic of degree d_b at every parameter value and $\deg N_b < d_b$. Two parameter values give the same output if and only if they give the same Y , so in this section $\mathcal{F}(\theta^*) = \{\theta : Y(\theta) = Y(\theta^*)\}$. If each block had its own output, the input-output map would factor over the blocks. With one summed output it does not, and identifiability of the model does not follow from identifiability of the blocks.

7.1. Separation.

Theorem 7.1. *Suppose that $\theta^* \in \mathbb{Q}^r$ and that*

- (S1) *the splitting field of $\prod_b D_b(\theta^*)$ over $\mathbb{Q}$ has as Galois group the full product $\prod_b S_{d_b}$ of the symmetric groups on the roots of the $D_b(\theta^*)$;*
- (S2) *the $D_b(\theta^*)$ are pairwise distinct;*
- (S3) *each $N_b(\theta^*)$ is nonzero and, when $d_b \geq 2$, is not a scalar multiple of the derivative $D_b(\theta^*)'$;*
- (S4) *no d_b is a sum of two or more of $d_1, \dots, d_B$.*

Then for every $\theta \in \mathcal{F}(\theta^*)$ there is a permutation σ of the blocks with $D_b(\theta) = D_{\sigma(b)}(\theta^*)$ and $N_b(\theta) = N_{\sigma(b)}(\theta^*)$ for all b .

Proof. Write $\Delta = \prod_b D_b(\theta^*)$, let Z_c be the set of roots of $D_c(\theta^*)$, and for a root ζ of Δ let ρ_ζ be the residue of $Y(\theta^*)$ at ζ .

Claim 1: $Y(\theta^*)$ is in lowest terms, with the squarefree denominator Δ . By (S1) the Galois group acts transitively on each Z_c , so each $D_c(\theta^*)$ is irreducible over $\mathbb{Q}$. By (S2) the $D_c(\theta^*)$ are then pairwise coprime, and Δ is squarefree. By (S3) each $N_b(\theta^*)$ is coprime to $D_b(\theta^*)$, since $\deg N_b < \deg D_b$. Hence the numerator of $Y(\theta^*)$ satisfies

$$\sum_c N_c \prod_{c' \neq c} D_{c'} \equiv N_b \prod_{c \neq b} D_c \not\equiv 0 \pmod{D_b(\theta^*)}$$

for every b , which gives the claim.

Claim 2: let $\theta \in \mathcal{F}(\theta^*)$. Then each $D_b(\theta)$ is $\prod_{\zeta \in S_b} (s - \zeta)$ for a set S_b of roots of Δ , the S_b partition the roots, and $N_b(\theta)$ has leading coefficient $\sum_{\zeta \in S_b} \rho_\zeta$. Since $Y(\theta) = Y(\theta^*)$ and $\prod_b D_b(\theta)$ is a monic denominator of it of the same degree as Δ , Claim 1 gives $\prod_b D_b(\theta) = \Delta$. As Δ is squarefree, each $D_b(\theta)$ is the product of $s - \zeta$ over a set S_b of its roots, and these sets partition the roots. The partial fraction decomposition of Y over the distinct roots of Δ is unique, so $N_b(\theta)/D_b(\theta) = \sum_{\zeta \in S_b} \rho_\zeta / (s - \zeta)$, and comparing coefficients of s^{d_b-1} gives the leading coefficient.

Claim 3: each S_b is one of the sets Z_c . The leading coefficient of $N_b(\theta)$ is $c_b^\top x_{0,b}$, which is known, so $\ell_b = \sum_{\zeta \in S_b} \rho_\zeta$ is rational. For $\zeta \in Z_c$ we have $\rho_\zeta = h_c(\zeta)$ with $h_c = N_c(\theta^*)/D_c(\theta^*)' \in \mathbb{Q}(s)$, so an element g of the Galois group maps ρ_ζ to $\rho_{g(\zeta)}$. Fix c and a permutation π of Z_c . By (S1) there is an element g acting as π on Z_c and trivially on every other $Z_{c'}$. Applying g to $\ell_b = \sum_{c'} \sum_{\zeta \in S_b \cap Z_{c'}} \rho_\zeta$ gives

$$\sum_{\zeta \in \pi(S_b \cap Z_c)} \rho_\zeta = \sum_{\zeta \in S_b \cap Z_c} \rho_\zeta.$$

Suppose that $T = S_b \cap Z_c$ is neither empty nor all of Z_c , so that $d_c \geq 2$. Taking π to be the transposition of a root $\zeta \in T$ and a root $\zeta' \in Z_c \setminus T$ gives $\rho_\zeta = \rho_{\zeta'}$, and varying ζ and ζ' shows that all ρ_ζ with $\zeta \in Z_c$ are equal, say to ρ . Then $N_c(\theta^*) - \rho D_c(\theta^*)'$ has degree less than d_c and vanishes at the d_c points of Z_c , so $N_c(\theta^*) = \rho D_c(\theta^*)'$, contrary to (S3). Hence each S_b is a union of sets Z_c . Their sizes sum to d_b , so by (S4) there is exactly one.

Claim 4: the conclusion. Write $S_b = Z_{\sigma(b)}$. Since the S_b partition the roots, σ is a permutation, and $D_b(\theta) = D_{\sigma(b)}(\theta^*)$. By Claim 2, $N_b(\theta)/D_b(\theta) = \sum_{\zeta \in Z_{\sigma(b)}} \rho_\zeta / (s - \zeta) = N_{\sigma(b)}(\theta^*)/D_{\sigma(b)}(\theta^*)'$, so $N_b(\theta) = N_{\sigma(b)}(\theta^*)$. $\square$

Note that nothing generic is assumed about θ , which ranges over all of $\mathbb{C}^r$. Hypothesis (S1) is what makes this possible: over $\mathbb{C}$ the $D_c(\theta^*)$ split into linear factors, and irreducibility over $\mathbb{Q}$ alone would not prevent some $D_b(\theta)$ from taking roots of several of them. Genericity enters only through the choice of θ^* . When the Galois group of $\prod_b D_b$ over $\mathbb{Q}(\theta)$ is $\prod_b S_{d_b}$, Hilbert's irreducibility theorem [35] gives (S1) for every rational θ^* outside a thin set. For quadratic blocks, (S1) says that no nonempty product of the discriminants of the $D_b(\theta^*)$ is a square, which is a test on their squarefree parts; Proposition 7.6 below proves the generic statement for two-compartment blocks.

7.2. The imitation digraph.

Definition 7.2. The *imitation digraph* at θ^* has vertices $1, \dots, B$ and an edge $b \rightarrow c$ if the system

$$D_b(s; v) = D_c(s; \theta^*), \quad N_b(s; v) = N_c(s; \theta^*),$$

in the unknowns v of block b , has a solution over $\overline{\mathbb{Q}}$.

An edge $b \rightarrow c$ says that block b can reproduce the contribution of block c to Y at θ^* , a pointwise and one-sided form of the indistinguishability of linear compartmental models studied by Godfrey and Chapman [12], for which Bortner and Meshkat [4] give graph-based sufficient conditions. Every vertex has a loop. An edge $b \rightarrow c$ with $b \neq c$ is decided exactly by a Gröbner basis in the unknowns of block b alone: the system has no solution if and only if the reduced basis is $\{1\}$. Before any algebra, the leading coefficient of N_b is $c_b^\top x_{0,b}$, which is known. Two blocks with different values of it therefore have no edge between them.

For blocks b and c , let $I_{b,c}$ be the set of values v of the unknowns of block b with $D_b(v) = D_c(\theta^*)$ and $N_b(v) = N_c(\theta^*)$. It is nonempty exactly when $b \rightarrow c$ is an edge, by the Nullstellensatz. Call a permutation σ of the blocks a *cycle cover* of the imitation digraph if $b \rightarrow \sigma(b)$ is an edge for every b .

Theorem 7.3. *Assume (S1)–(S4). Then*

$$\mathcal{F}(\theta^*) = \bigsqcup_{\sigma} \prod_{b=1}^B I_{b,\sigma(b)},$$

the union running over the cycle covers σ of the imitation digraph, and the union is disjoint.

Proof. Let $\theta \in \mathcal{F}(\theta^*)$, with permutation σ as in Theorem 7.1. The unknowns of block b at θ lie in $I_{b,\sigma(b)}$, so each $b \rightarrow \sigma(b)$ is an edge and σ is a cycle cover. Conversely, let σ be a cycle cover and choose $v_b \in I_{b,\sigma(b)}$ for every b . Since the blocks have disjoint unknowns, these choices define a point θ , and

$$Y(\theta) = \sum_b N_b(v_b)/D_b(v_b) = \sum_b N_{\sigma(b)}(\theta^*)/D_{\sigma(b)}(\theta^*) = Y(\theta^*),$$

since σ is a permutation. The union is disjoint because θ determines σ : by (S2), $D_b(\theta)$ equals $D_c(\theta^*)$ for only one c . $\square$

Every vertex has a loop, so the identity is always a cycle cover, and its term is $\prod_b I_{b,b}$, the part of $\mathcal{F}(\theta^*)$ on which each block reproduces itself. The values that a parameter of block b takes on $\mathcal{F}(\theta^*)$ are its values on the sets $I_{b,c}$ for the vertices c to which some cycle cover sends b , and their number is its identifiability degree.

Proposition 7.4. *Assume (S1)–(S4). Every $\theta \in \mathcal{F}(\theta^*)$ has $\sigma = \text{id}$ if and only if the imitation digraph has no cycle of length at least two.*

Proof. Every vertex has a loop, so by Section 2.10 a cycle cover other than the identity exists exactly when the digraph has a cycle of length at least two. The statement follows from Theorem 7.3. $\square$

Corollary 7.5. *If (S1)–(S4) hold and the imitation digraph has no cycle of length at least two, then $\mathcal{F}(\theta^*) = \prod_b \mathcal{F}_b(\theta^*)$, where $\mathcal{F}_b(\theta^*) = I_{b,b}$ is the set of values v of the unknowns of block b with $D_b(v) = D_b(\theta^*)$ and $N_b(v) = N_b(\theta^*)$. Hence each parameter has in Σ the identifiability degree it has in its own block.*

Proof. The identity is then the only cycle cover, and Theorem 7.3 gives the product. $\square$

7.3. Two-compartment blocks. For blocks of two compartments, $\mathcal{F}(\theta^*)$ can be counted directly. Let each block have a leak at its observed compartment, known initial condition (a_b, β_b) with $a_b + \beta_b \neq 0$, and output weight w_b , so that block b contributes $w_b N_b/D_b$ to Y , with

$$D_b = s^2 + (k_{10,b} + k_{12,b} + k_{21,b})s + k_{10,b}k_{21,b}, \quad N_b = a_b s + k_{21,b}(a_b + \beta_b).$$

The unknowns are the $3B$ rate constants.

Proposition 7.6. *For two-compartment blocks, (S1)–(S4) hold for every $\theta^* \in \mathbb{Q}^{3B}$ outside a thin set.*

Algorithm 3 Parallel split**Input:** a linear, input-free, block-diagonal Σ with one summed output and parameter-disjoint blocks**Output:** per-parameter verdicts, or the failing condition

- 1: draw rational θ^* ; test (S1)–(S4) exactly (for quadratic blocks, (S1) is the discriminant test)
- 2: **for** each ordered pair $b \neq c$ **do**
- 3: **if** the leading coefficients of N_b and N_c differ, **then** there is no edge
- 4: **else** decide $b \rightarrow c$ by a Gröbner basis in the unknowns of block b
- 5: **end for**
- 6: **if** the digraph has a cycle, **then** stop, since the blocks can be exchanged
- 7: **return** each block's own verdicts (Corollary 7.5)

Proof. The discriminant of D_b is $\delta_b = k_{12,b}^2 + 2(k_{10,b} + k_{21,b})k_{12,b} + (k_{10,b} - k_{21,b})^2$. As a quadratic in $k_{12,b}$ it has discriminant $16k_{10,b}k_{21,b}$, which is not a square in $\mathbb{Q}(k_{10,b}, k_{21,b})$, so δ_b is irreducible in $\mathbb{Q}[k_{10,b}, k_{12,b}, k_{21,b}]$. The δ_b involve disjoint sets of variables, so no nonempty product of them is a constant times a square in $\mathbb{Q}(\theta)$. By Kummer theory the splitting field of $\prod_b D_b$ over $\mathbb{Q}(\theta)$ then has degree 2^B , with Galois group $(\mathbb{Z}/2)^B = \prod_b S_2$. By Hilbert's irreducibility theorem [35], the specialisation at θ^* has the same Galois group for every $\theta^* \in \mathbb{Q}^{3B}$ outside a thin set, which is (S1). Conditions (S2) and (S3) fail only on proper Zariski-closed subsets, which are thin; for (S3) the condition is that N_b is not a multiple of $D'_b = 2s + k_{10,b} + k_{12,b} + k_{21,b}$. And (S4) holds because every $d_b = 2$ and any sum of two or more of them is at least 4. $\square$

Corollary 7.7. *If the effective weights $w_b a_b$ are pairwise distinct and every $a_b + \beta_b \neq 0$, then every rate constant is globally identifiable.*

Proof. The leading coefficient of the contribution of block b is $w_b a_b$, so distinct effective weights leave the imitation digraph without edges between distinct blocks. For θ^* as in Proposition 7.6, Corollary 7.5 then gives $\mathcal{F}(\theta^*) = \prod_b \mathcal{F}_b(\theta^*)$. In block b , the coefficients of D_b and N_b determine $k_{21,b} = N_b(0)/(a_b + \beta_b)$, then $k_{10,b} = D_b(0)/k_{21,b}$ and $k_{12,b} = [s]D_b - k_{10,b} - k_{21,b}$, wherever $k_{21,b} \neq 0$. So $\mathcal{F}(\theta^*)$ is a single point. The set of θ^* with this property is constructible and contains all rational points outside a thin set, so it contains a nonempty Zariski-open set. $\square$

Example 7.8. Take two blocks with $(k_{10}, k_{12}, k_{21}) = (1, 2, 3)$ and $(2, 1, 1)$. Then $D_1 = s^2 + 6s + 3$ and $D_2 = s^2 + 4s + 2$, with discriminants $24 = 2^2 \cdot 6$ and $8 = 2^2 \cdot 2$. Their squarefree parts 6 and 2 are not squares, and neither is their product 12, so (S1) holds. If the effective weights are equal instead, $w_1 a_1 = w_2 a_2$, then each block can reproduce the other: block 1 matches D_2 and $w_2 N_2$ by choosing $k_{21,1}$ from the constant term of N_2 and then $k_{10,1}$ and $k_{12,1}$ from D_2 . The transposition of the two blocks is a cycle cover, and by Theorem 7.3 the preimage has two points, exchanged by swapping the blocks. Every rate constant then has identifiability degree two.

Proposition 7.9. *Suppose that $\Delta = \prod_b D_b(\theta^*)$ is squarefree with $\Delta(0) \neq 0$, that every residue of $Y(\theta^*)$ is nonzero, and that the effective weights $w_b a_b$ are pairwise distinct. Call a partition of the $2B$ roots of Δ into B pairs admissible if the residues of $Y(\theta^*)$ over each pair sum to one of the $w_b a_b$, with each value used once, and the partial fraction numerator of $Y(\theta^*)$ over each pair is nonzero at $s = 0$. Then $\mathcal{F}(\theta^*)$ is in bijection with the admissible partitions, and the identifiability degree of every parameter is at most their number.*

Proof. Let $\theta \in \mathcal{F}(\theta^*)$. Since the residues are nonzero, $Y(\theta^*)$ is in lowest terms with denominator Δ , so $\prod_b D_b(\theta) = \Delta$. By uniqueness of partial fractions, each $D_b(\theta)$ is the quadratic over one pair of roots of Δ , the pairs partition the roots, and $w_b N_b(\theta)$ is the corresponding partial fraction numerator. Its leading coefficient $w_b a_b$ is the sum of the residues over the pair, and $N_b(\theta)(0) = k_{21,b}(a_b + \beta_b)$ is nonzero because $k_{10,b}k_{21,b} = D_b(\theta)(0) \neq 0$. So θ gives an admissible partition, and because the weights are distinct the pair assigned to each block is determined. Conversely, an admissible partition determines D_b and N_b for every block, and hence $k_{21,b} = N_b(0)/(a_b + \beta_b)$, $k_{10,b} = D_b(0)/k_{21,b}$ and $k_{12,b} = [s]D_b - k_{10,b} - k_{21,b}$. These two maps are mutually inverse. $\square$

There are $(2B - 1)!!$ partitions to test, so this count is feasible for small B only. Corollary 7.5 replaces it when (S1)–(S4) hold.

8. POINT COUNTS AND THE GALOIS GROUP

In this section and the next two, θ denotes all the unknowns, the parameters together with any unknown initial states, and they range over $V = \mathbb{C}^r$. We fix a map $\gamma: V \dashrightarrow \mathbb{C}^m$, defined over $\mathbb{Q}$, whose preimages are the sets of unknowns that produce the same output: the coefficient map or the Taylor map T_N of Section 2.3. We first set up its Galois group, and then recover the degree of γ , and information about the group, from the numbers of $\mathbb{F}_p$ -points of one specialised preimage over many primes.

8.1. The map and its preimages. Let U be the closure of the image of γ . We assume that $\gamma: V \dashrightarrow U$ is *generically finite*: the preimage of a generic point is finite, or equivalently, in characteristic zero, the Jacobian of γ has rank r at a generic point. This is local identifiability of all the unknowns. The number d of points in the preimage of a generic point of U is the *degree* of γ . For $\gamma^* \in U$, the preimage $\gamma^{-1}(\gamma^*)$ is the set of unknowns that γ sends to γ^* , and for $\theta^* \in V$ the preimage $\gamma^{-1}(\gamma(\theta^*))$ is the set of values indistinguishable from θ^* . A point $\gamma^* \in U$ is a *branch point* if $\gamma^{-1}(\gamma^*)$ is not a set of d reduced points; the branch points lie in a proper closed subset $\mathcal{B} \subset U$, the *branch locus*.

8.2. The Galois group. In this section and the next two, K and L denote the fields below, not those of Section 3.3. Write $L = \mathbb{Q}(\theta)$ for the function field of V and $K = \mathbb{Q}(\gamma(\theta)) \subseteq L$ for the subfield generated by the coordinates of γ . Then $[L : K] = d$. Let $\tilde{L}$ be a Galois closure of L/K and $G = \text{Gal}(\tilde{L}/K)$. The d embeddings of L into $\tilde{L}$ over K correspond to the points of a generic preimage, and G permutes them. We regard G as a permutation group of degree d ; it is transitive, since L is a field. The stabiliser of one point is $H = \text{Gal}(\tilde{L}/L)$.

For $f \in L$, its *identifiability degree* is $[K(f) : K]$, the number of values f takes on a generic preimage. So f is globally identifiable exactly when $f \in K$. By the Galois correspondence, the fields between K and L correspond to the subgroups between H and G , the field $K(f)$ to the stabiliser of f in G , and $[K(f) : K]$ is the index of that stabiliser.

We use the following vocabulary for a transitive permutation group G of degree d with point stabiliser H [8]. It is *regular* if $|G| = d$, that is, $H = 1$. A *block* is a nonempty set of points that each element of G maps to itself or to a disjoint set; the blocks through a point correspond to the subgroups between H and G , and G is *primitive* if its only blocks are the single points and the whole set, that is, if H is a maximal subgroup. The *rank* of G is the number of orbits of H , and G is *doubly transitive* if the rank is two. A doubly transitive group is primitive. The symmetric group S_d is doubly transitive for $d \geq 2$.

8.3. Monodromy. Over $\mathbb{C}$, the map γ restricts to a covering of degree d over $U \setminus \mathcal{B}$, since the preimages there are d reduced points that move analytically with the base point. Continuing the points of the preimage of a base point b_0 along a loop in $U \setminus \mathcal{B}$ permutes them, and the permutations obtained form the *monodromy group* of γ . It is transitive, since V is irreducible.

Harris identified the monodromy group with a Galois group [13]: it is $\text{Gal}(\tilde{L}_{\mathbb{C}}/K_{\mathbb{C}})$, where $K_{\mathbb{C}} = \mathbb{C}(\gamma(\theta))$ and $\tilde{L}_{\mathbb{C}}$ is a Galois closure of $\mathbb{C}(\theta)/K_{\mathbb{C}}$. This is the *geometric* Galois group. It is the normal subgroup of G that fixes the algebraic closure F of $\mathbb{Q}$ in $\tilde{L}$, and the quotient is $\text{Gal}(F/\mathbb{Q})$. The two groups therefore coincide exactly when the Galois closure adds no constants, $F = \mathbb{Q}$. Point counts see G , and monodromy sees the geometric group. For the map $\theta \mapsto \theta^3$, for instance, $G = S_3$ while the monodromy group is cyclic of order three, since the other preimages $\omega\theta$ and $\omega^2\theta$ need the cube root of unity ω .

Hauenstein, Rodriguez and Sottile compute monodromy groups from loops in a single generic line of the base, whose inclusion into $U \setminus \mathcal{B}$ is surjective on fundamental groups [15]; we use the same fact in Section 9.

8.4. The base point.

Definition 8.1. A point $\gamma^* \in U(\mathbb{Q})$ is a *good base point* if $\gamma^{-1}(\gamma^*)$ is finite and reduced of cardinality d , and the Galois group of its field of definition over $\mathbb{Q}$ is G .

Remark 8.2. If $\gamma^* = \gamma(\theta^*)$ with $\theta^* \in \mathbb{Q}^r$ and $d > 1$, then γ^* is not a good base point. The preimage then contains the rational point θ^* , so the Galois group of the specialised preimage fixes a point, whereas G is transitive of degree $d > 1$. In the same way, drawing θ^* in $\mathbb{F}_p^r$ at each prime puts an $\mathbb{F}_p$ -point in every preimage by construction, and then only the maximum of the counts remains meaningful.

A good base point is instead obtained as the image of an algebraic point with no rational preimage. For instance, in the Lotka–Volterra model, whose parameters a and b enter the coefficients only through $a + b$ and ab , we take a and b to be the roots of an integer quadratic with non-square discriminant. Every coefficient is then rational, while no preimage is.

8.5. Frobenius counts. Let γ^* be a good base point. Call a prime p *good* if $\gamma^{-1}(\gamma^*)$ has good reduction at p in the sense of Section 2.13; all but finitely many primes are good.

Proposition 8.3. *Let p be a good prime. Then $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)|$ equals the number of points fixed by a Frobenius element $\text{Frob}_p \in G$ acting on the d points of $\gamma^{-1}(\gamma^*)(\overline{\mathbb{Q}})$. Consequently:*

- (i) $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)| \leq d$ for every good p , with equality for a set of primes of density $1/|G|$;
- (ii) the average of $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)|$ over good primes, in the limit, is the number of orbits of G , which is 1;
- (iii) for each j , the density of good primes with $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)| = j$ is the proportion of elements of G fixing exactly j points.

Proof. At a good prime the reduction is étale, so by Section 2.13 the $\mathbb{F}_p$ -points of the reduction are the points of $\gamma^{-1}(\gamma^*)(\overline{\mathbb{Q}})$ fixed by a Frobenius element of the Galois group of its field of definition. Since γ^* is a good base point, that group is G in its action on the d points, and by the Chebotarev density theorem [37] the Frobenius conjugacy classes are equidistributed in G with density proportional to their size. Statement (i) follows because only the identity fixes all d points. For (ii), Burnside’s lemma says that the average number of fixed points over G is the number of orbits, and G is transitive. Statement (iii) is the same equidistribution, applied to the fixed-point count. $\square$

Proposition 8.4. *Let $\gamma^* \in U(\mathbb{Q})$ lie outside $\mathcal{B}$ and outside the poles of the coefficients of the minimal polynomial of θ_i over K , and let $\gamma^{-1}(\gamma^*)$ have good reduction at p . If two $\mathbb{F}_p$ -points of $\gamma^{-1}(\gamma^*)$ have distinct values of θ_i , then θ_i is not globally identifiable.*

Proof. By good reduction, each $\mathbb{F}_p$ -point of $\gamma^{-1}(\gamma^*)$ is the reduction of a point of $\gamma^{-1}(\gamma^*)(\overline{\mathbb{Q}})$. Two $\mathbb{F}_p$ -points with distinct values of θ_i are therefore reductions of two points of the preimage with distinct values of θ_i . On the preimage, θ_i takes values among the roots of its minimal polynomial over K specialised at γ^* , so it takes at most $[K(\theta_i) : K]$ values, and this degree is therefore at least two. $\square$

The algorithm cannot check good reduction. It keeps only the $\mathbb{F}_p$ -points at which the Jacobian of the defining system has full rank: at a good prime this is every point, and the filter discards what a bad prime or a positive-dimensional preimage adds. The rank condition is essential. On a positive-dimensional preimage, raw counts grow like $p^{\dim}$, while points of full rank do not occur. For the Lotka–Volterra model with all four parameters unknown, the preimage is positive-dimensional: at $p = 31$ and $p = 37$ there are 60 and 72 raw points, and none of full rank.

8.6. The Taylor map. The map γ need not be an input–output coefficient map. For the Taylor map T_N of Section 2.3, whose coordinates come from Lie differentiation alone, Propositions 8.3 and 8.4 apply verbatim with T_N in place of γ , so the degree and the fixed-point statistics are read without any elimination.

8.7. Reading the group. The counts carry more than the degree. They record how the ambiguity in the parameters is organised, and in particular whether it is explained by symmetries of the model.

Definition 8.5. A *deck transformation* of γ is a birational map $\sigma : V \dashrightarrow V$ with $\gamma \circ \sigma = \gamma$.

A deck transformation is a rational symmetry of the parameters that leaves the output unchanged. The exchange $a \leftrightarrow b$ in the Lotka–Volterra model is one.

Algorithm 4 Preimage point counts**Input:** a map γ (input–output coefficients, or the Taylor map T_N) and a good base point γ^* **Output:** the degree d and the fixed-point distribution, or a lower bound

- 1: **for** each good prime p in a list **do**
- 2: enumerate the $\mathbb{F}_p$ -points of $\gamma^{-1}(\gamma^*)$ by branching one unknown at a time, with cross-multiplied equations and no modular inverses
- 3: keep the points at which the Jacobian has full rank; record the count and the values of each θ_i
- 4: **end for**
- 5: **return** the maximum count, the distribution of counts, and every θ_i that shows two values at some prime (Proposition 8.4)

Proposition 8.6. *Let $H \leq G$ be the stabiliser of one point of a generic preimage.*

- (i) *The deck transformations form a group isomorphic to $\text{Aut}(L/K) \cong N_G(H)/H$, and a deck transformation other than the identity fixes no point of a generic preimage.*
- (ii) *The following are equivalent: every point of a generic preimage is $\sigma(\theta^*)$ for some deck transformation σ ; the extension L/K is Galois; G acts regularly, that is, $|G| = d$.*

Proof. A birational map σ of V with $\gamma \circ \sigma = \gamma$ is the same as a K -automorphism σ^* of $L = \mathbb{Q}(\theta)$, by pulling back functions. Since $L = \tilde{L}^H$, Galois theory gives $\text{Aut}(L/K) \cong N_G(H)/H$. The points fixed by a deck transformation other than the identity form a proper closed subset of V , which a generic point avoids. This proves (i). For (ii), the deck transformations act freely on the d points of a generic preimage, so they reach every point exactly when $|\text{Aut}(L/K)| = d = [L : K]$, which is the definition of L/K being Galois. That holds exactly when H is normal in G . Since G acts faithfully and transitively, the intersection of the conjugates of H is trivial, so H is normal exactly when $H = 1$, that is, when $|G| = d$. $\square$

Corollary 8.7. *Let γ^* be a good base point. Then G is regular if and only if, at a set of good primes of density one, $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)| \in \{0, d\}$. In particular, a single good prime at which $0 < |\gamma^{-1}(\gamma^*)(\mathbb{F}_p)| < d$ shows that G is not regular, so that not every point of a generic preimage is the image of a given one under a rational symmetry of the parameters.*

Proof. If G is regular, every element other than the identity fixes no point, so every count is 0 or d by Proposition 8.3. Conversely, suppose almost every count is 0 or d . By the Chebotarev density theorem, every element of G occurs as a Frobenius element for a set of primes of positive density. So every element either fixes every point or fixes none, and a transitive group in which every non-identity element is fixed-point-free has trivial point stabilisers. The last statement is the contrapositive, together with Proposition 8.6. $\square$

So point counts separate two kinds of local, non-global identifiability. When G is regular, all of the ambiguity comes from rational symmetries of the parameters, and those symmetries are the natural next object to compute. When G is not, some of it does not.

8.8. Parameters as blocks.

Proposition 8.8. *For each coordinate θ_i , let $H_i \leq G$ be the subgroup fixing θ_i , so that $K(\theta_i) = \tilde{L}^{H_i}$ and $H \leq H_i$. The relation “same value of θ_i ” on the points of a generic preimage is preserved by G . Its classes are $e_i = [G : H_i]$ blocks, each of size $[H_i : H]$, where e_i is the identifiability degree of θ_i . In particular e_i divides d , and θ_i is globally identifiable if and only if $H_i = G$.*

Proof. The points of the preimage correspond to the cosets G/H , and the values of θ_i to the cosets G/H_i . The map $gH \mapsto gH_i$ is G -equivariant, and the preimages of its points are the blocks. There are $[G : H_i] = [K(\theta_i) : K] = e_i$ of them, each of size $[H_i : H]$. $\square$

At a good prime, the number of distinct values of θ_i among the $\mathbb{F}_p$ -points of the preimage is the number of blocks that contain a point fixed by Frobenius. This number is at most e_i , which is the bound used in Proposition 8.4. When the group has no blocks at all, the identifiability degrees are forced to their extremes.

Corollary 8.9. *If G is primitive, in particular if $G = S_d$, then every $f \in L$ either lies in K , and is globally identifiable, or satisfies $[K(f) : K] = d$. In particular every coordinate θ_i is globally identifiable or has identifiability degree d .*

Proof. The fields between K and L correspond to the groups between H and G , the field $K(f)$ to the stabiliser of f . The group G is primitive exactly when H is a maximal subgroup, so that stabiliser is H or G , and $K(f)$ is L or K . $\square$

8.9. What the counts determine. Counting over the extensions $\mathbb{F}_{p^v}$ as well as over $\mathbb{F}_p$ refines the fixed-point statistics to cycle types.

Proposition 8.10. *Let p be a good prime. For $v \geq 1$, $|\gamma^{-1}(\gamma^*)(\mathbb{F}_{p^v})|$ is the number of points fixed by Frob_p^v , and the counts for $1 \leq v \leq d$ determine the cycle type of Frob_p . As p varies, they determine the proportion of elements of G of each cycle type, and nothing more: two permutation groups of degree d with the same proportions of cycle types give the same limiting statistics of counts.*

Proof. At a good prime the reduction is étale, so its $\mathbb{F}_{p^v}$ -points are the points fixed by the v -th power of Frobenius. If Frob_p has a_j cycles of length j , it fixes $\sum_{j|v} j a_j$ points after v steps, and Möbius inversion over $1 \leq v \leq d$ recovers every $j a_j$. By the Chebotarev density theorem the Frobenius elements are equidistributed in G , so the proportion of primes with a given cycle type is the proportion of elements of G of that type. The counts are functions of the cycle type, so this is all they record. $\square$

The first two moments of the counts already say something about the shape of the group.

Proposition 8.11. *Over good primes, the mean of $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)|$ tends to 1, and the mean of $|\gamma^{-1}(\gamma^*)(\mathbb{F}_p)|^2$ tends to the rank of G , the number of orbits of the point stabiliser H on the preimage. If the second mean is 2, then G is doubly transitive, hence primitive, and Corollary 8.9 applies.*

Proof. By the Chebotarev density theorem these means are the averages over G of $\text{fix}(g)$ and $\text{fix}(g)^2$. By Burnside's lemma, applied to the points and to ordered pairs of points, they are the numbers of orbits of G on points and on ordered pairs. The first is 1 by transitivity, and the second is the number of orbits of H on points. Rank two means that H is transitive on the remaining $d - 1$ points, that is, G is doubly transitive, and a doubly transitive group is primitive. $\square$

The limitation is real. For an odd prime q , the elementary abelian group of order q^3 and the Heisenberg group of order q^3 , which also has exponent q , have regular representations in which every element other than the identity has q^2 cycles of length q . The counts therefore see that such a group is regular and has order q^3 , but not which of the two it is.

Example 8.12. In the Lotka-Volterra model with a and b the roots of $x^2 - 7x + 3$, the preimage has two points, exchanged by $a \leftrightarrow b$. So $d = 2$ and $G = S_2$, which is regular. At a good prime the count is 2 when 37, the discriminant, is a square modulo p , and 0 otherwise, each for half of the primes, while at $p = 37$ the two points meet.

Example 8.13. For the map $\theta \mapsto \theta^3 - \theta$ we have $d = 3$ and $G = S_3$, of order 6, so the group is not regular: the other roots of $\theta^3 - \theta = \gamma^*$ are not rational functions of θ . The base point $\gamma^* = 1$ is good, since $x^3 - x - 1$ is irreducible with discriminant -23 . It has no root modulo 2 or 3 and exactly one modulo 5, so the prime 5 alone certifies, by Corollary 8.7, that the ambiguity is not explained by a rational symmetry. By Corollary 8.9 the coordinate θ has identifiability degree 3.

9. A COMPLETE PREIMAGE FROM BRANCH POINTS

Monodromy loops find points of the preimage and never show that none is missing. In one system with $r = 10$ unknowns and 120 sheets, random loops sat quiet for 25 consecutive rounds at 119 sheets. In this section we replace random loops by a finite set of loops known to generate the monodromy group.

Algorithm 5 Complete preimage from branch points**Input:** γ generically finite; a base point b_0 **Output:** the preimage of b_0 and the monodromy group, or a refusal

- 1: choose γ_{sub} ; draw a random line ℓ through b_0
- 2: compute $W = \mathcal{B} \cap \ell$ from the square system above
- 3: build the lollipop loops about W
- 4: track every held point round every loop until a full pass adds nothing
- 5: **return** the orbit, filtered by the remaining coordinates, and the group generated by the loop permutations

Assume $m \geq r$, choose r coordinates of γ whose Jacobian is generically nonsingular, and let $\pi: \mathbb{C}^m \rightarrow \mathbb{C}^r$ be the projection onto them. This gives a square map $\gamma_{\text{sub}} = \pi \circ \gamma: \mathbb{C}^r \rightarrow \mathbb{C}^r$, and $\gamma_{\text{sub}}^{-1}(\pi(\gamma^*)) \supseteq \gamma^{-1}(\gamma^*)$ for $\gamma^* \in U$. Let $\mathcal{B}$ now denote the branch locus of γ_{sub} , a hypersurface.

Theorem 9.1 ([15, Thm. 3.1, Cor. 3.2]). *Let ℓ be a line meeting $\mathcal{B}$ transversally in δ reduced points. Then the monodromy permutations of loops around any $\delta - 1$ of these points generate the monodromy group. The same holds for loops around the points of $\mathcal{B}' \cap \ell$, for any hypersurface $\mathcal{B}' \supseteq \mathcal{B}$.*

Corollary 9.2. *Under the hypotheses of Theorem 9.1, let $b_0 \in \ell \setminus \mathcal{B}$. The orbit of any one point of $\gamma_{\text{sub}}^{-1}(b_0)$ under the loops around $\mathcal{B} \cap \ell$ is all of $\gamma_{\text{sub}}^{-1}(b_0)$. If $\gamma^* \in U$ has $\pi(\gamma^*) = b_0$, then intersecting the orbit with the zero set of the remaining coordinates of $\gamma - \gamma^*$ gives $\gamma^{-1}(\gamma^*)$.*

Proof. The domain is irreducible, so the monodromy group is transitive. By Theorem 9.1 the loops generate it. Hence the orbit of one point under the loops is the orbit under the whole group, which is the preimage. $\square$

Theorem 9.1 is due to Hauenstein, Rodriguez and Sottile, whose algorithm takes the preimage as input and computes the group. We use the same loops the other way round, as a stopping rule that produces the preimage. Monodromy has also been used to recover the symmetries of a polynomial system [10], and to estimate the number of solutions statistically [16].

9.1. The witness set. By [15, Prop. 3.4, Rem. 3.6], the critical points of γ_{sub} over the line $\ell(s) = b_0 + sv$ are the solutions of the square system

$$\gamma_{\text{sub}}(\theta) = \ell(s), \quad J(\theta)w = 0, \quad a \cdot w = 1$$

in $(\theta, s, w) \in \mathbb{C}^{2r+1}$, with J the Jacobian of γ_{sub} and a random. The s -values of its solutions, clustered, form $W = \mathcal{B} \cap \ell$. The loops are lollipops based at $s = 0$: a radial segment to a circle of radius η about $w \in W$, the circle, and the segment back. Here η is smaller than half the least distance between points of $W \cup \{0\}$, and smaller than the distance from every other point of W to every segment. For a generic line no two points of W lie on a common ray from 0, so the segments do not overlap, and the loops form a geometric basis of $\pi_1(\ell \setminus W)$. If the coordinates of γ_{sub} are polynomials of degree at most δ , the square system consists of r equations of degree δ , r equations of degree at most δ in (θ, w) , and one linear equation, so by Bézout's theorem it has at most δ^{2r} isolated solutions. Hence $|W| \leq \delta^{2r}$, and by Theorem 9.1 at most $\delta^{2r} - 1$ loops are needed.

Remark 9.3. Each hypothesis is either checked or reported. A positive-dimensional preimage has no finite branch locus, and the algorithm refuses it rather than using the group of a slice. A line that is not transverse gives a proper subgroup without any sign of it, so the verdict is probabilistic. The theorem of [15] needs a rational base, and it has one, since the base of γ_{sub} is $\mathbb{C}^r$. The group reported is that of γ_{sub} , and it is the group of γ only when the preimages of γ_{sub} and γ coincide. It is the geometric Galois group of Section 8.3, which equals G when the Galois closure adds no constants.

Algorithm 6 Rationality trace test**Input:** sheets S over b_0 ; the degree bound D of Proposition 10.2**Output:** *complete* or *incomplete*

- 1: **for** r' independent random directions v and forms λ **do**
- 2: track S to sample points $t_1, \dots, t_M$; compute $T_S(t_i)$
- 3: fit p, q of degree $\leq D$, with q normalised, by least squares on $T_S(t_i) q(t_i) - p(t_i) = 0$
- 4: **end for**
- 5: **return** *complete* if every residual is below tolerance, otherwise *incomplete*

10. A RATIONALITY TRACE TEST

Let S be a set of sheets of the preimage found numerically over a base point. The trace test decides whether S is all of the preimage. In the classical setting [36, 21, 14], a curve is cut by a pencil of parallel hyperplanes in the space where the points live. The trace, meaning the sum of the points, is then affine-linear in the pencil parameter exactly when the set is complete. In our setting the natural slice is a line $b(t) = b_0 + tv$ in the base of the square map γ_{sub} of Section 9. Its preimages form a curve in V , but t is not a linear pencil parameter on V . Throughout this section the sheets are those of γ_{sub} , and d denotes their number.

Example 10.1. For the Lotka–Volterra model with the base normalised, one coordinate of a point of the preimage along $b(t)$ is $z(t) = z_0(1 + tv_1)/(1 + tv_0)$. This is a ratio with a pole, and every line in the base crosses the pole locus. The second difference of the trace, divided by h^2 , converged to 0.72 on the complete preimage as h decreased from 0.08 to 0.005, and to 2.27 with one sheet removed. Both values are nonzero, so no tolerance on linearity separates the two cases.

Let λ be a linear form on V and let $\theta_1(t), \dots, \theta_d(t)$ be the sheets over $b(t)$, as local analytic functions away from $\mathcal{B}$. For $S \subseteq \{1, \dots, d\}$ write $T_S(t) = \sum_{j \in S} \lambda(\theta_j(t))$.

Proposition 10.2. $T_{\{1, \dots, d\}}$ is a rational function of t . If the coordinates of γ_{sub} are polynomials of degree at most δ , its degree is at most δ^{r-1} .

Proof. The full trace is a symmetric function of the sheets, so continuation along any loop in $\ell \setminus \mathcal{B}$ fixes it, and it is single-valued. It is algebraic over $\mathbb{C}(t)$, since each $\lambda(\theta_j(t))$ is. A single-valued algebraic function on $\mathbb{P}^1$ minus finitely many points is rational.

For the bound, assume $v_1 \neq 0$ after reordering. Eliminating t through the first coordinate, the union of the sheets lies on the curve cut out by the $r - 1$ equations $\gamma_{\text{sub},j}(\theta) - b_{0,j} = (v_j/v_1)(\gamma_{\text{sub},1}(\theta) - b_{0,1})$, $j \geq 2$, each of degree at most δ . By Bézout's theorem the closure $C \subset \mathbb{P}^r$ of the union of the sheets has degree at most δ^{r-1} . The linear form λ , as a function on C , has its poles at the hyperplane at infinity, so its degree on C is at most $\deg C$. A pole of the trace at $t_0 \in \mathbb{P}^1$ comes from poles of λ at points of C over t_0 , and its order is at most the sum of their orders. So the degree of $T_{\{1, \dots, d\}}$ is at most the degree of λ on C . $\square$

Proposition 10.3. Let $\emptyset \neq S \subsetneq \{1, \dots, d\}$. Assume that $\sum_{j \in S} \theta_j(t) \neq \sum_{j \in S'} \theta_j(t)$, as functions, for every set $S' \neq S$ of the same size. Then T_S is not a rational function of t for a generic λ .

Proof. The monodromy group is transitive, so it stabilises no proper nonempty subset of the sheets. Choose a loop taking S to some $S' \neq S$. If T_S were rational, and in particular single-valued, then $T_S = T_{S'}$. For generic λ this equality of linear forms on the two vector sums contradicts the assumption. $\square$

The residual is numerical, so Algorithm 6 gives numerical evidence. A direction v that happens to flatter an incomplete set is caught by the independent repetitions. On a zero-dimensional preimage, the degree of θ_i is the number of distinct values it takes on the sheets of a complete S .

USE OF AI

The algorithms in this paper were developed by Noether 1.0, the Large Algorithmic Model (LAM) of Specht Labs, in companion with Fable 5.1 and GPT Astra from Anthropic and OpenAI respectively. The authors are responsible for the content of this paper.

REFERENCES

- [1] D. J. Bates, J. D. Hauenstein, and N. Meshkat. Identifiability and numerical algebraic geometry. *PLOS ONE*, 14(12):e0226299, 2019.
- [2] G. Bellu, M. P. Saccomani, S. Audoly, and L. D’Angiò. DAISY: a new software tool to test global identifiability of biological and physiological systems. *Comput. Methods Programs Biomed.*, 88:52–61, 2007.
- [3] M. Bôcher. The theory of linear dependence. *Ann. of Math. (2)*, 2:81–96, 1900–1901.
- [4] C. Bortner and N. Meshkat. Graph-based sufficient conditions for indistinguishability of linear compartmental models. *SIAM J. Appl. Dyn. Syst.*, 23(3):2179–2207, 2024.
- [5] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In *Proc. ISSAC*, pages 158–166, 1995.
- [6] D. A. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms*. Springer, fourth edition, 2015.
- [7] S. Demignot and D. Domurado. Effect of prosthetic sugar groups on the pharmacokinetics of glucose-oxidase. *Drug Des. Deliv.*, 1:333–348, 1987.
- [8] J. D. Dixon and B. Mortimer. *Permutation Groups*. Grad. Texts in Math. 163, Springer, 1996.
- [9] R. Dong, C. Goodbrake, H. A. Harrington, and G. Pogudin. Differential elimination for dynamical models via projections with applications to structural identifiability. *SIAM J. Appl. Algebra Geom.*, 2023. arXiv:2111.00991.
- [10] T. Duff, V. Korotynskiy, T. Pajdla, and M. H. Regan. Using monodromy to recover symmetries of polynomial systems. In *Proc. ISSAC*, 2023.
- [11] W. Fulton. *Intersection Theory*. Springer, second edition, 1998.
- [12] K. R. Godfrey and M. J. Chapman. Identifiability and indistinguishability of linear compartmental models. *Math. Comput. Simulation*, 32:273–295, 1990.
- [13] J. Harris. Galois groups of enumerative problems. *Duke Math. J.*, 46(4):685–724, 1979.
- [14] J. D. Hauenstein and J. I. Rodriguez. Multiprojective witness sets and a trace test. *Adv. Geom.*, 20(3):297–318, 2020.
- [15] J. D. Hauenstein, J. I. Rodriguez, and F. Sottile. Numerical computation of Galois groups. *Found. Comput. Math.*, 18:867–890, 2018.
- [16] J. D. Hauenstein and S. N. Sherman. Using monodromy to statistically estimate the number of solutions. In *2nd IMA Conference on Mathematics of Robotics*, Springer, 2021.
- [17] B. Hollering and S. Sullivant. Identifiability in phylogenetics using algebraic matroids. *J. Symbolic Comput.*, 104:142–158, 2021.
- [18] H. Hong, A. Ovchinnikov, G. Pogudin, and C. Yap. Global identifiability of differential models. *Comm. Pure Appl. Math.*, 73(9):1831–1879, 2020.
- [19] I. Kaplansky. *An Introduction to Differential Algebra*. Hermann, Paris, 1957.
- [20] E. R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, 1973.
- [21] A. Leykin, J. I. Rodriguez, and F. Sottile. Trace test. *Arnold Math. J.*, 4(1):113–125, 2018.
- [22] T. S. Ligon, F. Fröhlich, O. T. Chiş, J. R. Banga, E. Balsa-Canto, and J. Hasenauer. GenSSI 2.0: multi-experiment structural identifiability analysis of SBML models. *Bioinformatics*, 34(8), 2018.
- [23] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30(2):265–276, 1994.
- [24] G. Malić and I. Streinu. Combinatorial resultants in the algebraic rigidity matroid. In *Proc. SoCG, LIPIcs* 189, 2021.
- [25] N. Meshkat, C. E.-Z. Kuo, and J. J. DiStefano III. On finding and using identifiable parameter combinations in nonlinear dynamic systems biology models and COMBOS: a novel web implementation. *PLOS ONE*, 9(10):e110261, 2014.
- [26] N. Meshkat, Z. Rosen, and S. Sullivant. Algebraic tools for the analysis of state space models. In *The 50th Anniversary of Gröbner Bases*, Adv. Stud. Pure Math. 77, 2018.
- [27] O. Ore. Theory of non-commutative polynomials. *Ann. of Math. (2)*, 34(3):480–508, 1933.
- [28] A. Ovchinnikov, A. Pillay, G. Pogudin, and T. Scanlon. Multi-experiment parameter identifiability of ODEs and model theory. *SIAM J. Appl. Algebra Geom.*, 6(3):339–367, 2022.

- [29] A. Ovchinnikov, G. Pogudin, and P. Thompson. Parameter identifiability and input–output equations. *Appl. Algebra Engrg. Comm. Comput.*, 2023. arXiv:2007.14787.
- [30] J. Oxley. *Matroid Theory*. Oxford University Press, second edition, 2011.
- [31] X. Rey Barreiro et al. Structural identifiability and discrete symmetries. arXiv:2507.19884, 2025.
- [32] J. F. Ritt. *Differential Algebra*. Amer. Math. Soc. Colloq. Publ. 33, 1950.
- [33] Z. Rosen, J. Sidman, and L. Theran. Algebraic matroids in action. *Amer. Math. Monthly*, 127(3):199–216, 2020.
- [34] A. Sedoglavic. A probabilistic algorithm to test local algebraic observability in polynomial time. *J. Symbolic Comput.*, 33(5):735–755, 2002.
- [35] J.-P. Serre. *Topics in Galois Theory*. Jones and Bartlett, Boston, 1992.
- [36] A. J. Sommese, J. Verschelde, and C. W. Wampler. Symmetric functions applied to decomposing solution sets of polynomial systems. *SIAM J. Numer. Anal.*, 40(6):2026–2046, 2002.
- [37] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.
- [38] M. van der Put and M. F. Singer. *Galois Theory of Linear Differential Equations*. Springer, 2003.
- [39] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, third edition, 2013.

CHIEF EXECUTIVE OFFICER, SPECHT LABS, NEW YORK, NY

Email address: sanay@spechtlabs.ai

CHIEF TECHNOLOGY OFFICER, SPECHT LABS, NEW YORK, NY

Email address: davi@spechtlabs.ai