Differential Algebra

Gleb Pogudin

November 26, 2020

Contents

About

- If an exercise is marked with *, this means that Gleb does not know a solution.
- If an exercise is marked with §, this means that this is an open-ended or even philosophical question (therefore, Gleb does not know a solution).

All typos, errors, and comments to be sent to `gleb.pogudin@polytechnique.edu`

Notations and conventions

Unless stated otherwise, all the fields are assumed to be of characteristic zero. The ideal generated by elements $f_1, \ldots, f_\ell$ of a commutative ring R will be denoted $\langle f_1, \ldots, f_\ell \rangle$.

0 Before we start: arithmetic of differential polynomials

0.1 Differential rings, field, polynomials

Definition 0.1 (Some general definitions)**.**

- Let R be a commutative ring. An additive map $\delta \colon R \to R$ is called *a derivation* if it satisfies the Leibniz rule:
$$\delta(ab) = \delta(a)b + a\delta(b) \quad \text{for every } a, b \in R.$$
We will typically denote $\delta(a)$ by a' and, for $n \geqslant 0$, $\delta^n(a)$ by $a^{(n)}$.
- A commutative ring equipped with a derivation is called *a differential ring*. If the ring is a field, it is called *a differential field*.
- For a differential ring, a subring closed under the derivation is called *a differential subring*. The same for subfields.

- A differential ring which is an algebra over its differential subfield, is called *a differential algebra.*

Example 0.2.

- Any ring can be considered as a differential ring with respect to the zero derivation.
- Consider the ring $\mathbb{C}[x]$ and the field $\mathbb{C}(x)$. They are a differential ring and a differential field with respect to $\frac{\mathrm{d}}{\mathrm{dx}}$, respectively. Moreover, they are differential algebras over the constant field $\mathbb{C}$.
- Let $D \subset \mathbb{C}$ be a domain in the complex plane. By $\mathrm{Hol}(D)$ and $\mathrm{Mer}(D)$ we denote the set of all holomorphic and meromorphic functions in D, respectively. They are a differential ring and a differential field with respect to $\frac{\mathrm{d}}{\mathrm{dz}}$, respectively.

Remark on PDEs 0.3. The above definitions can be generalized to the PDE case by considering rings (fields, algebras) with respect to several commuting derivations yielding to the notion of *partial differential ring* (or *Δ-ring* if Δ is a fixed set of symbols for derivations).

For example, if $\Delta = \{\delta_1, \delta_2\}$, then $\mathbb{C}[x, y]$ can be equipped with the structure of Δ-ring by defining the actions of δ_1 and δ_2 to be $\frac{\partial}{\partial x}$ and $\frac{\partial}{\partial y}$, respectively.

Definition 0.4 (Differential polynomials)**.** Let R be a differential ring. Consider a ring of polynomials in infinitely many variables

$$R\{x\} := R[x, x', x'', x^{(3)}, \ldots]$$

and extend the derivation from R to this ring by $(x^{(j)})' := x^{(j+1)}$. The resulting differential ring is called *the ring of differential polynomials in x over R.*

The ring of differential polynomials in several variables is defined by iterating this construction.

Example 0.5. Weierstrass's elliptic function $\wp(z)$ satisfies the following differential equations: $(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. This equation can be written as the following differential polynomial over a constant field $\mathbb{Q}(g_2, g_3)$:

$$(x')^2 - 4x^3 - g_2 x - g_3.$$

Example 0.6. The Wronskian of differential variables $x_1, x_2, \ldots, x_n$

$$\mathrm{Wronsk}(x_1, \ldots, x_n) = \begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_1' & x_2' & \ldots & x_n' \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{(n-1)} & x_2^{(n-1)} & \ldots & x_n^{(n-1)} \end{vmatrix} \tag{1}$$

is a differential polynomial from $\mathbb{Q}\{x_1, \ldots, x_n\}$.

Remark on PDEs 0.7. For a fixed set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of symbols for derivations, one can define Δ-polynomials over a Δ-ring R in the same way by adding an infinite set of variables indexed by $\mathbb{Z}^m_{\geqslant 0}$ so that δ_i acts by incrementing the i-th coordinate. The ring will be denoted by $R\{x\}_\Delta$.

For example, for $\Delta = \{\delta_1, \delta_2\}$, the Jacobian $J = \begin{vmatrix} \delta_1 x & \delta_2 x \\ \delta_1 y & \delta_2 y \end{vmatrix}$ belongs to $\mathbb{Q}\{x, y\}_\Delta$.

Definition 0.8. Every differential polynomial $P \in k\{x_1, \ldots, x_n\}$ has the following properties:

- For every $1 \leqslant i \leqslant n$, we will call the largest j such that $x_i^{(j)}$ appears in P *the order of P with respect to x_i* and denote it by $\operatorname{ord}_{x_i} P$; if P does not involve x_i, we set $\operatorname{ord}_{x_i} P := -1$.
- *The order of P* is $\operatorname{ord} P := \max\limits_{1 \leqslant i \leqslant n} \operatorname{ord}_{x_i} P$.
- For every $1 \leqslant i \leqslant n$ such that x_i appears in P, *the initial of P with respect to x_i* is the leading coefficient of P considered as a univariate polynomial in $x_i^{(\operatorname{ord}_{x_i} P)}$. We denote it by $\operatorname{init}_{x_i} P$.
- For every $1 \leqslant i \leqslant n$ such that x_i appears in P, *the separant of P with respect to x_i* is

$$\operatorname{sep}_{x_i} P := \frac{\partial P}{\partial x_i^{(\operatorname{ord}_{x_i} P)}}.$$

Example 0.9. Consider the differential polynomial $P = (x')^2 - 4x^3 - g_2 x - g_3 \in \mathbb{Q}(g_2, g_3)\{x\}$ from Example 0.5. Then

$$\operatorname{ord}_x P = 1, \quad \operatorname{init}_x P = 1, \quad \operatorname{sep}_x P = 2x'.$$

Example 0.10. One can see that (see Example 0.6 for notation):

$$\operatorname{sep}_{x_i} \operatorname{Wronsk}(x_1, \ldots, x_n) = \operatorname{init}_{x_i} \operatorname{Wronsk}(x_1, \ldots, x_n) = (-1)^{i+1} \operatorname{Wronsk}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).$$

The importance of the notion of the separant is based on the following crucial observation.

Very important observation. *Let $P \in k\{x_1, \ldots, x_n\}$, and consider $1 \leqslant i \leqslant n$ such that $h := \operatorname{ord}_{x_i} P \geqslant 0$. Then, for every j, there exists $Q \in k\{x_1, \ldots, x_n\}$ with $\operatorname{ord}_{x_i} Q < h + j$ such that*

$$P^{(j)} = (\operatorname{sep}_{x_i} P) x_i^{(h+j)} + Q.$$

Remark on PDEs 0.11. The notions of initial and separant (from Definition 0.8) can be generalized to the PDE case. Since, for several derivatives, there is no canonical way to choose "the highest of the derivatves of x appearing in the polynomial", one should fix a monomial ordering on the derivatives of a single variable (considered as monomials in the elements of Δ).

0.2 Differential reduction

The differential reduction algorithm may be viewed as a generalization of the division with remainder for univariate polynomials.

Algorithm 1 Differential reduction

```
Input   differential polynomials $f, g \in k\{x\}$ such that $f \notin k$;
Output  a differential polynomial $\widetilde{g} \in k\{x\}$ such that
        • $\operatorname{ord}_x \widetilde{g} < \operatorname{ord}_x f$ or $\operatorname{ord}_x \widetilde{g} = \operatorname{ord}_x f = h$ and $\deg_{x^{(h)}} \widetilde{g} < \deg_{x^{(h)}} f$;
        • there exist $a, b \in \mathbb{Z}_{\geqslant 0}$ such that
              $(\operatorname{sep}_x f)^a (\operatorname{init}_x f)^b g - \widetilde{g} \in \langle f, f', f'', \ldots \rangle$.
(Step 1) Set $h := \operatorname{ord}_x f$ and $d := \deg_{x^{(h)}} f$;
(Step 2) While $\operatorname{ord}_x g > h$ do
        (a) Set $H := \operatorname{ord}_x g$, $D := \deg_{x^{(H)}} g$;
        (b) $g := (\operatorname{sep}_x f) g - (\operatorname{init}_x g)(x^{(H)})^{D-1} f^{(H-h)}$;
(Step 3) While $\deg_{x^{(h)}} g \geqslant d$ do
        (a) Set $D := \deg_{x^{(H)}} g$;
        (b) $g := (\operatorname{init}_x f) g - (\operatorname{init}_x g)(x^{(h)})^{D-d} f$;
(Step 4) Return $g$.
```

Lemma 0.12. *Algorithm 1 always terminates and returns a correct result.*

Proof. Left as an exercise. □

Example 0.13. We will show that the result of the reduction of $g = x'' - 1$ with respect to $f = (x')^2 - x$ is zero. Since $\operatorname{ord}_x g > \operatorname{ord}_x f$, we compute:

$$(\operatorname{sep}_x f) g - (\operatorname{init}_x g) f' = (2x')(x'' - 1) - 1 \cdot (2xx' - x') = 0.$$

One can interpret this as follows. The solutions of $f = 0$ are $x = (0.5t + c)^2$ (c — arbitrary constant) and $x = 0$, and the former is also a solution of $g = 0$ while the latter is a solution of $\operatorname{sep}_x f = 0$. Therefore, g is reducible to zero because it vanished at all "nonspecial" solutions of f.

0.3 Exercises

Exercise 0.1. Consider the polynomial P from Example 0.5 with $g_2 = 0, g_3 = 1$, that is, $P = (x')^2 - 4x^3 - 1$. Show that $x'' - 6x^2$ reduces to zero with respect to P.

Exercise 0.2. Verify that the following differential polynomials are reduced to zero with respect to $(x')^2 - x^2$

1. $x'' - x$;

2. $\operatorname{Wronsk}(x, x')$.

Try to explain why.

Exercise 0.3. Could it happen that a derivative of an irreducible nonconstant differential polynomial is

1. reducible?

2. non-squarefree?

Exercise 0.4.

1. Show that there is no $q \in \mathbb{C}\{x\}$ such that $q' = \operatorname{Wronsk}(x, x') = \begin{vmatrix} x & x' \\ x' & x'' \end{vmatrix}$ (see (1)).

2. Propose an algorithm that takes $p \in \mathbb{C}\{x\}$ as input and determines whether it has an integral (that is, there exists $q \in \mathbb{C}\{x\}$ such that $q' = p$).

Exercise* 0.5. Note that, although $\operatorname{Wronsk}(x, x') \in \mathbb{Q}\{x\}$ does not have an integral, the differential rational function $\frac{\operatorname{Wronsk}(x,x')}{(x')^2}$ does. Propose an algorithm that takes $p \in \mathbb{C}\{x\}$ and checks whether there exists a differential rational function r *of lower order* such that pr has an integral.

Exercise§ 0.6. Would it be possible to reformulate the algorithm from Exercise 0.4 in the language of homology, that is to define a "natural" map from $\mathbb{C}\{x\}$ so that its kernel is exactly the set of all the derivatives?

Exercise 0.7. Prove that the following identity holds in $\mathbb{Q}\{x_1, \ldots, x_n, y\}$:

$$\operatorname{Wronsk}(x_1 y, x_2 y, \ldots, x_n y) = y^n \operatorname{Wronsk}(x_1, \ldots, x_n).$$

1 Differential ideals

We will use the following fact from commutative algebra of polynomial rings in infinitely many variables.

Theorem 1.1 (Follows from the main theorem of [3])**.** *Let Λ be a countable set, F be a field, E be an algebraically closed field of uncountable transcendence degree over F, and I be an ideal in $F[x_\lambda \mid \lambda \in \Lambda]$. Then, for every $f \in F[x_\lambda \mid \lambda \in \Lambda]$, the following are equivalent:*

- *there exists N such that $f^N \in I$;*
- *for every homomorphism $\phi\colon F[x_\lambda \mid \lambda \in \Lambda] \to E$ such that $I \subset \ker \phi$, $\phi(f) = 0$.*

1.1 Differential ideals, their radicals and prime components

Definition 1.2 (Differential ideal)**.** Let $S := R\{x_1, \ldots, x_n\}$ be a ring of differential polynomials over a differential ring R. An ideal $I \subset S$ is called *a differential ideal* if $a' \in I$ for every $a \in I$.

One can verify that, for every $f_1, \ldots, f_s \in S$, the ideal generated by

$$\left\{ f_i^{(j)} \mid 1 \leqslant i \leqslant s,\ j \geqslant 0 \right\}$$

is a differential ideal. Moreover, this is the minimal differential ideal containing $f_1, \ldots, f_s$, and we will denote it by $[f_1, \ldots, f_s]$.

Example 1.3. TODO

It turns out that two fundamental operations in commutative algebra, taking the radical of an ideal and prime decomposition of a radical ideal, respect the differential structure.

Proposition 1.4 (Taking radical is differential-friendly)**.** *Let $I \subset R$ be a differential ideal in a differential ring R such that $\mathbb{Q} \subset R$. Then the radical*

$$\sqrt{I} := \{f \in R \text{ such that } \exists N \colon f^N \in I\}$$

is also a differential ideal.

Proof. We will prove the proposition by first proving that,

$$\text{for every } m \geqslant 1 \colon x' \in \sqrt{[x^m]} \subset \mathbb{Q}\{x\}. \tag{2}$$

Proving (2) would imply that there exists M such that $(x')^M$ can be written as a $\mathbb{Q}\{x\}$-linear combination of the derivatives of x^m. Then, if $a \in \sqrt{I}$ with $a^n \in I$, plugging $x = a$ into this representation would yield that $(a')^M \in I$.

In order to prove (2), consider any homomorphism (not necessarily differential) $\phi \colon \mathbb{Q}\{x\} \to \mathbb{C}$ to such that $[x^m] \subset \ker \phi$. Then $\phi(x) = 0$. Observe that, due to the pigeonhole principle, $(x^m)^{(m)}$ can be written as:

$$(x^m)^{(m)} = m!(x')^m + x \cdot Q,$$

for some $Q \in \mathbb{Q}\{x\}$. Applying ϕ to both sides of the equality and using $[x^m] \subset \ker \phi$, we obtain

$$0 = \phi((x^m)^{(m)}) = m!\phi((x')^m) + \phi(x)\phi(Q) = m!\phi(x')^m.$$

Therefore, $\phi(x') = 0$, so $x' \in \sqrt{[x^n]}$ due to Theorem 1.1. □

Remark 1.5. A refined version of this proof will be discussed in the next section (TODO: REF). A more "syntactic" proof can be found in [2, Lemma 1.7] which yields that $M \leqslant 2^m$ in the notation of the proof above. Sharp bounds these exponents were obtained in [5]. See also Exercise 1.1.

Proposition 1.6 (Prime decompositions are differential-friendly)**.** *Let R be a differential ring containing $\mathbb{Q}$. Then every radical differential ideal in R is an intersection of prime differential ideals.*

The proof of the proposition will rely on the following lemma "arithmetic" property of radical differential ideals.

Lemma 1.7. *Let $R \supset \mathbb{Q}$ be a differential ring. Let $A, B \subset R$. Then*

$$\sqrt{[A \cdot B]} = \sqrt{[A] \cdot [B]}.$$

Proof. Since $[A \cdot B] \subseteq [A] \cdot [B]$, we have $\sqrt{[A \cdot B]} \subseteq \sqrt{[A] \cdot [B]}$.

In the other direction, observe that the differential ideal $[A] \cdot [B]$ is generated as an ideal by products of the form $a^{(i)}b^{(j)}$, where $a \in A, b \in B, i, j \geqslant 0$. Exercise 1.2 implies that $a^{(i)}b^{(j)} \in \sqrt{[ab]} \subseteq \sqrt{[A \cdot B]}$. □

Corollary 1.8. *Let S be a multiplicatively closed subset of a differential ring $R \supset \mathbb{Q}$ such that $0 \notin S$. Consider a maximal differential ideal I not containing S. Then I is prime.*

Proof. Assume that I is not prime, so there are $a_1, a_2 \in R$ such that $a_1 a_2 \in I$ and $a_1, a_2 \notin I$. The maximality of I implies that there exist $s_1, s_2 \in S$ such that $s_i \in \sqrt{[I, a_i]}$ for $i = 1, 2$. Then Lemma 1.7 implies that

$$s_1 s_2 \in \sqrt{[I, a_1]}\sqrt{[I, a_2]} \subseteq \sqrt{[I, a_1] \cdot [I, a_2]} = \sqrt{I},$$

so we have arrived at a contradiction. □

Proof of Proposition 1.6. Let $I \subset R$ be a radical differential ideal. Consider $a \notin I$. Then $S := \{a^i \mid i \geqslant 1\}$ is a multiplicatively closed set disjoint with I. Consider a maximal differential ideal containing I and not intersecting S. Corollary 1.8 implies that this ideal is prime. Therefore, the intersection of all prime differential ideals containing I does not contain a. Thus, this intersection is equal to I. □

Remark 1.9. We will show later (REF) that a radical ideal in $k\{x_1, \ldots, x_n\}$ is an intersection of finitely many prime differential ideals yielding that the prime components of a radical differential ideal are differential ideals.

Remark on PDEs 1.10. All the proofs in this subsection can be used verbatim for the case of several commuting derivations.

Definition 1.11 (Differential spectrum)**.** We will call the set of all prime differential ideals of a differential ring R *the differential spectrum* of R and denote by $\operatorname{diffspec} R$ (we will introduce the corresponding topology later). We will denote the set of all prime differential ideals in R containing a set S by $\mathbb{V}(S) \subset \operatorname{diffspec} R$. Then Proposition 1.6 implies that, for radical ideals $I, J \subset R$, we have $I = J \iff \mathbb{V}(I) = \mathbb{V}(J)$. Using the language of algebraic geometry, we will say that an element $f \in R$ vanishes at $P \in \operatorname{diffspec} R$ if $f \in P$.

Lemma 1.12. *Let R be a differential ring. Prove that*

1. *for every subsets and $S, T \subset R$, $\mathbb{V}(S \cdot T) = \mathbb{V}(S) \cup \mathbb{V}(T)$;*
2. *a radical ideal $I \subset R$ is prime if and only if, for every subsets $S, T \subset R$, $\mathbb{V}(I) = \mathbb{V}(S) \cup \mathbb{V}(T)$ implies that $\mathbb{V}(I) = \mathbb{V}(S)$ or $\mathbb{V}(I) = \mathbb{V}(T)$.*

Proof. Left as Exercise 1.3 □

1.2 Bad news: no Noetherianity in general

Proposition 1.13. *The following chain of ideals in $\mathbb{Q}\{x\}$ is an infinite strictly ascending:*

$$[x^2] \subsetneq [x^2, (x')^2] \subsetneq [x^2, (x')^2, [x^2, (x'')^2] \subsetneq \dots$$

Proof. For $i \geqslant 0$, we denote $I_i := [x^2, (x')^2, \dots, (x^{(i)})^2]$. We will show that $p := (x^{(i+1)})^2 \not\in I_i$. Assume the contrary. Since I_i is generated by homogeneous polynomials of degree two, $(x^{(i+1)})^2$ must be a $\mathbb{Q}$-linear combination of the derivatives of the generators. Moreover, since the generators of I_i are also homogeneous with respect to the grading assigning weight $j+1$ to each $x^{(j)}$, $(x^{(i+1)})^2$ must be a $\mathbb{Q}$-linear combination of $p_0 := (x^2)^{(2i+2)}, p_1 := ((x')^2)^{(2i)}, \dots, p_i := ((x^{(i)})^2)''$. Since p_0 involves $xx^{(2i+2)}$ which does not appear in either of $p_1, \dots, p_i, p$, p_0 will not appear in the linear combination. Analogously, p_1 involves $x'x^{(2i+1)}$ which does not appear in either of $p_2, \dots, p_i, p$, so p_1 will not appear in the linear combination as well. Continuing in the same way, we show that none of $p_0, \dots, p_i$ will appear in the linear combination arriving at a contradiction. □

1.3 Prime univariate ideals

In this section we will show that prime univariate ideals over differential domains admit a concise representation. This fact is an important tool in differential algebra (see REF), and we will use it in the proof of the Ritt-Raudenbush theorem.

Notation 1.14. Let I be an ideal in ring R, and $a \in R$. Then:

$$I \colon a^\infty := \{b \in R \mid \exists N \colon a^N b \in I\}.$$

Proposition 1.15 (Univariate prime ideals)**.** *Let $R \supset \mathbb{Q}$ be a differential ring, and $P \subset R\{x\}$ be a prime differential ideal such that $P \neq \sqrt{[P \cap R]}$. Let f be an element of the lowest degree among the elements of the lowest order in $P \setminus \sqrt{[P \cap R]}$. Then*

$$P = [P \cap R, f] \colon (\operatorname{sep}_x(f) \operatorname{init}_x(f))^\infty.$$

Proof. Let $P_0 := \sqrt{[P \cap R]}$, $s := \operatorname{sep}_x f$, $\ell := \operatorname{init}_x f$, $h := \operatorname{ord}_x f$, and $d := \deg_{x^{(h)}} f$. We will show that $s, \ell \not\in P$.

- If $\ell \in P$, then due to the minimality of f, we have $\ell \in P_0$. Then $f - \ell(x^{(h)})^d \in P$ is of lower degree than f, so it belongs to P_0 as well implying that $f \in P_0$.
- If $s \in P$, then due to the minimality of f, we have $s \in P_0$. Then $f - \frac{1}{d}sx^{(h)}$ is of lower degree than f, so it belongs to P_0 as well implying that $f \in P_0$.

The primality of P implies that $s\ell \not\in P$. Let $P_1 := [P_0, f] \colon (s\ell)^\infty$.

First we show that $P_1 \subseteq P$. Let $g \in P_1$. Then there exists N such that $s^N \ell^N g \in [f, P_0] \subset P$. The primality of P implies that $g \in P$.

Now we show that $P \subseteq P_1$. Let $g \in P$. We perform the differential reduction 1 of g with respect to f. It will yield $a, b \in \mathbb{Z}_{\geqslant 0}$ and $\widetilde{g}$ such that

$$s^a \ell^b g - \widetilde{g} \in [f].$$

Since $g, f \in P$, $\widetilde{g}$ belongs to P as well. However, the minimality of f implies that $\widetilde{g} \in P_0$. Therefore, $g \in P_1$. □

1.4 Good news: Noetherianity for radical differential ideals (the Ritt-Raudenbush theorem and its corollaries)

The goal of this section is to prove the following fundamental fact in differential algebra.

Theorem 1.16 (Ritt-Raudenbush). *Let k be a differential field, and let $I \subset k\{x_1, \ldots, x_n\}$ be a radical differential ideal. Then there exist $f_1, \ldots, f_s \in k\{x_1, \ldots, x_n\}$ such that*

$$I = \sqrt{[f_1, \ldots, f_s]}.$$

Corollary 1.17 (ACC for radical differential ideals). *Let k be a differential field. Let*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

be an ascending chain of radical differential ideals in $k\{x_1, \ldots, x_n\}$. Then there exists N such that $I_N = I_{N+1} = I_{N+2} = \ldots$.

Proof of Corollary 1.17. Let $I := \bigcup\limits_{i=0}^{\infty} I_i$. Then I is a radical differential ideal. Theorem 1.16 provides us $f_1, \ldots, f_s$ such that $I = \sqrt{[f_1, \ldots, f_s]}$. There exists N such that $f_1, \ldots, f_s$. Therefore, $I_N = I_{N+1} = \ldots = I$. □

1.5 Proof of the Ritt-Raudenbash theorem

The Ritt-Raudenbash theorem (Theorem 1.16) will follow by induction on the number of differential variables from the Theorem 1.19 below.

Definition 1.18 (Basis property). Let I be a radical differential ideal in a differential ring R. A set $\{f_\lambda\}_{\lambda \in \Lambda} \subset R$ is called *a basis* of I if $I = \sqrt{[f_\lambda \mid \lambda \in \Lambda]}$. If $|\Lambda| < \infty$, we say that I has *a finite basis*.

We will say that a differential ring R *has the radical basis property* if every radical differential ideal R has a finite basis. In particular, Theorem 1.16 states that differential polynomial rings have this property.

Theorem 1.19. *Let R be a differential domain containing $\mathbb{Q}$ with the radical basis property. Then $R\{x\}$ also has the radical basis property.*

Lemma 1.20. *If a radical ideal I of a differential ring R has a finite basis, then one can choose a finite basis from any basis of I.*

Proof. Let $\{g_1, \ldots, g_s\}$ and $\{f_\lambda\}_{\lambda \in \Lambda}$ be two bases of I such that the former is finite. Since the expression of a suitable power of each of g_i's in terms of f_λ's involves only finitely many terms, then there exists a finite subset $\Omega \subset \Lambda$ such that $g_i \in \sqrt{[f_\lambda \mid \lambda \in \Omega]}$ for every $1 \leqslant i \leqslant s$. Therefore, $\{f_\lambda\}_{\lambda \in \Omega}$ is a finite subbasis. □

Proof of Theorem 1.19. Assume the contrary. Consider the set of all radical differential ideals in $R\{x\}$ not having a finite basis. This set satisfies the conditions of the Zorn's lemma. Let I be any maximal element in this set.

First we will prove that I is prime. Assume the contrary. The Lemma 1.12 implies that exist radical ideals J_1, J_2 such that $\mathbb{V}(I) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2)$ and $\mathbb{V}(I) \subsetneq \mathbb{V}(J_i)$ for $i = 1, 2$. Due to the maximality of I, there exist $B_1, B_2 \subset R$ such that $J_i = \sqrt{[B_i]}$ for $i = 1, 2$. Then, using Lemma 1.12, we have

$$\mathbb{V}(I) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2) = \mathbb{V}(B_1) \cup \mathbb{V}(B_2) = \mathbb{V}(B_1 B_2),$$

and this gives us a finite basis $B_1 B_2$ for I.

Let $I_0 := \sqrt{[I \cap R]}$. Applying Proposition 1.15 to I, we obtain that there exists $f \in I$ and $g \notin I$ such that $I = [I_0, f] \colon g^\infty$. The maximality of I implies that $\sqrt{[I, g]}$ has a finite basis. Lemma 1.20 implies that there exist $f_1, \ldots, f_m \in I$ such that $\sqrt{[I, g]} = \sqrt{[f_1, \ldots, f_m, g]}$. We claim that

$$I = I_1 := \sqrt{[I_0, f, f_1, \ldots, f_m]}. \tag{3}$$

Since $I_0 \subseteq I$ and $f, f_1, \ldots, f_m \in I$, $I_1 \subseteq I$. To prove the reverse inclusion, consider $q \in I$. Then there exists N such that $g^N q \in [I_0, f]$. Consider $P \in \mathbb{V}(I_1)$.

- If $g(P) \neq 0$, then q must vanish at P.
- If $g(P) = 0$, then $P \in \mathbb{V}(g, f_1, \ldots, f_m) \subset \mathbb{V}(I)$, so q vanishes at P.

Therefore, $q \in I_1$. Thus (3) is proved. Since $I_0 \subset R$, it has finite basis, so (3) gives a finite basis for I. □

1.6 Caveat: finite basis $\neq$ finitely generated

Although the Ritt-Raudenbash theorem shows that any radical differential ideal in a differential polynomial ring can be defined (as a radical differential ideal) by finitely many differential polynomials, it does not imply that any such ideal is finitely generated as a differential ideal.

Proposition 1.21. *The radical differential ideal $\sqrt{[xy]} \subset \mathbb{Q}\{x, y\}$ is not finitely generated as a differential ideal.*

Proof. First we show that $\sqrt{[xy]}$ is generated by $S = \{x^{(i)}y^{(j)} \mid i, j \geqslant 0\}$ as an ideal. $S \subset \sqrt{[xy]}$ due to Exercise 1.2. Consider any element $f \in \sqrt{[xy]}$. Since any monomial containing derivatives of both x and y is divisible by an element of S, modulo the ideal generated by S, f is equivalent to a differential polynomial of the form $f_0 + f_1 + c$, where $f_0 \in \mathbb{Q}\{x\}$ and $f_1 \in \mathbb{Q}\{y\}$ have zero constant term, and $c \in \mathbb{Q}$. We will show that $f_0 + c = 0$. Assume that $f_0 \neq 0$. Consider a homomorphism $\phi\colon \mathbb{Q}\{x, y\} \to \mathbb{Q}$ such that

$$\phi(y^{(i)}) = 0 \quad \text{for every } i \geqslant 0 \quad \text{and } \phi(f_0 + c) \neq 0.$$

Then $\ker \phi \supset \sqrt{[xy]}$ and $\phi(f) \neq 0$, so $f \notin \sqrt{[xy]}$. Similarly $f_1 + c = 0$, so $f_0 = f_1 = c = 0$. Therefore $\sqrt{[xy]}$ is generated by S.

Assume that $\sqrt{[xy]} = [g_1, \ldots, g_\ell]$ for some $g_1, \ldots, g_\ell \in \mathbb{Q}\{x, y\}$. Since all elements in S are homogeneous and isobaric (that is, the sum of the orders of derivatives in each monomial is the same), then, for every $f \in \sqrt{[xy]}$, its homogeneous isobaric components also belong to the ideal. Therefore, replacing $g_1, \ldots, g_\ell$ with their homogeneous isobaric components if necessary, we will further assume that they are homogeneous and isobaric. Moreover, we will assume that $\deg g_1 = \ldots = \deg g_r = 2$, and $\deg g_i > 2$ for $i > r$ (r may be zero). The homogeneity of the generators imply that each element of S must be a $\mathbb{Q}$-linear combination of the derivatives the $g_1, \ldots, g_r$. For every $1 \leqslant i \leqslant h$, we will denote the sum of the orders of the variables in any monomial of g_i (which is the same for different monomials due to the isobaricity) by h_i. Then the isobaricity of the generators implies that each element of

$$xy^{(r)},\ x'y^{(r-1)},\ \ldots,\ x^{(r)}y$$

is a $\mathbb{Q}$-linear combination of $g_1^{(r-h_1)}, \ldots, g_r^{(r-h_r)}$. However, it is impossible to write $r+1$ linearly independent vector as a linear combinations of r vectors. □

1.7 Special case: differential ideals of dynamical models

In this section, we consider a class of systems of differential equations ubiquitous in applications (so-called *state-space representation* of a model), show that they have extremely nice algebraic properties, and demonstrate a simple application of differential algebra to modeling. More precisely, we will **consider systems** of the form

$$\begin{cases} \mathbf{x}' = \mathbf{f}(\mathbf{p}, \mathbf{x}, \mathbf{u}), \\ \mathbf{y} = \mathbf{g}(\mathbf{p}, \mathbf{x}, \mathbf{u}), \end{cases} \tag{4}$$

where

- $\mathbf{p} = (p_1, \ldots, p_s)$ are unknown scalar parameter;
- $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_m)$, and $\mathbf{u} = (u_1, \ldots, u_\ell)$ are function variables refereed to as state, output, and input variables, respectively;
- $\mathbf{f}, \mathbf{g}$ are vectors of polynomials in $\mathbb{C}[\mathbf{p}, \mathbf{x}, \mathbf{u}]$ of dimensions n and m, respectively.

One should interpret the system (4) as follows. The input variables $\mathbf{u}$ are the functions determined by the experimenter/modeller (e.g., an external force or a drug injection). Together with the parameter values and the initial conditions for the state variables $\mathbf{x}$, they completely define the dynamics of the $\mathbf{x}$-variables. The output variables $\mathbf{y}$ are the quantities measured/observed in the experiment. The typical questions asked about such systems include:

- given the input-output data, is it possible to determine infer the values of the parameters (identifiability) or reconstruct the values of the state variables (observability);
- is it always possible to achieve the desired behaviour of the system by chosing appropriate input functions (controllability and control design);

- which functions in $\mathbf{x}$ and $\mathbf{u}$ remain constant along the trajectories (first integrals).

Example 1.22 (Predator-prey model)**.** The following model describes the coexistence of two species, prey (x_1) and predators (x_2), so that the population of prey can be observed and controlled:

$$x_1' = ax_1 - bx_1x_2 + u, x_2' = -cx_2 + dx_1x_2, y = x_1. \tag{5}$$

To put (4) into **the context of differential algebra**, consider a constant differential field $k = \mathbb{C}(\mathbf{p})$ to be a purely transcendental extension of $\mathbb{C}$ by the parameters. Then (4) can be recasted into the following $n + m$ differential polynomials:

$$\mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}),\ \mathbf{y} - \mathbf{g}(\mathbf{x}, \mathbf{u}) \in k\{\mathbf{x}, \mathbf{y}, \mathbf{u}\}, \tag{6}$$

where the dependence of $\mathbf{f}$ and $\mathbf{g}$ on $\mathbf{p}$ is now implicit as $\mathbf{p}$ now belongs to the field of coefficients.

Proposition 1.23. *In the notation above, consider differential ideal* $I := [\mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}),\ \mathbf{y} - \mathbf{g}(\mathbf{x}, \mathbf{u})] \subset k\{\mathbf{x}, \mathbf{y}, \mathbf{u}\}$.

1. *On the ring $k\{\mathbf{x}, \mathbf{y}, \mathbf{u}\}$ considered as a polynomial ring in infinitely many variables, consider the lexicographic monomial ordering corresponding to any ordering on the variables such that*

   (a) $y_{i_1}^{(i_2)} > x_{i_3}^{(i_4)} > u_{i_5}^{(i_6)}$ *for every* $i_1, \ldots, i_6$;

   (b) $i_1 > i_2 \implies a_{j_1}^{(i_1)} > a_{j_2}^{(i_2)}$ *for every* $a \in \{x, y, u\}$ *and* j_1, j_2.

   Then the set of all the derivatives of (6) for a Gröbner basis of I with respect to this ordering.

2. *As a commutative algebra, $k\{\mathbf{x}, \mathbf{y}\}/I$ is isomorphic to $k[\mathbf{x}]\{\mathbf{u}\}$. In particular, I is a prime differential ideal.*

Proof. 1. Note that the leading terms of $(x_i' - f_i(\mathbf{x}, \mathbf{u}))^{(j)}$ and $(y_i - g_i(\mathbf{x}, \mathbf{u}))^{(j)}$ will be $x_i^{(j+1)}$ and $y^{(j)}$, respectively. Therefore, the leading terms of all the derivatives of (6) will be distinct variables. Therefore, this set is a Gröbner basis by the first Buchberger's criterion.

2. The result of the reduction of any polynomial with respect to the Gröbner basis from the previous part of the proposition belongs to $k[\mathbf{x}]\{\mathbf{u}\}$, and none of the elements of this subring is reducible with respect to the basis. Therefore, the quotient with respect to I will be isomorphic to $k[\mathbf{x}]\{\mathbf{u}\}$.

□

Now we will demonstrate how the structure of this ideal can be used in **applications**.

Definition 1.24 (Field of definition)**.** Let $J \subset K\{x_1, \ldots, x_n\}$ be a differential ideal over a differential field K. Then the smallest differential subfield $L \subset K$ such that J is generated by $J \cap L\{x_1, \ldots, x_n\}$ is called the field of definition of J.

Consider the ideal I from Proposition 1.23. It has been shown in [4, Theorem 21] that the field of definition of

$$I \cap k\{\mathbf{y}, \mathbf{u}\}$$

is exactly the field of all functions in the parameters whose values can be determined from sufficiently many experiments with generic independent inputs and initial conditions.

Example 1.25. Consider the following model:

$$\begin{cases} x_1' = p_1x_2, \\ x_2' = p_2x_1, \\ y = x_1. \end{cases}$$

We can find at least one element $I \cap \mathbb{C}(p_1, p_2)\{y\}$ in by

$$y'' = x_1'' = p_1x_2' = p_1p_2x_1 = p_1p_2y.$$

Moreover, one can show that $I \cap \mathbb{C}(p_1, p_2)\{y\} = [y'' - p_1p_2y]$. Hence, its field of definition is $\mathbb{Q}(p_1p_2)$, so the value p_1p_2 can be found experimentally while p_1 and p_2 cannot (look at the system an convince yourself in this!).

Proposition 1.26. *Assume that $m = 1$, that is, the system has only one output. Consider a polynomial f in $I \cap k\{y, \mathbf{u}\}$ of the lowest possible degree among the polynomials of the lowest possible order in y.*

1. *Normalize f so that at least one of the coefficients is 1. Then the remaining coefficient generate the field of definition of $I \cap k\{y, \mathbf{u}\}$ and, consequently, the field of functions identifiable from multiple experiments.*

2. *For every $j \geqslant 0$, we define*

   $$I_j := \langle (\mathbf{x}' - \mathbf{f}(\mathbf{x}, \mathbf{u}))^{(i)}, (y - g(\mathbf{x}, \mathbf{u}))^{(i)}, (y - \mathbf{g}(\mathbf{x}, \mathbf{u}))^{(j)} \mid 0 \leqslant i < j \rangle \subset R_j := k[\mathbf{x}, \ldots, \mathbf{x}^{(j)}, y, \ldots, y^j, \mathbf{u}, \ldots, \mathbf{u}^{(j)}].$$

   Then f is contained in I_n. In particular, f can be found using a Gröbner basis computation.

Proof. 1. Proposition 1.23 implies that I is prime, so $J := I \cap k\{y, \mathbf{u}\}$ is prime as well. Since none of the derivatives of $\mathbf{u}$ appear as in the leading terms of the Gröbner basis of I described in Proposition 1.23, $I \cap k\{\mathbf{u}\} = \{0\}$. Applying Proposition 1.15 to J viewed as a univariate prime differential ideal over $k\{\mathbf{u}\}$, we deduce that

$$J = [f] \colon g^{\infty},$$

where g is the product of the initial and separant of f. Let F be the field generated by the coefficients of f (after the normalization). Due to the minimality of f, any set of generators of J must contain f, so F is contained in the field of definition of J. Now we will show that J is generated by $J \cap F\{y, \mathbf{u}\}$. Consider any element $p \in J$. Then there exists N, r and $a_0, \ldots, a_r \in k\{y, \mathbf{u}\}$ such that

$$g^N p = \sum_{i=0}^{r} a_i f^{(i)}. \tag{7}$$

Let $\{e_\lambda\}_{\lambda \in \Lambda}$ be a basis of k over F. We write $p = \sum\limits_{\lambda \in \Lambda} p_\lambda e_\lambda$ and $a_i = \sum\limits_{\lambda \in \Lambda} a_{i,\lambda} e_\lambda$ so that p_λ's and $a_{i,\lambda}$'s have the coefficient in F. Then, equating the coefficients at each e_λ in (7), we see that $p_\lambda \in J$ for every $\lambda \in \Lambda$, so p belongs to the ideal generated by $J \cap F\{y, \mathbf{u}\}$.

2. Since, in the Gröbner basis described in Proposition 1.23, the leading term has the highest order, reduction with respect to this basis does not increase the order. Therefore, we have, for every $j \geqslant 0$,

$$I \cap R_j = I_j.$$

Since the polynomials in R_n not reducible with respect to the Gröbner basis are exactly $k[\mathbf{x}, \mathbf{u}, \ldots, \mathbf{u}^{(n)}]$, the transcendence degree of R_n / I_n is equal to $|\mathbf{x}| + (n+1)|\mathbf{u}| = n + (n+1)\ell$. One the other hand, the transcendence degree of $k\{y, \mathbf{u}\} \cap R_n$ is equal to $(1 + |\mathbf{u}|)(n+1) = (n+1)^2$. Therefore, $I_n \cap k\{y, \mathbf{u}\} \neq \{0\}$. Since $I \cap k\{\mathbf{u}\} = \{0\}$, we have $\operatorname{ord}_y f \leqslant n$.

It remains to show that $f \in R_n$. If it is not, then it involves the derivatives of $\mathbf{u}$ of order higher than n. Since the reduction with respect to the Gröbner basis replaces y or $\mathbf{x}$ variables with a differential polynomial of the same or lower order, the order in y and $\mathbf{x}$ of all the intermediate results in the reduction of f with respect to the basis will not exceed n. Therefore, if we write f as a polynomial in $\mathbf{u}^{(n+1)}, \mathbf{u}^{(n+2)}, \ldots$ over R_n, then all the coefficients will also belong to I. If $f \notin R_n$, then some of them are of lower degree than f, but this contradicts the minimality of f.

□

Proposition 1.26 yields an algorithm for computing the functions identifiable from multiple experiments. We demonstrate it on a couple of examples.

Example 1.27 (Predator-prey, continued)**.** TODO

Example 1.28 (Compartment model)**.** TODO

1.8 Exercises

Exercise 1.1. Use [1, Theorem 1.3] to derive a bound $M \leqslant m^2$ (in the notation of the proof of Proposition 1.4) from the proof of Proposition 1.4.

Exercise 1.2. Use the argument from the proof of Proposition 1.4 to show that if I is a radical differential ideal in a differential ring R and $ab \in I$, then $ab' \in I$.

Exercise 1.3. Prove Lemma 1.12.

References

[1] Z. Jelonek. On the effective Nullstellensatz. *Inventiones mathematicae*, 162(1):1–17, 2005. URL https://doi.org/10.1007/s00222-004-0434-8.

[2] I. Kaplansky. *An introduction to differential algebra*. Hermann, 1957.

[3] S. Lang. Hilbert's Nullstellensatz in infinite-dimensional space. *Proceedings of the American Mathematical Society*, 3(3):407, 1952. URL https://doi.org/10.2307/2031893.

[4] A. Ovchinnikov, A. Pillay, G. Pogudin, and T. Scanlon. Computing all identifiable functions for ODE models, 2020. URL https://arxiv.org/abs/2004.07774.

[5] G. Pogudin. Primary differential nil-algebras do exist. *Moscow University Mathematics Bulletin*, 69(1):33–36, 2014. URL http://dx.doi.org/10.3103/S0027132214010069.