Separated Variables on Plane Algebraic Curves

Manfred Buchacher

Institut für Algebra
Johannes Kepler Universität Linz

Supported by the LIT with the grant LIT-2022-11-YOU-214

Let $r \in \mathbb{C}(x, y)$, and $p \in \mathbb{C}[x, y]$.

Let $r \in \mathbb{C}(x, y)$, and $p \in \mathbb{C}[x, y]$.

Problem

Solve

$$r + q(x, y)p = f(x) - g(y)$$

for q, f, $g \in \mathbb{C}(x, y)$.

Some field theoretic interpretations

Some field theoretic interpretations

Intersections of fields

Some field theoretic interpretations

Intersections of fields

$$q(x, y)p = f(x) - g(y)$$

Some field theoretic interpretations

Intersections of fields

$$f(x) \equiv g(y) \mod p$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r + q(x, y)p = f(x)$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \equiv f(x) \mod p$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \in \mathbb{C}(x) \mod p$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \in \mathbb{C}(x) \mod p$$

Sum-decomposition

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \in \mathbb{C}(x) \mod p$$

Sum-decomposition

$$r + q(x, y)p = f(x) - g(y)$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \in \mathbb{C}(x) \mod p$$

Sum-decomposition

$$r \equiv f(x) - g(y) \mod p$$

Some field theoretic interpretations

Intersections of fields

$$\mathbb{C}(x) \cap \mathbb{C}(y) \mod p$$

Field membership

$$r \in \mathbb{C}(x) \mod p$$

Sum-decomposition

$$r \in \mathbb{C}(x) + \mathbb{C}(y) \mod p$$

These problems arise in

- enumerative combinatorics
- computer vision
- parameter identifcation in ODE models
- algebraic independence of solutions of ODEs
- designing diffractive optical systems

Define

$$F(r, p) := \{(f, g) \in \mathbb{C}(x) \times \mathbb{C}(y) : f - g \in r + \langle p \rangle\}.$$

Define

$$F(r, p) := \{(f, g) \in \mathbb{C}(x) \times \mathbb{C}(y) : f - g \in r + \langle p \rangle\}.$$

Prop

Let (f, g) be any element of $F(r, p)$.

Define

$$F(r, p) := \{(f, g) \in \mathbb{C}(x) \times \mathbb{C}(y) : f - g \in r + \langle p \rangle\}.$$

Prop

Let (f, g) be any element of $F(r, p)$. Then

$$F(r, p) = (f, g) + F(0, p).$$

Define

$$F(r,p) := \{(f,g) \in \mathbb{C}(x) \times \mathbb{C}(y) : f - g \in r + \langle p \rangle\}.$$

Prop

Let (f,g) be any element of $F(r,p)$. Then

$$F(r,p) = (f,g) + F(0,p).$$

Furthermore,

$$F(p) \equiv F(0,p)$$

is a simple field.

The problem of computing $\mathrm{F}(\mathrm{r}, \mathrm{p})$ splits into

1) finding a generator of $\mathrm{F}(\mathrm{p})$, and
2) determining any element of $\mathrm{F}(\mathrm{r}, \mathrm{p})$.

The problem of computing $F(r, p)$ splits into

1) finding a generator of $F(p)$, and
2) determining any element of $F(r, p)$.

Strategy

The non-linear problem of solving

$$r + qp = f - g$$

is reduced to a linear problem. The reduction is based on the computation of the poles of f and g and their multiplicities.

1) Finding a generator of $\mathrm{F}(\mathrm{p})$

1) Finding a generator of $\mathrm{F(p)}$

Poles

There is a generator $(f, g) \in F(p)$ such that

$$f(\infty) = \infty.$$

There is a generator $(f, g) \in F(p)$ such that

$$f(\infty) = \infty.$$

If (s_1, s_2) is a root of p, then

$$f(s_1) = \infty \quad \text{iff} \quad g(s_2) = \infty.$$

There is a generator $(f, g) \in F(p)$ such that

$$f(\infty) = \infty.$$

If (s_1, s_2) is a root of p, then

$$f(s_1) = \infty \quad \text{iff} \quad g(s_2) = \infty.$$

Def

Let $\sim$ be the smallest equivalence relation on $\{p = 0\}$ such that

$$(x_0, y_0) \sim (x_1, y_1) \quad \text{whenever} \quad x_0 = x_1 \text{ or } y_0 = y_1.$$

There is a generator $(f, g) \in \mathrm{F}(p)$ such that

$$f(\infty) = \infty.$$

If (s_1, s_2) is a root of p, then

$$f(s_1) = \infty \quad \text{iff} \quad g(s_2) = \infty.$$

Def

Let $\sim$ be the smallest equivalence relation on $\{p = 0\}$ such that

$$(x_0, y_0) \sim (x_1, y_1) \quad \text{whenever} \quad x_0 = x_1 \text{ or } y_0 = y_1.$$

The equivalence class of (x_0, y_0) is called the orbit of (x_0, y_0).

Thm

The coordinates of the orbit of ∞ are poles of f and g, respectively. The orbit is finite, and it is exhaustive.

Thm

The coordinates of the orbit of ∞ are poles of f and g, respectively. The orbit is finite, and it is exhaustive. If

$$F(p) \cong \mathbb{C},$$

it might however be infinite.

1) Finding a generator of $\mathrm{F(p)}$

Multiplicities

The problem is reduced to one for homogeneous polynomials by studying $\mathfrak{p}$ locally at the elements of the orbit of ∞.

Any $\omega \in \mathbb{Z}^2$ induces a grading on $\mathbb{C}[x, y]$ by

$$\omega(ax^i y^j) = \omega_x i + \omega_y j.$$

The leading part of $p(x, y)$ is the sum of terms of maximal (weighted) degree $\omega(p)$. It is denoted by $\mathrm{lp}_\omega(p)$.

Any $\omega \in \mathbb{Z}^2$ induces a grading on $\mathbb{C}[x, y]$ by

$$\omega(ax^i y^j) = \omega_x i + \omega_y j.$$

The leading part of $p(x, y)$ is the sum of terms of maximal (weighted) degree $\omega(p)$. It is denoted by $\mathrm{lp}_\omega(p)$.

The weighted degrees of the terms of

$$p = xy - 1 - y - x^2 y - x^2 y^2$$

with respect to $\omega = (1, -2)$ are

$$-1, 0, -2, 0, -2.$$

Any $\omega \in \mathbb{Z}^2$ induces a grading on $\mathbb{C}[x, y]$ by

$$\omega(ax^i y^j) = \omega_x i + \omega_y j.$$

The leading part of $p(x, y)$ is the sum of terms of maximal (weighted) degree $\omega(p)$. It is denoted by $\mathrm{lp}_\omega(p)$.

The weighted degrees of the terms of

$$p = xy - 1 - y - x^2 y - x^2 y^2$$

with respect to $\omega = (1, -2)$ are

$$-1, 0, -2, 0, -2.$$

Its leading part is

$$\mathrm{lp}_\omega(p) = -1 - x^2 y.$$

Let us consider the example with

$$p = xy - 1 - y - x^2y - x^2y^2.$$

Let us consider the example with

$$p = xy - 1 - y - x^2y - x^2y^2.$$

The elements of the orbit of ∞ are

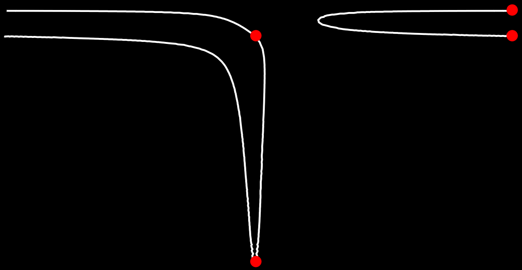
$$(\infty, 0),\ (\infty, -1),\ (0, -1) \quad \text{and} \quad (0, \infty).$$

Let us consider the example with

$$p = xy - 1 - y - x^2y - x^2y^2.$$

The elements of the orbit of ∞ are

$$(\infty, 0),\ (\infty, -1),\ (0, -1) \quad \text{and} \quad (0, \infty).$$



The leading part of p associated with $(\infty, 0)$ is

$$\mathrm{lp}_\omega(p) = -1 - x^2 y.$$

The leading part of p associated with $(\infty, 0)$ is

$$\mathrm{lp}_\omega(p) = -1 - x^2 y.$$

Since

$$F(\mathrm{lp}_\omega(p)) = \mathbb{C}((x^2, -y^{-1})),$$

there is a $k \in \mathbb{N}$ such that

$$(\mathrm{m}(\infty, f), \mathrm{m}(0, g)) = k \cdot (2, 1).$$

The analysis of the other poles is done analogously. It results in the following 1-parameter family for their multiplicities.

f		g	
∞	$2k$	∞	k
0	$2k$	0	k
		-1	$2k$

Making the ansatz

$$f = \frac{f_0 + f_1 x + \cdots + f_4 x^4}{x^2} \quad \text{and} \quad g = \frac{g_0 + g_1 y + \cdots + g_4 y^4}{y(1+y)^2}$$

and

$$q = \frac{q_{0,0} + q_{1,0} x + \cdots + q_{2,1} x^2 y}{x^2 y (1+y)^2}$$

we find that

$$F(p) = \mathbb{C}\left(\left(\frac{(1-x)^2(1+x+x^2)}{x^2}, -\frac{(1+y+y^2)^2}{y(1+y)^2}\right)\right).$$

Thm

If $F(p)$ is non-trivial, then choosing $k = 1$ results in the multiplicities of the poles of a generator.

If $\mathrm{F}(\mathrm{p})$ is non-trivial, then every orbit is finite.

The question of how the procedure can be turned into an algorithm raises the following

If $\mathrm{F(p)}$ is non-trivial, then every orbit is finite.

The question of how the procedure can be turned into an algorithm raises the following

Problem

Compute an upper bound on the size of a finite orbit.

Before we explain how to compute $F(r, p)$,
let us consider the following simpler problem.

Before we explain how to compute $F(r, p)$, let us consider the following simpler problem.

Problem

Solve

$$r + q(x, y)p = f(x)$$

for q, $f \in \mathbb{C}(x, y)$.

2) Determining an element of $F(r, p)$

2) Determining an element of $\mathrm{F}(\mathrm{r}, \mathrm{p})$

Poles

Let (s_1, s_2) be a root of p such that

$$r(s_1, s_2) = f(s_1) - g(s_2).$$

Let (s_1, s_2) be a root of p such that

$$r(s_1, s_2) = f(s_1) - g(s_2).$$

Then

$$f(s_1) = \infty \quad \text{or} \quad g(s_2) = \infty \quad \text{if} \quad r(s_1, s_2) = \infty.$$

Let (s_1, s_2) be a root of p such that

$$r(s_1, s_2) = f(s_1) - g(s_2).$$

Then

$$f(s_1) = \infty \quad \text{or} \quad g(s_2) = \infty \quad \text{if} \quad r(s_1, s_2) = \infty.$$

If

$$r(s_1, s_2) < \infty, \quad \text{then} \quad f(s_1) = \infty \quad \text{iff} \quad g(s_2) = \infty.$$

Do the orbits of the poles of r provide all poles of f and g?

Do the orbits of the poles of r provide all poles of f and g?

No!

Do the orbits of the poles of r provide all poles of f and g?

No!

It is also necessary to consider the orbits of its roots if $F(p)$ is non-trivial, and the finite orbits if $F(p)$ is trivial.

Do the orbits of the poles of r provide all poles of f and g?

No!

It is also necessary to consider the orbits of its roots if $F(p)$ is non-trivial, and the finite orbits if $F(p)$ is trivial.

Prop [Bell, Moosa, Topaz, Bellaïche]

If $F(p)$ is trivial, then the number of finite orbits is finite.

2) Determining an element of $\mathrm{F}(\mathrm{r}, \mathrm{p})$

Multiplicities

(Upper) bounds on the multiplicities are derived from

- the local behavior of r,
- its (weighted) degrees $\omega(r)$,
- and the generators of $F(\mathrm{lp}_\omega(p))$.

Let (x_1, y_1) and (x_2, y_2) be roots of p.

Let (x_1, y_1) and (x_2, y_2) be roots of p.

Problem

Decide whether (x_2, y_2) is in (some part of) the orbit of (x_1, y_1).

Let (x_1, y_1) and (x_2, y_2) be roots of p.

Problem

Decide whether (x_2, y_2) is in (some part of) the orbit of (x_1, y_1).

Problem

How do the semi-algorithms generalize?

Some references

- *Separating Variables in Bivariate Polynomial Ideals*
- *Separating Variables in Bivariate Polynomial Ideals: the Local Case*
- *Separated Variables on Plane Algebraic Curves*

Some references

- *Separating Variables in Bivariate Polynomial Ideals*
- *Separating Variables in Bivariate Polynomial Ideals: the Local Case*
- *Separated Variables on Plane Algebraic Curves*

- *Galoisian structure of large steps walks confined in the first quadrant*, Pierre Bonnet and Charlotte Hardouin

Some references

- *Separating Variables in Bivariate Polynomial Ideals*
- *Separating Variables in Bivariate Polynomial Ideals: the Local Case*
- *Separated Variables on Plane Algebraic Curves*
- *Galoisian structure of large steps walks confined in the first quadrant*, Pierre Bonnet and Charlotte Hardouin

Thank you!