Dimension and projection of solution sets to bivariate polynomials

Mohab Safey El Din

In the previous chapter, we studied properties of resultants and we introduced an algorithm for computing them, through the strong relationship between resultants and gcds (and consequently Euclide's algorithm).

Recall that, basically, the resultant associated to a couple of polynomials (a, b) in $\mathbb{K}[x_1, x_2]$ vanishes if and only if the gcd of (a, b) has positive degree.

We study now how to use the notion of resultant and algorithms for computing them to solve bivariate polynomial systems.

Recall that, at the end of the first Chapter, we introduced several algorithmic problems. One of which was related to the notion of *dimension*. For instance, given a (f_1, f_2) in $\mathbb{K}[x_1, x_2]$, we want to obtain algorithms which allow us to decide whether the solution set of the system $f_1 = f_2 = 0$ in $\overline{\mathbb{K}}^2$ (where $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$) is empty, or has finitely many solutions, or has infinitely many solutions.

We will first study these problems. Next, for bivariate polynomial systems (i.e. polynomial systems which involve at most 2 variables) which have finitely many solutions in $\overline{\mathbb{K}}^2$, we will design an algorithm which on input such systems, computes a *triangular* description of the solution (as sketched in previous chapters)

$$w(x_1) = 0, w_2(x_1, x_2) = 0.$$

We will see that in some exceptional cases, we will have to slightly change this and will output *finite* families of such triangular descriptions.

We will pay particular attention to complexity and efficiency issues at the end of this Chapter.

Contents

1 Dimension properties

1.1 Basic definitions and examples

We start with a precise definition of *dimension* for algebraic sets in $\overline{\mathbb{K}}^2$ (it will be extended further to algebraic sets of $\overline{\mathbb{K}}^n$, for arbitrary n).

Definition 1. *Let $V \subset \overline{\mathbb{K}}^2$ be the* $\mathbb{K}$-algebraic set *defined by a subset of $\mathbb{K}[x_1, x_2]$. One says that*

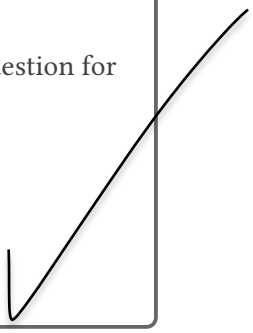
- *V has dimension -1 when it is empty,*
- *V has dimension 0 when its cardinality is finite in $\overline{\mathbb{K}}$,*
- *V has positive dimension when its cardinality is infinite in $\overline{\mathbb{K}}$.*

Further, we denote by $\dim(V)$ *the dimension of V.*

Exercise 1

- Prove that algebraic sets of $\overline{\mathbb{K}}^2$ which are defined by the vanishing of a single equation $f = 0$ with $f \in \mathbb{K}[x_1, x_2] - \mathbb{K}$ has positive dimension.
- What is the dimension of the algebraic set defined by $1 = 0$? Same question for the algebraic set defined by $0 = 0$.
- What is the dimension of algebraic sets defined by *linear* equations ?
- Compute the dimension of the algebraic set defined by

$$x^2 + y^2 - 1 = 2x^2 - y^2 + 3 = 0.$$



In the next subsection, we will describe an algebraic characterization of the stituations where V has *positive* dimension (given a polynomial system defining V). We will deduce from this charcaterization an algorithm which, on input the system defining V allows us to decide whether V has positive dimension or not. Before entering into these algorithmic considerations, let us study some examples and how this notion of dimension behaves when one takes unions and intersections of algebraic sets.

The very first example leading to an empty algebraic set is of course the polynomial system $1 = 0$. But there are more intricate polynomial systems leading to the empty algebraic set (of dimension -1) such as

$$x_1 x_2 - 1 = 0, \quad x_1 = 0.$$

Indeed, when *substituting* x_1 by 0 in the first equation, one obtains the equation $1 = 0$. We can also have a look at the following polynomial system

$$x_1^2 + x_2^2 - 1 = 0, \quad x_1 - x_2 = 0, \quad x_1 + x_2 = 0.$$

The first equation defines the unit circle C centered at the origin. The next two ones define two lines that we denote respectively L_1 and L_2. Note that the intersection of C with L_1 consists of the two points $\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$ and $\left(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right)$ (hence it has dimension zero). Also, the intersection of C with L_2 consists of the two points $\left(\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\right)$ and $\left(-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$ (it also has dimension zero). Since all these points are distinct, one easily deduces that the solution set of the above system is empty in $\overline{\mathbb{K}}^2$.

Exercise 2

Compute triangular representation of the intersection of C with L_1

$$w(x_1) = 0, w_2(x_1, x_2) = 0$$

and a triangular representations of the intersection of C with L_2

$$\tilde{w}(x_1) = 0, \tilde{w}_2(x_1, x_2) = 0.$$

Compute the resultant of $(w, \tilde{w})$.

A more algebraic (but less geometric) way to figure this out is to proceed as follows. Since the equation $x_1 - x_2 = 0$ holds, one can replace x_2 by x_1 in the other two equations, which leads to the new equivalent system

$$2x_1^2 - 1 = 0, \quad x_2 = x_1, \quad 2x_1 = 0.$$

Now, substituting x_1 by 0 in the first equation leads again to a reduction to the equation $1 = 0$.

Through the above study, we studied intermediate polynomial systems of dimension zero (i.e. which have finitely many solutions in $\overline{\mathbb{K}}^2$). There is one trivial observation to make: since those systems have finitely many solutions, the projection of their solutions on any coordinate axis is finite. This is trivial but important: since (non-zero) univariate polynomials have finitely many roots one may try to compute a univariate polynomial whose set of roots coincide the projection of the solutions of the input system on a given coordinate axis.

We can now investigate positive dimensional algebraic sets. The most trivial ones are of course the ones which are defined with a single equation $f = 0$ with $f \in \mathbb{K}[x_1, x_2]$ of positive degree. Indeed, in that case, the number of solutions in $\overline{\mathbb{K}}^2$ is infinite.

Exercise 3

Prove the above statement.
Hint. Use the fact that univariate polynomials with coefficients in $\overline{\mathbb{K}}$ and degree $d > 0$ have d solutions (counted with multiplicities) and look at the number of solutions of our equation when x_1 ranges over $\overline{\mathbb{K}}$.

Other interesting examples are solution sets to polynomial systems $f_1 = f_2 = 0$ where $f_1 = gh_1$ and $f_2 = gh_2$ with $g \in \mathbb{K}[x_1, x_2]$ of positive degree. Last but not least observe that the solution set of the whole system $0 = 0$ is the whole affine space $\overline{\mathbb{K}}^2$.

We investigate now the dimension behaves w.r.t. union and intersection of algebraic sets.

Corollary 2. *Let V_1 and V_2 be two algebraic sets of $\overline{\mathbb{K}}^2$. Then the following holds.*

- $\dim(V_1 \cup V_2) = \max(\dim(V_1), \dim(V_2))$,
- $\dim(V_1 \cap V_2) \leqslant \max(\dim(V_1), \dim(V_2))$

Proof. The proof is quite straightforward.

Assume that $V_1 \cup V_2$ is empty, then V_1 and V_2 are both empty and we indeed have $-1 = \max(-1, -1)$. Similarly, when $V_1 \cup V_2$ is finite, both V_1 and V_2 are finite and we indeed have $0 = \max(0, 0)$. Assume now that $V_1 \cup V_2$ has positive dimension. Then either V_1 or V_2 has positive dimension and it follows that $\max(\dim(V_1), \dim(V_2))$ is also positive.

Proving the identities of the dimension of the intersection of $V_1 \cap V_2$, is done with similar arguments. This is left to the reader. □

Exercise 4

Prove the identities for the dimension of the intersection of V_1 and V_2 by following similar arguments to the ones used in the above proof.

1.2 Characterization and algorithm

We try now to identify some *algebraic* conditions (i.e. conditions which are expressed with polynomial constraints) which allow us to detect when the algebraic set has positive dimension.

The core idea already appeared in the previous section. Take $V \subset \overline{\mathbb{K}}^n$ be an algebraic set given as the solution set of the polynomial system

$$f_1 = f_2 = 0$$

with $f_i \in \mathbb{K}[x_1, x_2]$.

Assume that V has positive dimension (hence, infinitely many solutions in $\overline{\mathbb{K}}$). Assume for the moment that the *projection* of V (which we will denote by U) on the x_1-axis has infinite

cardinality. Hence, for any $\alpha \in U$, there exists $\beta \in \overline{\mathbb{K}}$ such that $(\alpha, \beta) \in V$, which, in algebraic words, implies that

$$f_1(\alpha, \beta) = f_2(\alpha, \beta) = 0.$$

Hence, β is a common root of the polynomials of $\overline{\mathbb{K}}[x_2]$

$$f_1(\alpha, x_2), f_2(\alpha, x_2)$$

which, according to the first Chapter, is equivalent to state that the gcd of this sequence of polynomial has positive degree.

All in all, under the assumption that V and U have both infinite cardinality, we obtain that when α ranges over U, any gcd of the sequence of polynomials $f_1(\alpha, x_2), f_2(\alpha, x_2)$ has positive degree. The theorem below shows what this translates w.r.t. some resultant computations.

However, before stating it, let us see that the above assumption that U has infinite cardinality is not general enough. That will justify the statement of our theorem is more involved than what could have been suggested by the above examples.

Consider the following polynomial system:

$$(x_1^2 - 1)x_2 = 0, \quad x_1^2 - 1 = 0.$$

Observe that the solution set of this polynomial system is the union of the two lines defined respectively by $x_1 = 1$ and $x_1 = -1$. Hence, this system has infinitely many solutions in $\overline{\mathbb{K}}^2$ but the projection on the x_1-axis of the algebraic set it defines is finite. Note that considering the projection on the x_2-axis of this solution set has infinite cardinality.

Theorem 3. *Let $V \subset \mathbb{K}^2$ be an algebraic set defined by*

$$f_1 = f_2 = 0$$

with $f_i \in \mathbb{K}[x_1, x_2]$. Then, V has positive dimension if and only if, either

$$res_{x_2}(f_1, f_2) \text{ is identically zero}$$

or

$$res_{x_1}(f_1, f_2) \text{ is identically zero}$$

Proof. Further, for $i \in \{1, 2\}$, we denote by π_i the canonical projection $(x_1, x_2) \to x_i$.

We start by proving that either $\pi_1(V)$ or $\pi_2(V)$ has infinite cardinality. This is done by contradiction. Hence, we assume additionally that both $\pi_1(V)$ and $\pi_2(V)$ are finite and we will establish that this raises a contradiction. Since $\pi_1(V)$ is assumed to be finite, there exists $\{\alpha_1, \ldots, \alpha_k\} \subset \overline{\mathbb{K}}$ such that

$$\pi_1(V) = \{\alpha_1, \ldots, \alpha_k\}.$$

Similarly, since $\pi_2(V)$ is assumed to be finite, there exists $\{\beta_1, \ldots, \beta_\ell\} \subset \overline{\mathbb{K}}$ such that

$$\pi_2(V) = \{\beta_1, \ldots, \beta_\ell\}.$$

Hence one deduces that

$$V \subset \{(\alpha_i, \beta_j) \mid 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant \ell\}.$$

This latter set is finite (it has cardinality $k\ell$) and contains V. Then, V should be finite, which is a contradiction.

Below, without loss of generality (w.l.g.), we assume that $\pi_1(V)$ has infinite cardinality. We denote $\pi_1(V)$ by U (hence U has infinite cardinality) and we denote by $h_i \in \mathbb{K}[x_1]$ the leading coefficient of f_i w.r.t. x_2 for $1 \leqslant i \leqslant 2$. Since h_i is univariate, it has finitely many roots in $\overline{\mathbb{K}}$; we denote by Z_i the set of roots of h_i in $\overline{\mathbb{K}}$. Now, we consider $\widetilde{U} = U - (Z_1 \cup Z_2)$. Since U has infinite cardinality and the Z_i's are finite, we deduce that $\widetilde{U}$ has infinite cardinality.

We first prove that, assuming that V has infinite cardinality implies that $\mathrm{res}_{x_2}(f_1, f_2)$ is the zero polynomial. Assume by contradiction that $\mathrm{res}_{x_2}(f_1, f_2) \neq 0$; then it has finitely many roots in $\overline{\mathbb{K}}$; we denote its set of roots by Z. Note that $\widetilde{U} - Z$ has infinite cardinality.

Besides, using the specialization properties of resultants and denoting by ϕ_α the specialization map $f(x_1, x_2) \in \overline{\mathbb{K}}[x_1, x_2] \to f(\alpha, x_2) \in \overline{\mathbb{K}}[x_2]$ with $\alpha \in \overline{\mathbb{K}}$, one deduces that for any $\alpha \in \widetilde{U}$, $\phi_\alpha(\mathrm{res}_{x_2}(f_1, f_2)) = \mathrm{res}_{x_2}(\phi_\alpha(f_1), \phi_\alpha(f_2))$.

In particular, observe that since $\widetilde{U} - Z \subset \widetilde{U} \subset U$, for any $\alpha \in \widetilde{U} - Z$, $\phi_\alpha(\mathrm{res}_{x_2}(f_1, f_2)) = \mathrm{res}_{x_2}(\phi_\alpha(f_1), \phi_\alpha(f_2)) = 0$ (because the gcd of $\phi_\alpha(f_1), \phi_\alpha(f_2)$ has positive degree which, according to the previous Chapter is equivalent to the vanishing of the corresponding resultant).

We prove now the reverse inclusion, i.e. we prove that if $\mathrm{res}_{x_2}(f_1, f_2)$ is identically 0, then V has infinite cardinality. Again, we consider an evaluation map ϕ_α as above and the (finite) set Z of roots in $\overline{\mathbb{K}}$ of the leading coefficients of f_1 and f_2 w.r.t. x_2. Since $\mathrm{res}_{x_2}(f_1, f_2)$ is identically 0, then for any $\alpha \in \mathbb{K} - Z$, we deduce from the specialization properties of resultants that $\phi_\alpha(\mathrm{res}_{x_2}(f_1, f_2)) = \mathrm{res}_{x_2}(\phi_\alpha(f_1), \phi_\alpha(f_2)) = 0$. In other words, when α ranges over an infinite set, there exists at least one β in $\overline{\mathbb{K}}$ such that $f_1(\alpha, \beta) = f_2(\alpha, \beta) = 0$ (because when the resultant associated to $(\phi_\alpha(f_1), \phi_\alpha(f_2))$ vanishes, then $(\phi_\alpha(f_1), \phi_\alpha(f_2))$ have a gcd of positive degree). This shows that V has infinite cardinality. □

We deduce the following algorithm from the above theorem.

Input. a couple of polynomials $\boldsymbol{f} = (f_1, f_2)$ in $\mathbb{K}[x_1, x_2]$.

Output. true if the algebraic set defined by $\boldsymbol{f}$ has positive dimension, else false.

HasPositiveDimension($\boldsymbol{f}$)

1. Compute $R_1 = \mathrm{res}_{x_2}(f_1, f_2) \in \mathbb{K}[x_1]$.
2. if $R_1 = 0$ then return true.
3. Compute $R_2 = \mathrm{res}_{x_1}(f_1, f_2) \in \mathbb{K}[x_2]$.
4. if $R_2 = 0$ then return true.
5. return false.

Exercise 5

Decide whether the algebraic sets defined by the following polynomial systems have positive dimension.

- $x^2 + y^2 - 1 = x^2 - 2y^2 + 2 = 0$
- $x^3 + xy^2 - x = x^2 - xy = 0$.

Exercise 6

Assume that $\mathbb{K} = \mathbb{Q}$. Note that computing $\text{res}_{x_2}(f_1, f_2)$ or $\text{res}_{x_1}(f_1, f_2)$ can be costly because of the growth of the bit size of the coefficients.
Since we are only interested in deciding if these resultants are zero, we want to use modular computations (over a prime field) to avoid this growth of coefficients.
Show how to modify the above algorithm to achieve this goal.
Hint. Use specialization properties (through evaluation maps) which are proved in the previous chapter.

It remains to investigate how to generalize Algorithm HasPositiveDimension to decide if an algebraic set defined by more than 2 polynomials has positive dimension. Hence, let $V \subset \overline{\mathbb{K}}^n$ be the algebraic set defined by

$$f_1 = \cdots = f_p = 0$$

with $f_i \in \mathbb{K}[x_1, \ldots, x_n]$.

Exercise 7

Prove that if $\text{res}_{x_1}(f_i, f_j) = 0$ (or $\text{res}_{x_2}(f_i, f_j) = 0$) for all pairs (f_i, f_j) then V has positive dimension.

One could think that the reverse is true, by applying Theorem 3 to all pairs (f_i, f_j), i.e. that if V has positive dimension then $\text{res}_{x_1}(f_i, f_j) = 0$ (or $\text{res}_{x_2}(f_i, f_j) = 0$) for all pairs (f_i, f_j).

This is simply not true as illustrated by the following example. Take $p = 3$ and

$$f_1 = g_{1,2}g_{1,3}, \quad f_2 = g_{1,2}g_{2,3} \quad \text{and} \quad f_3 = g_{1,3}g_{2,3}$$

where $g_{1,2}, g_{1,3}$ and $g_{2,3}$ are co-prime polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ of positive degrees.

It is then clear that $g_{1,2}$ is a gcd of (f_1, f_2), $g_{1,3}$ is a gcd of (f_1, f_3) and $g_{2,3}$ is a gcd of (f_2, f_3). This implies that $\text{res}_{x_1}(f_i, f_j) = 0$ and $\text{res}_{x_2}(f_i, f_j) = 0$ for all i, j.

But we can then have a more careful look at the solution set to $f_1 = f_2 = f_3 = 0$. Clearly, the subsystem $f_1 = f_2 = 0$ can be decomposed as the union of the algebraic set V_1 defined by $g_{1,2} = 0$ and the algebraic set V_2 defined by $g_{1,3} = g_{2,3} = 0$. Note that f_3 vanishes on V_2. Hence V_2 is contained in the solution set of our input system.

Now we look at the intersection of V_1 with the curve defined by $f_3 = 0$. Again, it can be splitted as the union of the algebraic sets V_3 and V_4 which are respectively defined by $g_{1,2} = g_{1,3} = 0$

and $g_{1,2} = g_{2,3} = 0$. Hence, all in all, the solution set to $f_1 = f_2 = f_3 = 0$ is

$$V_2 \cup V_3 \cup V_4.$$

The following result shows that this set is finite (and then, not of positive dimension) because the distinct $g_{i,j}$'s are pairwise co-prime. This shows that the vanishing of the above resultants is not sufficient to assess that the algebraic set defined by our input system has positive dimension.

Proposition 4. *Let f_1 and f_2 be co-prime polynomials in $\mathbb{K}[x_1, x_2]$. Then, the algebraic set defined by $f_1 = f_2 = 0$ is finite.*

Proof. Since f_1 and f_2 are co-prime, then $\mathrm{res}_{x_1}(f_1, f_2)$ and $\mathrm{res}_{x_2}(f_1, f_2)$ are both non-zero (since a resultant of two polynomials vanishes if and only if there is a gcd of positive degree for these polynomials).

We let $R_1 = \mathrm{res}_{x_2}(f_1, f_2) \in \mathbb{K}[x_1]$ and $R_2 = \mathrm{res}_{x_1}(f_1, f_2) \in \mathbb{K}[x_2]$ and we consider the evaluation maps $\varphi_z : f \in \mathbb{K}[x_1, x_2] \to f(z, .)$ and $\psi_z : f \in \mathbb{K}[x_1, x_2] \to f(., z)$. We denote by $V \subset \overline{\mathbb{K}}^2$ the solution set of the system $f_1 = f_2 = 0$ and by π_i the canonical projection $(z_1, z_2) \to z_i$ for $i \in \{1, 2\}$.

Let $\alpha \in \overline{\mathbb{K}}$ be a root of R_1 which is not a root of the leading coefficients of f_1 and f_2 w.r.t. x_2. Thanks to the specialization properties of the resultant, we deduce that $\varphi_\alpha(f_1)$ and $\varphi_\alpha(f_2)$ have a gcd of positive degree and then there exists $\beta \in \overline{\mathbb{K}}$ such that $f_1(\alpha, \beta) = f_2(\alpha, \beta) = 0$. In other words, if $\mathscr{A} = \{\alpha_1, \ldots, \alpha_\ell\}$ denotes the set of roots of R_1 (this set is finite because we established that it is non zero and univariate), then $\pi_1(V) \subset \mathscr{A}$, or, equivalently $V \subset \pi_1^{-1}(\mathscr{A})$.

Similarly, using the evaluation maps ψ_β where β is a root of R_2 which does not cancel the leading coefficients of f_1 and f_2 w.r.t. x_1, one deduces that if $\mathscr{B} = \{\beta_1, \ldots, \beta_k\}$ denotes the roots of R_2, the following inclusion holds:

$$V \subset \pi_2^{-1}(\mathscr{B}).$$

All in all, we have $V \subset \pi_1^{-1}(\mathscr{A}) \cap \pi_2^{-1}(\mathscr{B})$. Now, remark that $\pi_1^{-1}(\mathscr{A}) \cap \pi_2^{-1}(\mathscr{B})$ is finite. Then, we deduce that V is also finite. □

Exercise 8

Deduce from Proposition 4 and its proof, an algorithm which on input (f_1, f_2) in $\mathbb{K}[x_1, x_2]$ decides whether the algebraic set defined by $f_1 = f_2 = 0$ is finite.

We now go back to our problem of deciding whether an algebraic set $V \subset \overline{\mathbb{K}}^2$ defined by $f_1 = \cdots = f_p = 0$ has positive dimension. In the example, we studied above, we were led to *split* the solution set into pieces which were discovered through resultant and gcd computations. What one then can do is to generalize this process. When handling a pair (f_i, f_j), one can first compute its resultant and if it is zero, compute gcd $g_{i,j}$ of this pair. Next, one can split our input system into two systems:

- one subsystem obtained by replacing $f_i = 0, f_j = 0$ with $g_{i,j} = 0$;

- one subsystem obtained by replacing $f_i = 0, f_j = 0$ with $\frac{f_i}{g_{i,j}} = 0$ and $\frac{f_j}{g_{i,j}} = 0$.

Of course, in the above process, it is better to remove redundant equations. All in all, if one of the constructed subsystem consists of a unique equation of positive degree, one can conclude that the algebraic set defined by the input system has positive dimension.

Exercise 9

From the above discussion, design an algorithm which on input $(f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$, decides if the algebraic set defined by

$$f_1 = \cdots = f_p = 0$$

has positive dimension.
Estimate the complexity of such an algorithm (denote by $\mathrm{C}(d)$ the cost of computing resultants of bivariate polynomials with coefficients in $\mathbb{K}$).

Exercise 10

Decide whether the algebraic sets defined by the following polynomial systems have positive dimension:

- $x_1x_2 = x_2x_3 = x_1x_3 = 0$
- $x_1^2 + 2x_2^2 - 2 = x_1^2 + 4x_2^2 + 8 = 0$ in $\frac{\mathbb{Z}}{2\mathbb{Z}}[x_1, x_2]$
- and

$$\begin{aligned} {x_1}^3 + {x_1}^2x_2 + x_1{x_2}^2 + {x_2}^3 + {x_1}^2 + {x_2}^2 - x_1 - x_2 - 1 &= 0 \\ {x_1}^3 + {x_1}^2x_2 + 2\,x_1{x_2}^2 + 2\,{x_2}^3 + {x_1}^2 + 2\,{x_2}^2 - x_1 - x_2 - 1 &= 0 \\ 3\,{x_1}^3 + 3\,{x_1}^2x_2 + 2\,x_1{x_2}^2 + 2\,{x_2}^3 + 3\,{x_1}^2 + 2\,{x_2}^2 - x_1 - x_2 - 1 &= 0 \end{aligned}$$

2 Projections and resultants

In the previous subsection, we investigated algorithms for deciding whether the algebraic set of $\overline{\mathbb{K}}^2$ defined by polynomial equations in $\mathbb{K}[x_1, x_2]$ has positive dimension or is finite (and hence it has dimension either 0 or -1 if it is empty).

One key ingredient of the results proved in the above subsection is to understand properties (such as finiteness) of the *projection* of the algebraic sets under consideration through the degree of the resultant of couples of their defining polynomials. To do that, what has been extensively used is the connection between resultants and gcds combined with the *specialization* properties of the resultant.

In this paragraph, we go further

2.1 A first example

To figure out this, you may consider the example

$$f_1 = -3x_2^2 - 3x_2 + x_1^2 - 1 \qquad \text{and} \qquad f_2 = -x_2^2 + x_1^2 \text{ in } \mathbb{Q}[x_1, x_2]$$

which is illustrated by Figure 1. The blue curve is defined (over the reals) by $f_1 = 0$ and the red one is defined by $f_2 = 0$.

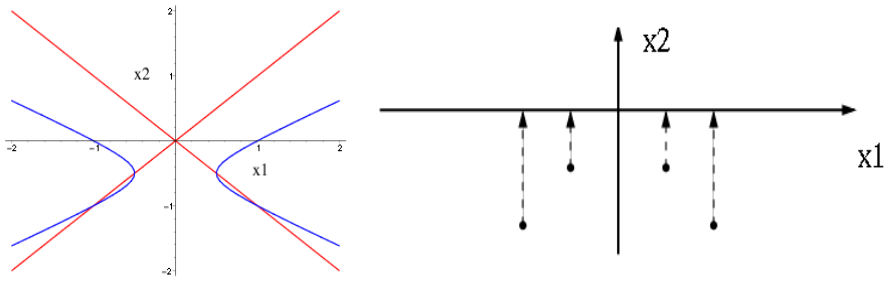


Figure 1. Illustration of the projection step.

Exercise 11

Compute $\text{res}_{x_2}(f_1, f_2)$ using the algorithm based on the Euclide's algrithm.

Exercise 12

By remarking that $f_2 = (x_1 - x_2)(x_1 + x_2)$ compute in an alternative way $\text{res}_{x_2}(f_1, f_2)$.
Hint. Use the relationships between $\text{res}_x(ab, c)$ and $\text{res}_x(a, c)$, $\text{res}_x(b, c)$ for a, b, c in $\mathbb{K}[x]$.

Solving the above exercises you should obtain

$$\text{res}_{x_2}(f_1, f_2) = 4\,{x_1}^4 - 5\,{x_1}^2 + 1.$$

Further, we denote by R the above resultant. Since all terms of this univariate polynomial have even degree, if α is a root of R, then $-\alpha$ is also a root of R. Also, looking carefully at the coefficients of R, it appears that 1 (and consequently -1) is a root of R. Hence, the polynomial $x_1^2 - 1$ divides R.

Exercise 13

Apply the univariate division algorithm to divide R by $x_1^2 - 1$.

One obtains that

$$R = (x_1^2 - 1)(4x_1^2 - 1) = (x_1 - 1)(x_1 + 1)(4x_1^2 - 1).$$

One easily factors $4x_1^2 - 1$ (since $x_1^2 = \frac{1}{4}$ leads to $x_1 = \frac{1}{2}$ or $x_1 = -\frac{1}{2}$) and we deduce that

$$R = (x_1 - 1)(x_1 + 1)(2x_1 - 1)(2x_1 + 1).$$

All in all the roots of R are $\{-1, -\frac{1}{2}, \frac{1}{2}, 1\}$; we denote them by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Exercise 14

For $1 \leqslant i \leqslant 4$, compute a gcd of $f_1(\alpha_i, x_2)$ and $f_2(\alpha_i, x_2)$ using Euclide's algorithm.

One deduces from the above exercise that the solutions to the system $f_1 = f_2 = 0$ are

$$(x_1 = -1, x_2 = -1), (x_1 = -1/2, x_2 = -1/2), (x_1 = 1, x_2 = -1), (x_1 = 1/2, x_2 = -1/2)$$

All in all, we remark the set of roots of $\mathrm{res}_{x_2}(f_1, f_2)$ is related to the projections of the solutions to the system $f_1 = f_2 = 0$. On our example, *all* of these roots were projections of such solutions. But this raises the following questions.

- Does the set of roots of the resultant contains *all* the projections of the solution to the system $f_1 = f_2 = 0$ in general?
- Are there roots of the resultant which do *not* correspond to projections of the aforementioned solution set ? In that case, how to identify those parasite roots?

2.2 A more involved example

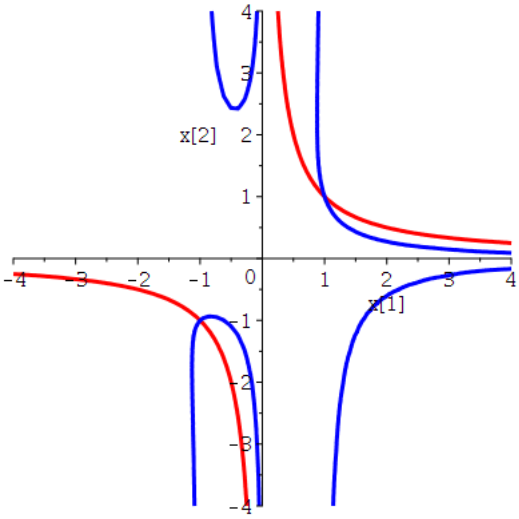


Figure 2. An example with asymptots.

This example will give an insight on the what is the answer to the above second question. Consider the following polynomial polynomials

$$f_1 = x_1x_2 - 1, \quad \text{and} \quad f_2 = (x_1^3 - x_1)x_2^2 + x_1x_2 - 1.$$

Exercise 15

Compute the resultant of these two polynomial w.r.t the variable x_2.

The resultant of (f_1, f_2) w.r.t. x_2 is the polynomial

$$x_1^3 - x_1$$

whose set of roots is $\{-1, 0, 1\}$. It is easy to see that instantiating x_1 to -1 and 1 in f_1 and f_2 yields the solutions

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

while instantiating x_1 to 0 in f_1 yields the equation $1 = 0$ which has no solution. This answers the last question raised in the previous subsection: the resultant of two polynomials f_1, f_2 in $\mathbb{K}[x_1, x_2]$ can indeed have a root in $\overline{\mathbb{K}}$ which is not the projection on the x_1-axis of one solution in $\overline{\mathbb{K}}^2$ to the system $f_1 = f_2 = 0$.

One can note however that on our current example, the extra root is 0, which cancels the leading coefficients of f_1 and f_2 w.r.t. x_2 (these leading coefficients are x_1 and $x_1^3 - x_1$).

In the next section, we prove that this simultaneous cancellation of the leading coefficients with respect the variable which is eliminated is the only case which induces "extra" roots to the corresponding resultant.

Exercise 16

Compute the resultant (w.r.t. x_2) of the following couples of polynomials and compare with the roots of the leading coefficients (w.r.t. x_2).

- $f_1 = x_1x_2 - 1$ and $f_2 = (x_1^3 - 2x_1)x_2^2 + x_1x_2 - 1$.
- $f_1 = x_1^2x_2 - x_1$ and $f_2 = (x_1x_2 - 2)(x_1^2 - x_2^2)$.

2.3 Main result

We prove now the main result of this section.

Theorem 5. *Let f_1 and f_2 be two polynomials in $\mathbb{K}[x_1][x_2]$ where $\mathbb{K}$ is a field. Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$ and $V \subset \overline{\mathbb{K}}^2$ be the algebraic set defined by $f_1 = f_2 = 0$. Then the following holds.*

(a) for all $(\alpha, \beta) \in V$, such that α does not cancel the leading coefficients of f_1 and f_2 w.r.t. x_2, $res_{x_2}(f_1, f_2)$ vanishes at α.

(b) for all $\gamma \in \overline{\mathbb{K}}$ in the set of roots of $res_{x_2}(f_1, f_2)$, at least one of the following statement holds:

- *either γ is a common root to the leading coefficients of f_1 and f_2 w.r.t. x_2;*

– *or there exists* $(\alpha, \beta) \in V$ *such that* $\alpha = \gamma$ *(hence* γ *is the* x_1*-coordinate of some solution to* $f_1 = f_2 = 0$*).*

Proof. The proof of this result basically relies on the same machinery of the previous results stated in this chapter.

We start by proving *(a)*. Hence, take $(\alpha, \beta) \in V$; our goal is to prove that $res_{x_2}(f_1, f_2)$ vanishes at α. Further, we denote by φ_α the specialization map $f(x_1, x_2) \in \mathbb{K}[x_1, x_2] \to f_\alpha = f(\alpha, x_2) \in \mathbb{K}[x_2]$. Note that this is a ring homomorphism.

As previously observed, since $(\alpha, \beta) \in V$, $\beta \in \overline{\mathbb{K}}$ is a common root of $\varphi_\alpha(f_1)$ and $\varphi_\alpha(f_2)$. Consequently, $\varphi_\alpha(f_1)$ and $\varphi_\alpha(f_2)$ have a gcd of positive degree.

Recall that this is equivalent to stating that $\mathrm{res}_{x_2}(\varphi_\alpha(f_1), \varphi_\alpha(f_2))$ is 0. Since we assume that α is not a common root to the leading coefficients of f_1 and f_2 w.r.t. x_2, we can use the specialization properties of the resultant to deduce that $\mathrm{res}_{x_2}(f_1, f_2)(\alpha) = \mathrm{res}_{x_2}(\varphi_\alpha(f_1), \varphi_\alpha(f_2))$ and then one can conclude that $\mathrm{res}_{x_2}(f_1, f_2)(\alpha) = 0$ as requested.

We prove now *(b)*. We take $\gamma \in \overline{\mathbb{K}}$ such that $\mathrm{res}_{x_2}(f_1, f_2)(\gamma) = 0$. Our goal now is to prove that either γ is a common root to the leading coefficients of f_1, f_2 w.r.t. x_2 or that there exists $(\alpha, \beta) \in V$ such that $\alpha = \gamma$. Equivalently, we prove below that if γ is *not* a common root to the leading coefficients of f_1, f_2 w.r.t. x_2 then there exists $(\alpha, \beta) \in V$ such that $\alpha = \gamma$.

Hence, we have *(1)* $\mathrm{res}_{x_2}(f_1, f_2)(\gamma) = 0$ and *(2)* γ is *not* a common root to the leading coefficients of f_1, f_2 w.r.t. x_2. From *(2)*, and the specialization properties of the resultant, we deduce that$\mathrm{res}_{x_2}(f_1, f_2)(\gamma) = \mathrm{res}_{x_2}(\varphi_\gamma(f_1), \varphi_\gamma(f_2))$. From *(1)*, and the previous equality, we deduce that $\mathrm{res}_{x_2}(\varphi_\gamma(f_1), \varphi_\gamma(f_2)) = 0$. Using the relationship between gcd and resultant, we deduce that $\varphi_\gamma(f_1)$ and $\varphi_\gamma(f_2)$ have a gcd of positive degree, which implies that they have at least one common root $\beta \in \overline{\mathbb{K}}$. Hence, we have $f_1(\gamma, \beta) = f_2(\gamma, \beta) = 0$ and then $(\gamma, \beta) \in V$ as requested. □

Remark. Let $V \subset \overline{\mathbb{K}}^2$ be the solution set to the polynomial system $f_1 = f_2 = 0$ in $\mathbb{K}[x_1, x_2]$. Note that there might exist $(\alpha, \beta) \in V$ such that α cancels $\mathrm{res}_{x_2}(f_1, f_2)$ and the leading coefficients of f_1, f_2 w.r.t. x_2 as well.

Exercise 17

Compute the projection on the line defined by $x_1 = x_2$ of the solution set to the polynomial equations

$$x_1^2 + x_2^2 - 1 = x_1^3 + x_2^3 - 1 = 0.$$

Exercise 18

Let f_1, f_2 be in $\mathbb{K}[x_1, x_2]$ of total degree d. Assume that the algebraic set $V \subset \overline{\mathbb{K}}^2$ defined by $f_1 = f_2 = 0$ is finite. Can one bound a prori the number of points in V ?

Note that the above exercise settles a question raised during the first class and stated in the first Chapter where we exhibitted some families of polynomial systems of equations of degree

d defining algebraic sets of cardinality d^n.

The exercise below is extremely important. Its statement will be generalized to arbitrary polynomial rings (involving more than 2 variables) but it is already nice and important to be able to prove such a statement in the bivariate case already.

Exercise 19

Let f_1, f_2 in $\mathbb{K}[x_1, x_2]$ and assume that the algebraic set defined by $f_1 = f_2 = 0$ is empty in $\overline{\mathbb{K}}^2$ and that the leading coefficients of f_1, f_2 w.r.t. x_2 are coprime.
Prove that $\mathrm{res}_{x_2}(f_1, f_2) = 1$. Deduce that $1 \in \langle f_1, f_2 \rangle$.
Design an algorithm which on input two arbitrary polynomials f_1, f_2 in $\mathbb{K}[x_1, x_2]$ decide whether the algebraic set defined by $f_1 = f_2 = 0$ is empty in $\overline{\mathbb{K}}^2$.