Algorithms for solving bivariate polynomial systems

In the previous chapter, we introduced the definition of the *dimension* of an algebraic set defined by polynomial equations in $\mathbb{K}[x_1, x_2]$ and we studied how to exploit *specialization properties* of the resultant to allow us to design algorithms for computing the dimension of such algebraic sets. We went deeper in this study by studying how these specialization properties allow us to compute the *projection* of such solution sets on some coordinate axis.

All in all, we have been able to design algorithms which on input a polynomial system of equations in $\mathbb{K}[x_1, x_2]$ defining an algebraic set $V \subset \overline{\mathbb{K}}^2$ ($\overline{\mathbb{K}}$ denotes an algebraic closure of $\mathbb{K}$) allow us to:

- decide whether V is empty;
- if it is not empty, decide whether V is finite.

These are two algorithmic problems which were raised in the first Chapter. The next one to be considered is as follows: assuming that V is finite, *solve* the system in the following sense:

- compute the number of points in V;
- compute a *triangular representation* of V.

Also called chain representation

To make things precise, we recall what we mean by a *triangular representation*. Given f_1, f_2 in $\mathbb{K}[x_1, x_2]$ whose simultaneous vanishing defines an algebraic set $V \subset \overline{\mathbb{K}}^2$, we aim at computing polynomials w_1 and w_2 such that

$$w_1 \in \mathbb{K}[x_1] \quad \text{and} \quad w_2 \in \mathbb{K}[x_1, x_2]$$

and V is also defined $w_1 = w_2 = 0$. Observe that given such a representation one can *extract* the roots by first solving the *univariate* equation $w_1 = 0$ and next substitute the x_1 variables with the solutions of w_1 and then solve *finitely many* univariate equations in $\mathbb{K}[x_2]$.

A few remarks are here in order. First note that the idea of computing a triangular polynomial system which is *equivalent* to the input one (i.e. which has the same solution set) is quite natural.

This is indeed what exactly what Gaussian elimination does for linear systems of equations. In our context, of course, the situation is a more difficult to handle because of the non-linearity. By contrast with linear systems, even when the solution set is finite, the number of solutions may be greater than 1.

Exercise 1

Assume that

- w_1 has degree $\boxed{d_1;}$
- w_2 has degree $\boxed{d_2}$ w.r.t. x_2.

Bound the number of points in the algebraic set of $\overline{\mathbb{K}}^2$ defined by $w_1 = w_2 = 0$ with respect to (w.r.t.) d_1 and d_2.
Let h be the leading coeffcient of w_2 w.r.t. x_2. Assume that $\gcd(w_1, h) = 1$ and that w_1 and w_2 are square-free. Give the $\underbrace{\text{exact number of solutions in } \overline{\mathbb{K}}^2}$ to the system of equations $w_1 = w_2 = 0$.

The bulk of this Chapter is to understand how, from resultant algorithms one can compute such polynomials w_1 and w_2. The notion of *ideal* generated by a set of polynomials will play a central role.

Exercise 2

Assume that one can compute (w_1, w_2) in the ideal $\langle f_1, f_2\rangle$ such that $\langle w_1, w_2\rangle = \langle f_1, f_2\rangle$. Prove that the algebraic set defined $w_1 = w_2 = 0$ coincides with the algebraic set defined by $f_1 = f_2 = 0$.

The core idea is then to manipulate our input polynomials, say f_1 and f_2 in $\mathbb{K}[x_1, x_2]$ to compute such polynomials w_1 and w_2 in the ideal generated by f_1 and f_2. Actually, we already illustrated already this idea in the first Chapter by studying the following example the algebraic set $V \subset \mathbb{C}^2$ defined by $f_1 = f_2 = 0$ where

$$f_1 = x_1^2 + x_2^2 - 4 \quad \text{and} \quad f_2 = x_1x_2 - 1$$

Observe that

$$f_3 = x_2f_1 - x_1f_2 = x_2^3 - 4x_2 + x_1. \qquad |3|$$

lies in the ideal $\langle f_1, f_2\rangle$. Hence f_3 vanishes at all points of V. Note also that

$$f_4 = f_2 - x_2f_3 = f_2 - x_2(x_2f_1 - x_1f_2) = (1 + x_1x_2)f_2 - x_2^2f_1 = -x_2^4 + 4x_2^2 - 1. \qquad |4|$$

lies also in the ideal $\langle f_1, f_2\rangle$ and hence vanishes at all points of V. Hence, one deduces that at all points of V, f_3 and f_4 vanish. One deduces that the solution set in $\mathbb{C}^2$ to the system $f_3 = f_4 = 0$ *contains* V. We prove below that this solution set actually is V, by now proving that both f_1 and f_2 lie in the ideal $\langle f_1, f_2\rangle$.

Indeed, one has $f_2 = f_4 + x_2 f_3$ which implies that $f_2 \in \langle f_3, f_4 \rangle$. One can also easily check that

$$f_1 = (x_1 - x_2^3 + 4 * x_2) f_3 + (x_2^2 - 4) f_4$$

which implies that $f_1 \in \langle f_3, f_4 \rangle$ as claimed. Now, remark that $f_4 \in \mathbb{Q}[x_2]$, and $f_3 \in \mathbb{Q}[x_1, x_2]$; moreover f_3 has degree 1 in x_1. Hence, we have obtained a *triangular representation* of V (the only difference with what is described above is that the univariate polynomial lies for this example in $\mathbb{Q}[x_2]$ – instead of $\mathbb{Q}[x_1]$).

Exercise 3

Prove that the number of points in V equals 4.

One new interesting observation with the above example is that it raises the ability to *parametrize* the coordinates of some algebraic sets with polynomials which depend on a single variable. That special triangular shape makes the identification of the finitely many solutions of the polynomial system under study easy. We will see how to exploit properties of Euclide's algorithm to recover such shapes for the triangular representations we will compute.

Last but not least, the way we computed f_3 and f_4 does not involve any denominator. Note that using the algorithm computing resultants which is based on Euclide's algorithm, one introduces denominators which is not so good for practical computations.

Exercise 4

Compute the resultant of the polynomials f_1, f_2 given above w.r.t. x_2 using the algorithm based on Euclide's algorithm. ✓

This chapter starts with the introduction of an algorithm for computing resultants (and other polynomials that are called *subresultants*) which avoids the introduction of denominators.

Contents

1 Better algorithms for computing resultants

1.1 Algorithm description

Most of the time, when one uses algorithms for computing resultants, the input polynomials have coefficients either over the ring $\mathbb{Z}$ of integers or over some other polynomial polynomial rings. These rings are somewhat particular ; they do enjoy properties that one can exploit (when combining them with e.g. specialization properties) to improve the computation of resultants. Hence, we start this section with some ingredients of ring theory.

Definition 1. *A ring R is said to be* integral *if and only if for all a, b in R, the following holds:*

$$a \times b = 0 \quad \Longrightarrow \quad a = 0 \quad \textit{or} \quad b = 0.$$

Example 2. The rings $\mathbb{Z}$ as well as $\mathbb{Z}[x]$, $\mathbb{K}[x]$ or $\mathbb{K}[x_1, \ldots, x_n]$ (where $\mathbb{K}$ is a field) are integral.

The rings $\frac{\mathbb{Z}}{12\mathbb{Z}}$ as well as $\frac{\mathbb{K}[x]}{x^2-1}$ are *not* integral.

Exercise 5

- Prove that all fields are integral domains.
- Let p_1, p_2 be two prime integers and $k = p_1p_2$. Prove that $\frac{\mathbb{Z}}{k\mathbb{Z}}$ is not an integral ring.
- Let f_1, f_2 be two irreducible polynomials of $\mathbb{K}[x]$ where $\mathbb{K}$ is a field and $f = f_1 f_2$. Prove that $\frac{\mathbb{K}[x]}{\langle f \rangle}$ is not an integral ring.
- Let $R = \frac{\mathbb{Z}}{34\mathbb{Z}}$. Is $R[x]$ an integral ring ?

Definition 3. *Let R be an integral ring. A* Euclidean function *on R is a function from $R - \{0\}$ to $\mathbb{N}$ such that for a, b in R with $b \neq 0$, there exist q and r, both in R, such that*

$$a = bq + r \quad \textit{with either} \quad r = 0 \quad \textit{or} \quad f(r) < f(b).$$

A Euclidean ring is an integral domain which can be endowed with one Euclidean function.

Observe that $\mathbb{Z}$ is a Euclidean ring (one defines a Euclidean division in $\mathbb{Z}$ by considering the absolute value) but the set of matrices of size $n \times n$ with coefficients in a field $\mathbb{K}$ is *not* a Euclidean ring.

Exercise 6

Prove that $\mathbb{K}[x]$ (where $\mathbb{K}$ is a field) is a Euclidean ring.
Prove that the ring of Gaussian integers $\mathbb{Z}[i]$ (where $i^2 = -1$) is a Euclidean ring.

We describe now an algorithm which on input f_1, f_2 in $\mathbb{D}[x_1, x_2]$ where $\mathbb{D}$ is a *Euclidean ring* (such rings are sometimes called *domains* in the litterature), computes the resultant associated to (f_1, f_2).

Definition 4. *Let f_1 and f_2 be two polynomials in $\mathbb{D}[x]$ where $\mathbb{D}$ is a ring. One denotes by h_2 the leading coefficients of f_2 w.r.t. x and by n, m the respective degrees of f_1 and f_2. The* pseudo-quotient *and* pseudo-remainder *of (f_1, f_2) are polynomials $\bar{q}$ and $\bar{r}$ in $\mathbb{D}[x]$ such that*

$$h_2^{n-m+1} f_1 = \bar{q} f_2 + \bar{r}$$

with $\deg(\bar{r}) < m$.

The operation which, given f_1, f_2 consists in computing $\bar{q}$ and $\bar{r}$ is called *pseudo-division* of f_1 by f_2. Further, we denote by $\text{prem}(f_1, f_2)$ (resp. $\text{pquo}(f_1, f_2)$) the pseudo-remainder (pseudo-quotient) of the two polynomials f_1, f_2. By a slight abuse of notation, we also denote by prem and pquo the routines which on input f_1, f_2 return respectively the pseudo-remainder and the pseudo-quotient of f_1, f_2.

Exercise 7

Write an algorithm which, given as input f_1, f_2, performs the pseudo-division of f_1 by f_2 by using only ring operations in $\mathbb{D}$.

Exercise 8

- What is the relationship between quotient and remainder on the one hand and pseudo-quotient and pseudo-remainder on the other hand?
- Prove that, given f_1 and f_2, the pseudo-quotient and pseudo-remainder are uniquely defined.

The algorithm, described below, for computing the resultant of two polynomials, relies on the idea of replacing the Euclidean divisions performed by Euclide's algorithm with pseudo-divisions and exact divisions.

We can now describe the algorithm. It takes as input two polynomials f_1 and f_2 in $\mathbb{D}[x]$ where $\mathbb{D}$ is a Euclidean ring. It outputs the resultant of (f_1, f_2) by performing operations in $\mathbb{D}$ (hence, the addition and multiplication in $\mathbb{D}$ and the exact division).

```
Resultant($(f_1, f_2)$)
  • $a \leftarrow f_1$ and $b \leftarrow f_2$
  • let $f = g = s = 1$
  • while $\deg(b) > 0$ do
      – $d \leftarrow \deg(a) - \deg(b)$
      – $r = \text{prem}(a, b)$
      – if $\deg(a)$ and $\deg(b)$ are odd $s \leftarrow -s$
      – $a \leftarrow b$
```

```
        – $b \leftarrow \frac{r}{fg^d}$
        – $f \leftarrow \mathrm{lc}(a)$
        – $g \leftarrow \frac{f^d}{g^{d-1}}$
    • $d \leftarrow \deg(a)$
    • return $\frac{sb^d}{g^{d-1}}$
```

The sequence of polynomials which are stored in the variable b are called *subresultants* associated to f_1, f_2. When $\delta = \max(\deg(f_1), \deg(f_2))$, we denote by $(s_\delta, s_{\delta-1}, \ldots, s_0)$ the sequence of subresultants ordered by *decreasing* degrees.

Proposition 5. *The above algorithm is correct and it performs only exact divisions in $\mathbb{D}$.*

Exercise 9

Prove that all subresultants associated to (f_1, f_2) lie in the ideal $\langle f_1, f_2 \rangle$.

The proof of the above result is skipped.

Exercise 10

Run the above algorithm on the following examples compare with the execution of the algorithm computing resultants based on Euclide's algorithm.

- $f_1 = x^4 + x^3 + x^2 + x + 1$ and $f_2 = 3x^2 + 2x + 1$
- $f_1 = x_1^3 + x1x2^2 + x1^2x2 + x2^3$ and $f_2 = x1^2 + x2^2 + 1$ (consider the resultant with respect to x_2).

The above algorithm is interesting mainly when the domain over which computations are performed admits a *height* function which measures the size of its elements (and when this size may vary a lot). Indeed, when $\mathbb{D} = \mathbb{Z}$ or when $\mathbb{D}$ is a polynomial ring, the denominators appearing in the algorithm computing resultants which is based on Euclide's algorithm induce a blow up of the coefficients which are manipulated during the execution of the algorithm.

Performing only exact divisions only as well as pseudo-remainder computations allow us to avoid this coefficient blow up. Of course, all of this is less crucial when $\mathbb{D}$ is a prime field (because then all its elements have the same bit size).

Still measuring the practical impact of the above algorithm is interesting and important.

Exercise 11

Implement the above algorithm and compare the runtimes obtained by this implementation with the runtimes obtained when using the algorithm based on Euclide's algorithm for couples of polynomials in $\mathbb{Z}[x]$ and in $\mathbb{Z}[x_1][x_2]$.

1.2 Example

We illustrate these remarks with the execution of the above algorithm on the following example (which is extracted from [1, page 127])

$$f_1 = 115x^5 + 7x^4 + 117x^3 + 30x^2 + 87x + 44 \quad \text{and} \quad f_2 = 91x^4 + 155x^3 + 3x^2 + 143x + 115.$$

We will also compare the size of the data generated by this algorithm with the size of the data generated by the algorithm based on Euclide's algorithm.

2 Solving Algorithm

2.1 Some examples

Before describing the whole algorithm, we start by studying some examples which illustrate well the difficulties which arise when one wants to design an algorithm for solving bivariate polynomial systems.

We start with the following example

$$f_1 = \quad \text{and} \quad f_2 = .$$

2.2 Algorithm specification

It takes as input f_1, f_2 in $\mathbb{D}[x_1, x_2]$ as well as the list of variables $[x_1, x_2]$. We denote by $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{D}$ and by $V \subset \overline{\mathbb{K}}^2$ the algebraic set defined by $f_1 = f_2 = 0$.

The algorithm below decides what is the dimension of V.

When the dimension is -1 (hence the algebraic set V is empty), it outputs the couple $(-1, [[1]])$.

When the dimension is zero, it outputs a couple $(0, (\boldsymbol{A}, \mathscr{L}))$ where $\mathscr{L}$ is a couple of polynomials

$$[(w_1, w_2)]$$

where, $\boldsymbol{A}$ is a 2×2 matrix, $w_1 \in \mathbb{D}[x_1]$ and $w_2 \in \mathbb{D}[x_1, x_2]$, w_2 has degree 1 w.r.t. x_2 and letting $Z \subset \overline{\mathbb{K}}^2$ be the algebraic set defined by $w_1 = w_2 = 0$, the following holds:

$$V = \{\boldsymbol{A}^{-1}z \mid z \in Z\}.$$

When the dimension is 1 (i.e. V contains infinitely many points but is not the whole affine space $\overline{\mathbb{K}}^2$), it outputs a couple $(1, [g])$ where $g \in \mathbb{D}[x_1, x_2]$ and the algebraic set $Z \subset \overline{\mathbb{K}}^2$ defined by $g = 0$ satisfies the following properties:

- $Z \subset V$;
- the set $V - Z = \{\alpha \in V \mid \alpha \notin Z\}$ is finite.

When the dimension is 2 (i.e. $V = \overline{\mathbb{K}}^2$), the algorithm outputs the couple $(2, [0])$.

Exercise 12

Describe the solution set of the following system of polynomial equations

$$x_1(x_1^2 + x_2^2 - 1) = x_2(x_1^2 + x_2^2 - 1) = 0.$$

What would be the output of our solving algorithm for this system ?

Exercise 13

Modify the algorithm HasPositiveDimension to design another algorithm which, on input (f_1, f_2) decides whether the dimension is positive, and in case it is positive, decides whether it is 1 or 2.

2.3 Algorithm description

Further, $\mathbb{K}$ denotes a field. We can now describe the main algorithm of this Chapter.

It uses the following subroutines:

- ComputeDimension. It takes as input a couple of polynomials (a, b) in some polynomial ring $\mathbb{K}[x_1, x_2]$ and it outputs an integer d which is the dimension of the algebraic set in $\overline{\mathbb{K}}^2$ defined by $a = b = 0$.

- GCD. It takes as input a couple of polynomials (a, b) in some polynomial ring $\mathbb{K}[x_1, x_2]$ and it outputs $g \in \mathbb{K}[x_1, x_2]$ such that g is a gcd of (a, b).

- gcd. It takes as input a couple of polynomials (a, b) in some polynomial ring $\mathbb{K}[x]$ and it outputs $g \in \mathbb{K}[x]$ such that g is a gcd of (a, b).

- Subresultants. It takes as input two polynomials f_1, f_2 in $\mathbb{D}[x_1, x_2]$ of maximum degree δ as well as a variable (e.g. x_2) and it returns the list $(s_\delta, s_{\delta-1}, \ldots, s_0)$ of the subresultants associated to (f_1, f_2).

- RandomMatrix. It takes as input two integers n, p and returns a matrix of size $n \times p$ with coefficients in $\mathbb{K}$ randomly chosen.

- ApplyChangeOfVariables. It takes as input two polynomials f_1, f_2 in $\mathbb{D}[x_1, x_2]$ where $\mathbb{D}$ is a ring as well as a (2×2)-matrix $\boldsymbol{A}$ with coefficients in $\mathbb{D}$ whose determinant is non-zero. It returns two polynomials $\widetilde{f_1}$ and $\widetilde{f_2}$ such that letting

$$\begin{bmatrix} \ell_1 \\ \ell_2 \end{bmatrix} = \boldsymbol{A} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$\widetilde{f_1} = f_1(\ell_1, \ell_2)$ and $\widetilde{f_2} = f_2(\ell_1, \ell_2)$.

The algorithm is randomized; it is a Las Vegas algorithm: it always returns the correct result but its execution depends on some internal choices which must be repeated as long as they are not suitable.

It actually proceeds as follows.

- First, it starts by computing the dimension of the algebraic set defined by $f_1 = f_2 = 0$. When $d = -1$ or $d > 0$, it returns the appropriate output according to the specifications which are described above.

- Next, we are in the situation where the dimension of the algebraic set under study is 0 (hence it is finite), we compute the gcd g of the leading coefficients of f_1 and f_2 with respect to x_2. Then, we distinguish the following two cases.
  - When the degree of g is positive (one cannot apply the specialization theorem of resultants and then compute projections of solutions as explain in the previous chapter), one performs a randomly chosen linear change of variables on f_1 and f_2 ;
  - When the degree of g is 0, then we compute the list of subresultants

    $$(s_\delta, s_{\delta-1}, \ldots, s_1, s_0)$$

    associated to (f_1, f_2) (where δ is the maximum degree of f_1 and f_2).

    Let i be the smallest integer $\geqslant 1$ such that $s_i \neq 0$ and let $\widetilde{s_i}$ be the square-free part of s_i. When $]widetildes_i$ has degree 1 w.r.t. x_2, we return $(s_0, \widetilde{s_i})$ which will stand for a triangular representation of the algebraic set defined by $f_1 = f_2 = 0$. Else, one performs a randomly chosen linear change of variables on f_1, f_2 and restart the computation of subresultants.

We can now describe the solving algorithm.

```
BivariateSolve($f_1, f_2$, $[x_1, x_2]$)

  1. $d \leftarrow$ ComputeDimension($f_1, f_2$)

  2. if $d = -1$ return $(-1, [1])$

  3. if $d = 2$ return $(2, [0])$

  4. if $d = 1$
       • $g \leftarrow$ GCD($f_1, f_2$)
       • return $(1, [g])$

  5. $\boldsymbol{A} \leftarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

  6. $g \leftarrow$ gcd(lc($f_1, x_2$), lc($f_2, x_2$))
```

```
7. if $\deg(g) > 0$
    • $\boldsymbol{B} \leftarrow \mathsf{RandomMatrix}(2, 2)$
    • $\boldsymbol{A} \leftarrow \boldsymbol{A} \times \boldsymbol{B}$
    • $(f_1, f_2) \leftarrow (\mathsf{ApplyChangeOfVariables}(f_1, \boldsymbol{B}), \mathsf{ApplyChangeOfVariables}(f_2, \boldsymbol{B}))$
    • go back to Step 6
8. $\mathscr{S} = (s_\delta, s_{\delta-1}, \dots, s_1, s_0) \leftarrow \mathsf{Subresultants}(f_1, f_2, x_2)$
9. find the smallest $i$ such that $s_i \neq 0$ and let $\widetilde{s_i}$ be the square-free part of $s_i$.
10. if $\widetilde{s_i}$ has degree greater than 1
    • $\boldsymbol{B} \leftarrow \mathsf{RandomMatrix}(2, 2)$
    • $\boldsymbol{A} \leftarrow \boldsymbol{A} \times \boldsymbol{B}$
    • $(f_1, f_2) \leftarrow (\mathsf{ApplyChangeOfVariables}(f_1, \boldsymbol{B}), \mathsf{ApplyChangeOfVariables}(f_2, \boldsymbol{B}))$
    • go back to Step 6
11. return $(\widetilde{s_i}, s_0)$
```

Before proving that the above algorithm is correct, a few intermediate results need to be proved. These will make explicit the role of the change of variables induced by the matrices $\boldsymbol{A}$ which are randomly generated during the algorithm.

Further we endow the set of 2×2 matrices with coefficients in $\mathbb{K}$ with the variables $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}$; the variable $a_{i,j}$ encoding the coefficient at the i-th row and j-th column in $\boldsymbol{A}$.

Given a polynomial $\mathscr{P} \in \mathbb{K}[a_{1,1}, a_{1,2}, a_{2,1}, a_{2,3}]$, we say that

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \end{bmatrix}$$

does not cancel $\mathscr{P}$ (i.e. $\mathscr{P}(\boldsymbol{A}) \neq 0$) when $\mathscr{P}(\alpha_{1,1}, \alpha_{1,2}, \alpha_{2,1}, \alpha_{2,2}) \neq 0$.

Further, for an invertible matrix $\boldsymbol{A} \in \mathbb{K}^{2\times 2}$ and a set $Z \in \overline{\mathbb{K}}^2$, we denote by $Z^{\boldsymbol{A}}$ the set

$$Z^{\boldsymbol{A}} = \{\boldsymbol{A}^{-1} z \mid z \in Z\}.$$

Given $f \in \mathbb{K}[x_1, x_2]$, we denote by $f^{\boldsymbol{A}}$ the polynomial obtained by substituting x_1, x_2 in f with the linear forms which are the entries of

$$\boldsymbol{A} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

Note that if Z is given as the vanishing set of a polynomial system $f_1 = \cdots = f_k = 0$ then $Z^{\boldsymbol{A}}$ is defined by $f_1^{\boldsymbol{A}} = \cdots = f_k^{\boldsymbol{A}} = 0$.

Exercise 14

Prove the above statement.

Proposition 6. *Let $\mathscr{X} = \{z_1, \dots, z_\ell\} \subset \overline{\mathbb{K}}^2$ be a finite $\mathbb{K}$-algebraic set. Then, there exists a polynomial $\mathscr{P}_{\mathscr{X}} \in \mathbb{K}[a_{1,1}, a_{1,2}, a_{2,1}, a_{2,3}]$ such that for all matrices $\boldsymbol{A} \in \mathbb{K}^2$ satisfying $\mathscr{P}(\boldsymbol{A}) \neq 0$ the following holds. The set of first coordinates of the points in $\mathscr{X}^{\boldsymbol{A}}$ has cardinality ℓ.*

Proof. We start by considering all lines $L_{i,j}$ such that $L_{i,j}$ is the line containing the couple of points (z_i, z_j) with $i \neq j$. Note that the number of such lines is finite.

Exercise 15

Count the number of such lines.
Prove that the union of these lines are defined by a system of polynomial equations with coefficients in $\mathbb{K}$.

We consider now the set $\mathscr{A}_{i,j}$ of matrices $\boldsymbol{A}$ such that $L_{i,j}^{\boldsymbol{A}}$ is the first coordinate axis. Finally, we take $\mathcal{A}$ as the union of the $\mathscr{A}_{i,j}$'s.

Exercise 16

Prove that $\mathscr{A}$ is a $\mathbb{K}$-algebraic set by exhibiting a polynomial system of equations in $\mathbb{K}[a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}]$ whose solution set is $\mathscr{A}$.

Finally, we take the product $\mathscr{P}$ of the polynomials defining $\mathscr{A}$. It is then immediate that for those matrices $\boldsymbol{A}$ satsifying $\mathscr{P}(\boldsymbol{A}) \neq 0$, the projection on the first coordinate axis of $\mathscr{X}^{\boldsymbol{A}}$ has the same cardinality as $\mathscr{X}$. □

Exercise 17

Prove that for matrices $\boldsymbol{A}$ such that $\mathscr{P}(\boldsymbol{A}) \neq 0$, the set of first coordinates of the points in $\mathscr{X}^{\boldsymbol{A}}$ is in bijection with $\mathscr{X}$

Proposition 7. *Let $f \in \mathbb{K}[x_1, x_2]$. There exists a non-zero polynomial $\mathscr{Q}_f \in \mathbb{K}[a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}]$ such that for matrices $\boldsymbol{A} \in \mathbb{K}^{2\times 2}$ satisfying $\mathscr{Q}_f(\boldsymbol{A}) \neq 0$, the leading coefficient of $f^{\boldsymbol{A}}$ w.r.t. x_2 lies in $\mathbb{K}$.*

Proof. The proof is immediate by performing the linear change of variables on the terms of f of highest degree. We leave it to the reader. □

Exercise 18

Prove the above proposition.

We now consider two polynomials f_1 and f_2 in $\mathbb{K}[x_1, x_2]$ and the algebraic set $V \subset \overline{\mathbb{K}}^2$ defined by $f_1 = f_2 = 0$ which we assume to be finite. Hereafter, we say that a matrix $\boldsymbol{A}$ satsifies assumption (G) if

$$\mathscr{P}_V(\boldsymbol{A}) \neq 0, \quad \mathscr{Q}_{f_1}(\boldsymbol{A}) \neq 0, \quad \mathscr{Q}_{f_2}(\boldsymbol{A}) \neq 0.$$

Theorem 8. *Algorithm BivariateSolve is correct.*

Proof. When the dimension of the algebraic set $V \subset \overline{\mathbb{K}}^2$ defined by $f_1 = f_2 = 0$ is either 2, 1 or -1, then the output match the specification.

We focus now on the case where the dimension of the aforementioned algebraic set is 0. Hence we enter at Step 5. At Step 6, we compute the gcd g of the leading coefficients of f_1 and f_2 w.r.t. x_2. There is here a case distinction.

Assume first that the degree of g is positive. Then, by the previous Chapters, one cannot apply the specialization theorem of resultants and relate the roots of both the resultant and g with the roots of V. However, by Proposition 7, the set of matrices $\boldsymbol{B}$ that we pick at Step 7 cancels a non-zero polynomial. Hence, after some several random choices, one should obtain a matrix $\boldsymbol{B}$ such that the leading coefficients of $f_1^{\boldsymbol{B}}$ and $f_2^{\boldsymbol{B}}$ with respect to x_2 have a gcd of degree 0.

One then enters at Step 8 and computes the subresultant sequence associated to (f_1, f_2) (which have been modified through the linear change of variables induced by $\boldsymbol{A}$ w.r.t. the original polynomials given as input). Since at this step g has degree 0, applying the projection theorem in the previous Chapter, one deduces that the set of roots of s_0 is the same as the projection on the x_1-axis of the set of points in V. Now, remark that s_i lies in the ideal $\langle f_1, f_2 \rangle$.

Exercise 19

Prove with all required details the above statement.

This implies that s_i vanishes at all points of V. Now, assume that the square-free part $\widetilde{s_i}$ of s_i has degree 1, hence it can be written as $h\, x_2 + t$ where h and t are polynomials of $\mathbb{K}[x_1]$. Note that since s_i vanishes at all points of V, then $\widetilde{s_i}$ vanishes at all points of V also.

Now, assume that $\widetilde{s_i}$ has degree greater than 1, let us denote this degree r. Then, applying the projection theorem, one deduces that above a root of s_0 (the resultant associated to (f_1, f_2)), say α, there exist $\beta_1, \ldots, \beta_r$ such that (α, β_i) lies in the algebraic set defined by $f_1 = f_2 = 0$ for $1 \leqslant i \leqslant r$. Now, applying Proposition 6 to the algebraic set defined by $f_1 = f_2 = 0$, one deduces that for a generic enough choice of $\boldsymbol{B}$, the projection on the x_1-axis of the algebraic set defined by $f_1^{\boldsymbol{B}} = f_2^{\boldsymbol{B}} = 0$ has the same cardinality as that algebraic set (and then these two sets will be in bijection). This ends the proof. □

Remark. Note that the algorithm BivariateSolve will always return the correct result but its runtime depends on the random choices of the matrices done during the execution of the algorithm.

Exercise 20

Design an algorithm which takes as input f_1, f_2, f_3 in $\mathbb{K}[x_1, x_2]$ and which solves the system of polynomial equations $f_1 = f_2 = f_3 = 0$.

3 The case of systems with integer coefficients

Exercise 21

Let f_1 and f_2 be two polynomials in $\mathbb{Z}[x]$ of degree bounded by d and coefficients of bit size bounded by τ.
Use Hadamard's bound to provide a bound on the bit size of the resultant associated to (f_1, f_2) w.r.t. d and τ.
Deduce from this a multi-modular algorithm based on the Chinese remainder theorem to compute the resultant of (f_1, f_2).
Hint. Use the specialization properties of resultants.

Exercise 22

Let f_1 and f_2 be two polynomials in $\mathbb{Z}[x_1, x_2]$ of degree bounded by d.
Bound the degree of the resultant associated to (f_1, f_2) w.r.t. x_2 with respect to d.
Deduce from this an algoritihm for computing the resultant which is based on an evaluation-interpolation scheme.

References

[1] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, and É. Schost. *Algorithmes efficaces en calcul formel.*