Preliminaries, basic definitions and notions

Mohab Safey El Din

Polynomial systems arise in numerous application areas of engineering and computing sciences such as robotics, imaging, cryptography, etc. They model non-linear (but static) situations and hence are the immediate generalization to linear systems.

However, non-linearity induces several difficulties and the algorithmic challenge of solving non-linear polynomial systems is, by far, much more difficult than solving linear systems.

Various methods exist for solving polynomial systems. In this course, we focus on the *algebraic* ones, in particular those based on *Gröbner bases*, because they are well-suited to solve problems coming from cryptography.
The course is built on the following bibliographic references.

- **Ideals, Varieties and Algorithms**, D. Cox, J. Little, D. O'Shea, Springer.
- **Algebra**, S. Lang, Springer.
- **De la résolution des systèmes linéaires à la résolution des systèmes polynomiaux**, J.-C. Faugère, M. Safey El Din, Pearson.
- **Polynomials**, V. Prasolov, Springer.
- **Algorithms in real algebraic geometry**, S. Basu, R. Pollack, M.-F. Roy, Springer.

Pre-requisites for this course. Basic notions of linear algebra will be frequently used. The notions of vector spaces, their dimension, the linear maps, their rank, the study of finite dimensional vector spaces and basic algorithms (matrix multiplication, Gauss elimination, etc.) must be known.

Contents

1 Overview and motivations

1.1 Motivations and first observations

Polynomial systems (of equations, inequations, inequalities) arise in many areas of engineering sciences such as robotics, biology, chemistry to cite a few and computing sciences such as cryptography, computer vision, computational geometry, program verification, etc. These systems encode *non-linear* but static phenomena.

One reason for the ubiquity of such systems in sciences is that most of operations in Euclidean geometry are encoded with polynomials. One can think for instance of scalar products, rank deficiency constraints, squares of Euclidean distances, which are all expressed with polynomials with respect to (w.r.t.) the entries/coordinates of the points/vectors/matrices which are considered.

Exercise 1

Recall how to compute:

- the scalar product of two vectors;
- the Euclidean distance between two points;
- a polynomial system encoding rank deficiencies in a matrix;
- a polynomial depending on the entries of a given matrix which must vanish when this matrix has one eigenvalue of multiplicity two.

One can already observe deep differences between (non-linear) polynomial systems of equations and linear systems of equations. Recall that one *univariate* linear equation $ax + b = 0$ (where a, b are the coefficients, say in $\mathbb{Q}$) has 1 unique solution in $\mathbb{Q}$ when $a \neq 0$, 0 solution if

$a = 0, b \neq 0$ or an infinity of solutions when $a = 0, b = 0$. Note that the last two cases are quite trivial. Polynomial univariate equations

$$a_d x^d + \cdots + a_0 = 0$$

where the a_i's are the coefficients lying in $\mathbb{Q}$ are already quite different than linear univariate equations. They can of course have much more that 1 solution in $\mathbb{Q}$; see for instance

$$\prod_{i=1}^{d} (x - \alpha_i) \qquad \text{where } \alpha_i \in \mathbb{Q}.$$

which has d solutions in $\mathbb{Q}$ while the considered polynomial has degree d.

Polynomial equations can also be non trivial and have 0 solution in $\mathbb{Q}$ as illustrated by this polynomial equations

$$x^2 - 2 = 0$$

which has degree 2, 0 solution in $\mathbb{Q}$ and 2 solutions in $\mathbb{R}$ (actually, $\pm\sqrt{2}$) or by

$$x^2 + 1 = 0$$

which has 0 solution in $\mathbb{Q}$, 0 solution in $\mathbb{R}$ and 2 solutions in $\mathbb{C}$.

Exercise 2

Let $d \in \mathbb{N}$ be an even positive integer.

- Provide a univariate polynomial equation with coefficients in $\mathbb{Q}$ which has 0 solution in $\mathbb{Q}$ and d solutions in $\mathbb{R}$.
- Provide a univariate polynomial equation with coefficients in $\mathbb{Q}$ which has 0 solution in $\mathbb{Q}$, 0 solution in $\mathbb{R}$ and d solutions in $\mathbb{C}$.

Is it possible to have a polynomial equation of degree $d + 1$ with coefficients in $\mathbb{R}$ with d real solutions ?

This already shows that when studying polynomial systems, one needs to be careful with the domain where the solutions are searched on the one hand and that, depending on the chosen domain, the number of solutions can be high.

Up to now, we have considered univariate polynomial equations. One will of course focus in this course on *multivariate* polynomials. It is of interest to understand how the number of variables may impact on the number of solutions, say in $\mathbb{C}$ when the input coefficients lie in $\mathbb{Q}$ (the situation will be a bit more involved when considering polynomial systems with coefficients in a finite field).

For instance, one can easily prove that the following polynomial system of equations

$$x_1^2 - 1 = x_2^2 - 1 = \cdots = x_n - 1^2 = 0$$

has 2^n solutions (actually in $\mathbb{N}$).

The following polynomial system shows that the number of complex solutions may vary also with the respective degrees of the input polynomials

$$x_1^{d_1} - 1 = \cdots = x_n^{d_n} - 1 = 0$$

since it has $d_1 \cdots d_n$ solutions. When all the polynomials have the same degree d, one obtains d^n complex solutions.

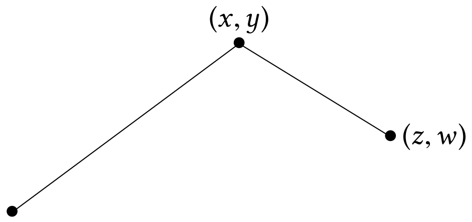
Exercise 3

Provide a lower bound on the complexity for enumerating complex solutions to polynomials systems with coefficients in $\mathbb{Q}$ (assuming those systems have finitely many complex solutions).

We claimed that polynomial system solving finds numerous applications in engineering sciences. We illustrate this with a first example coming from robotics in the next paragraph. Further, we will examine a polynomial system coming from cryptography.

1.2 An example from robotics

Consider a robot arm in the plane which consists of two linked rods of respective lengths 1 and 2, with the longer rod anchored at the origin:



The "state" of the arm is completely described by the coordinates (x, y) and (z, w) indicated in the figure. Thus the state can be regarded as a 4-tuple $(x, y, z, w) \in \mathbb{R}^4$. However, not all 4-tuples can occur as states of the arm. In fact, it is easy to see that the subset of possible states is the affine variety in $\mathbb{R}^4$ defined by the equations:

$$\begin{aligned} x^2 + y^2 &= 4 \\ (x-z)^2 + (y-w)^2 &= 1. \end{aligned}$$

Exercise 4

Assume that we want the end-effector of the robot to lie on the circle centered at the origin of radius 3/2 and such that the determinant of the matrix

$$\begin{bmatrix} x & z \\ y & w \end{bmatrix}$$

equals 1.

Try to solve this system of polynomial equations.

Notice how even larger dimensions enter quite easily: if we were to consider the same arm in 3-dimensional space, then the variety of states would be defined by two equations in $\mathbb{R}^6$. Understanding the possible motions and positions of such rigid mechanisms boils down to polynomial system solving.

Polynomial system solving is also a key tool for assessing the security of crypto-ciphers. Cryptography is based on the hardness of some algorithmic problems. Beyond them, polynomial system solving (even over a boolean field) is known to be NP-hard.

1.3 An example from cryptology

We provide below an example of a cryptocipher based on the hardness of polynomial system solving. Assume that A wants to send a message to B in the following context.

- B makes public the polynomials $f_1, \ldots, f_p$ which lie in $\mathbb{F}_q[x_1, \ldots, x_n]$ (where $\mathbb{F}_q = \frac{\mathbb{Z}}{q\mathbb{Z}}$ is a prime field or a finite one), this is the *public key*.
- B keeps secret the solution $\boldsymbol{x}$, this is the *secret key*.

Then A sends a message $m \in \mathbb{F}_q^n$ to B by

- choosing a matrix H of size $n \times p$ with entries $h_{i,j}$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant p$;
- and sending the polynomial $c = m + H.\boldsymbol{f}$ where $\boldsymbol{f}$ is the vector
$$\begin{bmatrix} f_1 \\ \vdots \\ f_p \end{bmatrix}.$$

B decodes the message by evaluating c at $\boldsymbol{x}$ (because $c(\boldsymbol{x}) = m + \sum_{i=1}^{p} h_i(\boldsymbol{x}) f_i(\boldsymbol{x}) = m$).

Hence, either attacking this crypto-cipher or assessing its security boils down to the ability to solve the polynomial system

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

over $\mathbb{F}_q$.

Exercise 5

Let $\mathbb{K} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ be a prime field (hence p is a prime and $\mathbb{K}$ has cardinaltity p). Consider a polynomial system S of equations in $\mathbb{K}[x_1, \ldots, x_n]$. We assume further that none of these equations is the trivial equation $0 = 0$ (all polynomials have positive degrees).

- Prove that S has finitely many solutions.
- Provide an upper bound on the number of solutions of S (in $\mathbb{K}^n$).
- Provide an algorithm for finding these solutions in $\mathbb{K}^n$.

1.4 Some first ideas towards algorithms

Let us assume that we want to solve the following polynomial system

$$\begin{aligned} x^2y + 3xyz - z^2y^2 &= 1 \\ x^2y - 4xyz - z^2y^2 &= 2 \\ x^2y + 2xyz - 3z^2y^2 &= 3 \end{aligned}$$

One claims that solving such a polynomial system is "easy" since it can be reduced to basic Gaussian elimination in some matrix.

Indeed, the number of *monomials* of positive degree which appear in this system coincides with the number of equations. Hence, one can rewrite this system as follows:

$$\begin{bmatrix} 1 & 3 & -1 \\ 1 & -4 & -1 \\ 1 & 2 & -3 \end{bmatrix} \begin{bmatrix} x^2y \\ xyz \\ z^2y^2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

Finally, solving the underlying linear system yields values for the monomials x^2y, xyz, z^2y^2.

Of course, when the number of monomials is larger than the number of equations, the above strategy cannot be applied. For instance, one can consider the polynomial system of equations:

$$\begin{aligned} x^2y + 3xy - x^2yz + xyz &= 1 \\ x^2y - xy + x^2yz - 2xyz &= 2 \\ x^2y + 5xy &= 0 \end{aligned}$$

which can be linearized as follows:

$$\begin{bmatrix} 1 & 3 & -1 & 1 \\ 1 & -1 & 1 & -2 \\ 1 & 5 & 0 & 0 \end{bmatrix} \begin{bmatrix} x^2y \\ xy \\ x^2yz \\ xyz \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$$

Observe that, in some sense, one relation is *missing* to enable an approach which is similar to the above one. Remark that multiplying the last equation by z yields the equation

$$x^2yz + 5xyz = 0.$$

Since this is a consequence of the whole system, adding this new constraint will not change the solution set. Now, one remarks that one can linearize the system as follows:

$$\begin{bmatrix} 1 & 3 & -1 & 1 \\ 1 & -1 & 1 & -2 \\ 1 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 \end{bmatrix} \begin{bmatrix} x^2y \\ xy \\ x^2y^2z \\ xyz \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix}$$

We will see during this course some algorithmic strategies that mimic and make systematic this linearization process.

At the moment, let us see how we can go further with the idea of multiplying by monomials a given equation to deduce some useful information on the solution set. Let us consider the following example.

$$\begin{aligned} x^2 + y^2 - 4 &= 0 \\ xy - 1 &= 0. \end{aligned}$$

Since the system is bivariate one can see the input polynomials as *univariate* polynomials with respect to the variable x with coefficients which are polynomials with respect to the variable y.

We let $f_1 = x^2 + y^2 - 4$ and $f_2 = xy - 1$. Note that

$$yf_1 - xf_2 = y^3 - 4y + x.$$

Now, letting $f_3 = y^3 - 4y + x$, we observe that the system $f_1 = f_2 = f_3 = 0$ has exactly the same solution set as $f_1 = f_2 = 0$.

Now, note that

$$f_4 = f_2 - yf_3 = -y^4 + 4y^2 - 1.$$

One can again observe that the system $f_1 = f_2 = 0$ has exactly the same solution set as $f_1 = f_2 = f_3 = f_4 = 0$. One can also easily show that the solution set of $f_1 = f_2 = 0$ is the same as the one of the system $f_3 = f_4 = 0$.

Exercise 6

Prove carefully the above statement.

One interesting thing to note is that this last system is *triangular*:

$$\begin{aligned} x + y^3 - 4y &= 0 \\ -y^4 + 4y^2 - 1 &= 0 \end{aligned}$$

Hence one can retrieve *all* solutions to our input by identifying first the solutions to the last univariate equation (which involves the variable y) and next plug these solutions in f_3 to retrieve the corresponding x coordinate.

Actually, this triangular form allows us to *parametrize* the x-coordinates of the solutions w.r.t. the solutions of a univariate equation whose solutions are the *projections* on the y-axis of the solutions to the input polynomial system.

We will develop further algorithms for computing such parametrizations (triangular form) from which one can extract the solutions. One first key idea that appears in the above examples is to compute extra relations/polynomials that can be deduced from our input in order to provide useful informations on the solution set.

Note also that by **eliminating variables** we were able to **compute projections** of the solutions.

1.5 Solving: what does it mean?

All in all, one already sees the following algorithmic challenges which are interesting when studying algebraic sets:

- Decision problem: Given $(f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$, decide whether the solution set V to $f_1 = \cdots = f_p = 0$ in $\bar{\mathbb{K}}^n$, where $\bar{\mathbb{K}}$ is field containing $\mathbb{K}$, is empty or not.

- Finiteness: When V is not empty, decide whether it is finite or not.

  When it is finite, we may also be interested in counting and isolating (enumerating) the solutions to the input system. Recall that in this context, one will try to compute a representation of the solution in triangular form

  $$w_n(x_n) = 0, w_{n-1}(x_{n-1}, x_n) = 0, w_{n-2}(x_{n-2}, x_{n-1}, x_n) = 0, \ldots, w_1(x_1, \ldots, x_n) = 0.$$

- Dimension: When V is not finite, what is its dimension?

Our goal now is to design algorithms for tackling these problems. To do so, we will use algebraic computations, exploiting the algebraic structure of our problems.

2 Basic algebra

We start by recalling the definitions of fundamental algebraic structures.

Definition 1 (Group)**.** *Let G be a set equipped with the binary operation $\star : G \times G \to G$. One says that $(G, \star)$ is a group if the following hold:*

1. *the operation $\star$ is associative (i.e. $\boldsymbol{x} \star (\boldsymbol{y} \star \boldsymbol{z}) = (\boldsymbol{x} \star \boldsymbol{y}) \star \boldsymbol{z}$) ;*
2. *there exists $\boldsymbol{e} \in G$ (called identity element) such that for all $\boldsymbol{x} \in G$, $\boldsymbol{x} \star \boldsymbol{e} = \boldsymbol{e} \star \boldsymbol{x} = \boldsymbol{x}$;*
3. *for all $\boldsymbol{x} \in G$, there exists $\boldsymbol{y} \in G$ (called invert of $\boldsymbol{x}$) such that $\boldsymbol{x} \star \boldsymbol{y} = \boldsymbol{e}$. Usually, such an element $\boldsymbol{y}$ is denoted by $\boldsymbol{x}^{-1}$.*

A group is said to be abelian (or commutative) if the binary operation is commutative. Also, a group is said to be finite when its cardinality is finite.

Exercise 7

Let e be the identity element of a group $(G, \star)$. Prove that e is unique.

Example 2. The following are classical examples of groups:

- The set of permutations[1] over $\{1, \ldots, n\}$ is a finite group. This group is usually denoted by Σ_n.
- The set of integers equipped with the classical addition $(\mathbb{Z}, +)$ is a group (it is not finite!). Of course, $(\mathbb{Z}, \times)$ is not a group.
- When p is prime, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\}, \times\right)$ is a group.

Definition 3. *Let $(G, \star)$ be a group and H be a subset of G. One says that H is a subgroup of G if the following holds:*

- *the target space of the restriction $\star_H$ of $\star$ to $H \times H$ is H;*
- *$(H, \star_H)$ is a group.*

Observe that $(\{e\}, \star)$ is a subgroup of G. The structure of a group G is governed by its subgroups. Let H is a subgroup of G and $g \in G$. The left coset associated to g and H is defined as:

$$gH = \{g \star h \mid h \in H\}.$$

A subset S of G is said to be a coset of H if there exists $g \in G$ such that $S = gH$.

One proves easily that

- the map $h \to gh$ is a bijection ; hence one deduces that gH and H have the same cardinality.
- every element of G is contained in a *unique* coset of H ; we denote the number of cosets of G by $[G : H]$.

Hence one deduces the following theorem, which is known as Lagrange's theorem for groups.

Theorem 4 (Lagrange's theorem)**.** *Let $(G, \star)$ be a group and H be a subgroup of G. Assume that G is finite. Then, the following holds:*

$$\sharp G = \sharp H \ . \ [G : H]$$

[1] i.e. the set of bijections from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$

Exercise 8

In group theory, a generating set of a group G is a subset such that every element $g \in G$ can be expressed as the combination (under the group operation) of **finitely** many elements of the subset and their inverses.
Besides, given $S \subset G$, one denotes by $\langle S \rangle$ the smallest subgroup of G containing S.
Prove that

1. $\langle S \rangle$ is the intersection over all subgroups containing the elements of S;
2. $\langle S \rangle$ is the subgroup of all elements of G that can be expressed as the finite product of elements in S and their inverses.

Here are some additional questions.

1. What is a generating set for the additive group $(\mathbb{Z}, +)$?
2. Same question for $\left(\frac{\mathbb{Z}}{p\mathbb{Z}} - \{0\}, \times\right)$ when p is prime?
3. What is the cardinality of Σ_n? Is Σ_n a commutative group? What is a generating set for Σ_n?

Warning. Some groups cannot be finitely generated; this is the case for, e.g. $(\mathbb{Q}, +)$.

Definition 5 (Ring). *Let R be a set equipped with two binary operations $+ : R \times R \to R$ and $\times : R \times R \to R$. One says that $(R, +, \times)$ is a ring if the following holds:*

1. *$(R, +)$ is an abelian group ;*
2. *$\times$ is an associative binary operation ;*
3. *$\times$ is distributive with respect to $+$.*

- Unitary rings are those rings which contain an identity element for $\times$; this one is usually denoted by 1_R.

  Further, 0_R will denote the identity element for $+$.

  When R is clearly identified from the context, one may omit the subscript R.

- A ring is said to be commutative when $\times$ is commutative.

- A ring is said to be integral when it is commutative and when for all $(\boldsymbol{x}, \boldsymbol{y}) \in R \times R$, $\boldsymbol{x} \times \boldsymbol{y} = 0$ implies $\boldsymbol{x} = 0$ or $\boldsymbol{y} = 0$.

  When this occurs, one says that R does not admit a zero divisor.

Example 6. The following are classical examples of rings:

- $(\mathbb{Z}, +, \times)$ is a ring (but of course $(\mathbb{Z}, \times, +)$ is not).
- $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times\right)$ is a ring for *any* positive integer p.
- $(M_{p,p}(\mathbb{Z}), +, \times)$ is a ring (where $M_{p,p}(\mathbb{Z})$ is the set of $p \times p$ matrices with entries in $\mathbb{Z}$).

Exercise 9

Let $(R, +, \times)$ be a ring. Prove that:

1. the identity elements of a ring are unique;
2. 0 (the identity element for $+$) is absorbing, i.e. $0 \times x = x \times 0 = 0$ for any $x \in R$.
3. if $0 = 1$, then R has cardinality 1.
4. Let p and q be prime numbers. What are the zero-divisors of $\frac{\mathbb{Z}}{pq\mathbb{Z}}$?

Let $(R, +, \times)$ and $(R', +', \times')$ be two rings.

Definition 7. *Let $\varphi : R \to R'$ be a map. One says that φ is a ring homomorphism if it preserves the ring structure, i.e.*

- *for all a, b in $R \times R$, $\varphi(a + b) = \varphi(a) +' \varphi(b)$;*
- *for all a, b in $R \times R$, $\varphi(a \times b) = \varphi(a) \times' \varphi(b)$.*

Example 8. An important example of ring homomorphism is the modular image morphism. Recall that $(\mathbb{Z}, +, \times)$ is a ring. Now, let p be a positive integer and recall that $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times\right)$ is also a ring. We consider now the map $\varphi : x \in Z \to x \mod p$. One proves easily that this map is a ring homomorphism.

Exercise 10

Use modular ring homomorphisms to speed-up the following problem: given a $n \times n$ matrix A with coefficients in $\mathbb{Z}$, decide whether the determinant of A is zero.

Definition 9 (Field)**.** *Let $\mathbb{K}$ be a set equipped with two binary operations $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ and $\times : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$. On says that $(\mathbb{K}, +, \times)$ is a field if the following holds:*

1. *$(\mathbb{K}, +, \times)$ is a unitary commutative ring ;*
2. *the identity elements of $+$ and $\times$ (denoted respectively $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$) do not coincide ;*
3. *$(\mathbb{K}^\star, \times)$ is a group (where $\mathbb{K}^\star = \mathbb{K} - \{0\}$).*

As for groups, one defines finite fields as those fields which have finite cardinality. Prime fields $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times\right)$ with p prime play a crucial role, both for *multi-modular arithmetic* and in cryptography.

3 Polynomials: definitions and first properties

3.1 Preliminaries

Let $\mathbb{K}$ be a field and $x_1, \ldots, x_n$ be variables.

Definition 10. *Let $\alpha_1, \ldots, \alpha_n$ be* positive integers. *Then, the product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is a* monomial.
For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ we denote by $\underline{x}^\alpha$ the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
A term *is a product $c\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $c \in \mathbb{K}$.*
Let S be a finite *set in $\mathbb{N}^n$. Then $\sum_{\alpha \in S} c_\alpha \underline{x}^\alpha$ is a polynomial with coefficients in $\mathbb{K}$ with variables $x_1, \ldots, x_n$.*

The set of polynomials with coefficients in $\mathbb{K}$ with variables $x_1, \ldots, x_n$ is denoted by $\mathbb{K}[x_1, \ldots, x_n]$.
In the above definition, the subset $S' \subset S$ such that

$$\sum_{\alpha \in S} c_\alpha \underline{x}^\alpha = \sum_{\alpha' \in S'} c_{\alpha'} \underline{x}^\alpha \qquad \text{and} \qquad \forall \alpha' \in S \quad c_{\alpha'} \neq 0$$

is called the suppport of that polynomial.

Proposition 11. *$\mathbb{K}[x_1, \ldots, x_n]$ equipped with the natural addition and multiplication is a ring.*

Exercise 11

Prove the above proposition.

Definition 12. *Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.*

- *The* degree *of the monomial $\underline{x}^\alpha$ is $|\alpha| = \sum_{i=1}^n \alpha_i$. It will be denoted by $\deg(\underline{x}^\alpha)$.*
- *The* degree *of the term $c\underline{x}^\alpha$ (when $c \neq 0$) is $|\alpha| = \sum_{i=1}^n \alpha_i$. It will be denoted by $\deg(c\underline{x}^\alpha)$.*
- *The* total degree *of a polynomial $f = \sum_{\alpha \in S} c_\alpha \underline{x}^\alpha$ is $\max(|\alpha|, \alpha \in S$ and $c_\alpha \neq 0)$. It will be denoted by $\deg(f)$.*
- *The degree of f in the variable x_i is $\max(\alpha_i, \alpha \in S$ and $c_\alpha \neq 0)$. It will be denoted by $\deg(f, x_i)$.*
- *When $n = 1$ and $f = \sum_{i=0}^D c_i x^i$ with $c_D \neq 0$, c_D is the* leading coefficient *of f.*

By convention, the degree of $0 \in \mathbb{K}[x_1, \ldots, x_n]$ is $-\infty$.
By abuse of language, we call *degree* of f the *total degree* of f.

Definition 13 (Homogeneous polynomials)**.** *Let $f = \sum_{\alpha \in S} c_\alpha \underline{x}^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$ of degree D. We say that f is* homogeneous *iff*

$$\forall \alpha \in S \qquad \text{s.t.} \qquad c_\alpha \neq 0, \quad |\alpha| = D.$$

The set of homogeneous polynomials of degree D in $\mathbb{K}[x_1, \ldots, x_n]$ is denoted by $\mathbb{K}[x_1, \ldots, x_n]_D$.

Remark. One can make the following observations.

- The product of 2 homogeneous polynomials is a homogeneous polynomial.
- $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^D f(x_1, \ldots, x_n)$
- $\mathbb{K}[x_1, \ldots, x_n] = \oplus_{i=0}\mathbb{K}[x_1, \ldots, x_n]_i$.

We say that f is homogeneous in the block of variables $x_{i+1}, \ldots, x_n$ if it is hom. when seen as a polynomial in $\mathbb{K}[x_1, \ldots, x_i][x_{i+1}, \ldots, x_n]$.

Lemma 14. *The following holds.*

1. *The maximum number of monomials appearing in polynomials of* $\mathbb{K}[x_1, \ldots, x_n]$ *of degree* D *is*
$$\binom{n+D}{D}$$
2. *The maximum number of monomials appearing in* **homogeneous** *polynomials of* $\mathbb{K}[x_1, \ldots, x_n]$ *of degree* D *is*
$$\binom{n+D-1}{D}$$

Exercise 12

Prove the above lemma. Deduce from these bounds, the complexity of basic algorithms for

1. adding polynomials in $\mathbb{K}[x_1, \ldots, x_n]$
2. multiplying polynomials in $\mathbb{K}[x_1, \ldots, x_n]$

Observe that given f and g in $\mathbb{K}[x_1, \ldots, x_n]$ with $g \neq 0$, the product $f.g$ has degree equalled to $\deg(f) + \deg(g)$. We shall study in more details univariate polynomials but the following observation is important.

Lemma 15. *Let* $f \in \mathbb{K}[x]$ *of degree* $k > 0$. *Then* f *has at most* k *roots.*

Proof. Our reasonning is by induction on k. When $k = 1$, the result is immediate. Now, let us make that the assumption is true for $k-1$ and let $f \in \mathbb{K}[x]$ of degree k.

Let also $\boldsymbol{x}$ be a root of f. Then $(x - \boldsymbol{x})$ divides f ; the quotient q then has degree $k-1$. Observe that the roots of f are $\boldsymbol{x}$ and the roots of q. Using the induction assumption on q, our conclusion follows. □

We already observed that for a root $\boldsymbol{x} \in \mathbb{K}'$, where $\mathbb{K}'$ is a field containing $\mathbb{K}$, of $f \in \mathbb{K}[x]$, $(x - \boldsymbol{x})$ divides f in $\mathbb{K}'[x]$ (it suffices to look at the Euclidean division of f by $(x - \boldsymbol{x})$ in $\mathbb{K}'[x]$). Let $m \geqslant 1$ be the largest integer such that $(x - \boldsymbol{x})^m$ divides f. Then m is called the *multiplicity* of $\boldsymbol{x}$ as a root of f.

Definition 16 (Algebraic closure). *Let $\mathbb{K}$ be a field such that for any $f \in \mathbb{K}[x]$ of degree $k > 0$, f has k roots (counted with multiplicities).*

Of course, not all fields are algebraically closed (for instance, $\mathbb{R}$, the field of real numbers is not). However, given an arbitrary field $\mathbb{K}$, we call *algebraically closure* of $\mathbb{K}$ a field $\mathbb{F}$ containing $\mathbb{K}$ such that $\mathbb{F}$ is algebraically closed.

The first (and basic) example of algebraically closed fields if the field $\mathbb{C}$ of complex numbers. It is an algebraically closure of $\mathbb{R}$ (and of $\mathbb{Q}$).

3.2 Derivatives and Fröbenius map.

Definition 17. *Let $f = \sum_{i=0}^{D} c_i x^i \in \mathbb{K}[x]$; the* derivative *of f w.r.t x is the polynomial $\frac{\partial f}{\partial x} = \sum i c_i x^{i-1}$.*

Let $t = c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be a term. The partial derivative *of t with respect to x_i is*

$$\frac{\partial t}{\partial x_i} = \alpha_i c_\alpha x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i - 1} x_{i+1}^{\alpha_{i+1}} x_n^{\alpha_n}.$$

Let f be a polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. Then the partial derivative *of f w.r.t x_i is the sum of the partial derivatives of its terms w.r.t. x_i.*

Some properties.

- Let $f \in \mathbb{K}[x]$ and $\boldsymbol{x}$ be a root of f of multiplicity m. Then $\frac{\partial f^{(i)}}{\partial x}$ vanishes at $\boldsymbol{x}$ for $1 \leqslant i \leqslant m-1$.

- (Euler relation). Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree D. Then

$$D\, f = \sum_{i=1}^{n} x_i \frac{\partial f}{\partial x_i}$$

Let $(f_1, \ldots, f_p)$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The Jacobian matrix associated to $(f_1, \ldots, f_p)$ is the $p \times n$ matrix

$$\mathrm{jac}(f_1, \ldots, f_p) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial x_1} & \cdots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}$$

Let $f_1, \ldots, f_{n+k}$ in $\mathbb{K}[x_1, \ldots, x_n, Y_1, \ldots, Y_k]$. Assume that $f_1, \ldots, f_{n+k}$ are homogeneous of degree 1 in the variables $x_1, \ldots, x_n$ and homogeneous in the variables $Y_1, \ldots, Y_k$ of degree 1. Then the following identities hold.

$$\mathrm{jac}_{\boldsymbol{x}}(\boldsymbol{F}) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} F_1 \\ \vdots \\ F_{n+k} \end{bmatrix} \text{ and } \mathrm{jac}_{\boldsymbol{Y}}(\boldsymbol{F}) \begin{bmatrix} Y_1 \\ \vdots \\ Y_k \end{bmatrix} = \begin{bmatrix} F_1 \\ \vdots \\ F_{n+k} \end{bmatrix}$$

Proposition 18. *Let $f \in \mathbb{K}[x]$. Assume that $\mathbb{K}$ has characteristic 0 and $\deg(f) \geqslant 1$. Then $\frac{\partial f}{\partial x} \neq 0$.*

Assume that $\mathbb{K}$ has characteristic $p > 0$. Then $\frac{\partial f}{\partial x} = 0$ iff (if and only if) p divides all $\alpha \in \mathbb{N}$ such that $f = \sum_{\alpha=0}^{D} c_\alpha \underline{x}^\alpha$ with $c_\alpha \neq 0$.

3.3 Symmetric polynomials.

Let $\vartheta_1, \ldots, \vartheta_n$ be algebraically independent variables over $\mathbb{K}$ and x be a variable over $\mathbb{K}[\vartheta_1, \ldots, \vartheta_n]$.

Consider

$$\begin{aligned} F(x) &= (x - \vartheta_1) \cdots (x - \vartheta_n) \\ &= x^n - E_1 x^{n-1} + \cdots + (-1)^n E_n \end{aligned}$$

where each $E_i \in \mathbb{K}[\vartheta_1, \ldots, \vartheta_n]$.

Definition 19. *The polynomials $E_1, \ldots, E_n$ are called the elementary symmetric polynomials of $\vartheta_1, \ldots, \vartheta_n$.*

The polynomials E_i are *homogeneous* of degree i in $\vartheta_1, \ldots, \vartheta_n$.

Let σ be a permutation of the integers $\{1, \ldots, n\}$ and for $f \in \mathbb{K}[\vartheta_1, \ldots, \vartheta_n]$ let

$$\sigma f = f(\vartheta_{\sigma(1)}, \ldots, \vartheta_{\sigma(n)}).$$

Note that $\sigma\tau f = \sigma(\tau f)$.

Definition 20. *A polynomial is called symmetric if $\sigma f = f$ for any permutation σ.*

Property:

- The set of symmetric polynomials is a subring of $\mathbb{K}[\vartheta_1, \ldots, \vartheta_n]$.
- It contains the constant polynomials and the elementary symmetric polynomials.

Definition 21. *Let $x_1, \ldots, x_n$ be variables. we define the weight of a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ to be $\sum_{i=1}^{n} i\alpha_i$. The weight of a polynomial is the maximum of the weights of its monomials.*

Theorem 22. *Let $f \in \mathbb{K}[\vartheta_1, \ldots, \vartheta_n]$ be symmetric of degree D. Then there exists a polynomial $g(x_1, \ldots, x_n)$ of weight $\leqslant D$ such that*

$$f = g(E_1, \ldots, E_n).$$

Examples: $x_1^2 + x_2^2 + x_3^2 = E_1^2 - 2E_2$
$x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2 = E_1 E_2 - 3E_3$

Theorem 23. *The elementary symmetric functions are independent over $\mathbb{K}$.*

4 Affine and projective spaces and algebraic varieties

4.1 The affine case

Definition 24 (Affine space)**.** *Let $\mathbb{K}$ be a field and n be a positive integer. The n-dimensional* affine space *over $\mathbb{K}$ is the set $\{(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \mid \boldsymbol{x}_i \in \mathbb{K}\}$.*

Now, let $f \in \mathbb{K}[x_1, \ldots, x_n]$. One can consider the evaluation map

$$f : \boldsymbol{x} \in \mathbb{K}^n \to f(\boldsymbol{x}) \in \mathbb{K}.$$

The *zero test* may have different meanings:

1. is f the zero polynomial (the one with all coefficients equalled to 0)?

2. is f the zero function (i.e. $\forall \boldsymbol{x} \in \mathbb{K}^n, f(\boldsymbol{x}) = 0$)?

First, observe that deciding if a polynomial is the zero polynomial may not be so easy when polynomials are not given in a dense form (as the vector of their coefficients indexed by multi-degrees). For instance, deciding if a polynomial defined as the determinant of a given matrix (with polynomial entries) is the zero one, requires some computations.

Exercise 13

Find algorithms for the above decision problem.

These are different questions which may get different answers. For instance, when $\mathbb{K}$ is the boolean field, i.e. $\frac{\mathbb{Z}}{2\mathbb{Z}}$ (sometimes also denoted by $\mathbb{F}_2$), the polynomial $f = x(x-1)$ is obviously not the zero polynomial. However, observe that the evaluation map $\boldsymbol{x} \in \mathbb{F}_2 \to f(\boldsymbol{x})$ is the zero function.

Exercise 14

Generalize the above construction to arbitrary prime fields.

The following result provides a sufficient condition for ensuring the equivalence for both conditions.

Proposition 25. *Let $\mathbb{K}$ be an infinite field and $f \in \mathbb{K}[x_1, \ldots, x_n]$. Then f is the zero polynomial if and only if f is the zero function.*

Proof. Since the zero polynomial defines the zero function, we only need to show that if for all $\boldsymbol{x} \in \mathbb{K}^n$, $f(\boldsymbol{x}) = 0$, then f is the zero polynomial (under the inifiniteness assumption on $\mathbb{K}$). The proof is done by induction on n.

When $n = 1$, one deduces that f is a univariate polynomial with infinitely many roots. Hence the linear factors $(x - \boldsymbol{x})$ divide f when $\boldsymbol{x}$ ranges over $\mathbb{K}$. Since $\mathbb{K}$ is inifnite, f wouldn't have finite degree and then wouldn't be a polynomial.

Now, let us assume that for polynomials in $\mathbb{K}[x_1, \ldots, x_{n-1}]$ with $\mathbb{K}$ infinite, the following holds. If for all $\boldsymbol{x} \in \mathbb{K}^{n-1}$, one has $g(\boldsymbol{x}) = 0$ (for $g \in \mathbb{K}[x_1, \ldots, x_{n-1}]$), then g is the zero polynomial. This is our induction assumption.

Now, take $f \in \mathbb{K}[x_1, \ldots, x_n]$ and assume that for all $\boldsymbol{x} \in \mathbb{K}^n$, $f(\boldsymbol{x}) = 0$. Let k be the degree of f in x_n. Then, one can decompose f as

$$f = \sum_{i=0}^{k} g_i \cdot x_n^i$$

with $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. It is quite clear that if all the g_i's are the zero polynomial, then f is the zero polynomial. Now, we pick infinitely many points $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{n-1})$ in $\mathbb{K}^{n-1}$. Observe that for all of them $f(\boldsymbol{\alpha}, x_n)$ is the zero function. From the case $n = 1$ studied above, we deduce that all the g_i's take the value 0 at $\boldsymbol{\alpha}$. In other words, for all $\boldsymbol{\alpha} \in \mathbb{K}^{n-1}$, $g_i(\boldsymbol{\alpha}) = 0$ with $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. From our induction assumption, we deduce that the g_i's are the zero polynomial and we are done. □

Corollary 26. *Let $\mathbb{K}$ be an infinite field and (f, g) be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Assume that the maps $\boldsymbol{x} \to f(\boldsymbol{x})$ and $\boldsymbol{x} \to g(\boldsymbol{x})$ coincide. Then, $f = g$ holds.*

Exercise 15

Prove the above corollary. Find counter-examples when $\mathbb{K}$ is finite.

When solving polynomial systems such as

$$f_1 = \cdots = f_N = 0$$

one is interested in the set of points at which the f_i's vanish simultaneously.

Definition 27 (Algebraic set / variety)**.** *Let $\mathbb{K}$ be a field, $\bar{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$ and a natural integer n. An algebraic set V of the affine space $\bar{\mathbb{K}}^n$ is a subset of $\bar{\mathbb{K}}^n$ such that the following holds. There exists a subset S in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ such that for all $f \in S$ and $\boldsymbol{x} \in V$, $f(\boldsymbol{x}) = 0$.*

When one can choose S in $\mathbb{K}[x_1, \ldots, x_n]$, one says that V is a $\mathbb{K}$-algebraic set.

Also, given a subset S in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ (or $\mathbb{K}[x_1, \ldots, x_n]$), we denote by $V(S)$ the subset of points in $\bar{\mathbb{K}}^n$ such that for all $f \in S$ and $\boldsymbol{x} \in V(S)$, one has $f(\boldsymbol{x}) = 0$.

Remark. We did not assume that S is finite here. In most of the situations we will consider herafter, S will be finite (and composed of the polynomials forming the system of equations we aim at solving). However, we will deal later with situations where S is not finite (it will actually be an algebraic object called *ideal*).

Famous geometric objects are actually algebraic sets. The very first ones are lines and planes which are obviously solutions to linear equations (polynomials of degree 1).

Maybe the first obvious non-linear one is the circle centered at the origin of radius one. While it is parametrized by the sin and cos functions, it is the solution set to the equation:

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

Its drawing over the real plane is well-known but maybe misleading: recall that algebraic sets are defined over algebraically closed fields. In our case, we would work with $\mathbb{C}$ as base field. Define π_1 as the canonical projection $(\boldsymbol{x}_1, \boldsymbol{x}_2) \rightarrow \boldsymbol{x}_1$. Hence, observe (and prove) that for any value $\boldsymbol{x} \in \mathbb{C}$, $\pi_1^{-1}(\boldsymbol{x})$ has a non-empty intersection with the algebraic set defined by the above equation.

Exercise 16

Prove the above assertion.

A second geometric object studied in high-school and which is an algebraic set is the hyperbola, i.e. the solution to the equation

$$x_1 x_2 - 1 = 0.$$

Exercise 17

For which value $\boldsymbol{x} \in \mathbb{C}$, does the pre-image $\pi_1^{-1}(\boldsymbol{x})$ has an empty intersection with the hyperbola?

Lemma 28. *Let V_1 and V_2 be two algebraic sets in $\bar{\mathbb{K}}^n$. Then $V_1 \cup V_2$ and $V_1 \cap V_2$ are algebraic sets.*

Proof. Let F and G be polynomial subsets in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$ such that:

$$V_1 = V(F) \qquad \text{and} \qquad V_2 = V(G).$$

Observe that $V_1 \cap V_2 = V(F \cup G)$ (the left and right inclusions are immediate).

It remains to handle the situation for $V_1 \cup V_2$. Let

$$S = \{fg \mid f \in F \text{ and } g \in G\}.$$

For $\boldsymbol{x} \in V_1 \cup V_2$, we have that for all $h \in S$, $h(\boldsymbol{x}) = 0$ (because either $\boldsymbol{x} \in V_1$ and then any $f \in F$ vanishes at $\boldsymbol{x}$ or, symmetrically, $\boldsymbol{x} \in V_2$ and any $g \in G$'s vanish at $\boldsymbol{x}$). We deduce that $V_1 \cup V_2 \subset V(S)$.

We prove now the reverse inclusion $V(S) \subset V_1 \cup V_2$ which will end the proof. Take $\boldsymbol{x} \in V(S)$. If for all $f \in F$, f vanishes at $\boldsymbol{x}$, then $\boldsymbol{x} \in V_1$. Else, there exists $f \in F$ such that $f_\ell(\boldsymbol{x}) \neq 0$. But since $\boldsymbol{x} \in V(S)$, we deduce that for any $g \in G$, $g(\boldsymbol{x}) = 0$ and then $\boldsymbol{x} \in V_2$. We deduce that $\boldsymbol{x} \in V_1 \cup V_2$ in both situations and then $V(S) \subset V_1 \cup V_2$ as claimed. □

More generally, graphs of polynomial and rational maps are algebraic sets. Also, in higher dimension, solutions to linear systems of equations $A.x = b$ (where A is a matrix with entries in $\bar{\mathbb{K}}$, x is a vector of variables and b is a vector of scalars in $\bar{\mathbb{K}}$) are algebraic sets. These solution sets are affine linear subsets of the affine space and their dimension is well understood: when the matrix A is full rank, the dimension is the number of variables minus the number of equations. When A is not full rank, one can get rid of some equations (which are a linear combination of the others) and retrieve a "regular" situation.

One could expect something similar for *non-linear* algebraic sets. Unfortunately, the situation is more difficult and subtle as illustrated by the following example. Consider the algebraic set in $\mathbb{C}^3$ defined by the two quadratic equations:

$$x_1 x_2 = 0 \qquad \text{and} \qquad x_1 x_3 = 0.$$

It is clearly the union of the plane defined by $x_1 = 0$ and the line defined by $x_2 = x_3 = 0$. Hence it can be decomposed into one set of dimension 2 (the plane) and one set of dimension 1 (the line).

4.2 The projective case

Definition 29 (Projective space). *Let $\mathbb{K}$ be a field and n be a positive integer. For $\boldsymbol{x} = (\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) \in \mathbb{K}^{n+1} - \mathbf{0}$, denote by $L_{\boldsymbol{x}}$ the line*

$$\{(\lambda \boldsymbol{x}_0, \ldots, \lambda \boldsymbol{x}_n) \mid \lambda \in \mathbb{K}\}$$

The n-dimensional projective space *over $\mathbb{K}$ is the set of lines*

$$\{L_{\boldsymbol{x}} \mid \boldsymbol{x} \in \mathbb{K}^{n+1}\}.$$

An element of $\mathbb{P}^n(\mathbb{K})$ is denoted by $(\boldsymbol{x}_0 : \boldsymbol{x}_1 : \cdots : \boldsymbol{x}_n)$. Note that for any $\boldsymbol{x} \neq 0$ and $\lambda \neq 0$, the following holds

$$(\lambda \boldsymbol{x}_0 : \lambda \boldsymbol{x}_1 : \cdots : \lambda \boldsymbol{x}_n) = (\boldsymbol{x}_0 : \boldsymbol{x}_1 : \cdots : \boldsymbol{x}_n)$$

Let $\boldsymbol{x} = (\boldsymbol{x}_0 : \cdots : \boldsymbol{x}_n) \in \mathbb{P}^n(\mathbb{K})$ and $F \in \mathbb{K}[x_0, \ldots, x_n]$. Assume that F is homogeneous and $F(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n) = 0$. Then for any λ, $F(\lambda \boldsymbol{x}_0, \ldots, \lambda \boldsymbol{x}_n) = 0$.