Multivariate division algorithm

In the previous Chapter, we introduced algorithms to solve all algorithmic questions which were raised in the first one, namely, determining if an algebraic set contains infinitely many points or if it is finite, in case it is finite, determine if it is empty and if it is not, compute a *triangular representation* of the solution set.

All this was possible through *resultants* and their specialization properties that enabled us to relate, under some conditions, the solutions to the algebraic set under study and their projections on the coordinate axis which was corresponding to the variable which was not *eliminated*.

Doing so, we introduced ideals of polynomial rings and exploited some properties of ideals of univariate polynomial rings.

In this Chapter, we introduce the material which is necessary to go further and towards algorithms for solving polynomial systems over polynomial rings with an arbitrary number of variables.

To do so, we target to introduce a generalization of the Euclidean division which was introduced in the univariate setting to an n-variate one. More precisely, given polynomials f and $f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$, we would like to be able to compute a polynomial r such that

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

where r *reduces* something. For instance, in the univariate case, when $s = 1$, one succeeds to have r with a degree smaller than the divisor and then build upon this division Euclide's algorithm. However, this scheme works only for principal ideals.

General polynomial rings such as $\mathbb{K}[x_1, \ldots, x_n]$ with $n \geqslant 2$ are no more *principal*.

Exercise 1

Let $\mathbb{K}$ be a field and consider the polynomial ring $\mathbb{K}[x_1, x_2]$. Prove that the ideal $I = \langle x_1, x_2 \rangle$ is not generated by a single polynomial.

Hint. Make a reasonning by contradiction by assuming that I is generated by a single polynomial g and look at the degrees of g w.r.t. x_1 and x_2.

A consequence of this is that we will not be able to obtain something which is as strong as what we got for univariate polynomial rings, in particular, recall that one can decide if some

univariate polynomial f lies in the ideal generated two univariate polynomials f_1, f_2 by checing if f is divisible by the gcd of f_1, f_2.

Exercise 2

Prove the above statement.

These differences constitute a strong obstruction to mimicking what was done for the bivariate case. Still, we can build upon two ideas which were introduced previously.

- The euclidean division is made to decrease the degree of the remainder and then exploits the natural ordering over univariate monomials $x^i > x^j \Leftrightarrow i > j$. One can think about introducing *monomial orderings* and mimick the Euclidean division.

  By introducing *monomial orderings* and a reduction operator, we will see that one can obtain kind of generalization of the Euclidean division. We will also see that it is not as powerful as it is in the univariate case.

- The notion of *ideal* and its properties played an important role in the previous Chapters to obtain algorithms for solving bivariate polynomial systems.

  We can go further with ideals of polynomial rings and study their properties to build algorithms which are more general than what we had.

This Chapter is organized as follow. We start by studying extra properties of polynomial ideals and go deeper in how to use their properties to solve polynomial systems and study algebraic sets. Next, we go back to a description of our initial motivations and study again some examples. This will lead us to introduce monomial orderings and in the final section of this Chapter the new *multivariate division algorithm*.

Contents

1 Ideals of polynomial rings

Ideals are the algebraic counterpart to the geometric sets which are algebraic. In this section, we study basic properties of ideals of polynomial rings.

Definition 1. *Let I be a subset of $R = \mathbb{K}[x_1, \ldots, x_n]$. One says that I is an* ideal *of the polynomial ring R if the following holds:*

- $0 \in I$;
- *for any f, g in I, $f + g \in I$;*
- *for any $f \in R$ and $g \in I$, $f\ g \in I$.*

Remark that $\mathbb{K}[x_1, \ldots, x_n]$ is an ideal.

Definition 2. *Let $(f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$. We define $\langle f_1, \ldots, f_p \rangle$ as the set*

$$\{q_1 f_1 + \cdots + q_p f_p \mid q_i \in \mathbb{K}[x_1, \ldots, x_n], \quad 1 \leqslant i \leqslant p\} \subset \mathbb{K}[x_1, \ldots, x_n].$$

Lemma 3. *For $\boldsymbol{f} = (f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$, $\langle f_1, \ldots, f_p \rangle$ is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. We call it the ideal generated by $\boldsymbol{f}$.*

Proof. The proof consists in checking all axioms that must be satisfied by polynomial ideals. □

Definition 4. *An ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is said to be principal if there exists $f \in \mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle f \rangle$.*

Not all ideals in $\mathbb{K}[x_1, \ldots, x_n]$ are principal (however, in the next section, we will prove that when $n = 1$, this is the case).

Also, remark that starting with a *finite* set of polynomial equations (which is usually the situation we face when solving polynomial systems), the ideal generated by this set of equations is the algebraic object that contains *all* other equations which are satisfied by the solutions (in an algebraic closure $\bar{\mathbb{K}}$ of $\mathbb{K}$) of the initial polynomial system.

A nice illustration of this is obtained when considering the following example[1]

$$x = 1 + t, \qquad y = 1 + t^2$$

One can show that the equation $x^2 - 2x + 2 - y = 0$ (where t does not appear), is satisfied by the solutions of the above system. Indeed, this new equation is obtained from $t = x - 1$, squaring t, and substitute t^2 in the other equation.

This way, one has discovered a new equation, where t does not appear (we say that we have *eliminated* t). The new equation we obtain actually defines the *projection* of the solution set of the input system on the (x, y)-plane. Note also that from this process we guess a *triangular* description of the solution set as follows:

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

[1] This example is extracted from the book *Ideal, Varieties and Algorithms by Cox, Little and O'Shea, Springer*

Of course, it is not possible to compute *all* polynomials in an ideal generated by a polynomial family. We aim at computing those which will allow us to compute useful informations about the solution set only.

Further, we say that an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is finitely generated when there exists $\boldsymbol{f} = (f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that $I = \langle \boldsymbol{f} \rangle$. The sequence is then said to be a *basis* of I. Further, we will study *Gröbner bases* which are bases with special properties that are crucial to *solve* polynomial systems.

A topical question that we will study later understand if all ideals of $\mathbb{K}[x_1, \ldots, x_n]$ are finitely generated. We will actually establish such a result later. For the moment, we keep on our study with more elementary properties.

Lemma 5. *Let $\boldsymbol{f} = (f_1, \ldots, f_p)$ and $\boldsymbol{g} = (g_1, \ldots, g_k)$ be polynomial sequences in $\mathbb{K}[x_1, \ldots, x_n]$. Assume that $\langle \boldsymbol{f} \rangle = \langle \boldsymbol{g} \rangle$. Then, $V(\boldsymbol{f}) = V(\boldsymbol{g})$.*

Proof. The proof is immediate. □

We reuse again examples from the book *Ideal, Varieties and Algorithms by Cox, Little and O'Shea, Springer.* The above lemma can be used to show that

$$V(x^2 + 3y^2 - 7, x^2 - y^2 - 3) = V(x^2 - 4, y^2 - 1).$$

This also illustrates how the choice of a basis of an ideal can make easier the extraction of the solution set of the algebraic set which is associated to it.

Also, note that the polynomial sequence

$$\boldsymbol{g} = (x^2 - 4, y^2 - 1)$$

allows us to decide if, given another finite polynomial sequence $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n], V(\boldsymbol{g}) \subset V(\boldsymbol{g})$ (it suffices to substitute x be 2, -2 and y by 1, -1 and check that all entries of $\boldsymbol{f}$ vanish). At last, observe the triangular shape of $\boldsymbol{g}$.

Definition 6. *Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and $\bar{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$. We define the algebraic set associated to I (and denote it by $V(I)$) as the subset of points in $\bar{\mathbb{K}}^n$ at which all polynomials in I vanish.*

Exercise 3

We observed that $\mathbb{K}[x_1, \ldots, x_n]$ is an ideal. What is the algebraic set associated to it?

Lemma 5 also settles a deep question. Assume we are given a basis $\boldsymbol{f}$ of an ideal I. Then all polynomials in I vanish on $\boldsymbol{f}$. But are these polynomials the only ones. The answer is obviously no and we are led to consider the notion of ideal associated to an algebraic set.

Definition 7. *Let $V \subset \bar{\mathbb{K}}$ be a $\mathbb{K}$-algebraic set. Then, we define*

$$I_{\mathbb{K}}(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \forall \boldsymbol{x} \in V, \quad f(\boldsymbol{x}) = 0\}.$$

When $\mathbb{K}$ is explicit from the context, we remove the index $\mathbb{K}$ from the notation above.

Exercise 4

What is the ideal associated to $\bar{\mathbb{K}}^n$?

Lemma 8. *Let $V \subset \bar{\mathbb{K}}$ be a $\mathbb{K}$-algebraic set. Then $I_{\mathbb{K}}(V)$ is an ideal ; we call it* the *ideal associated to V.*

Proof. It is clear $0 \in I_{\mathbb{K}}(V)$. Now, take f and g in $I_{\mathbb{K}}(V)$. Then, they vanish at all points of V as do $f+g$. Now, consider $h \in \mathbb{K}[x_1, \ldots, x_n]$. Again observe that $h.f$ vanishes at all points of V (because f does). □

Exercise 5

Let $V = \{(0,0)\} \subset \mathbb{C}^2$. Prove that $I_{\mathbb{K}}(V) = \langle x, y \rangle$.

A more elaborated example is the so-called twisted cubic $V \subset \mathbb{C}^2$ defined by

$$y - x^2 = z - x^3 = 0.$$

We prove below that $I_{\mathbb{C}}(V) = \langle y - x^2, z - x^3 \rangle$ using techniques that will be useful further (they bring the foundations of more general algorithms that we will study later).

A start is to prove that all polynomials in $\mathbb{C}[x, y, z]$ can be written as follows

$$f = q_1(y - x^2) + q_2(z - x^3) + r$$

with q_1 and q_2 in $\mathbb{K}[x, y, z]$ and $r \in \mathbb{C}[x]$.

We start with the case where f is a single monomial $x^\alpha y^\beta z^\gamma$. We obviously have

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (y - x^2 + x^2)^\beta (z - x^3 + x^3)^\gamma \\ &= x^\alpha (x^2 + y - x^2)^\beta (x^3 + z - x^3)^\gamma \\ &= x^\alpha (x^{2\beta} + \sum_{i=1}^{\beta} x^{2i} (y - x^2)^i)(x^{3\gamma} + \sum_{i=1}^{\gamma} x^{3i} (z - x^3)^i)^\gamma \end{aligned}$$

from which we deduce that

$$x^\alpha y^\beta z^\gamma = q_1(y - x^2) + q_2(z - x^3) + x^{\alpha + 2\beta + 3\gamma}$$

where q_1 and q_2 lie in $\mathbb{C}[x, y, z]$.

Now, recall that any polynomial f of degree say d is a *linear* combination of monomials of degree $\leqslant d$. Hence, applying the above to each of these monomial, multiplying the obtained writing by the corresponding coefficients and summing up those results, we deduce our claim, i.e. all polynomials f in $\mathbb{C}[x, y, z]$ can be written as

$$f = q_1(y - x^2) + q_2(z - x^3) + r$$

with q_1 and q_2 in $\mathbb{C}[x, y, z]$ and $r \in \mathbb{C}[x]$.

We can go now to the heart of the proof that $I_{\mathbb{C}}(V) = \langle y - x^2, z - x^3 \rangle$. First note that $y - x^2$ and $z - x^3$ obviously lie in $I_{\mathbb{C}}(V)$. We deduce that $\langle y - x^2, z - x^3 \rangle \subset I_{\mathbb{C}}(V)$. Now take $f \in I_{\mathbb{C}}(V)$. From the above discussion, there exist q_1, q_2 in $\mathbb{C}[x, y]$ and $r \in \mathbb{C}[x]$ such that

$$f = q_1(y - x^2) + q_2(z - x^3) + r.$$

If one proves that r is actually the zero polynomial, then one can deduce that $I_{\mathbb{C}}(V) \subset \langle y - x^2, z - x^3 \rangle$ which will end the proof.

To do that, observe that all points of V are of the form (t, t^2, t^3) for $t \in \mathbb{C}$. We also have by definition that $f(t, t^2, t^3) = 0$. From the above decomposition of f, we conclude that $r(t) = 0$ for any $t \in \mathbb{C}$. Since $\mathbb{C}$ is infinite, we conclude that $r = 0$ and this ends the proof.

Observe that in the above exercise, we were able to *decide if a polynomial belongs to an ideal given by a basis.* In the above, we used some kind of parametrization of the algebraic set which is a strong requirement. But can we do that more generally, without such a knowledge[2]?

Lemma 9. *Let $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n]$ be a finite polynomial sequence. Then $\langle \boldsymbol{f} \rangle \subset I_{\mathbb{K}}(V(\boldsymbol{f}))$.*

Proof. The proof is rather straighforward ; it is sufficient to check that all polynomials in $\langle \boldsymbol{f} \rangle$ vanish at any point of $V(\boldsymbol{f})$. □

Exercise 6

Provide an example where the inclusion in the above lemma does not occur.

Proposition 10. *Let V and W be algebraic sets in $\bar{\mathbb{K}}^n$. Then, the following holds:*

1. *$V \subset W$ if and only if $I_{\mathbb{K}}(W) \subset I_{\mathbb{K}}(V)$;*
2. *$V = W$ if and only if $I_{\mathbb{K}}(V) = I_{\mathbb{K}}(W)$.*

Proof. Assume first that $V \subset W$ and let $f \in I_{\mathbb{K}}(W)$; then it vanishes at all points of W and consequently at all points of V. We deduce that $f \in I_{\mathbb{K}}(V)$ and then $I_{\mathbb{K}}(W) \subset I_{\mathbb{K}}(V)$.

Now assume that $I_{\mathbb{K}}(W) \subset I_{\mathbb{K}}(V)$ and let $\boldsymbol{x} \in V$. Then, all polynomials in $I_{\mathbb{K}}(V)$ vanish at $\boldsymbol{x}$. Since $I_{\mathbb{K}}(W) \subset I_{\mathbb{K}}(V)$, we deduce that all polynomials of $I_{\mathbb{K}}(W)$ vanish at $\boldsymbol{x}$ and then $\boldsymbol{x} \in W$.

The second assertion is a consequence of the first one. □

Exercise 7

Complete the above proof by showing that the second assertion is a consequence of the first one.

[2] It is not true that all algebraic sets can be parametrized

Exercise 8

Let I and J be ideals in $\mathbb{K}[x_1, \ldots, x_n]$. Prove that if $I \subset J$ then $V(J) \subset V(I)$.

Observe that what we have studied so far raises the following questions:

1. Can every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ be finitely generated?

   For instance, it would be useful to know that $I_{\mathbb{K}}(V)$ has such a property.

2. Given $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n]$ a finite sequence, and $f \in \mathbb{K}[x_1, \ldots, x_n]$ is there an algorithm that is able to decide if $f \in \langle \boldsymbol{f} \rangle$?

3. Given $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n]$ a finite sequence, what is the exact relation between $\langle \boldsymbol{f} \rangle$ and $I_{\mathbb{K}}(V(\boldsymbol{f}))$?

2 Back to initial motivations and examples

Let $\mathbb{K}$ be a field and $x_1, \ldots, x_n$ be variables. Recall that our preliminary study of polynomial ideals raised the following questions:

(1) Can every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ be finitely generated?

   For instance, it would be useful to know that $I_{\mathbb{K}}(V)$ has such a property.

(2) Given $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n]$ a finite sequence, and $f \in \mathbb{K}[x_1, \ldots, x_n]$ is there an algorithm that is able to decide if $f \in \langle \boldsymbol{f} \rangle$?

(3) Given $\boldsymbol{f} \subset \mathbb{K}[x_1, \ldots, x_n]$ a finite sequence, what is the exact relation between $\langle \boldsymbol{f} \rangle$ and $I_{\mathbb{K}}(V(\boldsymbol{f}))$?

Recall also that we want to *solve* polynomial systems and hence extract some information about algebraic sets associated to ideals (e.g. generated by a set of input equations). More precisely, we had identified the following algorithmic problems, given $(f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$:

(a) Decision problem: Given $(f_1, \ldots, f_p)$ in $\mathbb{K}[x_1, \ldots, x_n]$, decide whether $V(f_1, \ldots, f_p)$ is empty or not.

(b) Finiteness: When $V(f_1, \ldots, f_p)$ 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.

(c) Dimension: When $V(f_1, \ldots, f_p)$ is not finite, what is its *dimension*[3]?

[3] recall that we did not define it rigorously yet

Recall that when $n = 1$ (the univariate case), we already proved that any ideal in $\mathbb{K}[x]$ is finitely generated. More precisely, we established that these ideals are principal, i.e. generated by a single element of $\mathbb{K}[x]$, and that this element is a gcd of all polynomials in the ideal under consideration.

We even provided an *algorithmic* way to compute such a canonical generator on input a finite set of polynomials $f_1, \ldots, f_p$ in $\mathbb{K}[x]$. The key algorithmic tool we used to do so is the Euclidean division algorithm and Euclide's algorithm. It is important to note that given

$$a = a_p x^p + \cdots + a_0$$

and

$$b = b_q x^q + \cdots + b_0$$

in $\mathbb{K}[x]$ (with $p \geqslant q$), the Euclidean division algorithm aims at rewriting a "modulo" b and hence it actually sees b as a rewriting rule

$$x^q \longleftarrow -\frac{b_{q-1}x^{q-1} + \cdots + b_0}{b_q}$$

and substitutes x^q in a until one obtains a polynomial (the remainder) of degree less than q.

Note also that after this process, we have computed a new polynomial in the ideal $\langle a, b\rangle$ and Euclide's algorithm uses this new polynomial to compute other polynomials in the ideal, decreasing the degree at each step, until one finds the gcd g which generates the ideal.

In the whole process, one implicitely uses the natural ordering induced by the degree on the univariate monomials

$$1 \prec x \prec x^2 \prec x^3 \prec \cdots \prec x^q \prec \cdots \prec x^p \prec \cdots$$

and we try to find a polynomial in $\langle a, b\rangle$ whose *leading monomial*, w.r.t. this ordering, is the smallest possible.

We will aim at generalizing these ideas to multivariate polynomial ideals. However, things won't go as smoothly as they do for the univariate case. In particular, one immediately sees that it is not possible to order multivariate monomials using the notion of degree. For instance the monomials x_1^2, x_1x_2 and x_2^2 have the same degree while they are distinct.

To overcome this difficulty, one needs, at least, to order variables. This actually is to be related with Gauss'algorithm for solving linear systems. For instance, let us solve the following system of linear equations:

$$\begin{cases} x_1 + x_2 + x_3 & = 1 \\ x_1 + 2x_2 + 2x_3 & = 0 \\ x_1 + 3x_2 - x_3 & = 1 \end{cases}$$

When solving such a system with Gauss'algorithm, one eliminates first the variable x_1, using the rewriting rule:

$$x_1 \longleftarrow 1 - x_2 - x_3$$

from the polynomial point of view. This gives rise to the equations

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ x_2 + x_3 = -1 \\ 2x_2 - 2x_3 = 0 \end{cases}$$

Implicitely, here, by giving the priority to x_1 to be eliminated, we can consider it as a variable which is "greater" than x_2 and x_3.

Continuing again with Gaussian elimination, one uses the rewriting rule

$$x_2 \longleftarrow -1 - x_3$$

which gives rise to the equivalent system:

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ x_2 + x_3 = -1 \\ -4x_3 = 2 \end{cases}$$

Here, we have given the priority to x_2 to be eliminated and hence consider it as a "greater" variable than x_3. All in all, we have implicitely considered an ordering on the variables

$$x_1 \succ x_2 \succ x_3.$$

Since we were manipulating *linear* equations, this ordering is complete on the monomials of degree 1. Hence, thanks to this linearity, the ambiguity and obstruction that is raised above for ordering monomials of degree 2 does not occur.

In order to generalize Euclidean division *and* Gaussian elimination to a multivariate non-linear setting, we need now to introduce orderings on monomials of $\mathbb{K}[x_1, \ldots, x_n]$.

3 Monomial orderings

Below, we use intensively the one-to-one correspondance between monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i \in \mathbb{N}$, for $1 \leqslant i \leqslant n$, and elements of $\mathbb{N}^n$.

Observe that we require these orderings to:

- enable to sort unambiguously all the monomials appearing in a polynomial (recall that polynomials are finite linear combinations of polynomials);
- be compatible with mutliplication, to ensure the transitivity of the ordering: when multiplying a polynomial with a monomial, the respective orderings on monomials should not change.

We can now define monomial orderings.

Definition 11. *A monomial ordering $\succ$ on $\mathbb{K}[x_1, \ldots, x_n]$ is a relation on $\mathbb{N}^n$ satisfying the following properties:*

1. *$\succ$ is a total order on $\mathbb{N}^n$;*
2. *for α, β in $\mathbb{N}^n$, if $\alpha \succ \beta$ and $\gamma \in \mathbb{N}$, then $\alpha + \gamma \succ \beta + \gamma$;*
3. *$\succ$ is a well-ordering, i.e. every non-empty subset A of $\mathbb{N}^n$, has a least element for $\succ$ (there exists $\alpha \in A$ such that for all $\beta \in A - \{\alpha\}$, $\beta \succ \alpha$).*

Also, given α and β in $\mathbb{N}^n$, we will say that $\alpha \succeq \beta$ if $\alpha \succ \beta$ or $\alpha = \beta$.

Lemma 12. *An order relation $\succ$ of $\mathbb{N}^n$ is not a well-ordering if and only if there is an infinite strictly decreasing sequence in $\mathbb{N}^n$.*

Proof. Assume first that $\succ$ is not a well-ordering. Then, there exists $A \subset \mathbb{N}^n$ which is non-empty and has no least element. Pick $\alpha^{(1)} \in A$. Since A has no least element, there exists $\alpha^{(2)} \in A - \{\alpha^{(1)}\}$ such that $\alpha^{(1)} \succ \alpha^{(2)}$. Now, observe that $A - \{\alpha^{(1)}\}$ has no least element (else A would have one). Then, $\alpha^{(2)}$ is not a least element and there exists $\alpha^{(3)} \in A$ such that

$$\alpha^{(1)} \succ \alpha^{(2)} \succ \alpha^{(3)}.$$

Continuing this way, one deduces that there exists an inifnite strictly decreasing sequence in A.

We prove now the reciprocal assertion. Let $\{\alpha^{(1)}, \ldots, \alpha^{(i)}, \ldots,\}$ be a strictly decreasing sequence in $\mathbb{N}^n$. Then, this set, by definition does not contain a least element and $\succ$ is not a well-ordering. □

We will use further this lemma to prove the termination of some algorithms because some terms will be strictly decreasing at each step of the algorithm as for the Euclidean division in the univariate case.

We will also prove further that the last condition of Definition 11 is equivalent to $\alpha \succeq \mathbf{0}$ for all $\alpha \in \mathbb{N}^n$.

We can now start with important examples of monomial orderings.

Definition 13 (Lexicographic order)**.** *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{N}^n$. We say that $\alpha \succ_{lex} \beta$ if the leftmost non zero entry of $\alpha - \beta$ is positive.*

We can study here the examples given by Cox, Little and O'Shea:

- $(1, 2, 3) \succ_{lex} (0, 3, 4)$
- $(3, 2, 4) \succ_{lex} (3, 2, 1)$
- The variables $x_1, \ldots, x_n$ are ordered in the usual way

  $$(1, 0, \ldots, 0) \succ_{lex} (0, 1, 0, \ldots, 0) \succ_{lex} \cdots \succ_{lex} (0, \ldots, 0, 1)$$

  or in other words $x_1 \succ_{lex} \cdots \succ_{lex} x_n$.

Lemma 14. *The lexicographical ordering is a monomial ordering.*

Proof. There is no major difficulty in this proof. We must only pay attention to the third property which is proved by contradiction and using Lemma 12. □

Exercise 9

Provide a detailed proof for the above lemma.

Exercise 10

Sort the following monomials with respect to the lexicographic ordering.

$$x_1^2x_2^3x_3^4,\ x_1x_2x_3,\ x_1^2x_2,\ x_2^2x_3,\ x_1x_3^2,\ x_2x_3^2,\ x_3^{100},\ x_2^2,\ x_1,\ x_2x_3,\ x_1x_2,\ x_1x_3$$

Observe that the lexicographical order, as it is defined, imposes the ordering on variables $x_1, \dots, x_n$. Unless said otherwise, when using variables $x_1, \dots, x_n$, we will assume that we take

$$x_1 \succ \cdots \succ x_n.$$

Also, when worksing with variables as letters such as $a, b, c, \dots$ or x, y, z, we will assume

$$a \succ b \succ c \cdots$$

or

$$x \succ y \succ z.$$

Changing the ordering on variables is doable but that would lead to "other" lexicographical orderings (which are obtained up to renaming the variables to coincide with the above definition).

An important property of the lexicographical ordering is that a variable is greater than *any* monomial involving only smaller variables, without taking into account the degree of this monomial. For instance, observe that reusing the above notations, $x_1 \succ_{lex} x_2^{34}x_3^{57}$. Sometimes, there is interest in taking into account the degrees of the monomials in the definition of monomial orderings.

The Graded Lexicographical Order defined below is the first of that kind.

Definition 15 (Graded Lexicographical Order)**.** *Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ be in $\mathbb{N}^n$. We say that $\alpha \succ_{grlex} \beta$ if*

$$\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i \qquad \text{or} \left(\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \text{ and } \alpha \succ_{lex} \beta \right).$$

In other words, sorting two monomials with the Graded Lexicographical Order consists in sorting using the degree first. When both monomials have the same degree, it applies the lexicographical ordering.

Again, one can study some examples:

- $(1, 2, 3) \succ_{grlex} (3, 2, 0)$
- $(1, 2, 4) \succ_{grlex} (1, 1, 5)$

- Since all monomial variables have the same degree, we have

$$x_1 \succ_{grlex} \cdots \succ_{grlex} x_n.$$

We introduce now the Reverse Lexicographic ordering.

Definition 16 (Reverse Lexicographic order). *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{N}^n$. We say that $\alpha \succ_{revlex} \beta$ if the rightmost non-zero entry of $\alpha - \beta$ is negative.*

Observe that with the reverse lexicographic order, we have

$$x_1 \succ_{revlex} \cdots \succ_{revlex} x_n$$

since, applying the definition, one has:

$$(1, 0, \ldots, 0) \succ_{revlex} \cdots \succ_{revlex} (0, \ldots, 0, 1).$$

Exercise 11

Compare monomials previously given as examples for the lexicographical ordering with the reverse lexicographical ordering.

It is important to note that lexicographical and reverse lexicographical orderings are rather different. While the lexicographical ordering looks at the leftmost power (or larger variable) to favor the one of *larger* degree, the reverse lexicographical ordering will look at the rightmost variable (the smaller one) and favor the one of *smaller* degree.

Exercise 12

Compare the monomials $x_1^2 x_2 x_3$ and $x_1 x_2 x_3^2$ with the *lex* and *revlex* orderings.

The mostly used ordering for computational purpose is the following Graded Reverse Lexicographical Order (grevlex order in short).

Definition 17 (Graded Reverse Lexicographical Order). *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{N}^n$. We say that $\alpha \succ_{grevlex} \beta$ if*

$$\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i \qquad or \left(\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \text{ and } \alpha \succ_{revlex} \beta \right).$$

For instance, we have:

- $(4, 7, 1) \succ_{grevlex} (4, 2, 3)$
- $(1, 5, 2) \succ_{grevlex} (4, 1, 3)$
- Observe that we have

$$x_1 \succ_{grevlex} \cdots \succ_{grevlex} x_n.$$

Exercise 13

Prove that the *grlex* and the *grevlex* orderings are monomial orderings.

Exercise 14

Sort the following monomials with respect to the graded reverse lexicographic ordering.

$$x_1^2x_2^3x_3^4,\ x_1x_2x_3,\ x_1^2x_2,\ x_2^2x_3,\ x_1x_3^2,\ x_2x_3^2,\ x_3^{100},\ x_2^2,\ x_1,\ x_2x_3,\ x_1x_2,\ x_1x_3$$

The *grlex* a nd *grevlex* both start by sorting with respect to degree. However, in case monomials have the same degree, the behaviour and the differences of the *grlex* and the *grevlex* orderings reflect the ones of the *lex* and *revlex* orderings. The *grevlex* looks at the largest variable and will privilege larger degree. In contrast, the *grevlex* order looks at the smallest variable and favors the smallest degree !

Exercise 15

Order the terms of the polynomial $f = 4x_1x_2^2x_3 + 4x_3^2 - 5x_1^3 + 7x_1^2x_3^3$ using the *lex*, the *grlex* and the *grevlex* orderings.

Once $\mathbb{K}[x_1, \ldots, x_n]$ is equipped with a monomial ordering, one can extend the definitions of leading coefficient and monomial that arise naturally in the univariate case to the multivariate setting.

Definition 18. *Let S be a finite subset of $\mathbb{N}^n$ and $f = \sum_{\alpha \in S} c_\alpha \underline{x}^\alpha$ with $c_\alpha \in \mathbb{K}$ and $\underline{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$. Consider a monomial order $\succ$. We define:*

1. *the* multidegree *of f*
$$\mathsf{multidegree}(f) = \max(\alpha \in S \mid c_\alpha \neq 0)$$
where the maximum is taken with respect to $\succ$.

2. *The leading coefficient of f is*
$$\mathsf{LC}_\succ(f) = c_{\mathsf{multidegree}(f)}.$$

3. *The leading monomial of f is*
$$\mathsf{LM}_\succ(f) = \underline{x}^{\mathsf{multidegree}(f)}.$$

4. *The leading term of f is*
$$\mathsf{LT}_\succ(f) = \mathsf{LC}_\succ(f)\mathsf{LM}_\succ(f).$$

One can easily illustrate these notions with the polynomials used in the above examples. Most of the time, the monomial ordering $\succ$ which we use will be clear from the context. In these cases, we will just omit to mention $\succ$ as an index for LC, LM and LT.

Lemma 19. *Let f and g be in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering. Then, the following holds:*

1. $\mathsf{multidegree}(fg) = \mathsf{multidegree}(f) + \mathsf{multidegree}(g)$.
2. *If $f + g \neq 0$, then* $\mathsf{multidegree}(f + g) \leqslant \max(\mathsf{multidegree}(f), \mathsf{multidegree}(g))$ *and the equality holds when* $\mathsf{multidegree}(f) \neq \mathsf{multidegree}(g)$.

Exercise 16

Prove the above lemma.

Exercise 17

What are the leading terms of with respect to both the graded reverse lexicographic and the lexicographic orderings of the following polynomials.

$$77\,x_1{x_2}^2x_3 - 10\,{x_1}^2x_2 + 31\,x_1{x_2}^2 - 51\,x_2{x_3}^2 + 68\,x_1x_3 + 91\,x_2$$
$$30\,{x_1}^2x_5 - 27\,x_1{x_2}^2 - 15\,x_1{x_4}^2 - 59\,{x_2}^3 + 16\,x_1x_4 - 28\,x_2$$
$$98\,{x_1}^2x_4x_5 - 64\,x_1x_2{x_5}^2 + 64\,x_1x_3{x_4}^2 - 90\,x_1x_3{x_5}^2 - 60\,x_2x_3{x_4}^2 - 34\,x_3{x_5}^3 + 25\,x_1{x_4}^2$$

4 Multivariate division algorithm

We have now sufficient ingredients to revisit the division algorithm in $\mathbb{K}[x_1, \ldots, x_n]$. On input f and $\boldsymbol{f} = (f_1, \ldots, f_p)$, we aim at writing:

$$f = q_1f_1 + \cdots + q_pf_p + r$$

with some constraints on the multidegree of r (which is expected to play the role of the remainder of the classical Euclidean division).

The basic idea is roughly the same as the one used in the Euclidean division. We will cancel the leading term of f by multiplying some f_i with an appropriate term. Of course, there are many ways to do that (because we divide by several polynomials and we are tackling the case $n \geqslant 2$).

Before stating the algorithm, let us investigate some examples. As done before, these are the ones used in the book entitled *Ideals, varieties and algorithms* authored by Cox, Little and O'Shea.

Example 20. Let us start by considering $f = x_1x_2^2 + 1$ that we divide by $f_1 = x_1x_2 + 1$ and $f_2 = x_2 + 1$ using the *lex* ordering with $x_1 \succ_{lex} x_2$.

Observe that we have

$$\mathsf{LT}(f) = x_1x_2^2, \qquad \mathsf{LT}(f_1) = x_1x_2, \qquad \mathsf{LT}(f_2) = x_2.$$

Hence the leading terms of both f_1 and f_2 divide the one of f. Let us use f_1 first (as it was listed first). One obtains that

$$f = x_2 f_1 + 0.f_2 - x_2 + 1$$

Repeating the process with $-x_2 + 1$ whose leading term is $-x_2$, one is lead to use f_2 because the leading term of f_1 does not divide x_2 while $\mathsf{LT}(f_2)$ does. One now obtains

$$f = x_2 f_1 + (-1).f_2 + 2$$

Now, $\mathsf{LT}(f_1)$ and $\mathsf{LT}(f_2)$ do not divide 2 and we deduce that the remainder is 2.

Observe that from the above computation, we deduce that 2 lies in $\langle f, f_1, f_2\rangle$. We deduce that $\langle f, f_1, f_2\rangle = \mathbb{K}[x_1, x_2]$ the algebraic set defined by $f = f_1 = f_2 = 0$ is empty. Hence, applying the division algorithm was here sufficient to solve the problem of deciding whether a polynomial system defines a non-empty algebraic set.

The above example illustrates how things can turn smoothly when dividing a multivariate polynomial by other ones. A less favourable example is as follows (again extracted from the book entitled *Ideals, varieties and algorithms* authored by Cox, Little and O'Shea.

Example 21. We keep on using the *lex* ordering and we take

$$f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$$

with

$$\begin{cases} f_1 &= x_1 x_2 - 1 \\ f_2 &= x_2^2 - 1. \end{cases}$$

The first two steps go as above as we do have $\mathsf{LT}(f_1) = x_1 x_2$ and $\mathsf{LT}(f_2) = x_2^2$ with $\mathsf{LT}(f) = x_1^2 x_2$. We actually do have

$$f = (x_1 + x_2) f_1 + 0.f_2 + g$$

with $g = x_1 + x_2^2 + x_2$. Observe that $\mathsf{LT}(g) = x_1$; then neither $\mathsf{LT}(f_1)$ nor $\mathsf{LT}(f_2)$ divide $\mathsf{LT}(g)$.

We may see g as a potential remainder for the division of f by $[f_1, f_2]$ BUT a phenomenon which we never encounter in the univariate case arises here (!)

Indeed, observe that $\mathsf{LT}(f_2)$ divides some monomials in the support of g ; more precisely $\mathsf{LT}(f_2)$ divides x_2^2. Hence, while $\mathsf{LT}(g) = x_1$ surely appears in what we expect to be the remainder of the division of f by $[f_1, f_2]$, one can still continue to reduce / divide $x_2^2 + x_2$ modulo $[f_1, f_2]$. We obtain this way

$$f = (x_1 + x_2) f_1 + f_2 + x_1 + x_2 + 1.$$

None of the terms of $x_1 + x_2 + 1$ are divisible by $\mathsf{LT}(f_1)$ and $\mathsf{LT}(f_2)$.

From the above example, one can now fully describe what we expect from a multivariate division algorithm and the algorithm itsself.

Definition 22. *Let $f, f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. One says that $r \in \mathbb{K}[x_1, \ldots, x_n]$ is a remainder of the division of f by $[f_1, \ldots, f_s]$*

with respect to $\succ$ *if there exist* $q_1, \ldots, q_s$ *such that*

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

and all terms of r *are not divisible by any term in* $\{\mathsf{LT}_\succ(f_1), \ldots, \mathsf{LT}_\succ(f_s)\}$.

We can now describe the Division algorithm. It takes as input:

- $f, f_1, \ldots, f_s$ in $\mathbb{K}[x_1, \ldots, x_n]$;
- a monomial ordering $\succ$ on $\mathbb{K}[x_1, \ldots, x_n]$.

It returns a remainder for the division of f by $[f_1, \ldots, f_s]$ w.r.t. $\succ$ as defined by Definition 22.

$Division(f, [f_1, \ldots, f_s], \succ)$

- $q_i = 0$ for $1 \leqslant i \leqslant s$ and $r = 0$.
- $p = f$;
- while $p \neq 0$ do
  - $i = 1$ and $division\_done = false$
  - while $i \leqslant s$ and $division\_done = false$ do
    - if $\mathsf{LT}_\succ(f_i)$ divides $\mathsf{LT}(p)$ then
      - $q_i = q_i + \frac{\mathsf{LT}_\succ(p)}{\mathsf{LT}_\succ(f_i)}$
      - $p = p - \frac{\mathsf{LT}_\succ(p)}{\mathsf{LT}_\succ(f_i)} f_i$
      - $division\_done = true$
    - else
      - $i = i + 1$
  - If $division\_done = false$ then
    - $r = r + \mathsf{LT}_\succ(p)$
    - $p = p - \mathsf{LT}_\succ(p)$
- return r.

Note that in the above algorithm one can also return $q_1, \ldots, q_s$ so that the algorithm returns all data to recover the information to retrieve

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Exercise 18

Implement the above algorithm in a computer algebra system (such as SageMath or Maple). Provide also a variant of this implementation that yields the list of polynomials $q_1, \ldots, q_s$.

Theorem 23. *Let $f, f_1, \ldots, f_s$ be in $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering on $\mathbb{K}[x_1, \ldots, x_n]$. There exists a remainder r for the division of f by $[f_1, \ldots, f_s]$ w.r.t. $\succ$.*

Moreover, on input $f, f_1, \ldots, f_s$ and $\succ$, the algorithm Division described above terminates and returns the remainder r of the division of f by $[f_1, \ldots, f_s]$ w.r.t. $\succ$.

Moreover, if $q_i f_i \neq 0$, then

$$\mathsf{multidegree}(f) \succ \mathsf{multidegree}(f_i q_i).$$

Proof. To prove the existence of r (and of $q_1, \ldots, q_s$), we actually prove that the algorithm *Division* is correct (hence the proof is constructive).

We start by proving that at each step of the algorithm we actually have

$$f = q_1 f_1 + \cdots + q_s f_s + p + r. \tag{1}$$

Remark that at the initialization of $q_1, \ldots, q_s$ and p, r the above relation is clear. Assume now that (1) holds when entering in the while loops. If a division occurs for some i in $\{1, \ldots, s\}$, $\mathsf{LT}(f_i)$ divides $\mathsf{LT}(p)$ and from the inequality:

$$q_i f_i + p = \left(q_i + \frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)}\right) f_i + p - \frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)} f_i.$$

one deduces that $q_i f_i + p$ remains unchanged. All other variables in the algorithm are also unchanged, so we deduce that (1) holds when a division occurs. If there is no division, then r and p are changed (in the "if" statement). But note that $p + r$ does not change since we have

$$p + r = (p - \mathsf{LT}(p)) + (r + \mathsf{LT}(p))$$

and again (1) still holds.

Moreover, the algorithm stops when $p = 0$. From (1), we deduce that we have in this case

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

Note also that we come to $p = 0$ when all terms of r are not divisible by any of the terms in $\{LT(f_1), \ldots, \mathsf{LT}(f_s)\}$.

Finallly, we need now to prove that the algorithm stops, hence that at some point, we will have $p = 0$. To prove this, observe first that each time we enter in the main while loop p is changed and either p becomes 0 or its multi-degree decreases.

More precisely, when a division occurs (i.e. $\mathsf{LT}(f_i)$ divides $\mathsf{LT}(p)$), p is updated to

$$p - \frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)} f_i$$

Lemma 19 establishes that

$$\mathsf{LT}\left(\frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)} f_i\right) = \frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)} \mathsf{LT}(f_i) = \mathsf{LT}(p).$$

We deduce that p and $\frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)} f_i$ have the same leading term and then the leading term of the update is less than $\mathsf{LT}(p)$.

When there is no division, p is updated to

$$p - \mathsf{LT}(p)$$

which also has a leading term less than $\mathsf{LT}(p)$. Hence, each time p is updated (and this happens each time we enter in the loop), the updated value for p has a leading term less than the leading term of the former one. Since $\succ$ is a monomial ordering, we deduce that at some point p must be 0. Indeed, if this was not the case, the algorithm would produce a infinite sequence of strictly decreasing leading terms. This cannot happen because $\succ$ is a well-ordering (Lemma 12).

Finally, it remains to prove that if $q_i f_i \neq 0$, then

$$\mathsf{multidegree}(f) \succ \mathsf{multidegree}(f_i q_i).$$

To establish this last assertion, observe that every term in q_i is of the form $\frac{\mathsf{LT}(p)}{\mathsf{LT}(f_i)}$ for some value of the variable p. When the algorithm starts, on has $p = f$ and we just established that the multidegree of p is decreasing at each step of the algorithm. Hence, we deduce that $\mathsf{LT}(p) \preccurlyeq \mathsf{LT}(f)$ through all steps of the algorithm. Using Definition 11, one deduces that $\mathsf{multidegree}(q_i f_i) \succcurlyeq \mathsf{multidegree}(f)$ when $q_i f_i \neq 0$. □

It is now interesting to compare the properties of the above multivariate division algorithm with the one we have in the univariate case. A first crucial property we enjoy in the univariate case is the fact that the remainder is unique. The example below (again extracted from the book entitled *Ideals, varieties and algorithms* authored by Cox, Little and O'Shea) that this is no more true in the multivariate setting.

Example 24. We take the *let* order and

$$f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$$

with

$$\begin{cases} f_1 &= x_2^2 - 1 \\ f_2 &= x_1 x_2 - 1 \end{cases}$$

This is almost the same as in Example 21, except that we inverted f_1 with f_2. Performing the Division algorithm with this input leads to

$$f = (x_1 + 1) f_1 + x_1 f_2 + (2x_1 + 1).$$

When replacing f_1 by f_2 and vice-versa in Example 21 we obtained $x_1 + x_2 + 1$ as a remainder.

This shows that the remainder actually depends on the order we use to consider the divisors. Actually, when we fix an ordering on those divisors, the algorithm Division is deterministic and the quotients $q_1, \ldots, q_s$ and r are uniquely determined. But the fact that they depend on the order on $f_1, \ldots, f_s$ show that this algorithm is still not very canonical.

Also, we can also illustrate that the algorithm Division is not sufficient to solve the Ideal membership problem with the following example.

Example 25. Take

$$f_1 = x_1x_2 - 1 \qquad \text{and} \qquad f_2 = x_2^2 - 1$$

with $f = x_1x_2^2 - x_1$ and the *let* order. Running the Division algorithm one obtains

$$f = x_2f_1 + 0f_2 + (-x_1 + x_2).$$

But now, if we invert the order on (f_1, f_2) and perform the division considering first f_2 and next f_1, one obtains

$$f = x_1f_2 + 0f_1 + 0.$$

At the first round, we obtained a non-zero remainder while the result of the second round establishes that $f \in \langle f_1, f_2 \rangle$.

The conclusion from these last examples is that the behaviour of the Division algorithm depends on the way we sort the divisors $f_1, \ldots, f_s$.

Still, the Division algorithm is nice and important. It will reveal its full potential and power when the divisors $f_1, \ldots, f_s$ enjoy extra properties and when it is combined with the notion of Gröbner bases.

Exercise 19

Compute the division of the polynomial f with respect to the list of polynomials f_1, f_2, f_3 below for both the lexicographic and the graded reverse lexicographic ordering.

$$\begin{aligned} f &= 8\,{x_1}^2x_3 - 2\,x_1{x_3}^2 - x_1x_2 + 10 \\ f_1 &= {x_1}^2 + 3\,{x_3}^2 - 2\,x_1 \\ f_2 &= -x_1x_3 + 7\,x_2x_3 + 2\,x_3 \\ f_3 &= 3\,x_1x_2x_3 - 8\,x_2x_3 - 4\,{x_3}^2 \end{aligned}$$

and

$$\begin{aligned} f &= 4\,x_1{x_2}^2 - x_1x_2x_3 + x_2{x_3}^2 - 4\,x_2 \\ f_1 &= -{x_2}^3 + 9\,x_2x_3 + 5\,x_1 \\ f_2 &= 9\,{x_1}^2x_3 - 4\,{x_3}^3 - 3\,{x_2}^2 \\ f_3 &= {x_2}^3 - {x_2}^2 - 2\,x_2x_3 \end{aligned}$$

Exercise 20

Let $f_1, f_2, \ldots, f_s$ be polynomials in the ring $\mathbb{K}[x_1, \ldots, x_n]$ and $\succ$ be a monomial ordering over this polynomial ring. Assume that $\text{Division}(f_1, [f_2, \ldots, f_n], \succ)$ is a constant in $\mathbb{K}$. Prove that the ideal $\langle f_1, f_2, \ldots, f_s \rangle$ contains 1.
What can you deduce about the algebraic set defined by $f_1 = f_2 = \cdots = f_s = 0$?

Exercise 21

Perform a complexity analysis of the DIVISION algorithm.