

## Rewriting Polynomials

In this lecture we present mainly an algebraic (or symbolic view) on solving polynomial systems. We define the ideal membership problem and show how the division algorithm solves it, provided the ideal is given by a Groebner (also spelled as Gröbner) basis. We end by stating the Hilbert basis theorem. Introductions are in [1], [3], and in [5].

### 1 Roots and Eigenvalues

Let  $p(x) = x^4 - 5x^3 + 7x^2 - x + 3 \in \mathbb{C}[x]$ , a polynomial in one variable  $x$ . Consider the equation  $p(x) = 0$ . By the fundamental theorem of algebra, we know that  $p(x) = 0$  has 4 complex solutions, or more geometrically, we may write  $p(x) = (x - z_1)(x - z_2)(x - z_3)(x - z_4)$  and identify  $p$  with its roots  $z_1, z_2, z_3$ , and  $z_4$ .

Algebraically, the equation  $p(x) = 0$  implies  $x^4 = 5x^3 - 7x^2 + x - 3$ , or in words: we may write  $x^4$  as a linear combination of the monomials  $1, x, x^2$ , and  $x^3$ . Furthermore, we may then also rewrite  $x^5, x^6$ , etc. as cubic polynomials. The relation  $p(x) = 0$  allows us to rewrite (or reduce) every polynomial as a cubic. This rewriting (or reduction) maps  $\mathbb{C}[x]$  onto the quotient ring

$$\mathbb{C}[x]/\langle p \rangle = \{ a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in \mathbb{C} \}, \quad (1)$$

which we view as a 4-dimensional vector space with basis  $\{1, x, x^2, x^3\}$ . If we look at what happens when we multiply the basis elements by  $x$ , we arrive at the following matrix equation:

$$x \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -3 & 1 & -7 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ x \\ x^2 \\ x^3 \end{bmatrix}. \quad (2)$$

The matrix in (2) is the so-called companion matrix  $C_p$  of  $p$ . The format in which we derived (2) brings us back to the geometry. Observe that we may abbreviate (2) as  $\lambda X = C_p X$ , where  $X$  is the vector of the monomial basis, and where the  $\lambda$  equals  $x$ . As  $\lambda X = C_p X$  is an eigenvalue problem, the 4 eigenvalues of  $C_p$  are the 4 roots of  $p$ .

Techniques to solve eigenvalue problems are well developed in numerical linear algebra and widely used in scientific computing. The term rewriting techniques we introduce in this lecture serve as a bridge between symbolic and numeric algorithms.

We can generalize the notion of a quotient ring for systems  $f = (f_1, f_2, \dots, f_N)$  of polynomial equations in  $\mathbb{C}[\mathbf{x}]$ . The basic algebraic object associated with a system  $f$  is the ideal generated by the polynomials in  $f$ , defined as

$$\langle f \rangle = \{ a_1 f_1 + a_2 f_2 + \dots + a_N f_N \mid a_i \in \mathbb{C}[\mathbf{x}] \}. \quad (3)$$

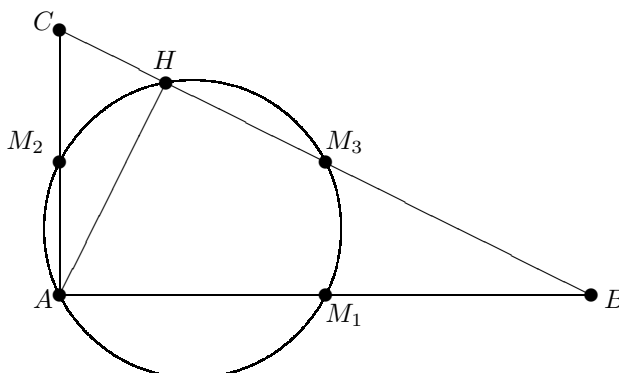
An important problem is the so-called ideal membership problem, i.e.: for a given ideal  $I$  and polynomial  $p$ , determine whether  $p \in I$ . We can solve this problem if we have a way to rewrite (or reduce) every polynomial modulo the ideal so that the outcome is unique.

If the system  $f(\mathbf{x}) = \mathbf{0}$  has finitely many solutions, then the quotient ring  $\mathbb{C}[\mathbf{x}]/\langle f \rangle$  can be viewed as a finite dimensional vector space, where the dimension equals the number of solutions. The eigenvalues of the multiplication maps give the coordinates of the solutions. However, the construction of the eigenvalue problems is more involved and requires in general a so-called Groebner basis for the ideal.

For systems with infinitely many solutions, we may be mainly be interested in deciding whether a given polynomial vanishes on the solution set, or algebraically, whether the polynomial belongs to the ideal, as is the case in the next application.

## 2 Automatic Geometric Theorem Proving

The following example (taken from [3]) shows the relevance of polynomial equations to the fields of artificial intelligence and geometric modeling. Consider the following picture:



**Theorem 2.1 (The Circle Theorem of Apollonius)** Consider a right triangle spanned by  $A$ ,  $B$ , and  $C$ , with the right angle at  $A$ . The midpoints of the three sides of the triangle, and the foot of the altitude drawn from  $A$  to the edge spanned by  $B$  and  $C$  all lie on one circle.

The coordinates of the triangle are as follows: we place  $A$  at  $(0, 0)$ ,  $B$  at  $(u_1, 0)$ , and  $C$  at  $(0, u_2)$ , where  $u_1$  and  $u_2$  are arbitrary. The three midpoints at the sides  $M_1$ ,  $M_2$ , and  $M_3$  have their coordinates respectively at  $(x_1, 0)$ ,  $(0, x_2)$ , and  $(x_3, x_4)$ . Expressing that  $M_1$  is the midpoint of the edge spanned by  $A$  and  $B$  imposes the condition  $h_1 = 2x_1 - u_1 = 0$ . The second condition  $h_2 = 2x_2 - u_2 = 0$  is imposed by stating that  $M_2$  is the midpoint of the edge spanned by  $A$  and  $C$ . For  $M_3$  we have two conditions:  $h_3 = 2x_3 - u_1 = 0$  and  $h_4 = 2x_4 - u_2 = 0$ .

For the foot of the altitude  $H$  we choose coordinates  $(x_5, x_6)$ . Then we formulate two hypotheses. First:  $h_5 = x_5u_1 - x_6u_2 = 0$  expresses that the line segment  $AH$  is perpendicular to the edge  $BC$ . Second:  $h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0$  means that the points  $B$ ,  $H$ , and  $C$  are collinear. To formulate these conditions we use the slopes defined by the segments.

Finally, we consider the statement that the three midpoints and  $H$  lie on a circle by saying that the circle through the three midpoints must also contain  $H$ . Let  $(x_7, x_8)$  be the coordinates of the center  $O$  of the circle. We have two more conditions:  $M_1O = M_2O$  and  $M_1O = M_3O$ , given respectively by  $h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0$  and  $h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$ .

The eight hypotheses form the following system

$$f(\mathbf{u}, \mathbf{x}) = \begin{cases} 2x_1 - u_1 = 0 \\ 2x_2 - u_2 = 0 \\ 2x_3 - u_1 = 0 \\ 2x_4 - u_2 = 0 \\ x_5u_1 - x_6u_2 = 0 \\ x_5u_2 + x_6u_1 - u_1u_2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \\ (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0. \end{cases} \quad (4)$$

With respect to these eight hypotheses, the conclusion must then be that  $HO = M_1O$ , expressed by  $g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0$ .

The theorem is true if  $g$  belongs to the ideal spanned by the polynomials which vanish over the zero set of the hypotheses. Notice however, that typically we are interested only in the real solutions and also degenerate configurations must be dealt with separately. These two problems complicate the automatic geometric theorem proving.

### 3 The Division Algorithm

We look for an algorithm to solve the ideal membership problem for polynomials. For a given polynomial  $g \in \mathbb{C}[\mathbf{x}]$  and an ideal generated by  $f = (f_1, f_2, \dots, f_N)$ , the goal is to express  $g$  as

$$g = q_1 f_1 + q_2 f_2 + \dots + q_N f_N + r, \quad q_i \in \mathbb{C}[\mathbf{x}], i = 1, 2, \dots, N, \quad r \in \mathbb{C}[\mathbf{x}]. \quad (5)$$

Obviously, if  $r = 0$ , then  $g \in \langle f \rangle$ , but the opposite is not necessarily true.

When we rewrite polynomials in several variables, we must define an order on the monomials. We start by imposing an order on the variables, ordered in decreasing order, we write  $x_1 > x_2 > \dots > x_n$ . Then there are several ways to order monomials:

- **lexicographic:** We sort as in a dictionary.  $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$  if the leftmost nonzero entry in  $\mathbf{a} - \mathbf{b}$  is positive. For example:  $x_1^2 x_2 >_{\text{lex}} x_1 x_2^3$ .
- **graded lexicographic:** We first sort the monomials according to their total degree and sort monomials with the same degree lexicographically. It is also called the total degree order, denoted by `tdeg` in Maple. We have  $\mathbf{x}^{\mathbf{a}} >_{\text{tdeg}} \mathbf{x}^{\mathbf{b}}$  if  $\deg(\mathbf{x}^{\mathbf{a}}) > \deg(\mathbf{x}^{\mathbf{b}})$  or if  $\deg(\mathbf{x}^{\mathbf{a}}) = \deg(\mathbf{x}^{\mathbf{b}})$  and  $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$ . For example:  $x_1^2 x_2 >_{\text{tdeg}} x_1 x_2^2$ .
- **weighted lexicographic:** For a nonzero weight vector  $\omega \in \mathbb{Z}^n$ , denote  $\langle \mathbf{a}, \omega \rangle = a_1 \omega_1 + a_2 \omega_2 + \dots + a_n \omega_n$ . Then:  $\mathbf{x}^{\mathbf{a}} >_{\omega} \mathbf{x}^{\mathbf{b}}$  if  $\langle \mathbf{a}, \omega \rangle > \langle \mathbf{b}, \omega \rangle$  or  $\langle \mathbf{a}, \omega \rangle = \langle \mathbf{b}, \omega \rangle$  and  $\mathbf{x}^{\mathbf{a}} >_{\text{lex}} \mathbf{x}^{\mathbf{b}}$ .

Once we fixed a monomial ordering, the notion of leading term of a polynomial makes sense. Denote the leading term of a polynomial  $g$  by  $\text{LT}(g)$ . The division algorithm to rewrite  $g$  modulo an ideal generated by  $(f_1, f_2, \dots, f_N)$  repeatedly takes the first polynomial  $f_i$  for which  $\text{LT}(f_i)$  divides  $\text{LT}(g)$  and then subtracts from  $g$  a monomial multiple of  $f_i$  which eliminates  $\text{LT}(g)$ . The algorithm terminates when nothing remains of  $g$  (in which case the remainder  $r = 0$ ) or when there is no  $\text{LT}(f_i)$  which divides  $\text{LT}(g)$ .

**Algorithm 3.1** The division algorithm to compute the remainder.

Input:  $f = (f_1, f_2, \dots, f_N)$  and  $p \in \mathbb{C}[\mathbf{x}]$ .

Output:  $r$ , the remainder of  $p$  modulo  $f$ .

$r := p$ ;

repeat

$k := 0$ ;

  for  $i$  from 1 to  $N$  do

    if  $\text{LT}(f_i)$  divides  $\text{LT}(r)$

      then  $k := i$ ; exit for loop;

    end if;

  end for;

  if  $k \neq 0$  then  $r := r - \frac{\text{LT}(r)}{\text{LT}(f_k)} f_k$ ; end if;

until  $r = 0$  or  $k = 0$ .

We say that  $p$  reduces to  $r$  modulo the polynomials in  $f$  and write  $p \rightarrow_f r$ . Unlike for polynomials in one variable, in several variables, the outcome of the division algorithm may depend on the order of the polynomials in  $f$ . Consider  $f_1 = xy + 1$ ,  $f_2 = y^2 - 1$ ,  $g = xy^2 - x$  and use  $>_{\text{lex}}$ .

$$\langle f_1, f_2 \rangle : \text{LT}(g) = y\text{LT}(f_1) \rightarrow g := g - yf_1 = xy^2 - x - y(xy + 1) = -x - y. \quad (6)$$

But when we swap the order of the polynomials in  $\langle f \rangle$ :

$$\langle f_2, f_1 \rangle : \text{LT}(g) = x\text{LT}(f_2) \rightarrow g := g - xf_2 = xy^2 - x - x(y^2 - 1) = 0, \text{ so } g \in \langle f \rangle. \quad (7)$$

In order to have a unique outcome of the division algorithm, we need a Groebner basis for the ideal  $I$ . Denote by  $\langle \text{LT}(I) \rangle$  the ideal generated by the leading terms of  $I$ . Then  $G = \{g_1, g_2, \dots, g_s\}$  is a Groebner basis for  $I$  if  $\langle \text{LT}(g_1), \text{LT}(g_2), \dots, \text{LT}(g_s) \rangle = \langle \text{LT}(I) \rangle$ . At this stage we do not (yet) explain algorithms to calculate a Groebner basis, for now, type `?Groebner` in a Maple session and let Maple compute many examples.

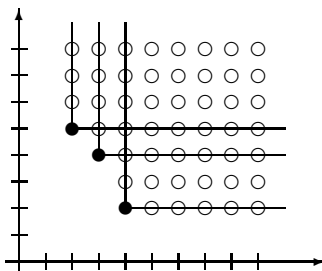
In addition to solving the ideal membership problem, two properties of Groebner bases are very much relevant to polynomial system solving:

1. For a lexicographic term order, the resulting Groebner basis has a triangular structure. In this sense Groebner bases not only generalize the Euclidean algorithm for univariate polynomials and resultants for eliminating one variable, but also generalize Gaussian elimination for solving linear systems.
2. For systems with a finite number of solutions, the leading monomials of the Groebner basis define a staircase (see the picture below). The number of monomials under this staircase equals the number of solutions. With these monomials one can define multiplication maps and compute the coordinates of the solutions via eigenvalue problems.

## 4 Monomial Ideals and Dickson's Lemma

In addition to their importance to solving polynomial systems, Groebner bases can be used to show that every ideal has a finite basis. First we focus on the particular case of monomial ideals. A monomial ideal is generated by monomials.

For two variables, we can visualize a monomial ideal as those lattice points above a “staircase” defined by the monomials in the basis. For example, for  $\langle x^2y^5, x^3y^4, x^4y^2 \rangle$ , the staircase looks like picture below. The filled black disks correspond to the three generators in the monomial ideal. The generated monomials are represented by the empty disks. All disks inside one rectangular region of the staircase correspond to multiples of the same generator monomial.



**Lemma 4.1 (Dickson's Lemma)** *Every monomial ideal is finitely generated.*

*Proof.* We need to prove that for every monomial ideal  $I$ , there exists a finite subset  $S$  so that for all  $\mathbf{x}^{\mathbf{a}} \in I$  there is a monomial  $\mathbf{x}^{\mathbf{b}} \in S$  that divides  $\mathbf{x}^{\mathbf{a}}$ . We proceed by induction on  $n$ , the number of variables.

For  $n = 1$ ,  $d = \min_{x^a \in I} a$  is unique, so  $S = \{x^d\}$ .

For  $n > 1$ , take  $\mathbf{x}^{\mathbf{b}} \in I$ . Every monomial in  $I$  not divisible by  $\mathbf{x}^{\mathbf{b}}$  belongs to one of the following sets:

$$R_{i,j} = \{ \mathbf{x}^{\mathbf{a}} \in I \mid a_i = j \}, \quad \text{for } i = 1, 2, \dots, n \text{ and } j = 0, 1, \dots, b_i - 1.$$

Denote  $\widehat{R}_{i,j} = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in R_{i,j} \}$  as the set of monomials in  $R_{i,j}$  with the  $i$ th coordinate removed. By the induction hypothesis, there is a finite set  $\widehat{S}_{i,j}$  that generates  $I_i = \{ \mathbf{x}^{\mathbf{a}}|_{x_i=1} \mid \mathbf{x}^{\mathbf{a}} \in I \}$ . Define  $S_{i,j} = \{ x_i^j \mathbf{x}^{\mathbf{a}} \mid \mathbf{x}^{\mathbf{a}} \in \widehat{S}_{i,j} \}$  and let

$$S = \{ \mathbf{x}^{\mathbf{b}} \} \cup \left( \bigcup_{i=1}^n \bigcup_{j=0}^{b_i-1} S_{i,j} \right).$$

$S$  generates  $\mathbf{x}^{\mathbf{b}}$  and every  $\mathbf{x}^{\mathbf{a}} \in I$  not divisible by  $\mathbf{x}^{\mathbf{b}}$ . Thus  $S$  generates  $I$ . □

**Theorem 4.1 (Hilbert’s basis theorem)** *Every ideal has a finite generating set.*

This theorem follows when we prove that every ideal has a Groebner basis with respect to any monomial order and that every Groebner basis generates its ideal.

Complete proofs can be found in [3]. The use of ideals marks the era of “modern algebraic geometry” see [4]. The resultants we encountered in previous lectures belong to so-called classical algebraic geometry. Bruno Buchberger [2] developed in his 1965 PhD thesis an algorithm to compute bases for polynomial ideals. He named these bases Gröbner bases in honor of his thesis advisor Wolfgang Gröbner.

## 5 Exercises

1. For the polynomial  $p(x) = x^4 - 5x^3 + 7x^2 - x + 3$ , use MATLAB (Octave will do as well) or Maple to define the companion matrix and to compute its eigenvalues. What are the eigenvectors?
2. Consider the polynomial  $p(x) = (x - 1)^3(x - 2)$  and describe the eigenvalues and eigenvectors of the companion matrix, using MATLAB or Maple. Can you recognize the multiplicities of the two roots?
3. Write a Maple procedure to implement the division algorithm. Extend your implementation so that in addition to the remainder  $r$  the algorithm also returns the “quotients”  $q_i$  in the combination  $f = q_1g_1 + q_2g_2 + \dots + q_Ng_N + r$ , for any basis  $g$  and input polynomial  $f$ . You may also use another computer algebra system.
4. Consider the monomial ideal  $I = \langle x^3y, x^2y^2, xy^6 \rangle$ . Draw the exponent vectors of the monomials in the plane and visualize the staircase and all elements generated by  $I$ .
5. How can you see from the staircase that the monomial ideal has only finitely many solutions? Give examples and justify your observation.
6. For some finite support set  $A$ , let  $I = \langle \mathbf{x}^{\mathbf{a}} \mid \mathbf{a} \in A \rangle$  be the monomial ideal defined by  $A$ . Show that  $\mathbf{x}^{\mathbf{b}} \in I$  if and only if  $\mathbf{x}^{\mathbf{b}}$  is divisible by some monomial  $\mathbf{x}^{\mathbf{a}}$  for some  $\mathbf{a} \in A$ .
7. Let  $f = (\mathbf{x}^{\mathbf{a}_1}, \mathbf{x}^{\mathbf{a}_2}, \dots, \mathbf{x}^{\mathbf{a}_N})$  define a monomial ideal. Show that  $p \in \langle f \rangle \Leftrightarrow p \rightarrow_f 0$ .
8. Use Maple or Sage (in particular: Singular) to compute a Groebner basis of the ideal generated by the polynomial in the system  $f(\mathbf{u}, \mathbf{x})$  in (4), using a lexicographic order on the monomials. Does the form of the Groebner basis allow you to reduce the conclusion  $g$  to zero?

## References

- [1] W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*, volume 3 of *Graduate Studies in Mathematics*. AMS, 1994.
- [2] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional System Theory*, chapter 6, pages 184–232. D. Reidel Publishing Company, Dordrecht Boston Lancaster, 1985.
- [3] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer–Verlag, second edition, 1997.
- [4] W. Gröbner. *Moderne Algebraische Geometrie. Die Idealthoretischen Grundlagen*. Springer-Verlag, 1949.
- [5] B. Mishra. *Algorithmic Algebra*. Springer–Verlag, 1993.