Introduction to Symbolic Computation for Engineers

Solving systems of algebraic equations symbollically

Resultants

Sonia Rueda & Juana Sendra

Universidad Politécnica de Madrid

We approach the problem of solving symbolically systems of algebraic equations.

The theory behind the methods that will be exposed is purely algebraic, relaying essentially in Commutative Algebra and in particular in the theory of ideals.

The goal of this presentation is to explain how to use the methods developed with the mentioned theory through Maple.

The methods presented are valid over polynomial rings over any field. We restrict our presentation to the field of complex numbers.

Statement of the problem:

- Given a finite set of polynomials

$$p_1(x_1, \dots, x_r), \dots, p_n(x_1, \dots, x_r) \in \mathbb{C}[x_1, \dots, x_r].$$

- Decide if the system of algebraic equations

$$\left.\begin{array}{c} p_1(x_1, \dots, x_r) = 0 \\ \vdots \\ p_n(x_1, \dots, x_r) = 0 \end{array}\right\}$$

  has a solution in $\mathbb{C}$

- In the affirmative case compute the solutions.

In the context of Galois Theory:

Abel's Theorem. For $n \geq 5$ the general algebraic equation of degree n

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

is not solvable in radicals.

Thus a purely symbolic procedure cannot be designed to solve the problem algorithmically.

The main idea is:

To reduce the problem symbolically to the numeric computation of roots of polynomials in one variable.

Algebraic resultant of two polynomials

Let $\mathbb{D}$ be a unique factorization domain and $p_1(x), p_2(x) \in \mathbb{D}[x]$ two nonzero polynomials with coefficients in $\mathbb{D}$.

Problem: Find necessary and sufficient conditions for $p_1(x)$ and $p_2(x)$ to have a common factor.

The first approximation is the next result.

The next statements are equivalent:

1. $p_1(x)$ and $p_2(x)$ to have a common nonconstant factor.
2. There exist nonzero polynomials $q_1(x), q_2(x) \in \mathbb{D}[x]$ with $\deg(q_1(x)) < \deg(p_1(x))$ and $\deg(q_2(x)) < \deg(p_2(x))$ such that

$$q_2(x)p_1(x) + q_1(x)p_2(x) = 0.$$

Let us suppose that the degree of $p_1(x)$ is n and the degree of $p_2(x)$ is m, that is

$$p_1(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_n \neq 0,$$
$$p_2(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0, \quad b_m \neq 0.$$

The Sylvester matrix of p_1 and p_2 with respect to x is defined as:

$$\mathrm{Syl}(p_1, p_2, x) = \left[\begin{array}{cccccccc} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & a_n & a_{n-1} & \cdots & a_0 & \\ b_m & b_{m-1} & \cdots & b_0 & & & & \\ & b_m & b_{m-1} & \cdots & b_0 & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & b_m & b_{m-1} & \cdots & b_0 & \end{array}\right] \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \end{array}$$

Example in Maple with $n = 3$ and $m = 2$. See Maple session resultants.mw

The next statement are equivalent:

1. $p_1(x)$ and $p_2(x)$ have a common nonconstant factor.
2. There exist nonzero polynomials $q_1(x), q_2(x) \in \mathbb{D}[x]$ with $\deg(q_1(x)) < \deg(p_1(x))$ and $\deg(q_2(x)) < \deg(p_2(x))$ such that

$$q_2(x)p_1(x) + q_1(x)p_2(x) = 0.$$

3. $\det(\mathrm{Syl}(p_1, p_2)) = 0$.

We define the Sylvester resultant of p_1 and p_2 with respect to x as

$$\mathrm{Res}_x(p_1, p_2) = \det(\mathrm{Syl}(p_1, p_2, x)).$$

Remarks. If p_1 and/or p_2 is a nonzero constant C_1 or C_2 then

1. $\mathrm{Res}_x(C_1, p_2(x)) = \mathrm{Res}_x(p_2(x), C_1) = C_1^{\deg(p_2)}$,
2. $\mathrm{Res}(C1, C2) = 1$.
3. $\mathrm{Res}(p_1, p_2) \in \mathbb{D}$
4. $\mathrm{Res}(p_1, p_2) = (-1)^{\deg(p_1)\deg(p_2)}\mathrm{Res}(p_2, p_1)$
5. The resultant can be expressed as the determinant of other matrices as the matrices of Bezout, Dixon $\ldots$.

Theorem. $p_1(x)$ and $p_2(x)$ have a common nonconstant factor if and only if $\mathrm{Res}_x(p_1, p_2) = 0$.

We focus now in polynomials in $\mathbb{C}[x, y]$, that is $\mathbb{D}[y]$ with $\mathbb{D} = \mathbb{C}[x]$.

Theorem. Let $p_1(x, y), p_2(x, y) \in \mathbb{D}[y]$ and

$$R(x) = \mathrm{Res}_y(p_1, p_2) \in \mathbb{D}.$$

Let us suppose that

$$p_1(x, y) = \sum_{i=0}^{m} a_i(x) y^i \text{ and } p_2(x, y) = \sum_{i=0}^{n} b_i(x) y^i.$$

The following statements hold:

1. If $(a, b) \in \mathbb{C}^2$ is a common zero of p_1 and $p_2 \Longrightarrow R(a) = 0$.
2. If $a \in \mathbb{C}$ verifies $R(a) = 0$ and $a_m(a) \neq 0$ or $b_n(a) \neq 0$ then there exists $b \in \mathbb{C}$ such that (a, b) is solution of $\{p_1(x, y) = 0, p_2(x, y) = 0\}$.

From the previous theorem an algorithm is derived to solve systems of algebraic equations, of two polynomials in two variables.

The base ground of this method is Linear Algebra.

Algorithm.

- Given two polynomials $p_1(x,y), p_2(x,y) \in \mathbb{C}[x,y]$
- Decide if the system of algebraic equations

$$\left.\begin{array}{l} p_1(x,y)=0 \\ p_2(x,y)=0 \end{array}\right\}$$

has a solution over $\mathbb{C}$ and in the affirmative case determine all its solutions.

1. Perform a linear change of coordinates so that at least one of the polynomials p_1, p_2 has constant leading coefficient as a polynomial in the variable y.
2. $R(x) = \mathrm{Res}_y(p_1(x, y), p_2(x, y))$
3. If $R(x)$ is zero, then $p_1(x, y)$ and $p_2(x, y)$ have an infinite number of solutions in common, namely they are the zeros of the polynomial $\gcd(p_1, p_2)$ (one has to perform the inverse change of coordinates of the mentioned change in (1)).
4. If $R(x)$ is a nonzero constant then the system has no solution.
5. If $R(x)$ is a nonconstant polynomial the system has a finite number of solutions that can be computed as follows:
   - Given a root a of $R(x)$ compute the polynomial
   $$M_a(y) = \gcd(p_1(a, y), p_2(a, y)).$$
   - The set of solutions is $\{(a, b) \,/\, R(a) = 0,\ M_a(b) = 0\}$

With Maple. The next Maple commands will be needed:

$$\boxed{\text{resultant}(p_1, p_2, y)}$$

to compute $\mathrm{Res}_y(p_1(x,y), p_2(x,y))$ and

$$\boxed{\text{gcd}(subs(x=a, p_1), subs(x=a, p_2))}$$

to compute $\gcd(p_1(a,y), p_2(a,y))$

Examples with Maple. See Maple session resultants.mw

Application to Plane Curves

The resultant plays an important role in the symbolic theory and manipulation of algebraic curves.

We show next how to obtain the implicit equation of a curve $\mathcal{C}$ given its parametrically by rational functions.

Theorem. Let $\mathcal{C}$ be the curve generated by $\mathcal{P}(t) = \left(\frac{p_1(t)}{q_1(t)}, \frac{p_2(t)}{q_2(t)}\right) \in \mathbb{C}(t)^2$ and defined implicitly by a polynomial $f(x, y)$. Let

$$R(x, y) = \mathrm{Res}_t(q_1(t)x - p_1(t), q_2(t)y - p_2(t)).$$

Then it holds

$$f(x, y) = \frac{R(x, y)}{\gcd(R(x, y), \frac{\partial R(x,y)}{\partial x})}.$$

Example with Maple. See Maple session resultants.mw