Introduction to Symbolic Computation for Engineers

Solving systems of algebraic equations symbollically

Gröebner Basis

Sonia Rueda & Juana Sendra

Universidad Politécnica de Madrid

The symbolic resolution of systems of algebraic equations is a grate success of Symbolic Computation.

The symbolic resolution of systems of algebraic equations is based on the theory of Gröbner Basis.

The concept of Gröbner Basis and the algorithm for its computation was introduced by B. Buchberger in his PhD Thesis (1965).

> *Buchberger B.,* Ein Algoritmus zum Baseselemente de Restklassenringen nach einen nulldimensionen Polynomideal*, Ph. D. Thesis Math. Inst., Univ. of Innsbruk, Austria (1965) y Aequationes Math. n. 4, 3, pp 374-383 (1970)*

Gröbner basis have numerous applications in Mathematics, some examples of areas of application are: Logics, Automated Theorem Proving, Algebraic Geometry, Commutative Algebra, Elimination Theory.

We focus on their application to problem of solving algebraic equations.

We can consider Gröbner basis as a generalization of gaussian elimination to the case of nonlinear algebraic equations.

Let $p_1, \ldots, p_n$ be polynomials in $\mathbb{C}[x_1, \ldots, x_r]$. Given a system of algebraic equations

$$\left.\begin{array}{c} p_1(x_1, \ldots, x_r) = 0 \\ \vdots \\ p_n(x_1, \ldots, x_r) = 0 \end{array}\right\} \text{ with } p_i \text{ not necessarily linear.}$$

the essential idea is to obtain an equivalent triangular system of equations,

that is a triangular system of equations with the same set of solutions. In this sense the notion of ideal generated by a set of polynomials is important.

The ideal generated by the polynomials $p_1, \ldots, p_n$ in the ring $R = \mathbb{C}[x_1, \ldots, x_r]$ is the following subset of R

$$(p_1, \ldots, p_n) = \{\sum_{i=1}^{n} r_i p_i \text{ where } a_1, \ldots, a_n \in R\}.$$

The set $\{p_1, \ldots, p_n\}$ is called a basis of the ideal.

Given polynomials $q_1, \ldots, q_m \in R$ if $(q_1, \ldots, q_m) = (p_1, \ldots, p_n)$ then the systems

$$\left.\begin{array}{c} p_1(x_1, \ldots, x_r) = 0 \\ \vdots \\ p_n(x_1, \ldots, x_r) = 0 \end{array}\right\} \text{ and } \left.\begin{array}{c} q_1(x_1, \ldots, x_r) = 0 \\ \vdots \\ q_m(x_1, \ldots, x_r) = 0 \end{array}\right\}$$

have the same solution set.

Thus the idea is to find a basis $\{G_1, \ldots, G_n\}$ of the ideal $(p_1, \ldots, p_n)$ with a triangular structure.

The intrinsic difficulty of the problem is that $R = \mathbb{C}[x_1, \ldots, x_r]$ is not an euclidean domain and thus there is no division operation defined in R.

To overcome this difficulty an admissible ordering will be defined in the set of monomials in the variables $x_1, \ldots, x_r$ and by successive polynomial reductions a basis $\{G_1, \ldots, G_n\}$ of the ideal $(p_1, \ldots, p_n)$ is obtained with the desired properties. The desired basis is the Gröbner basis.

Given the system

$$\begin{cases} p_1(x,y,z) = y^2 - x^2 - 1 = 0 \\ p_2(x,y,z) = x^2 + z^2 - 4 = 0 \\ p_3(x,y,z) = x^3 - 2x - 2 + z^2 + xz^2y^2 - x^3z^2 - xz`^2 = 0 \end{cases}$$

using Gröbner basis the following equivalent triangular system is obtained

$$\begin{cases} G_1(x,y,z) = x^2 + z^2 - 4 = 0 \\ G_2(x,y,z) = y^2 - x^2 - 1 = 0 \\ G_3(x,y,z) = (x-1)(x^2-2) = 0. \end{cases}$$

We obtain 12 solutions of the system.

$$(1,\sqrt{2},\sqrt{3}), (1,\sqrt{2},-\sqrt{3}, (1,-\sqrt{2},\sqrt{3}, (1,-\sqrt{2},-\sqrt{3})$$

$$(\sqrt{2},\sqrt{2},\sqrt{3}), (\sqrt{2},\sqrt{2},-\sqrt{3}), (\sqrt{2},-\sqrt{2},\sqrt{3}), (\sqrt{2},-\sqrt{2},-\sqrt{3})$$

$$(-\sqrt{2},\sqrt{2},\sqrt{3}), (-\sqrt{2},\sqrt{2},-\sqrt{3}), (-\sqrt{2},-\sqrt{2},\sqrt{3}), (-\sqrt{2},-\sqrt{2},-\sqrt{3})$$

Monomial orderings

We introduce the most commonly used monomial ordering in the computation of Gröbner basis.

Let $\mathcal{M}$ be the set of all monomials in the variables $x_1, \ldots, x_r$

$$\mathcal{M} = \{x_1^{\alpha_1} \cdots x_r^{\alpha_r} \mid \alpha_1, \ldots, \alpha_r \in \mathbb{N}\}$$

- The pure lexicographical ordering $<_{\text{plex}}$ with $x_1 > x_2 > \ldots > x_r$ is defined by
$$s = x_1^{\alpha_1} \cdots x_r^{\alpha_r} <_{\text{plex}} t = x_1^{\lambda_1} \cdots x_r^{\lambda_r}$$
if $\alpha_1 < \lambda_1$ or there exists $l \in \mathbb{N}$ such that $\alpha_k = \lambda_k$ for $1 \leq k < l$ and $\alpha_l < \lambda_l$.

- The graded lexicographical ordering $<_{\text{grlex}}$ with $x_1 > x_2 > \ldots > x_r$ is defined by
$$s = x_1^{\alpha_1} \cdots x_r^{\alpha_r} <_{\text{grlex}} t = x_1^{\lambda_1} \cdots x_r^{\lambda_r}$$
if $\sum_{i=1}^{r} \alpha_i < \sum_{i=1}^{r} \lambda_i$ or if $\sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r} \lambda_i$ and $s <_{plex} t$.

Example with Maple. See Maple session groebner.mw

To solve the system of algebraic equations

$$\left.\begin{array}{c} p_1(x_1,\ldots,x_r)=0 \\ \vdots \\ p_n(x_1,\ldots,x_r)=0 \end{array}\right\} \text{ with } p_i \text{ not necessarily linear.}$$

we work with Gröbner basis as a *black box* as follows:

1. Compute the reduced Gröbner basis of the polynomials $\{p_1,\ldots,p_r\}$ with respect to the pure lexicographic ordering with $x_1 > x_2 > \ldots > x_r$.
2. If the Gröbner basis is $\{1\}$, the system does not have a solution.
3. If for each x_i, $i = 1,\ldots,r$ there exists a polynomial in the Gröbner basis whose leading monomial with respect to the order chosen in (1) is of the form $x_i^{\alpha_i}$ then the system has finitely many solutions. Otherwise the system has an infinite number of solutions.
4. Solve the triangular system given by the Gröbner basis.

Maple session

There is a Maple library on Gröbner basis.

Groebner.

The Maple statement to compute the reduced Gröebner basis of $[p_1, \ldots, p_n]$ with respect to the pure lexicographical ordering with $x_1 > \cdots > x_r$ is:

Basis($[p_1, \ldots, p_n], plex(x_1, \ldots, x_r)$)

Example

Given 3 polynomials

```
>   p1:=y^2+z^2+x^2-4;
```

$$p1 := y^2 + z^2 + x^2 - 4$$

```
>   p2:=x*y-1;
```

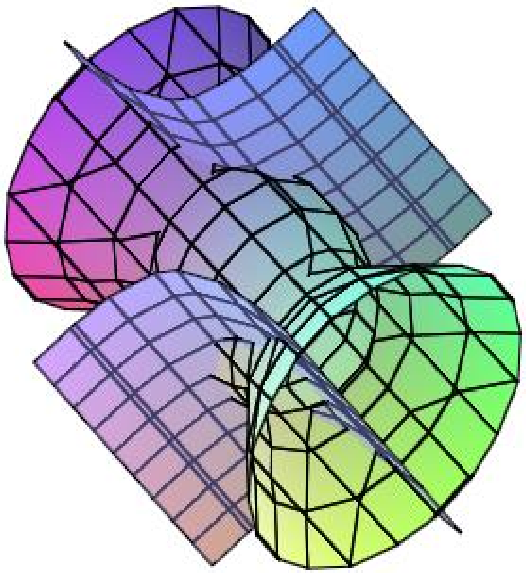
$$p2 := x\,y - 1$$

```
>   p3:=x^2-y^2+z^2-1;
```

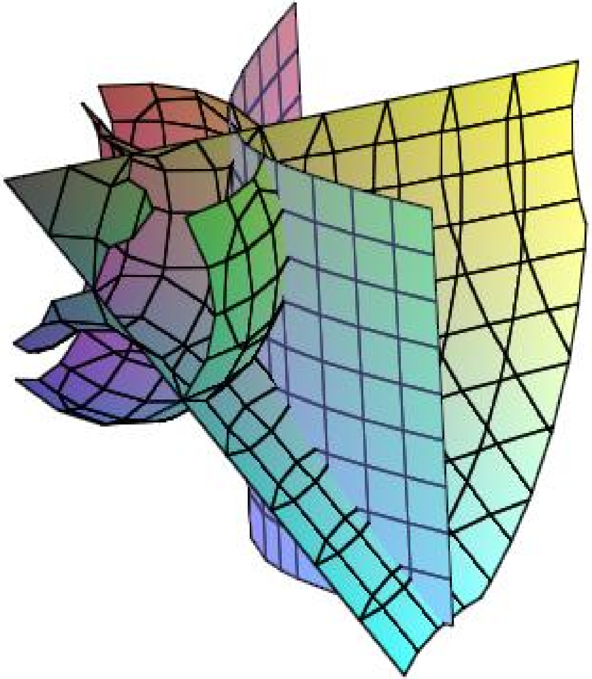
$$p3 := x^2 - y^2 + z^2 - 1$$

We visualize the problem geometrically.

```
>   implicitplot3d({p1,p2,p3},x=-4..4,y=-3..3,z=-4..4);
```



```
>   implicitplot3d({p1,p2,p3},x=-1..4,y=-1..4,z=-1..4);
```



We charge the library Groebner.

```
>   with(Groebner):
```

We compute the Gröbner basis of p_1, p_2, p_3 with respect to the pure lexicographic ordering with $x > y > z$.

```
>   GB:=Basis([p1,p2,p3],plex(x,y,z));
```

$$GB := [6\,z^2 - 11,\; 2\,y^2 - 3,\; -2\,y + 3\,x]$$

We obtain a new system with triangular form, the polynomials of the new system are:

```
>   q1:=GB[1];q2:=GB[2];q3:=GB[3];
```

$$q1 := 6\,z^2 - 11$$

$$q2 := 2\,y^2 - 3$$

$$q3 := -2\,y + 3\,x$$

We solve the triangular system:

- The variable z takes values $\pm\sqrt(\frac{11}{6})$.
- The variable y takes the values $\pm\sqrt(\frac{3}{2})$.
- For each value of y the variable x takes values $\pm\frac{2}{3}\sqrt(\frac{3}{2})$.

Therefore the solutions are:

```
>   SOL1:=[2/3*sqrt(3/2),sqrt(3/2),sqrt(11/6)];
```

$$SOL1 := [\frac{1}{3}\sqrt{6},\ \frac{1}{2}\sqrt{6},\ \frac{1}{6}\sqrt{66}]$$

```
>   SOL2:=[-2/3*sqrt(3/2),-sqrt(3/2),sqrt(11/6)];
```

$$SOL2 := [-\frac{1}{3}\sqrt{6},\ -\frac{1}{2}\sqrt{6},\ \frac{1}{6}\sqrt{66}]$$

```
>   SOL3:=[2/3*sqrt(3/2),sqrt(3/2),-sqrt(11/6)];
```

$$SOL3 := [\frac{1}{3}\sqrt{6},\ \frac{1}{2}\sqrt{6},\ -\frac{1}{6}\sqrt{66}]$$

```
>   SOL4:=[-2/3*sqrt(3/2),-sqrt(3/2),-sqrt(11/6)];
```

$$SOL4 := [-\frac{1}{3}\sqrt{6},\ -\frac{1}{2}\sqrt{6},\ -\frac{1}{6}\sqrt{66}]$$

We check the correctness of the answer.

```
> for i from 1 to 4 do
> simplify(subs(x=SOL.i[1],y=SOL.i[2],z=SOL.i[3],[p1,p2,p3]))
> od;
```

$$[0, 0, 0]$$
$$[0, 0, 0]$$
$$[0, 0, 0]$$
$$[0, 0, 0]$$

Implicitization of parametric equations

Gröbner basis allow the elimination of variables in a system of algebraic equations.

An application of this fact is the implicitization of rational representations.

Let us suppose that we are given a parametric representation of an algebraic object. We are given the parametric equations:

$$\left\{ \begin{array}{l} x_1 = \frac{p_1(t_1,\ldots,t_r)}{q_1(t_1,\ldots,t_r)} \\ \qquad \vdots \\ x_n = \frac{p_n(t_1,\ldots,t_r)}{q_n(t_1,\ldots,t_r)} \end{array} \right.$$

where p_i, q_i are polynomials in the variables $t_1, \ldots, t_r$.

In this situation the goal is to find the implicit equations of the geometric object (that is, the algebraic variety) defined by the previous parametrization.

For this purpose the following method can be applied:

1. Consider the polynomials $Q_i(x_i, t_1, \ldots, t_r) = q_i x_i - p_i$, $i = 1, \ldots, n$.
2. Compute a Gröbner basis of the polynomials
$$\{Q_1, \ldots, Q_n, W \prod_{i=1}^{n} lcm(q_1, \ldots, q_n) - 1\}$$
where W is a new variable, with respect to the pure lexicographical order with $\{t_1 < \ldots < t_r < W < x_1 < \ldots < x_n\}$. This means that t_i are the weakest variables. Observe that the polynomial $Q = W \prod_{i=1}^{n} lcm(q_1, \ldots, q_n) - 1$ guaranties that the denominators do not vanish.
3. Those polynomials in the Gröbner basis depending only on the variables $\{x_1, \ldots, x_n\}$ are the implicit equations we are looking for.

Maple session

1. with(Groebner);
2. Define p_i, q_i, $i = 1$.
3. for i from 1 to n do $Q||i := q||i * x||i - p||i$ od;
4. $Q := W * lcm(q||1, \ldots, q||n) - 1$;
5. $GB := Basis([Q1, \ldots, Q_n, Q], plex(t_1, \ldots, t_r, W, x_1, \ldots, x_n))$;
6. Those polynomials in the Gröbner basis depending only on the variables $\{x_1, \ldots, x_n\}$ are the implicit equations.

```
> with(Groebner);
```

$$[fglm, gbasis, gsolve, hilbertdim, hilbertpoly, hilbertseries, inter\_reduce, is\_finite, is\_solvable, leadcoeff, leadmon, leadterm, normalf, pretend\_gbasis, reduce, spoly, termorder, testorder, univpoly]$$

Step-2

```
> PARAM:=[(t1*t2)/(t1^2+t2^2+1),(t1^2+1)/(t1^2+t2^2+1),
> (t2+1)/(t1^2+t2^2+1)];
```

Step-3

```
> for i from 1 to 3 do Q||i:=numer(x||i-PARAM[i]) od;
```

$$Q1 := x1\ t1^2 + x1\ t2^2 + x1 - t1\ t2$$

$$Q2 := x2\ t1^2 + x2\ t2^2 + x2 - t1^2 - 1$$

$$Q3 := x3\ t1^2 + x3\ t2^2 + x3 - t2 - 1$$

Step-4

```
> Q:=lcm(denom(PARAM[1]),denom(PARAM[2]),denom(PARAM[3]))*W-1;
```

$$Q := (t1^2 + t2^2 + 1)\,\mathrm{W} - 1$$

Step-5

```
> GB:=Basis([Q1,Q2,Q3,Q],plex(t1,t2,W,x1,x2,x3));
```

$$GB := [x3^2\,x2^2 - 2\,x3^2\,x2 + 3\,x1^2\,x2^2 - 4\,x2\,x1^2 + x1^4 + x3^2 + 2\,x2^4 - 5\,x2^3 - 2\,x3\,x2^3 + 4\,x2^2\,x3 - 2\,x3\,x2\,x1^2 + 4\,x2^2 - 2\,x3\,x2 + 2\,x1^2\,x3 + x1^2 - x2,\ -x2^2 + x2 - x1^2 + x2\,\mathrm{W} - \mathrm{W},\ x1^2\,\mathrm{W} + 2\,x2\,x1^2 - 2\,x1^2\,x3 - x1^2 + 2\,x2^3 - 2\,x2^2\,x3 - 3\,x2^2 + x3^2\,x2 + 2\,x3\,x2 + x2 - x3^2,\ \mathrm{W}^2 - 2\,x3\,\mathrm{W} + x1^2 + x2^2 - x2 + x3^2,\ x2 - 1 + x3\,t2 - x3 + \mathrm{W},\ -x3\,x2 + x3 + x1^2\,t2 + x1^2 + t2\,x2^2 - t2\,x2 + x2^2 - x2,\ -x3 + \mathrm{W}\,t2 + \mathrm{W},\ x2\,t1 - t1 + x1\,t2,\ x1\,t1 - t2\,x2 - \mathrm{W} + x3,\ \mathrm{W}\,t1 - x3\,t1 + x1,\ x3\,t1^2 - t2\,x2 - x2 + x3]$$

Step-6

```
> IMPLICIT:=GB[1];
```

$$IMPLICIT := x3^2\,x2^2 - 2\,x3^2\,x2 + 3\,x1^2\,x2^2 - 4\,x2\,x1^2 + x1^4 + x3^2 + 2\,x2^4 - 5\,x2^3 - 2\,x3\,x2^3 + 4\,x2^2\,x3 - 2\,x3\,x2\,x1^2 + 4\,x2^2 - 2\,x3\,x2 + 2\,x1^2\,x3 + x1^2 - x2$$

CHECKING THE ANSWER

```
>   simplify(subs(x1=PARAM[1],x2=PARAM[2],x3=PARAM[3],
>   IMPLICIT));
```

$$0$$