Mathematical background of Groebner basis

Markiyan Hirnyk
Lviv Academy of Commerce
10, Tuhan-Baranovskyi St., 79005 Lviv ,Ukraine

14.11.14

This is an elementary and self-sufficient (Only the definitions of a ring and a field are assumed to be known.) introduction to Groebner basis. Let $\mathbb{K}$ be a field (mainly $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$). Let $x_1, x_2, \ldots, x_n$ be variables and $P_1(x_1, x_2, \ldots, x_n), P_2(x_1, x_2, \ldots, x_n), \ldots$ be polynomials in $x_1, x_2, \ldots, x_n$ over $\mathbb{K}$, i. e. with the coefficients from $\mathbb{K}$.

Definition. A system of polynomial equations (PS) is a system of the form

$$\begin{cases} P_1(x_1, x_2, \ldots, x_n) = 0, \\ P_2(x_1, x_2, \ldots, x_n) = 0, \\ \ldots \end{cases} \tag{1}$$

with, possibly, a countable set of equations.

Definition. A list $[a_1, a_2, \ldots, a_n]$ of elements of $\mathbb{K}$ s. t.

$$P_1(a_1, a_2, \ldots, a_n) = 0, P_2(a_1, a_2, \ldots, a_n) = 0, \ldots$$

is called a solution of (1).

Definition. Two polynomial systems are equivalent if their solution sets are equal.

Example. The two systems

$$\begin{cases} x^2 + y^2 = -1; \end{cases} \quad \text{and} \quad \begin{cases} x + y = 2, \\ x^2 + 2xy + y^2 = 3; \end{cases}$$

are equivalent over $\mathbb{R}$ because their solution sets are empty. These systems are not equivalent over $\mathbb{C}$: $(i, 0)$ is a solution of the former system, but is not a solution of the latter one.

To solve a system means to find its solution set (or to prove the one is empty). The questions arise:

i) Does there exist a solution of a polynomial system?

ii) Are two given polynomial systems equivalent?

iii) Is the solution set of a polynomial system finite?

Let us recall some algebraic notions and notations. We denote by $\mathbb{K}[x_1, x_2, \ldots, x_n]$ the set of all the polynomials in $x_1, x_2, \ldots, x_n$ over $\mathbb{K}$. This set equipped with the operations $+$ and $\cdot$ forms a ring. As usually, $\deg(P)$ stands for the degree of polynomial $P(x)$.

Definition. A non-constant polynomial $P(x_1, x_2, \ldots, x_n)$ is said to be irreducible if $P = P_1 P_2$ implies P_1 or P_2 is a constant.

Definition. Two polynomials are associates if these differ by a constant multiplier.

Irreducible polynomials are an analog of the primers. The following theorem is an analog for polynomials of the prime decomposition for the integers.

Theorem 1. *Each non-constant polynomial from* $\mathbb{K}[x_1, x_2, \dots, x_n]$ *equals the product of irreducible polynomials. That decomposition is unique up to the order of the multipliers and invertible constants.*

There is a substantial difference between polynomial systems over $\mathbb{R}$, and $\mathbb{C}$ which is caused by the algebraic closeness of $\mathbb{C}$.

Definition.A field $\mathbb{K}$ is called algebraically closed if every non-constant polynomial over $\mathbb{K}$ has zero belonging $\mathbb{K}$.

Example. The field $\mathbb{R}$ is not algebraically closed because the polynomial $x^2 + 1$ has no real solution.

Theorem 2. *Every non-constant polynomial over* $\mathbb{C}$ *has a complex root.*

Exercise. Is the field $\mathbb{C}(x)$ of all the rational functions over $\mathbb{C}$, i. e. fractions of polynomials (assuming the denominator is not identically 0), algebraically closed?

It is clear that every finite polynomial system over $\mathbb{R}$ is equivalent to a single equation:

$$\begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ P_k(x_1, x_2, \dots, x_n) = 0; \end{cases} \Leftrightarrow P_1(x_1, x_2, \dots, x_n)^2 + \dots + P_k(x_1, x_2, \dots, x_n)^2 = 0.$$

Exercise. Prove that the system $\begin{cases} x = 0, \\ y = 0; \end{cases}$ over $\mathbb{C}$ is not equivalent any polynomial equation $P(x, y) = 0$.

Let R be a commutative and associative ring with the unit.

Definition. A nonempty $J \subseteq R$ is called an ideal of R (we will use the notation $J \lhd R$) if i) $\forall a \in J \, \forall a \in J \; a - b \in J$; ii) $\forall a \in J \, \forall c \in R \; ac \in R$.

Example. The set $n\mathbb{Z}$ of all the integers which are divisible by a fixed integer n forms an ideal of $\mathbb{Z}$. It is easy to see all the ideals of $\mathbb{Z}$ are of this form.

Definition. An ideal J is principal if $\exists \, a \in R$ s. t. $J =< a >:= \{ar : r \in R\}$. In this case the element $a \in R$ is called a generator of J.

Example. The set of polynomials of $\mathbb{K}[x, y]$ equal to zero at the origin $x = 0, y = 0$ forms an ideal which is not principal.

Definition. A ring R is said to be a principal ideal domain (PID) if every its ideal is principal.

The notion of a principal ideal can be generalized as follows. It is easy to see that the set $< a_1, a_2, \dots, a_k >:= \{r_1 a_1 + r_2 a_2 + \dots + r_k a_k : r_1 \in R, r_2 \in R, \dots, r_k \in R\}$ forms an ideal $J \lhd R$.

Definition. Elements $a_1, a_2, \dots, a_k$ make a basis of the ideal $< a_1, a_2, \dots, a_k > \lhd R$. It should be noted no minimality condition and uniqueness condition are required. The ideal J is said to be finitely generated if $J =< a_1, a_2, \dots, a_k >$ for some basis.

Theorem 3. *Every ideal* $J \lhd \mathbb{K}[x_1, x_2, \dots, x_n]$ *is finitely generated.*

Exercise. 1. What is a basis of the ideal $< x, y^2, xy^3, x^2y^4, \cdots >$? 2. Give an example of an ideal $J \lhd R$ which is not finitely generated (take the set of polynomials in the countable set of variables $\mathbb{K}[x_1, x_2, \dots]$ by R).

Every polynomial system S consisting of

$$\begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \end{cases}$$

defines the ideal $J(S) :=< P_1(x_1, x_2, \dots, x_n), P_2(x_1, x_2, \dots, x_n), \cdots >$.

Let
$P_1(x_1, x_2, \dots, x_n), P_2(x_1, x_2, \dots, x_n), \dots, P_k(x_1, x_2, \dots, x_n)$ and
$Q_1(x_1, x_2, \dots, x_n), Q_2(x_1, x_2, \dots, x_n), \dots, Q_s(x_1, x_2, \dots, x_n)$ be two bases of the ideal J, then . Theorem 3 implies that every polynomial system is equivalent to some finite polynomial system. Thus, we will consider only finite polynomial systems in that follows. One may suppose if polynomial systems S_1 and S_2 are equivalent, then $J(S_1) = J(S_2)$. This is not true:$\{x = 0 \Leftrightarrow \{x^2 = 0$, but $< x > \neq < x^2 >$. The question arises: is it possible, knowing the ideals $J(S_1)$ and $J(S_2)$, to determine whether $S_1 \Leftrightarrow S_2$ (of course, not solving the systems)? For example, the systems $\{x^2+y^2-2xy+1 = 0$ and $\{x^4+y^4+2 = 0$ over $\mathbb{R}$ are equivalent (no solutions), but any relation between $< x^2+y^2-2xy+1 >$ and $< x^4+y^4+2 >$ is not seen. However, D. Hilbert obtained the answer in the case of algebraically closed fields. To state it, we need a few notions.

Informally speaking, an affine algebraic variety is the solution set of a polynomial system. In fact, its definition is very technical. We will take the following (somewhat naive) view.

Definition. A set $A \subset \mathbb{K}^d$ is called an affine algebraic variety if there is a polynomial system

$$S := \begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ P_d(x_1, x_2, \dots, x_n) = 0 \end{cases}$$

s.t. $x = (x_1, x_2, \dots, x_n) \in A \Leftrightarrow x$ is a solution of S.

Example. The set$\{(t, t^2, t^3) : t \in \mathbb{K}\} \subset \mathbb{K}^3$ is an affine variety defined by the system

$$\begin{cases} y = x^2 \\ z = x^3. \end{cases}$$

The corresponding ideal is $< -x^2 + y, -x^3 + z$.

We will denote the solution set of a polynomial system S by $X(S)$. If $J \lhd \mathbb{K}[x_1, x_2, \dots, x_n]$, then we define $X(J)$ as the subset of $\mathbb{K}^d$ s. t. all the polynomials belonging to J equal zero on $X(J)$. It is clear that $S_1 \Leftrightarrow S_2$ implies $X(S_1) = X(S_2)$. Also $X(S) = X(J(S))$. As mentioned above, different ideals can define the same varieties. At the same time for every variety X there is a maximal ideal $J(X)$ which defines X: $J(X) := \{P \in \mathbb{K}[x_1, x_2, \dots, x_n] : \forall a \in X \, P(a) = 0\}$.

Exercise. Find the maximal ideal $J(X)$ if $X = \{(x, y, z) \in \mathbb{K}^3 : x = y, y = z\}$.

Theorem 4. *Polynomial systems S_1 and S_2 are equivalent iff $J(X(S_1)) = J(X(S_2))$.*

The ideal $J(X(S))$ over $\mathbb{C}$ can be described in constructive way. To this end, we need the following notion.

Definition. The radical $r(J)$ of an ideal $J \lhd \mathbb{K}[x_1, x_2, \dots, x_n]$ is the set $\{P \in \mathbb{K}[x_1, x_2, \dots, x_n] : \exists s \in \mathbb{N} P^s = 0\}$.

One can prove that i) $J \subseteq r(J)$; ii) $r(J) \lhd \mathbb{K}[x_1, x_2, \dots, x_n]$, i. e. J is an ideal; iii) $X(J) = X(r(J))$.

Exercise. Find the radical $r(J)$ for $J :=< x^2 > \lhd \mathbb{K}[x]$.

Now we formulate the Hilbert's theorem about zeros.

Theorem 5. *For every polynomial system S over the complexes the relation*

$$J(X(S)) = r(J(S))$$

holds.

Let us reformulate Theorem 5 in terms of polynomial systems: a polynomial $P(x_1, x_2, \dots, x_n)$ equals zero on the solution set of a polynomial system

$$\begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ P_k(x_1, x_2, \dots, x_n) = 0; \end{cases}$$

iff there exist polynomials $r_1(x_1, x_2, \dots, x_n), \dots, r_k(x_1, x_2, \dots, x_n)$ and $s \in \mathbb{N}$ s. t. $F^s = r_1 P_1 + \dots + r_k P_k$. For example, one can add the equation $x + y = 0$ to the system

$$\begin{cases} x + 2y + 4yz^2 = 0, \\ 4xz^2 - y = 0, \end{cases}$$

obtaining an equivalent system since $(x + y)^2 = (x + 2y + 4yz^2)x - (4xz^2 - y)y$.

Exercise. Give a counterexample to Theorem 5 in the case of the reals.

Corollary. Systems S_1 and S_2 are equivalent iff $r(J(S_1)) = r(J(S_2))$.

This gives the possibility to determine whether two given systems are equivalent, not solving those.

Definition. An ideal J is said to be radical if $J = r(J)$.

Now we turn to Groebner basis.

Definition. A monomial is a polynomial consisting of one term $P = ax_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$. We correspond to a monomial its multi-power (which is a multi-index) $k := [k_1, k_2, \dots, k_n]$.

Definition. A multi-power $i := [i_1, i_2, \dots, i_n]$ is said to be greater than a multi-power $j := [j_1, i_2, \dots, j_n]$ if there exists a natural $s < n$ s. t. $i_1 = j_1$, $i_2 = j_2 \dots, i_{s-1} = j_{s-1}, i_s > j_s$.

For example, $[3, 3, 0, 7] < [4, 0, 0, 0]$ and $[3, 1, 5, 2] > [3, 1, 5, 1]$. This way of ordering multi-powers is called *pure lexicographic* (plex in Maple).

Definition. The leading term of a polynomial

$$P(x_1, x_2, \dots, x_n) = \sum a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

is called its term with maximum multi-power.

For example, the leading term of $3x_1 + x_2^2 x_3^4 + x_4^7$ is $3x_1$ and the leading term of $x_1^2 x_2 + x_1 x_2^2 + x_3^5$ is $x_1^2 x_2$. It is cleat that the leading term of the product $P_1 P_2$ equals the product of the leading terms of P_1 and P_2.

The occurrence problem arises: how to determine whether a polynomial $P(x)$ belongs to a principal ideal $< Q(x) >$? The answer is simple. Let us divide $Px)$ by $Q(x)$. If the remainder equals 0, then $P(x) \in < Q(x) >$, in the other case $P(x) \notin < Q(x) >$. The answer to the same question in higher dimensions is much more complicated. Let an ideal $J \lhd \mathbb{K}[x_1, x_2, \dots, x_n]$ be defined by its basis $f_1, f_2, \dots, f_k$. The algorithm which determines whether a given polynomial $P(x_1, x_2, \dots, x_n) \in J$ in a finite number of steps is required. For example, does $x_2 x_3^2 x_4 - x_1 x_3 x_4^2$ belong to $< x_1 + x_2, x_3 + x_4 > \lhd \mathbb{K}[x_1, x_2, x_3, x_4]$? The answer is yes in view of $x_2\, x_3^2\, x_4 - x_1\, x_3\, x_4^2 = (x_1 + x_2)\, x_3^2\, x_4 - (x_3 + x_4)\, x_1\, x_3\, x_4$.

We consider the reduction algorithm. The idea is simple to express. We will use the representation of a polynomial $P = P_L + P_R$, where P_L is its leading term. For example, for $P = 2x_1^2 + x_1^2 x_2^3 - 4x_3^3$ we have $P_L = x_1^2 x_2^3$ and $P_R = 2x_1^2 - 4x_3^3$. Let a polynomial $H \in < P_1, P_2, \dots, P_k >$. Let the leading term of H be divisible by the leading term of a certain polynomial from the basis, say, $H_L = P_{i_L}\, Q$. Then $H_1 = H - QP_i \in < P_1, P_2, \dots, P_k >$ too. It is important that the leading term of H_1 is less than the leading term of H.

Example. $H = x_2\, x_3^2\, x_4 - x_1\, x_3\, x_4^2$, $P_1 = x_1 + x_2$, $P_2 = x_3 + x_4$. The monomial $H_L = -x_1\, x_3\, x_4^2$ is divisible by $P_{1_L} = x_1$.

Step 1. $H \to x_2 x_3^2 x_4 + x_2 x_3 x_4^3 =: H_1$. Here $H_{1_L} = x_2 x_3^2 x_4$ is divisible by $P_{2_L} = x_3$.

Step 2. $H_1 \to x_2 x_4 s + x_2 x_3 x_4^2 =:= H_2$ (the second reduction). Here $H_{2_L} = x_2 x_3 x_4^2$ is divisible by $P_{2_L} = x_3$.

Step 3. $H_2 \to x_2 x_4^3 - x_2 x_4^3 = 0$. Thus, $H \in < P_1, P_2 >$.

At last,

Definition. A basis $f_1, f_2, \dots, f_m$ of an ideal J is said to be a Groebner basis of J if each polynomial $h \in J$ is reducible to zero by $f_1, f_2, \dots, f_m$.

The equivalent definition is as follows.

Definition. The set of polynomials $f_1, f_2, \dots, f_m$ is a a Groebner basis of an ideal J if for every $h \in J$ the polynomial h_L is divisible by at least one of $f_1, f_2, \dots, f_m$.

Exercise. To prove that equivalence.

Examples. 1. The set $\{f_1 = x, f_2 = y\}$ forms a Groebner basis of the ideal $< x, y > \lhd \mathbb{K}[x, y]$. Let $h(x, y)$ be an arbitrary polynomial from $< x, y >$. If its leading term is divisible by x,then The reduction with f_1 is the replacement of x by 0.The same with y. Therefore every polynomial from $< x, y >$ is reducible to its constant term. It remains to note that a polynomial belongs to the ideal $< x, y >$ iff its constant term equals zero.

2. Let us consider the ideal $J := < x^2 - y, x^2 - z > \lhd \mathbb{K}[x, y, z]$, $f_1 := x^2 - y$, $f_2 := x^2 - z$. The polynomial $x - y = f_1 - f_2 \in J$. On the other hand, the leading term of $x - y$ is not divisible by the leading terms off_1 and f_2 (These equal x^2.). Because of this reason $\{f_1, f_2\}$ does nor form Groebner basis of J. It will be proved below that f_1, f_2 and $f - 3 := z - y$ form Groebner basis of J.

Now we turn to the solution of the occurrence problem. Let us assume that Groebner basis of an ideal J is known. Let a polynomial h be given. We produce all possible reductions of h by the elements of the basis (Each reduction takes a finite number of steps.). The polynomial $h \in J$ iff all the results are zero. This solution can be programmed. Making use of the Hilbert's theorem, it is not difficult to prove the existence of Groebner basis for every ideal. However, this proof is not constructive.

Now we consider Buchberger's algoritrhm for finding Groebner basis. Let $J \triangleleft \mathbb{K}[x_1, \dots, x_n]$ be an ideal with the basis $f_1, f_2, \dots, f_m$.

Definition. Polynomials f_i and f_j are said to be linked if their leading terms f_{i_L} and f_{j_L} are divisible by a nonconstant monomial w.

If f_i and f_j are linked, i. e. $f_{i_L} = wg_i$, $f_{j_L} = wg_j$, then we consider the polynomial $F_{i,j} := f_i g_j - f_j g_i$. This is called the S-polynomial of the pair f_i, f_j and is drnoted by $S(f_i, f_j)$ or $S(i, j)$. We reduce $F_{i,j}$ by the basis $f_1, f_2, \dots, f_m$ as far as possible, resulting in the irreducible polynomial $G_{i,j}$. If $G_{i,j} = 0$, then this link is solvable. In the other case we add $G_{i,j}$ to the basis: $f_{m+1} := G_{i,j}$. We will find all links and reduce corresponding polynomials $F_{i,j}$.in the new basis $f_1, \dots, f_{m+1}$ we will do the same again.

Example. Let us consider the ideal $J :=< f_1 := x^2 - y, f_2 := x^2 - z >$. There is a link f_{1_L} and f_L are divisible by x^2. This implies $F_{1,2} = -y + z$. We put $f_3 := y - z$. There are no other links.

Example. Let $J =< f_1 := x^2 + y^2 + z^2,\ f_2 := x + y - z,\ f_3 := y + z^2 >$. Only f_1 and f_2 are linked:

$$F_{1,2} = f_1 - xf_2 = y^2 + z^2 - xy + xz = -xy + xz + y^2 + z^2.$$

We reduce by f_2:

$$-xy + xz + y^2 + z^2 \rightsquigarrow (y - z)y - (y - z)z + y^2 + z^2 = 2y^2 + 2z^2 - 2yz.$$

Then we reduce it by f_3:

$$2y^2 + 2z^2 - 2yz \rightsquigarrow 2z^4 + 2z^3 + 2z^2.$$

The further reduction is not possible so $f_4 := 2z^4 + 2z^3 + 2z^2$.

It appears that only a finite number of irreducible links is possible in the general case too.

Theorem 6. *Every set of polynomials $\{f_1, \dots, f_m\}$ from $\mathbb{K}[x_1, \dots, x_n]$ is reducible in a finite number of steps to a set $\{f_1, \dots, f_m, f_{m+1}, \dots, f_M\}$ where each link is solvable.*

Now the so-called Diamond Lemma is formulated.

Theorem 7. *A basis of an ideal is a Groebner basis iff this basis has no links or each its link is solvable.*

Theorems 6 and 7 base the Buchberger's algoritrhm for finding Groebner basis (There are also other algorithms to this end.). Let us state this algorithm again. Let a set of polynomials $\{f_1, \dots, f_m\}$ form a basis of an ideal J.

1. We examine whether the basis has links. If there are no links, then the the basis is a Groebner basis of J else we turn to step 2.

2. According to a link of polynomials f_i and f_j, we put $f_{i_L} = wq_i$, $f_{j_L} = wq_j$ and construct the polynomial $F_{i,j} := f_i q_j - f_j q_i$. Then we reduce $F_{i,j}$ by $\{f_1, \dots, f_m\}$ as far as possible. If $F_{i,j}$ is reduced to a non-zero polynomial f, then we move to step 3 else we move to step 4.

3. We add f to the basis and turn to step 4.

4. We find a new link which was not previously considered in the extended basis and move to step 2. If all the links were considered, then the algorithm is over. We obtain a set $\{f_1, \dots, f_M\}$ where each link is solvable in a finite number of steps. This is a Groebner basis of J.

Thus, the Groebner basis is found. Can it be simplified?

Simplification 1. Let f_1, f_2 be elements of a Groebner basis s. t. f_{1_L} is divisible by f_{2_L}. The we exclude f_1 from the basis. The reduced basis still is a Groebner basis.

Definition. The Groebner basis $\{f_1, \ldots, f_m\}$ is called minimal if f_{i_L} is not divisible by f_{j_L} for $i \neq j$.

Every Groebner basis can be reduced to the minimal one.

Simplification 2 deals with non-leading terms of $f_1, \ldots, f_m$. Let us assume some term q of f_i is divisible by the leading term of f_j. In this case we reduce q by f_j and replace q by the result of the reduction. The reduced Groebner basis still is a Groebner basis.

Definition. A Groebner basis $\{f_1, \ldots, f_m\}$ is said to be reduced if any term of f_i is not divisible by the leading term of f_j for every pair (i, j), $i, j = 1, \ldots, m$, $i \neq j$.

Every Groebner basis can be reduced to the minimal one.

Theorem 8. *The minimal reduced Groebner basis of an ideal $J \triangleleft \mathbb{K}[x_1, \ldots, x_n]$is uniquely determined, i. e. it does not depend on the choice of the basis of J we begin where.*

Example. Let us consider the Groebner basis $f_1 := x^2+y^2+z^2$, $f_2 := x+y-z$, $f_3 := y+z^2, f_4 := z^4+z^3+z^2$. Its minimization: the leading term of f_1 is divisible by the leading term of f_2. Therefore, f_1 can be eliminated and we have the basis f_2, f_3, f_4. The reduction: we replace y in f_2 by$-z^2$, obtaining $f_2 \rightsquigarrow x - z^2 - z$. Hence, the minimal reduced basis is $x - z^2 - z, y + z^2, z^4 + z^3 + z^2$.

It can be showed that for linear algebraic systems the Buchberger's algoritrhm together with the minimization make the Gauss method. We do not discuss the estimate of the complexity of the Buchberger's algoritrhm here. We only indicate how to measure that complexity. Let an ideal J of the ring $\mathbb{K}[x_1, \ldots, x_n]$ generated by k polynomials of degree less than or equal to d be given. One has to estimate:

(i) the maximal degree of the polynomials in the minimal reduced Groebner basis:

(ii) the number of elements of the minimal reduced Groebner basis;

(iii) the number of operations to obtain the minimal reduced Groebner basis.

Now we turn to the effective algorithm to detect the inconsistency of the system of polynomial equations over the complex numbers.

Theorem 9. *A system S of polynomial equations is inconsistent iff the Groebner basis of the ideal $J(S)$ includes a nonzero constant.*

The next theorem determines the equivalence of two polynomial systems.

Theorem 10. *Polynomial systems*

$$\begin{cases} P_1(x_1, x_2, \ldots, x_n) = 0, \\ P_2(x_1, x_2, \ldots, x_n) = 0, \\ \ldots \\ P_k(x_1, x_2, \ldots, x_n) = 0 \end{cases} \text{and} \begin{cases} Q_1(x_1, x_2, \ldots, x_n) = 0, \\ Q_2(x_1, x_2, \ldots, x_n) = 0, \\ \ldots \\ Q_s(x_1, x_2, \ldots, x_n) = 0 \end{cases}$$

are equivalent over $\mathbb{C}$ iff $P_i \in r(Q_1, \ldots, Q_s)$.

At last, the next theorem says us whether the solution set is finite.

Theorem 11. *The solution set of a polynomial system S in $x_1, \ldots, x_n$ over $\mathbb{C}$ is finite iff the Groebner basis of the ideal $J(S)$ includes polynomials $f_1, \ldots, f_n$ s.t. their leading terms are powers of $x_1, \ldots, x_n$ correspondingly.*