GRÖBNER BASES AND INVOLUTIVE BASES

A.V. ASTRELIN, O.D. GOLUBITSKY, AND E.V. PANKRATIEV

Abstract. Recently, constructive methods became widely used in commutative algebra. These methods are mainly based on the theory of Gröbner bases and involutive bases. Due to various applications, the investigations of effectiveness of constructing of the Gröbner bases are very urgent. The algorithm of constructing of the Gröbner bases is bases on considering of S-polynomials and applying of a normal simplificator. Usually, in order to refine the algorithm of the Gröbner bases construction, one uses more elaborate choice of S-polynomials. The influence of the normal simplificator on the effectiveness of the Gröbner bases construction is studied insufficiently.

In the paper we try to establish a relation between the theory of Gröbner bases and the theory of involutive bases. It is known that any involutive basis contains as a subset the Gröbner basis of the ideal. It is shown that the involutive basis corresponds to the Gröbner basis with a fixed normal simplificator. Thus, the dependence of the effectiveness of the Gröbner basis construction on the chosen normal simplificator is emphasized. An attempt to describe the normal simplificators corresponding to involutive bases is fulfilled.

Let K be a field, $R = K[x_1, \ldots, x_n]$ the ring of polynomials over K, I an ideal of R. The ideal I as well as the factor-ring R/I are linear K-spaces, in general, of infinite dimension. How one can find bases of these spaces? In R considered as a K-space there is a basis which consists of the set M of all monomials. It is natural to try to partition the set M into two parts $M = M_1 \cup M_2$ such that the images of elements from M_1 in the factor-ring R/I form a basis of the K-space R/I, and the elements of the basis of the K-space I correspond one-to-one to the elements of M_2.

Suppose that we have an admissible order on the set of monomials, i.e. we have a relation $<$ with the following properties:

(1) $1 < m$ for any non-trivial monomial m;
(2) if $t_1 < t_2$ for some monomials t_1 and t_2, then $t_1 m < t_2 m$ for any monomial m.

The work was supported in part by RFBR, grant 96-01-01349.

Thus, for any polynomial f we define the *leading monomial* $\mathrm{lm}(f)$ and the *leading coefficient* $\mathrm{lcoef}(f)$, and the set $M$is divided into two subsets: M_1 consists of the monomials which are not leading monomials for $f \in I$, and M_2 consists of the leading monomials of the elements of I.

Now the question of constructive description of the sets M_1 and M_2 arises.

An answer to this question as well as to many other questions of the constructive theory of polynomial ideals is given by the theory of Gröbner bases. There are many equivalent definitions of the Gröbner bases (see, e.g. [5] or [2], in [1, p. 40] these definitions are considered taking into account the normal simplificator chosen). For example, a set $G \subset I$ is called a *Gröbner basis* of the ideal I, if any $f \in I$ admits a representation of the form $f = \sum_{i=1}^{N} c_i m_i g_i$, where $c_i \in K$, $m_i \in M$, $g_i \in G$ and the condition $\mathrm{lm}(m_i g_i) > \mathrm{lm}(m_j g_j)$ holds for $j > i$ (a representation of this form is called a G-representation). Firstly, this definition is not constructive; secondly, it does not define the Gröbner basis uniquely. A constructive method of obtaining of a Gröbner basis is given by the *completion algorithm*. In order to choose a uniquely defined basis among all the Gröbner bases of an ideal, we introduce a notion of an autoreduced set.

A set of polynomials $G = \{g_\alpha : \alpha \in \mathbb{I}\}$ is called *autoreduced*, if for any $\alpha \in \mathbb{I}$ every monomial which is present in g_α with nonzero coefficient is non-divisible by any monomial $\mathrm{lm}(g_\beta)$ for $\beta \neq \alpha$. The Gröbner basis which is an autoreduced set and whose leading coefficients are equal to 1 is defined uniquely for any ideal I. We call such a basis by the *autoreduced Gröbner basis*.

Suppose that we know the autoreduced Gröbner basis G of an ideal I. In order to obtain a basis of I considered as a linear space, it is sufficient to show a procedure which any monomial $m \in M_2$ maps into an element $g(m) \in G$ whose leading monomial divides m, i.e. $m = t(m) \cdot \mathrm{lm}(g(m))$ for a monomial $t(m)$. Then the set of the polynomials $t(m) \cdot g(m) \mid m \in M_2$ forms a basis of the linear space I. We call any such a procedure by a *normal simplificator*.

Example. The simplest normal simplificator can be obtained by enumerating the elements of the autoreduced Gröbner basis G in an order from 1 to k and mapping every monomial $m \in M_2$ into the element $g_i \in G$ with the minimal index i such that $\mathrm{lm}(g_i)|m$. Of course, there exist more complicated normal simplificators.

Consider this example in detail. Suppose that the autoreduced Gröbner basis of I consists of polynomials $g_1, \ldots, g_k$. Then a basis

of the linear space I can be obtained as the union of the following sets
the set B_1 of all the products $m \cdot g_1$, where $m \in M$;
the set B_2 of all the products $m \cdot g_2$ such that $\mathrm{lm}(m \cdot g_2) \notin \mathrm{lm}(B_1)$;
the set B_3 of all the products $m \cdot g_3$ such that $\mathrm{lm}(m \cdot g_3) \notin \mathrm{lm}(B_1) \cup \mathrm{lm}(B_2)$;
...
the set B_k of all the products $m \cdot g_k$ such that $\mathrm{lm}(m \cdot g_k) \notin \bigcup_{i=1}^{k-1} \mathrm{lm}(B_i)$.

The same basis can be described in other words.

For any g_i we take the maximal subset $x_{i_1}, \ldots, x_{i_s}$ of the variables such that the product of g_i by any monomials containing only these variables (the set of such monomials will be denoted by $S(g_i)$) belongs to B_i. We call these variables *multiplicative* for the monomial $\mathrm{lm}(g_i)$, the remaining variables will be called *non-multiplicative*. We exclude the monomial g_i and all its products by monomials belonging to $S(g_i)$ from B_i. If the set obtained is not empty, then we take there the minimal monomial g_i' and repeat the process for g_i'. In this way we can represent the basis of the linear space I as the union of a finite family of the sets, each one described by a polynomial and a set of multiplicative variable for this polynomial. The basis obtained is an example of an *involutive basis*. The notion of the involutive basis in commutative algebra has been introduced by Zharkov and Blinkov [6].

Thus, in order to construct an involutive basis we used the Gröbner basis, normal simplificator and partition of the variables into multiplicative and non-multiplicative for some family of monomials.

Let us recall the algorithm which allows to check whether a given set is the Gröbner basis of the ideal generated and to construct a gröbner basis, when we have a system of generators of an ideal I (this algorithm is known as the *completion algorithm*).

Let a set of polynomials G and a relation of order $<$ on the set of monomials be given. In order to verify that G is a Gröbner basis of the ideal $I = (G)$ with respect to the order $<$, one uses a normal simplificator whose choice does not influence the result. We should form the set of S-polynomials and check that each of these polynomials can be reduced to zero. Refined versions of the algorithm use different criteria, which allow diminish the set of S-polynomials considered (e.g. "triangle rule").

It has been said that the set of polynomials $G = \{g_1, \ldots, g_k\}$ and the normal simplificator allow to form the sets B_i which are obtained by multiplying the polynomials g_i by a set of monomials. S-polynomials correspond to the polynomials g_i and monomials m_i such that m_i is the minimal monomial (with respect to division of monomials) satisfying the condition $m_i \cdot g_i \notin B_i$. In fact, we must check reducibility to zero

only for theses polynomials (note that in this case we consider not all S-polynomials, "the triangle rule" works automatically). It is natural to require the set G to be autoreduced.

The completion algorithm is based on the method of S-polynomials and differs from the algorithm above by adding nonzero normal forms of the S-polynomials to the set G. Usually, the normal simplificator, hence the sets B_i, should be changed after such adding.

As a rule, when refining the algorithms for construction of the Gröbner bases one improves the enumeration of S-polynomials, and the influence of the admissible normal simplificators is studied insufficiently.

Up to now we did not restrict the choice of the normal simplificator, i.e. obtaining of the sets B_i for a given family of polynomials $G = \{g_i\}$. Suppose that some relation of "divisibility" $|_L$ is fixed on the set of monomials, and this relation satisfies the following axioms (the axioms of the *involutive division*, see, for instance [4]):

(1) $u\big|_L v \implies u|v$ (in the sense of usual division);
(2) $1\big|_L u$;
(3) $u\big|_L w \wedge v\big|_L w \implies u\big|_L v \vee v\big|_L u$;
(4) $u\big|_L uvw \iff u\big|_L uv \wedge u\big|_L uw$;
(5) $u\big|_L v \wedge v\big|_L w \implies u\big|_L w$ (transitivity).

In the case when the relation $u\big|_L v$ holds, we say that u *divides involutively* v.

Axioms 3 and 4 in the case of two variables can be illustrated in the following way:
Let a point (i, j) of the plane represent the monomial $x^i y^j$. Then

- for any pair of monomials, the sets of their involutive multimples either are disjoint or one of them contains the other;
- the set of involutive multiples of a monomial $x^i y^j$ is either one point (i, j), or vertical or horizontal half-line starting from this point, or the angle between the vertical and horizontal half-lines starting from this point.

The generalization to the case of several variables is obvious.

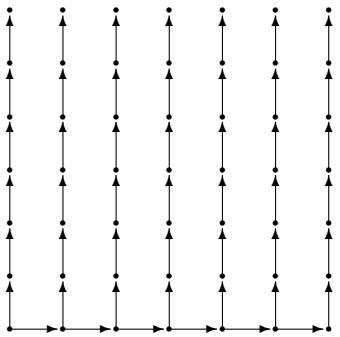
An involutive division can be determined by defining for every monomial u the set $M(u)$ of its *multiplicative variables* as the set of variables such that u divides involutively any product u by a monomial containing only multiplicative variables. The remaining variables will be called *non-multiplicative* for the monomial u (denoted $NM(u)$).

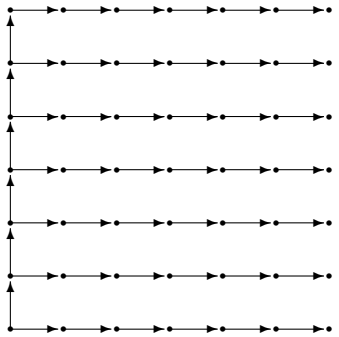
Examples of involutive divisions:

(1) $M(x_1^{i_1} \dots x_k^{i_k}) = \{x_k, \dots, x_n\}$ — *right Pommaret division.*
(2) $M(x_k^{i_k} \dots x_n^{i_n}) = \{x_1, \dots, x_k\}$ — *left Pommaret division.*

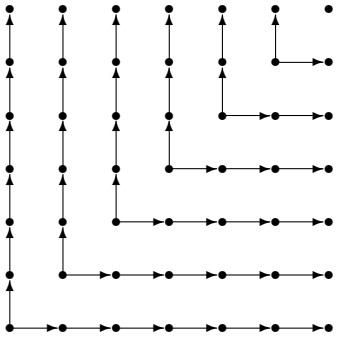
(3) $M(x_1^{i_1} \dots x_n^{i_n}) = \{x_k \ : \ i_k = \max_{m=1}^{n} i_m\}$.

In the bivariate case the right and left Pommaret divisions can be illustrated in the following way:





The geometrical illustration of the third example is the following one:



We say that a polynomial f is *involutively reducible to a polynomial g with the help of a polynomial h by a monomial m*, which is present in f, if f is reducible to g in the usual sense and $\mathrm{lm}(h)|_L m$. If a relation of reduction is fixed, then a *normal form* is defined, which is called in this case *involutive*. A generating set G of an ideal I is called an *involutive basis* of I if the involutive normal form of any polynomial $f \in I$ with respect to G is equal to 0.

The product of a polynomial f by a variable non-multiplicative for the leading monomial of f will be called a *non-multiplicative extension* of f. A generating set G of an ideal I is an involutive basis of I if and only if the normal forms of non-multiplicative extension of all elements of G are equal to zero. This fact implies the standard completion algorithm for constructing an involutive basis.

The involutive basis of an ideal I can easily be constructed if we know the autoreduced Gröbner basis G of I and the involutive division.

This construction is reduced to multiplying the elements of G by non-multiplicative variables.

If we have an involutive basis $G = \{g_i\}$ and an involutive division, then we can construct a normal simplificator in the following way: for any polynomial g_i we take the set B_i of its multiplicative multiples; the set $\bigcup_i B_i$ is a basis of the linear space I, and every leading monomial is present just in one element of this basis; we shall use this basis in order to construct G-representations.

Of course, not every normal simplificator can be obtained in this way. The problem arises to describe the normal simplificators which can be constructed via the involutive bases.

Proposition. *If the set of leading monomials of polynomials of an ideal I can be divided into disjoint cones such that the elements of one cone is reducible with respect of one polynomial of the basis, then the appropriate involutive division has the following form:*
the multiplicative variables for the vertex of the cone are those which correspond to the generators and inside the cone the division can be defined in an arbitrary way.

Proof. Formally, these involutive division $\big|_L$ is given in the following way: let $\big|_{Ls}$ be an arbitrary involutive division corresponding to the cone C_s with the vertex at the monomial s. We set

$$\forall u, v \in C_s \; u\big|_L v \iff u\big|_{Ls} v.$$

If $\nexists s : \; u, v \in C_s$, then we set $u \not|_L v$. We also set $\forall u \; 1\big|_L u$. Let us verify that the axioms of involutive divisions hold:

(1) $u\big|_L v \implies \exists s : \; u \in C_s, \, u\big|_{Ls} v \implies u|v$
(2) $1\big|_L u$, by the definition of $\big|_L$
(3) $u\big|_L w, \, v\big|_L w \implies \exists s_1, s_2 : \; u, w \in C_{s_1}, \, v, w \in C_{s_2}$, however, then $C_{s_1} \cap C_{s_2} \neq \emptyset$, hence, $s_1 = s_2 =: s$. Therefore, $u\big|_{Ls} w, \, v\big|_{Ls} w \implies u\big|_{Ls} v \vee v\big|_{Ls} u \implies u\big|_L v \vee v\big|_L u$
(4) $u\big|_L uvw \implies \exists s : \; u\big|_{Ls} uvw \implies u\big|_{Ls} uv \wedge u\big|_{Ls} uw \implies u\big|_L uv \wedge u\big|_L uw \implies \exists s : \; u, uv, uw \in C_s, \, u\big|_{Ls} uv \wedge u\big|_{Ls} uw \implies u\big|_{Ls} uvw \implies u\big|_L uvw$
(5) $u\big|_L v, \, v\big|_L w \implies \exists s : \; u, v, w \in C_s, \, u\big|_{Ls} v, \, v\big|_{Ls} w \implies u\big|_{Ls} w \implies u\big|_L w$

By the definition of $\big|_L$, any leading monomial of a polynomial from the ideal is involutively reducible to the vertex of the corresponding cone, moreover, the involutive normal form is always unique. The normal simplificator defined by these cones is constructed in the same

way. Therefore, the correspondence of the normal simplificator to the involutive division is established. □

References

[1] Mikhalev, A.V., Pankratiev, E.V., *Computer Algebra. Computations in differential and difference modules*, (in Russian), Moscow, Moscow Univer. Press, 1989.

[2] Becker, T., Weispfenning, V., Kredel, H., *Gröbner Bases. A Computational Approach to Commutative Algebra*. Graduate Texts in Mathematics **141**, Springer-Verlag, New York, 1993.

[3] Buchberger, B., *Ein Algorithmus zum Zufinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. Thesis, Univ. Innsbruck, 1965

[4] Gerdt, V.P., Blinkov, Y.A., *Minimal Involutive Bases*, Preprint JINR E5-97-4, Dubna, 1997.

[5] Möller, H.M., Mora, F., New constructive methods in classical ideal theory. *J. Algebra* **100** (1986), 138–178.

[6] Zharkov, A.Yu., Blinkov, Yu.A., Involutive Approach to Investigating Polynomial Systems. In: Proceedings of "SC 93", International IMACS Symposium on Symbolic Computation: New Trends and Developments (Lille, June 14–17, 1993). *Math. Comp. Simul.* **42** (1996), 323–332.