PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 97(111) (2015), 43–48 DOI: 10.2298/PIM141104001L

A NOTE ON MULTIVARIATE POLYNOMIAL DIVISION AND GRÖBNER BASES

Aleksandar T. Lipkovski and Samira Zeada

ABSTRACT. We first present purely combinatorial proofs of two facts: the well-known fact that a monomial ordering must be a well ordering, and the fact (obtained earlier by Buchberger, but not widely known) that the division procedure in the ring of multivariate polynomials over a field terminates even if the division term is not the leading term, but is freely chosen. The latter is then used to introduce a previously unnoted, seemingly weaker, criterion for an ideal basis to be Gröbner, and to suggest a new heuristic approach to Gröbner basis computations.

1. Introduction

The division algorithm for multivariate polynomials over fields has been introduced not so long ago, in connection with algorithmic and computational problems in these rings. It generalizes the univariate algorithm. There is no natural monomial ordering in the multivariate ring $K[x_1, x_2, \dots, x_n]$. Still, there are many possibilities to totally order monomials in n variables, such as lexicographic or degree-lexicographic orders. The multivariate division algorithm depends on the choice of this ordering.

In what follows, we use the standard multiindex notation for multivariate monomials $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} = x^i$, their coefficients $a_{i_1 i_2 \dots i_n} = a_i$ where $i = (i_1, i_2, \dots, i_n) \in \mathbb{N}_0^n$, and polynomials $f = \sum_{i \in \mathbb{N}_0^n} a_i x^i$. Denote $\operatorname{Supp}(f) = \{i \in \mathbb{N}_0^n \mid a_i \neq 0\} \subset \mathbb{N}_0^n$, support of the polynomial f. Then, $f = \sum_{i \in \operatorname{Supp}(f)} a_i x^i$. Note that monomial x^i is divisible by monomial x^j precisely when $i = j + k$ for some $k \in \mathbb{N}_0^n$, or, written in a different way, $i \in j + \mathbb{N}_0^n$. Here we use the standard semigroup structure of $\mathbb{N}_0^n$.

2. Monomial orderings

The ordering of the set of monomials is equivalent to the ordering of the set of exponents $\mathbb{N}_0^n$. As usual, the sign $\prec$ denotes the strict, nonreflexive ordering, while the corresponding reflexive ordering is denoted by $\preceq$.

2010 *Mathematics Subject Classification:* 13P10, 12Y05, 06A07.
Communicated by Žarko Mijajlović.

Definition 2.1. A *monomial ordering* $\preceq$ on $\mathbb{N}_0^n$ is a linear (or total) ordering on $\mathbb{N}_0^n$ such that it respects vector addition in $\mathbb{N}_0^n$ i.e., $i \preceq j \Rightarrow i + k \preceq j + k$ and such that $0 \preceq i$ for all $i \in \mathbb{N}_0^n$.

From these conditions it follows that $\preceq$ must be a well ordering. The proof of this fact is usually based on Hilbert's basis theorem or its weaker form, Dickson's lemma [**1**]. Here we give a simple combinatorial proof based on the idea suggested by Siniša Vrećica.

Proposition 2.1. *Let the ordering $\preceq$ on $\mathbb{N}_0^n$ satisfy the following properties:* 1) *it is a linear ordering;* 2) *it is additive in $\mathbb{N}_0^n$ i.e., $i \preceq j \Rightarrow i+k \preceq j+k$;* 3) $0 \preceq i$ *for all $i \in \mathbb{N}_0^n$. Then $\preceq$ is a well ordering.*

Proof. Conditions 2) and 3) clearly imply that $i \in j + \mathbb{N}_0^n \Rightarrow j \preceq i$ or equivalently, $i \prec j \Rightarrow i \notin j + \mathbb{N}_0^n$. Now, it is sufficient to prove that $\prec$ satisfies the descending chain condition (DCC for short). We shall use mathematical induction on n. The statement obviously holds for $n = 1$. Let

$$S : \cdots \prec i^{(k)} = \big(i_1^{(k)}, \ldots, i_n^{(k)}\big) \prec \cdots \prec i^{(1)} = \big(i_1^{(1)}, \ldots, i_n^{(1)}\big)$$

be a descending chain in $\mathbb{N}_0^n$. It would suffice to show that the set $S_1 = \big\{i \in S \mid i_1 < i_1^{(1)}\big\} \subset S$ is finite, since this can be applied to any coordinate $i_1, \ldots, i_n$ of i. Let $i'_1 = \max\{i_1 \mid i \in S_1\} < i_1^{(1)}$ be the biggest first coordinate of elements in S_1. and $i' \in S_1$ any point with this first coordinate. The interval subset $\{i \in S_1 \mid i' \prec i \prec i^{(1)}\} \subset S_1$ is finite. The hyperplane subset $S'_1 = \{i \in S_1 \mid i \prec i',\ i_1 = i'_1\} \subset S_1$ of all points in S_1 less (with respect to $\prec$) than i' and with the first coordinate i'_1 forms a DCC in $\mathbb{N}_0^{n-1}$. By induction hypothesis, S'_1 must be finite. Therefore, there can be only finitely many points in S_1 with the first coordinate i'_1 and there is the smallest one (with respect to $\prec$) $i^{(m)} \in S_1$. So, $i_1^{(m)} = i'_1 < i_1^{(1)}$ and $i \prec i^{(m)} \Rightarrow i_1 < i'_1$. Since the set of first coordinates $i_1 < i'_1$ is finite, by infinite descent reasoning one obtains that the set S_1 must be finite. $\square$

3. Multivariate reduction and division

First, let us recall the standard multivariate polynomial reduction and division. Choose the monomial ordering $\prec$ in $\mathbb{N}_0^n$ once for all. The multidegree of polynomial f is the n-tuple $\deg(f) := \max \operatorname{Supp}(f) \in \mathbb{N}_0^n$. The maximum is attained because $\operatorname{Supp}(f)$ is finite. If $\alpha = \deg(f)$, then f has a leading term $\operatorname{lt}(f) = a_\alpha x^\alpha$ with leading monomial $\operatorname{lm}(f) = x^\alpha$ and leading coefficient $\operatorname{lc}(f) = a_\alpha$. The standard division algorithm in the ring $K[x_1, \ldots, x_n]$ is performed in the following way (see [**1**] or [**2**]).

Let $f, g \in K[x_1, \ldots, x_n]$ be two polynomials, and suppose first that $\operatorname{lm}(f)$ is divisible by $\operatorname{lm}(g)$. This is equivalent to $\deg(f) \in \deg(g) + \mathbb{N}_0^n$ and implies that $\deg(g) \prec \deg(f)$. In this case, the leading terms of two polynomials f and $\frac{\operatorname{lt}(f)}{\operatorname{lt}(g)}g$ are identical, and polynomial $r = f - \frac{\operatorname{lt}(f)}{\operatorname{lt}(g)}g$ has smaller multidegree $\deg(r) \prec \deg(f)$. In such case, one says that f reduces to r modulo g, and this is denoted by $f \to_g r$. This is sometimes called a one-step reduction of f by g.

If the leading monomial $\mathrm{lm}(f)$ is not divisible by $\mathrm{lm}(g)$, then one takes the maximum of all terms which *are* divisible – the term corresponding to $\max\{i \in \mathrm{Supp}(f) \mid i = \deg(g)+k \text{ for some } k \in \mathbb{N}_0^n\}$. This process is continued until no term in r is divisible by $\mathrm{lm}(g)$. One says then that f completely reduces to r modulo g or that r is the remainder in the division algorithm $f = gh + r$. It is not difficult to prove that polynomials r and h are uniquely determined.

Since in $K[x_1, \dots, x_n]$ we have to deal with nonprincipal ideals, one needs division algorithm for an ordered m-tuple $(g_1, \dots, g_m)$ of polynomials rather than a single polynomial g. So, f is usually reduced using the left-most g_i with the property that $\mathrm{lt}(g_i)$ divides some term in the remainder. It is easy to see that this algorithm always terminates, but it is clear that the remainder r (the polynomial such that none of its terms is divisible by some of $\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_m)$) depends on the choice of order of polynomials $g_1, \dots, g_m$.

Now, introduce the support of f with respect to g

$$\begin{aligned}\mathrm{Supp}_g(f) &= \{i \in \mathrm{Supp}(f) \mid i = \deg(g) + k \text{ for some } k \in \mathbb{N}_0^n\}\\ &= \mathrm{Supp}(f) \cap (\deg(g) + \mathbb{N}_0^n)\end{aligned}$$

of multiindices of all monomials in f divisible by $\mathrm{lt}(g)$. The standard algorithm described above takes for the next division step the maximal divisible term in f, which corresponds to the multiindex $\max \mathrm{Supp}_g(f)$. Clearly, r is the remainder in the division algorithm $f = gh + r \Leftrightarrow \mathrm{Supp}_g(r) = \emptyset$. It is not obvious whether the algorithm would stop if, instead of always choosing the maximal index in the set $\mathrm{Supp}_g(f)$, one chooses an arbitrary one. This is because after reducing f modulo g_1 and then modulo g_2, it is possible that some terms divisible by $\mathrm{lt}(g_1)$, which were previously eliminated, reappear. Therefore, it is natural to ask whether *any* reduction process modulo a given m-tuple $(g_1, \dots, g_m)$, with arbitrary choice of division term in each step would terminate? For a set of m polynomials $G = \{g_1, \dots, g_m\}$ let us introduce $\mathrm{Supp}_G(f) = \mathrm{Supp}_g(f) \cup \dots \cup \mathrm{Supp}_g(f)$.

THEOREM 3.1. *Let $f \in K[x_1, \dots, x_n]$ and $G = \{g_1, \dots, g_m\}$ a set of m polynomials, $g_i \in K[x_1, \dots, x_n]$. Then, any reduction process (with arbitrary choice of the next reduction term in* $\mathrm{Supp}_{g_{i_j}}(f_{j-1})$*)*

$$f \to_{g_{i_1}} f_1 \to_{g_{i_2}} f_2 \to \cdots$$

with $g_{i_k} \in G$ must terminate in finitely many steps. This means that there exists k such that f_k does not contain a term divisible by any of the $\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_m)$.

PROOF. Let $m_j = \max \mathrm{Supp}_{g_{i_{j+1}}}(f_j)$ and let r_j be the index used for reduction by $g_{i_{j+1}}$ ($j = 0, 1, 2, \dots,\ f_0 := f$). Clearly, $r_j \in \mathrm{Supp}_{g_{i_{j+1}}}(f_j)$ and $r_j \leqslant m_j$. It is easy to see that $m_0 \geqslant m_1 \geqslant \cdots$. According to DCC, from some point on $m_{k_1} = m_{k_1+1} = \cdots$. Let $m_{k_1}^{(1)} = \max\bigl[\mathrm{Supp}_{g_{i_{k_1+1}}}(f_{k_1}) \setminus \{m_{k_1}\}\bigr] < m_{k_1}$. Clearly, $r_{k_1} \leqslant m_{k_1}^{(1)} < m_{k_1}$. Repeat the process for the sequence $m_{k_1}^{(1)} \geqslant m_{k_1+1}^{(1)} \geqslant \cdots$. In this way we obtain a sequence of indices $m_{k_1}^{(1)} \geqslant m_{k_2}^{(2)} \geqslant \cdots$. Again, according to DCC, this sequence must be stationary from some point on $m_{k_p}^{(p)} = m_{k_{p+1}}^{(p+1)} = \cdots$, which means that from that point on, $\mathrm{Supp}_{g_{i_p}}(f_{p-1}) = \emptyset$ and the reduction process terminates. $\square$

So, no matter how we choose the next term in the division algorithm (in the set of all possible terms), the algorithm will stop in finitely many steps. The polynomial f_k obtained in this way is then the remainder of the particular reduction process. As we have already noted, the remainder depends on the order in which the reductions are performed.

4. Ordered sets and multivariate division

The fact that in the reduction process, one can arbitrarily choose the term for the next reduction in the set $\mathrm{Supp}_G(f)$ was known to Buchberger (see [**3**, p. 14]). However, it was not widely used and even not mentioned in the standard textbooks. Buchberger's argument in [**3**] involves extension of a given monomial order to a partial order on the set of all polynomials. This order seems somehow unnatural. It is not total because the coefficients are also taken into account. However, we have already seen that it is not necessary to speak about monomials and polynomials, but about underlying monomial orders on the exponent set $\mathbb{N}_0^n$ $(= \mathbb{Z}_+^n)$ instead. When we took a closer look, we discovered more natural, underlying combinatorial fact about total orders, which actually belongs to set theory.

Recall that a set X together with binary partial order relation $\leqslant$ (reflexive, antisymmetric and transitive) is called (partially) ordered set. Ordered set $(X, \leqslant)$ is totally ordered if for any two elements $x, y \in X$ either $x \leqslant y$ or $y \leqslant x$. Recall the following trivial fact.

LEMMA 4.1. *Let $(X, \leqslant)$ be totally ordered and $A \subset X$ its nonempty finite subset. Then the minimal element* $\min A$ *and the maximal element* $\max A$ *of A exist and are unique. Actually, the elements in A are ordered in a unique way.*

Ordered set $(X, \leqslant)$ is well ordered if every nonempty subset has a least element. A well-ordered set is totally ordered. We now come to the set-theoretic essence of the division algorithm in the multivariate polynomial ring, Buchberger's polynomial order and Buchberger's proof.

Let $(X, \leqslant)$ be a well-ordered set and $\mathcal{F}$ the family of all its (nonempty) finite subsets. Consider the following binary relation on $\mathcal{F}$

$$A < B \Leftrightarrow \max(A \,\Delta\, B) \in B.$$

Here, $A \,\Delta\, B = (A \setminus B) \cup (B \setminus A)$ is a common symmetric difference of two sets. It is easy to see that this definition is equivalent to the following:

$$\begin{aligned} A < B \Leftrightarrow\ & \text{there exists } b \in B \setminus A \text{ such that the strict upper} \\ & \text{intervals } A_{>b} \text{ and } B_{>b} \text{ are either empty or coincide.} \end{aligned}$$

Here, $A_{>b} = \{x \in A \mid x > b\}$ is the upper interval of b in A. Clearly, such element must be unique.

THEOREM 4.1. *With respect to this (strict) order $<$, the set $\mathcal{F}$ is well ordered.*

PROOF. (1) It is easy to see that this is an order on $\mathcal{F}$. Reflexivity is obtained in the usual way by reflexive completion of the given strict order $A \leqslant B \Leftrightarrow (A < B) \vee (A = B)$. Antisymmetry is obvious, since $A < B$ and $B < A$ leads to a contradiction. Now, let $A < B$ and $B < C$, and let $b = \max(A \,\Delta\, B) \in B$ and $c = \max(B \,\Delta\, C) \in C$. Then $c \notin B$ and therefore $c \neq b$. There are two possibilities: either $b < c$ or $b > c$. In the first case, $c \notin A$ and $\max(A \,\Delta\, C) = c$. In the second case, $b \in C$ and $\max(A \,\Delta\, C) = b$. This proves transitivity. This is a total order since the maximal element in $A \,\Delta\, B \neq \emptyset$ has to be either in A or in B.

(2) Now, let us prove that this is a well order i.e., it satisfies the DCC. Let $A_1 > A_2 > \cdots > A_n > \cdots$ be a strictly descending chain in $\mathcal{F}$. For $n \in \mathbb{N}$, define two sequences in X,

$$a_n = \max(A_n \smallsetminus A_{n+1}) \in A_n \quad \text{and} \quad p_n = \max\{a_1, \ldots, a_n\}.$$

The last sequence is actually an ascending chain

$$p_1 \leqslant p_2 \leqslant \ldots \leqslant p_n \leqslant \cdots .$$

Now notice that if there is a strict jump in the sequence i.e., if $p_n > p_{n-1}$, then $p_n = a_n \in A_i$ for all $i \leqslant n$. But A_1 is finite, so the number of strict jumps is also finite, and the chain must be stationary. Let $p^{(1)}$ be its stationary value: $p_m = p_{m+1} = \cdots = p^{(1)}$, which means that from that point on all subsets $A_{m+i} \cap \big\{x \in X \mid x \geqslant p^{(1)}\big\} = S \subset A_{m+i}$ coincide for all $i \geqslant 1$.

The following easy fact will be used without proof.

LEMMA 4.2 ("cut-off"). *Let $A < B$, $\max(A \,\Delta\, B) = b \in B \smallsetminus A$, and $S \subset A \cap B$. Denote $A^{(1)} = A \smallsetminus S$ and $B^{(1)} = B \smallsetminus S$. Then $A^{(1)} < B^{(1)}$ and $\max\big(A^{(1)} \Delta\, B^{(1)}\big) = b$.*

Let $A_i^{(1)} = A_{m+i} \cap \big\{x \in X \mid x < p^{(1)}\big\} \subset A_{m+i}$ (we "cut-off" the set S i.e., all elements in the original chain which are $\geqslant p^{(1)}$). If $A_1^{(1)} \neq \emptyset$, then $A_i^{(1)}$ also form a strictly descending chain of finite sets

$$A_1^{(1)} > A_2^{(1)} > \cdots > A_n^{(1)} > \cdots .$$

such that all corresponding maxima coincide: $a_i^{(1)} = a_{m+i}$. Now apply the same construction to this chain and obtain the stationary value $p^{(2)} < p^{(1)}$. In this way, we obtain a strictly descending chain

$$p^{(1)} > p^{(2)} > \cdots > p^{(k)}$$

in X which eventually must stop since X is well ordered. This means that at this point $A_1^{(k)} = \emptyset$, the construction can not be continued and the original sequence must be finite. This proves the theorem. $\square$

If we now apply this theorem to the sequence of finite sets of exponents of polynomials in the division algorithm, we obtain the previous theorem: the fact that in the reduction process, one can arbitrarily choose the term for the next reduction in the set $\mathrm{Supp}_G(f)$. This leads to a conclusion that for certain special classes of polynomials, one could try to find heuristics which could improve the calculation speed of a Gröbner basis. This remark could open a quite new and broad area of research.

5. Application to Gröbner bases

As an illustration of free choice in the reduction process, we will apply it in order to obtain a new equivalent characterisation of Gröbner basis. One of the standard definitions of a Gröbner basis of an ideal is the following (see [**1**]).

DEFINITION 5.1. The basis $G = \{g_1, \ldots, g_m\}$ of an ideal $(g_1, \ldots, g_m) = I \subset K[x_1, \ldots, x_n]$ is called a *Gröbner basis*, if the leading term $\mathrm{lt}(f)$ of any $f \in I$ is divisible by some of the leading terms $\mathrm{lt}(g_1), \ldots \mathrm{lt}(g_m)$.

Its nice properties, such as the uniqueness of the reduced Gröbner basis of a given ideal and the uniqueness of the remainder obtained by complete reduction process with respect to Gröbner basis, are widely used for algorithmic and calculational purposes. Using the above theorem, this standard definition of Gröbner basis could be slightly relaxed, as the following statement in (3) shows. Recall that the syzygy in (6) below is the polynomial

$$S(g, h) := \frac{\mathrm{lcm}(\mathrm{lt}(g), \mathrm{lt}(h))}{\mathrm{lt}(g)} \cdot g - \frac{\mathrm{lcm}(\mathrm{lt}(g), \mathrm{lt}(h))}{\mathrm{lt}(h)} \cdot h.$$

THEOREM 5.1. *Let $I = (g_1, \ldots, g_m) \subset K[x_1, \ldots, x_n]$ be the ideal generated by the set $G = \{g_1, \ldots, g_m\}$. The following conditions are equivalent.*

(1) *$G = \{g_1, \ldots, g_m\}$ is a Gröbner basis;*
(2) *For all nonzero $f \in I$, $\mathrm{lt}(f) \in \mathrm{Supp}_G(f)$;*
(3) *For all nonzero $f \in I$, $\mathrm{Supp}_G(f) \neq \emptyset$;*
(4) *The remainder h of a complete reduction process $f \to_G h$ with $\mathrm{Supp}_G(h) = \emptyset$ is uniquely determined;*
(5) *For all $f \in I$, $f \to_G 0$;*
(6) *All syzygies $S(g_i, g_j) \to_G 0$*

PROOF. Equivalences (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) $\Leftrightarrow$ (6) are standard (see [**1**] or [**2**]) and are stated here just for reasons of completeness. The proof is required only for the new equivalent condition (3). Obviously, (2) $\Rightarrow$ (3). Suppose that (3) holds and let $f \to_G h_1$ and $f \to_G h_2$. Then $h_1 - h_2 \in I$ and $\mathrm{Supp}_G(h_1 - h_2) = \emptyset$ which contradicts (3). Therefore, (3) $\Rightarrow$ (4) is proved. $\square$

References

1. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997
2. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Grad. Stud. Math. 3, American Mathematical Society, 1994
3. B. Buchberger, *Introduction to Gröbner bases*; in: B. Buchberger, F. Winkler (editors), *Gröbner Bases and Applications*, London Math. Soc. Lect. Notes 251, Cambridge Univ. Press, 1998, pp. 3–31

Matematički fakultet
Univerzitet u Beogradu
Beograd
Serbia
acal@matf.bg.ac.rs

(Received 15 08 2014)