Some bounds for the construction of Gröbner bases

Volker Weispfenning
Mathematisches Institut der Universität
D-6900 Heidelberg, FRG

Abstract. Let $R = K[X_1, \ldots, X_n]$ be a polynomial ring over a field. For any finite subset $F$ of $R$, we put $m = |F|$, $d = \max(\deg(f) : f \in F)$, and we let $s$ be the maximal size of the coefficients of all $f \in F$. $G = GB(F)$ denotes the unique reduced Gröbner basis for the ideal $(F)$ (see [B3]). We show that the number $m' = |G|$ of polynomials in $G$ and their maximal degree $d'$ as well as the length of the computation of $G$ from $F$ (with unit cost operations in $K$) are bounded recursively in $(n, m, d)$. The same applies to the degrees of the polynomials occurring during the computation. Moreover, for fixed $(n, m, d)$, $G$ can be computed from $F$ in polynomial time and linear space, when the operations of $K$ can be performed in polynomial time and linear space; in addition, the vector space dimension of the residue ring $R/(F)$ is computably stable under variation of the coefficients of polynomials in $F$. Corresponding facts hold for polynomial rings over commutative regular rings (see [We']) and non-commutative polynomial rings of solvable type over fields (see [KRW]). Our method does not apply to polynomial rings over $\mathbb{Z}$ or other Euclidean rings; in fact, we show that over $\mathbb{Z}$, the length of the computation of $G$ from $F$ with unit cost operations in $\mathbb{Z}$ does depend on $s$.

Introduction. The success of Buchberger's method for computing Gröbner bases in the algorithmic theory of polynomial ideals has aroused a strong interest in the complexity of the method (see [B1], [Gi], [Gi'], [Hu], [La], [MaMe], [MM], [Wi]): Most of the results concern upper bounds on the degrees of the polynomials in a reduced Gröbner basis for the case of two variables ([B1], [Gi'], [La]), three variables ([Wi], [MM]), or special assumptions on the ideals considered ([Gi'], [La], [MM]); [Gi] provides a bound on these degrees for arbitrary homogeneous polynomials. In [B1], [Wi] these bounds concern also all polynomials arising during the Gröbner basis calculation. [B1] provides in addition a tight bound for the number of polynomials in a reduced Gröbner basis for the bivariate case. Worst case lower bounds are obtained in [MaMe], [B1], [MM], [Hu].

Let $K$ be an arbitrary field, let $R$ be the polynomial ring $K[X_1, \ldots, X_n]$, let $<$ be an admissible linear ordering of the set $T$ of terms in $R$ and let $F$ be a set of $m$ polynomials of total degree at most $d$ in $R$. $G = GB(F)$ denotes the unique reduced Gröbner basis for the ideal $I = (F)$ generated by $F$ in $R$ (see [B3]). We assume that the elements $a$ of $K$ are presented as words over a fixed finite alphabet in such a way that the field operations in $K$ and tests ($a = 0$) can be performed in polynomial time and linear space. (This assumption is satisfied in most of the fields studied in computer algebra.) We let $s(a)$ denote the size of $a$, i.e. the length of a word representing the field element $a$.

In this note, we show that the following items are bounded by functions of $n, m, d$: The number $|G|$ of polynomials in $G$, the maximal degree of all polynomials occurring in a computation of $G$ from $F$, and the number of steps required for such a computation, when the field operations in $K$ cost unit time. The bounds are independent of the field $K$. From the proof presented here, they seem to depend on the choice of the admissible ordering $<$ of $T$; in fact, however, this dependence can be eliminated by an application of König's tree lemma. This and further consequences of our method will be presented in [We'']. We have no explicit description of the bounds; their existence is proved by an application of the compactness theorem of first-order logic (see [Ke]). Nevertheless, we can show (using the decidability of the theory of algebraically closed fields) that
the bounds depend recursively on \( n, m, d \). Moreover, we find that for fixed \( n, m, d \), the size \( s(G) \) of the coefficients of the polynomials in \( G \) is linear in the corresponding coefficient size \( s(F) \) for \( F \), and that \( G \) can be computed from \( F \) in polynomial time and linear space, when the field operations in \( K \) can be performed in polynomial time and linear space. The same applies to the finitely many vector space dimensions of \( R/(F) \) obtainable by varying the coefficients of the polynomials in \( F \). In addition, these dimensions are completely determined by the zeroes of a finite computable system of polynomials.

The crux of the argument is the fact that the single steps in the computation of \( G \) can be coded by first-order formulas in \( K \), and that the class of fields is axiomatized by first-order axioms. Thus corresponding results are valid in related situations, including polynomial rings over commutative regular rings (see [We']) and non-commutative polynomial rings of solvable type over fields (see [KRW]). The method fails for polynomial rings over the integers (see [B2] and the references given there), and more generally for polynomial rings over Euclidean rings (see [KRK]). Here, the termination of the algorithm depends not only on Dickson's lemma, but also on the termination of the Euclidean algorithm in the ground ring, which may fail in non-standard models of this ring. In fact, we prove that over the ground ring \( \mathbb{Z} \) of integers, the length of the computation of \( G \) from \( F \) does depend on \( s(F) \), even if the ring cost only unit time.

I am indebted to R. Looij, who made me aware of the questions studied in this note.

1. CODING GRÖBNER BASIS CONSTRUCTIONS IN FIELD THEORY

We consider formulas of the elementary theory of fields. They are obtained inductively from equations

\[ f(x_1, \ldots, x_m) = g(x_1, \ldots, x_m), \]

where \( f, g \) are polynomials with integer coefficients in some variables \( x_i \), by means of \( \neg \) (negation), \( \land \) (conjunction), \( \lor \) (disjunction), and quantification \( \exists x \forall x \) over some variables. A formula is quantifier-free \((q.f.)\) if it contains no quantifier \( \exists x \forall x \).

Our goal is to express the construction of a reduced Gröbner basis \( G \) from a given ideal basis \( F \) (see [B3]) by q.f. formulas, provided this construction is bounded in 'size' in a suitable way.

Let \( n, m, d \) be positive integers, let \( K \) be a field, \( R = K[X_1, \ldots, X_n] \) a polynomial ring over \( K \), \( T \) the set of terms \((\text{power-products of the } X_i)\) in \( R \), and let \( < \) be an admissible ordering of \( T \). Then any polynomial \( f \in R \) of (total) degree \( \leq d \) can be recovered uniquely from its sequence \( c = c(f) = (c_1, \ldots, c_s) \) of coefficients. \( c \) is the coefficient vector of the head-term of \( f \). (We regard \( f \) as polynomial of formal degree \( d \) in dense representation, adding zero coefficients as necessary; the coefficients are ordered in the decreasing order of their associated terms. So \( s = \binom{d+n}{n} \), and \( c_i \) is the coefficient of the head-term of \( f_i \) of \( F \), provided \( c_i \neq 0 \).)

A sequence \( F = (f_1, \ldots, f_m) \) of polynomials in \( R \) of degrees \( \leq d \) can then be recovered from \( d \) and the concatenated sequence \( c(F) = c(f_1) * \ldots * c(f_m) \).

Let us now consider a computation leading from a finite sequence \( F \) of polynomials in \( R \) to a reduced Gröbner basis \( G = GB(F) \) for the ideal \( I = (F) \) generated by \( F \) in \( R \). Disregarding the control structure of the computation, we may view it as a finite sequence \( F = F_0 \mapsto F_1 \mapsto \ldots \mapsto F_s = G \) of finite sequences \( F \) of polynomials in \( R \) such that each \( F' = F_{k+1} \) is obtained from its predecessor \( H = F_k \) by one of the following steps \( S_1, \ldots, S_4 \):

\[(S_1) \quad H' = (f_1, \ldots, f_m, h), \text{ where } h = S\text{Pol}(f_i, f_j), 1 \leq i < j \leq m, \text{ is the S-polynomial of two members of } H.\]

\[(S_2) \quad H' = (f_1, \ldots, f_{i-1}, f_i', f_{i+1}, \ldots, f_m), \text{ where } f_i, 1 \leq i \leq m, \text{ is a member of } H, \text{ and } f_i' \text{ is obtained from } f_i \text{ by a 1-step reduction using the polynomials } \{f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m\}.\]