TUM

INSTITUT FÜR INFORMATIK

Exponential space computation of Gröbner bases

Klaus Kühnle
Ernst W. Mayr

TUM-I9606
Januar 1996

TECHNISCHE UNIVERSITÄT MÜNCHEN

TUM-INFO-01-1996-I9606-350/1.-FI

Alle Rechte vorbehalten
Nachdruck auch auszugsweise verboten

©1996 MATHEMATISCHES INSTITUT UND
INSTITUT FÜR INFORMATIK
TECHNISCHE UNIVERSITÄT MÜNCHEN

Typescript: ---

Druck: Mathematisches Institut und
Institut für Informatik der
Technischen Universität München

Exponential space computation of Gröbner bases

Klaus Kühnle Ernst W. Mayr

16th January 1996

Abstract

Given a polynomial ideal and a term order, there is a unique reduced Gröbner basis and, for each polynomial, a unique normal form, namely the smallest (w.r.t. the term order) polynomial in the same coset. We consider the problem of finding this normal form for any given polynomial, without prior computation of the Gröbner basis. This is done by transforming a representation of the normal form into a system of linear equations and solving this system. Using the ability to find normal forms, we show how to obtain the Gröbner basis in exponential space.

1 Introduction

Let us first fix some of the notation used in the remainder of this paper. Let $\mathbb{Q}[x_1, \ldots, x_n]$ be the polynomial ring in the indeterminates $x_1, \ldots, x_n$ over the rationals. Let T be the set of terms or power products in these indeterminates and let $\prec$ be some term order on T. We will consider an ideal I in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ that is generated by s polynomials $f_1, \ldots, f_s$. With respect to this ideal I and the term order $\prec$ we then have, for any polynomial h, a unique normal form, denoted by $\mathrm{NF}(h)$, with the following defining property: $\mathrm{NF}(h)$ is the smallest, w.r.t. the term order, monic polynomial in the I-coset of h. In other words: $\mathrm{NF}(h)$ is the outcome of a complete reduction of h w.r.t. the Gröbner basis for I and $\prec$. (Of course, $\mathrm{NF}(h)$ depends on the ideal I and the term order $\prec$, which we disregard in our notation, since there will be no ambiguity.)

This paper presents an algorithm for finding the normal form of a given polynomial h and for computing the unique reduced Gröbner basis for a given ideal, both requiring exponential space. It is structured as follows: First, we fix a way to represent the term order, allowing us to talk about its representation size and to bound the length of a reduction w.r.t. a Gröbner basis in terms of the size of the representation of the term order; this will yield a bound on the degree of the normal form of h. As a consequence, it is possible to bound the degrees of the coefficients of a representation of $h - \mathrm{NF}(h)$ as a linear combination of the given generators $f_1, \ldots, f_s$ and to transform this representation into a system of linear equations over the scalar field $\mathbb{Q}$, whose solution is just the vector of coefficients of the normal form of h. We will solve this system of linear equations efficiently and thus obtain the normal form of h. Using the calculation of normal forms as a subroutine, we will compute the Gröbner basis of the given ideal by enumerating all terms up to the known bound on the degree of the Gröbner basis and calculating their normal forms. If a term is not irreducible (i.e. is not equal to its normal form) but all its divisors are, then we will add the difference of this term and its normal form to the Gröbner basis.

2 A bound on the degree of normal forms

A term order $\prec$ on the set T of all terms of $\mathbb{Q}[x_1, \ldots, x_n]$ is defined by the properties $\forall t \in T : 1 \prec t$ and $\forall t, u, v \in T : u \prec v \Rightarrow tu \prec tv$. Robbiano showed in [Rob85] that any such term order can be represented by at most n weight functions $W_1, \ldots, W_n$ mapping from the set of terms into the set of real numbers as follows: Let $u = {x_1}^{u_1} {x_2}^{u_2} \ldots {x_n}^{u_n}$ be a term; then

$$W_k(u) := \sum_{i=1}^{n} w_{k,i} u_i$$

where $w_{k,i}$ are real numbers, specifying the term order. A term u is greater than another term v in this term order if

$$\exists k : W_k(u) > W_k(v) \wedge \forall j > k : W_j(u) = W_j(v)$$

A constructive proof of this was given by Dubé, Mishra and Yap in [DMY86]; they also show that the weights $w_{k,i}$ can be assumed to be nonnegative.

Since it is not easy to represent numbers in such a way that all reals are finitely describable, we will restrict ourselves to term orders that are representable by weight functions with rational weights. This is a proper restriction, i.e. there are term orders that cannot be represented with rational weights; however, every term order can be arbitrarily tightly approximated with rational weights in the following sense: Given a term order and a natural number, there is a term order representable with rational weights that agrees with the given term order on all terms whose degrees are bounded by the given number.

Let the weights $w_{k,i}$ be given as fractions $\frac{a_{k,i}}{b_{k,i}}$ where $a_{k,i}$ and $b_{k,i}$ are natural numbers. Let A be the maximum of all the $a_{k,i}$ and $b_{k,i}$. Note that $\max_k(\operatorname{lcm}_i(b_{k,i}))$ is bounded by nA.

We are going to recall parts of [DMY86]: We combine the characterizing weight functions W_i to a single weight function W by simulating their lexicographic interrelation by means of a combination of them reminiscent of the B-adic representation of numbers:

$$W(u) = \sum_{i=1}^{n} B^{i-1} W_i(u)$$

For any given set of terms, it is possible to choose B large enough, so that W will properly represent the term order on these terms, i.e. $W(u) < W(v)$ if and only if $u \prec v$. We will now find an appropriate value for B.

Let d be a bound on the degrees of the generating polynomials $f_1, \ldots, f_s$ of the ideal I. Dubé showed in [Dub90] the existence of a Gröbner basis G for I where the degrees of all polynomials in G are bounded by $2(\frac{d^2}{2}+d)^{2^{n-1}}$ (remember that n was the number of indeterminates in the polynomial ring). Hence, the maximal weight of any term occurring in a polynomial in G is bounded by $2A(\frac{d^2}{2}+d)^{2^{n-1}}$. The minimal difference between the weights of two terms is at least $\frac{1}{nA}$, because this difference must be an integer if multiplied by the lcm of the denominators of the weights. Setting $B := 2nA^2(\frac{d^2}{2}+d)^{2^{n-1}}$ in the definition

$$W(u) = \sum_{i=1}^{n} B^{i-1} W_i(u)$$

of the unified weight function therefore guarantees that W will properly represent the term order on G.

Though we do not know any Gröbner basis as yet, we consider the process of reducing h w.r.t. G according to Buchberger's algorithm ([Buc65]). In such a reduction, a step consists of deleting some monomial in the current polynomial by subtracting a suitable multiple of a suitable polynomial of the Gröbner basis in such a way that the largest monomial of the multiple of the Gröbner basis element and the monomial chosen for deletion cancel out. Here, we always choose the largest possible monomial for deletion; this strategy implies that the monomials that are deleted during the reduction process strictly decrease w.r.t. the term order. We want to bound the degrees and therefore the number of these monomials in order to get a bound on the length (i.e. the number of steps) of the reduction.

The fact that the unified weight function W represents the term order on G immediately implies that in any reduction step, the weights of the monomials that are inserted into the polynomial are strictly smaller than the weight of the monomial that is deleted. Hence, the weight of a polynomial, defined to be the maximal weight of its monomials, will not increase in any step of the reduction w.r.t. G. The weight of h is therefore a bound on the weights of all monomials that are deleted during the reduction of h. These monomials are all distinct; consequently, the number of them and with it the length of the reduction is bounded by the number of monomials whose weights are at most as large as the weight of h.

Let u be the monomial of h with maximal weight. Then

$$\begin{aligned} W(u) &= \sum_{i=1}^{n} B^{i-1} W_i(u) \\ &\leq \sum_{i=0}^{n-1} B^{i} A \deg(u) \\ &\leq \frac{B^n - 1}{B-1} A \deg(h) \\ &\leq B^n A \deg(h) \end{aligned}$$

Since the weight of any monomial is at least $\frac{1}{A}$, we have $B^n A^2 \deg(h)$ as a bound on the degrees of all those monomials whose weights do not exceed the weight of h. The number of these monomials and with it the length of the reduction of h is therefore bounded by $(B^n A^2 \deg(h))^n = ((2nA^2(\frac{d^2}{2}+d)^{2^{n-1}})^n A^2 \deg(h))^n$.

In every reduction step, the degree of the polynomial to be reduced increases by at most the maximal degree of the polynomials in the Gröbner basis. The product of this maximal degree and the number of reduction steps is clearly a bound on the increase of the degree of h during its reduction. Thus, we have as the result of this section:

Proposition: In $\mathbb{Q}[x_1,\ldots,x_n]$, let a polynomial ideal I be given by generators whose degrees are bounded by d and let a term order be given by n weight functions with rational weights, as described at the beginning of this section, where the numerators and denominators of the weights are bounded by A. Then the degree of the unique normal form of a given polynomial h w.r.t. the given ideal and term order is bounded by $((2n(\frac{d^2}{2}+d)^{2^{n-1}})^n A^{2n} \deg(h))^{n+1} =: N$.

3 Reducing the membership problem to a matrix equation

We will now exploit the upper bound on the degrees of normal forms for actually finding them. The difference of h and its normal form is certainly in the ideal and thus representable as a linear combination of the generators (note that we take the original ideal basis rather than the Gröbner basis G, whose existence we only used for bounding the degree of the normal form). Hermann showed in [Her26] that there is a representation

$$h - \mathrm{NF}(h) = \sum_{i=1}^{s} f_i c_i$$

where the degrees of the coefficients c_i are bounded by $D := \deg(h - \mathrm{NF}(h)) + (sd)^{2^n} \le N + (sd)^{2^n}$ (remember that d was the bound on the degrees of the f_i and N the bound on the degree of $\mathrm{NF}(h)$ developed in the last section).

Expanding all polynomials to sums of monomials, i.e. the ideal generators to $f_i = \sum\{f_{i,t}t \mid t \in T \wedge \deg(t) \le d\}$, the unknowns to $c_i = \sum\{c_{i,t}t \mid t \in T \wedge \deg(t) \le D\}$ and, finally, $\mathrm{NF}(h) = \sum\{y_t t \mid t \in T \wedge \deg(t) \le N\}$, we get

$$\begin{aligned} h &= \mathrm{NF}(h) + \sum_{i=1}^{s} f_i c_i \\ &= \sum_{\substack{t\in T\\ \deg(t)\le N}} y_t t + \sum_{i=1}^{s} \left(\sum_{\substack{t\in T\\ \deg(t)\le d}} f_{i,t} t \right) \left(\sum_{\substack{t\in T\\ \deg(t)\le D}} c_{i,t} t \right) \end{aligned}$$

$$= \sum_{\substack{t\in T\\ \deg(t)\le N}} y_t t + \sum_{i=1}^{s} \sum_{\substack{t\in T\\ \deg(t)\le d+D}} \left(\sum_{\substack{u,v\in T\\ uv=t}} f_{i,u} c_{i,v} \right) t$$

$$= \sum_{\substack{t\in T\\ \deg(t)\le N}} y_t t + \sum_{\substack{t\in T\\ \deg(t)\le d+D}} \left(\sum_{i=1}^{s} \sum_{\substack{u,v\in T\\ uv=t}} f_{i,u} c_{i,v} \right) t$$

If we also expand h to $h = \sum\{h_t t \mid t \in T \wedge \deg(t) \le \deg(h)\}$ and compare coefficients in our polynomial equation, we get, for every term t involved, an equation in $\mathbb{Q}$ of the form

$$h_t = y_t + \sum_{i=1}^{s} \sum_{\substack{u,v\in T\\ uv=t}} f_{i,u} c_{i,v}$$

where we assume all coefficients with too high an index to be zero.

The bound on the degrees of the terms involved in the polynomial equation was $\max(N, d+D)$, therefore we get at most $(\max(N, d+D))^n$ equations in $\mathbb{Q}$. We can write all these equations as a single matrix equation by forming a vector H of the coefficients of h, a vector C of unknowns consisting of the y_t and the $c_{i,t}$ and a matrix $\mathcal{F}$ whose entries are the coefficients $f_{i,t}$ of the generating polynomials f_i (the same coefficient may occur quite often in this matrix), some 1's and a lot of 0's. The matrix equation is then just

$$H = \mathcal{F} C$$

This matrix equation is a direct translation of the above polynomial equation, so the solutions are just the vectors of coefficients y_t of polynomials y in the coset of h whose degrees do not exceed N and the corresponding coefficients $c_{i,t}$ of representations of $h - y$ as linear combinations of the f_i. The solution we are aiming for is one with minimal y w.r.t. the term order.

We already mentioned that the number of equations or the number of rows of $\mathcal{F}$ is bounded by $(\max(N, d+D))^n$. Now we will bound the number of columns of $\mathcal{F}$ or the number of unknowns in the vector C. We get N^n unknowns y_t from $\mathrm{NF}(h)$ and D^n unknowns $c_{i,t}$ from every c_i, hence there are altogether $N^n + sD^n$ unknowns. The format of the matrix, i.e. the maximum of its height and width, is therefore bounded by $N^n + s(d+D)^n =: M$.

For the calculation of $\mathcal{F}$, we have to determine the places in $\mathcal{F}$ where the coefficients of the generating polynomials f_i go. The entry in the matrix $\mathcal{F}$ in the row corresponding to the term t and the column corresponding to the unknown y_u is one if and only if $u = t$ and zero otherwise. The entry in the matrix $\mathcal{F}$ in the row corresponding to the term t and the column corresponding to the unknown $c_{i,u}$ is the coefficient $f_{i,\frac{t}{u}}$ if t is divisible by u and zero otherwise. So, the required coefficient is determined by computing the place where to look it up in the table containing the coefficients of the f_i. The space required for that is the space needed for the division of a term by another one; such a division is merely a subtraction of the corresponding exponent vectors. Hence, the space requirement is essentially that for writing down two terms. The degrees of the terms involved are bounded by $\max(N, d+D)$, so the space needed is at most $2n(\log\max(N, d+D)+1)$.

The space for writing down the entire matrix is far too large, therefore we do not determine the matrix in advance but compute each entry when it is needed during the further treatment of $\mathcal{F}$.

4 Finding the normal form

Now we are going to find a solution to the matrix equation $H = \mathcal{F}C$ where the polynomial $y = \sum_t y_t t$ built from the entries of the solution vector is minimal w.r.t. the term order. It is clear that this y is the normal form of h we are looking for.

As an intermediate step, we want to have a maximal regular minor $\mathcal{F}'$ of $\mathcal{F}$ such that the solution to the corresponding matrix equation $H' = \mathcal{F}'C'$ represents the normal form of h. To this end we have to remove rows and columns of $\mathcal{F}$ that are linearly dependent on the others. Note that we do not have enough space to write down the matrix $\mathcal{F}$ and therefore can not actually remove anything. What we will develop is a method to determine with reasonable space requirements whether a given row or column is in $\mathcal{F}'$. This method will consist of two rank computations as follows: If we fix an arbitrary order on the rows (resp., columns) of $\mathcal{F}$, then the k-th row (resp., column) is in $\mathcal{F}'$ if the ranks of the minor of $\mathcal{F}$ consisting of the first $k-1$ rows (resp., columns) and the one consisting of the first k rows (resp., columns) differ, whereas that row (resp., column) will be dispensable if those two ranks are equal. It is clear that the maximal regular minor resulting from this method depends on the chosen order of the rows and columns. It is also clear that the solution of the matrix equation with this maximal regular minor will represent the normal form of h if and only if the order of the columns is chosen such that the columns corresponding to the y_t come last (i.e. after the ones corresponding to the $c_{i,t}$) and in ascending term order of their indices (i.e. the column corresponding to y_t comes before the column corresponding to y_u if $t \prec u$). Incidentally, the order of the rows does not influence the solution.

The tools needed for determining this maximal regular minor of $\mathcal{F}$ are an efficient way of enumerating in the given term order all terms up to the given degree bound and an efficient method for calculating the rank of a matrix.

Comparing two terms essentially requires the space for writing down their weights multiplied by the lcm (or the product) of the denominators of all weights. This space does not exceed $2(\log(n^2A^2\max(N, d+D))+1)$. The space needed for the enumeration of the terms is essentially that for writing down three terms, namely the last one output and two others for an exhaustive search of the next one to output, and for the comparison of two terms. Altogether we need space not exceeding $3n\log\max(N, d+D)+1+2(\log(n^2A^2\max(N, d+D))+1)$. The exhaustive search is possible since we can enumerate all terms up to the given degree bound in lexicographic order.

As to the rank calculation, we will, for simplicity's sake, multiply each row of the matrix and the right hand side by the lcm (or even simpler, by the product) of their denominators to get an integer matrix and then adopt the method of Ibarra, Moran and Rosier, described in [IMR80], which runs in parallel as follows: First, the matrix gets multiplied by its transpose; from the resulting matrix we calculate the characteristic polynomial. Finally, the rank of the original matrix is the difference of the degree of the characteristic polynomial and the highest power of the indeterminate that divides the characteristic polynomial.

Let K be a bound on the numerators and denominators of the coefficients of the polynomial h to be reduced and the generating polynomials $f_1, \ldots, f_s$. Then, K is a bound on the numerators and denominators of the entries of H and $\mathcal{F}$ and, consequently, the lcm (or the product) of the denominators is at most K^M and the entries of the integer matrix are bounded by K^{M+1}. The multiplication of the matrix by its transpose can be done in $O(\log M \log\log(M(K^{M+1})^2))$ parallel time, since $\log(M(K^{M+1})^2)$ is an upper bound on the number of bits required for writing down any number occurring during that calculation. As shown by Galil and Pan in [GP89], the characteristic polynomial of an integer matrix can be computed in $O(\log^2(Mp))$ parallel time, where p is an upper bound on the number of bits required for writing down any number occurring during the calculation. In our case, $p = \log((M(K^{M+1})^2)^M M!) \leq 2M(M+1)\log(2K)$ will suffice. The determination of the index of the smallest nonvanishing coefficient of the characteristic polynomial can be done in $O(\log M)$ parallel time.

By the parallel computation thesis, shown by Fortune and Wyllie in [FW78], we can do all this sequentially using no more space than the square of the time required by a parallel algorithm. In our case, we need space amounting to $O(\log^4(M \log K))$. Thus, we have an efficient method to determine for a given row or column of $\mathcal{F}$ whether this row or column is in our maximal regular minor.

Next we have to compute the unique solution of the matrix equation $H' = \mathcal{F}'C'$ where $\mathcal{F}'$ is the maximal regular minor of $\mathcal{F}$ determined above and H' and C' are the corresponding shortened versions of H and C.

In [GP89], Galil and Pan also showed that the inverse of a regular $M \times M$-matrix can be computed in $O(\log^2(Mp))$ parallel time, where p is an upper bound on the number of bits required for writing down any number occurring during the calculation. This will easily yield the solution of the matrix equation within essentially the same time. Again by the parallel computation thesis of [FW78], we therefore can obtain a solution to the matrix equation requiring $O(\log^4(M \log K))$ space.

Once more, note that we do never write down the entire matrix for all that has been described, because this would take too much space. Instead, we calculate each entry when it is needed, and we determine for each row or column whether it is in our maximal regular minor at the time when we consider the entries of that row or column.

It is already clear how the solution of the matrix equation represents the normal form of the given polynomial. Thus we can calculate this normal form within the space bound just stated and have the result of this section:

Proposition: In $\mathbb{Q}[x_1,\ldots,x_n]$, let the polynomial ideal I be given by s generators whose degrees are bounded by d. Then the normal form of a given polynomial h can be computed using $O(log^4((N^n+s(d+N+(sd)^{2^n})^n)\log K))$ space where N is the bound on the degree of the normal form of h stated in the proposition at the end of section 2 and K is a bound on the numerators and denominators of the coefficients of the given polynomials.

5 Computing the Gröbner basis

We will now use the calculation of normal forms as a subroutine for the computation of Gröbner bases. To this end, let us introduce some more terminology: We will call a term u a direct divisor of another term $t \neq u$ if u divides t but there is no term $v \notin \{u,t\}$ such that u divides v and v divides t; in other words, the direct divisors of a term are just those terms where the exponent vector is smaller by 1 in exactly one coordinate and equal in all others. It is obvious that any term has at most n direct divisors. If a monic monomial m is reducible (i.e. is different from its normal form) but all its direct divisors are irreducible, then we will call m minimally reducible. Clearly, if all direct divisors of a monomial are irreducible, then so are all its (not necessarily direct) proper divisors.

It is not hard to see that the unique reduced Gröbner basis of a given ideal is just the set G of all the polynomials $m-\mathrm{NF}(m)$ where m is a minimally reducible monic monomial. Indeed, on the one hand, every polynomial that is not minimal in its coset will be reducible w.r.t. G; on the other hand, any such minimally reducible monic monomial m could not be reduced w.r.t. $G\setminus\{m-\mathrm{NF}(m)\}$.

For generating G, we enumerate all monic monomials (= terms) up to the degree bound on Gröbner bases, shown by Dubé in [Dub90]. For every such monomial m, we calculate its normal form and also the normal forms of all its direct divisors. If m turns out to be minimally reducible, then we output $m-\mathrm{NF}(m)$ as an element of the Gröbner basis. It is clear that the overall output we will produce by this method is the unique reduced Gröbner basis.

The space needed for the enumeration of all monic monomials is essentially that for writing down a term. For the direct divisors we need space for another term; and for the normal form calculations the space bound from the preceding section applies. This gives a space requirement of $O(\log^4(M\log K))$ altogether. However, note that one of the parameters in the space bound of the preceding section was the degree of the input polynomial h but here we do not have such a polynomial as part of the input. Therefore, we have to replace this parameter in the space bound by the bound on the degrees of the polynomials whose normal form we calculate. This new parameter is just the degree bound of Dubé ([Dub90]) on the Gröbner basis. We will take this into account in the next section; let us now briefly summarize the calculation of the Gröbner basis.

The outermost loop of our algorithm is an enumeration of all monic monomials up to Dubé's degree bound. In every pass through the loop we call $n+1$ times the subroutine for the normal form calculation applied to the n direct divisors of the current monomial and the monomial itself. As the result of these $n+1$ calls of the normal form calculating subroutine we get the information whether h is minimally reducible, in addition to the normal form of h. In case h is minimally reducible we output $h - \mathrm{NF}(h)$ as an element of the Gröbner basis and proceed by taking the next monic monomial in the outermost loop.

Let us also summarize the subroutine for the calculation of normal forms. Let h denote the monic monomial that is the input of the subroutine. We consider (but do not write down) the matrix equation $H' = \mathcal{F}'C'$ where $\mathcal{F}'$ is our maximal regular minor of $\mathcal{F}$ and $H = \mathcal{F}C$ is the matrix equation representing the polynomial equation $h = \mathrm{NF}(h) + \sum_{i=1}^{s} f_i c_i$ in the way described in section 3. We calculate, one by one, those entries of the solution vector C' which are the coefficients of the normal form of h (in case h is a direct divisor, we actually need only the coefficient y_h in order to know whether h is in normal form) by performing the necessary parts of the multiplication $\mathcal{F}'^{-1} \cdot H'$. We never write down the matrix $\mathcal{F}'^{-1}$ but compute each entry when it is needed. The computation of the entries of $\mathcal{F}'^{-1}$ can be done within the required space bound by virtue of [GP89] and [FW78]. Note that the entries of $\mathcal{F}'$ used in this computation are also determined from scratch each time they are used. As has been shown in the previous sections the decision whether a row or column is in the maximal regular minor as well as the determination of any entry of $\mathcal{F}$ can be done within the required space bounds.

The effort necessary for the normal form subroutine does not increase substantially if we also calculate the entries $c_{i,t}$ of the solution vector C' and thus obtain the coefficients c_i of the representation of $h - \mathrm{NF}(h)$ as a linear combination of the ideal generators $f_1, \ldots, f_s$. This means that we can, for each element of the Gröbner basis, compute, in addition, the coefficients of a representation as a linear combination of the original basis within the same space bound.

6 Complexity considerations

In this section we will summarize the statements about the space requirements of the methods described so far.

Let us first consider the problem of computing the normal form of a polynomial. We are given an ideal I, a term order $\prec$ and a polynomial h to be reduced. Let *size* be the number of bits needed to write down this input. Here we assume that I is given by a collection $f_1, \ldots, f_s$ of polynomials whose degrees are bounded by d and whose coefficients' numerators and denominators are bounded by K. The term order is given by a collection of n^2 rational weights (n is the number of indeterminates) whose numerators and denominators are bounded by A.

It is clear that d, K and A are bounded by 2^{size} and that n and s are bounded by *size*. The degree of h is also bounded by 2^{size}, but in view of the problem of calculating Gröbner bases we will only use a bound of $2^{2^{O(size)}}$ on this degree.

The bound N on the degree of the normal form of h is

$$\begin{aligned} N &= ((2n(\frac{d^2}{2}+d)^{2^{n-1}})^n A^{2n} \deg(h))^{n+1} \\ &\in (2^{2^{O(size)}} \deg(h))^{O(size)} \\ &\subseteq 2^{2^{O(size)}} \end{aligned}$$

Next we express Hermann's bound (from [Her26]) on the degrees of the coefficients in the representation of $h - \mathrm{NF}(h)$ in terms of the input-size.

$$D \le N + (sd)^{2^n} \in 2^{2^{O(size)}}$$

It remains to give a bound on the format M of $\mathcal{F}$ in terms of the input-size.

$$M = N^n + s(d+D)^n \in 2^{2^{O(size)}}$$

Note that in all these estimates we used $2^{2^{O(size)}}$ as a bound on the degree of h.

Since $O(\log^4(M \log K)) \subseteq 2^{O(size)}$ the above arguments imply the first main result of this paper.

Theorem: The calculation of the normal form of a given polynomial w.r.t. a given ideal and term order can be done in exponential space.

Let us now turn to the calculation of Gröbner bases. Here, we are given an ideal and a term order in the same way as described above (only the polynomial h is missing this time). We enumerate all monic monomials m up to Dubé's degree bound ([Dub90]) which is $2^{2^{O(size)}}$ and use m and its direct divisors as the polynomial h to be reduced in the normal form calculation. Note that, in the consideration of the normal form calculation, we took $2^{2^{O(size)}}$ as bound on the degree of h, therefore we can adopt the results from there. After each such normal form calculation, the space for that calculation can be freed completely, because in the case of a direct divisor the result only influences whether we proceed testing or interrupt the work on the current monomial, and in the case of the monomial itself we will immediately output the difference of the monomial and its normal form, if nonzero, as an element of the Gröbner basis. Thus, we need space for enumerating all monic monomials, negligible space for the control of the order in which the direct divisors are tested and space for the normal form calculation. The second main result follows:

Theorem: The unique reduced Gröbner basis of a given ideal w.r.t a given term order can be computed in exponential space.

It is not hard to see that the two main results remain valid if we assume a fixed term order that is not part of the input, i.e. if the input consists only of the ideal basis and possibly the polynomial to be reduced.

Another variant to be considered is the case of a fixed term order and a fixed ideal, both not being part of the input. It is clear that it does not make sense to look at the complexity of the Gröbner basis calculation in this case. But if we take a polynomial h as input, we can consider the complexity of its normal form calculation. Here, n, s, d and A are constant, because we consider the ideal as well as the term order as fixed. Only $\deg(h)$ and K as a bound on the numerators and denominators of the coefficients of h are bounded by $2^{O(size)}$. Note that we do not have to use a more generous bound on $\deg(h)$ here, since there is no Gröbner basis calculation we want to provide for. It turns out that, in this case, the space needed for the calculation of the normal form of h is bounded by $O(size^4)$; in other words, the normal form calculation can be done in polynomial space.

7 Bibliographic notes

The representation of term orders by a collection of weight functions is due to Robbiano. His presentation [Rob85], where he shows that every term order can be represented by at most n weight functions (n is the number of indeterminates) is essentially an excerpt from his more comprehensive treatment [Rob86] on generalized standard bases. Dubé, Mishra and Yap take up this idea, give a constructive proof of the representability of term orders by weight functions and use this representation for bounding the length of a reduction of a polynomial with respect to some basis in [DMY86]. By a reduction we always mean a process like the one appearing in Buchberger's algorithm which was originally described in [Buc65].

The doubly exponential bound on the degrees of the elements in Gröbner bases has been proved by Dubé in [Dub90]. Hermann proved in her dissertation [Her26] the doubly exponential bound on the degrees of the coefficients in the representation of a polynomial as a linear combination of the ideal generators. Mayr and Meyer showed in [MM82] that this bound is asymptotically tight. The first application of this complexity bound to the polynomial ideal membership problem was given in [May92].

Efficient parallel matrix calculations as used here for the solution of our system of linear equations have been widely studied since the appearance of Csanky's paper [Csa76]. Many researchers contributed improvements, cf. [PS78], [IMR80], [BvzGH82], [Ber84], [Mul86] and [Pan87]. The work of Galil and Pan ([GP89]) gives a better account for the Boolean complexity, which is important in our case of very large numbers. The easy transition between parallel time complexity and sequential space requirements is justified by the parallel computation thesis of Fortune and Wyllie in [FW78].

Let us finally mention that Koppenhagen and Mayr present an optimal Gröbner basis algorithm for binomial ideals (each generator is a difference of two monomials) in [KM96]. This algorithm is based on combinatorial principles and does not rely on the parallel computation thesis.

A survey on recent developments concerning the algorithmic aspects of polynomial ideal theory can be found in [May95].

References

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[BvzGH82] Allan Borodin, Joachim von zur Gathen, and John Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52:241–256, 1982.

[Csa76] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.

[DMY86] Thomas W. Dubé, B. Mishra, and C. K. Yap. Admissible orderings and bounds for Gröbner bases normal form algorithms. Technical Report 258, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, 1986.

[Dub90] Thomas W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM Journal on Computing*, 19:750–773, 1990.

[FW78] Stephen Fortune and James Wyllie. Parallelism in random access machines. In *Proceedings of the 10th Annual ACM Symposium on Theory of Computing*, pages 114–118. ACM Press, 1978.

[GP89] Zvi Galil and Victor Pan. Parallel evaluation of the determinant and of the inverse of a matrix. *Information Processing Letters*, 30:41–45, 1989.

[Her26] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Mathematische Annalen*, 95:736–788, 1926.

[IMR80] Oscar H. Ibarra, Shlomo Moran, and Louis E. Rosier. A note on the parallel complexity of computing the rank of order n matrices. *Information Processing Letters*, 11:162, 1980.

[KM96] Ulla Koppenhagen and Ernst W. Mayr. An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals. Technical Report TUM-I 9605, Institut für Informatik, Technische Universität München, 1996.

[May92] Ernst W. Mayr. Polynomial ideals and applications. *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, XII(4):1207–1215, 1992.

[May95] Ernst W. Mayr. On polynomial ideals, their complexity, and applications. In *Fundamentals of Computation Theory, 10th International Conference, FCT '95*, LNCS 965, pages 89–105. Springer-Verlag, 1995.

[MM82] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982.

[Mul86] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 338–339. ACM Press, 1986.

[Pan87] Victor Pan. Complexity of parallel matrix computations. *Theoretical Computer Science*, 54(1):65–85, 1987.

[PS78] F. P. Preparata and D. V. Sarwate. An improved parallel processor bound in fast matrix inversion. *Information Processing Letters*, 7(2):148–150, 1978.

[Rob85] Lorenzo Robbiano. Term orderings on the polynomial ring. In *Proceedings of the 10th European Conference on Computer Algebra, EUROCAL '85. Vol. 2: Research contributions*, LNCS 204, pages 513–517. Springer-Verlag, 1985.

[Rob86] Lorenzo Robbiano. On the theory of graded structures. *Journal of Symbolic Computation*, 2(2):139–170, 1986.

Index of notations

$\prec$	the term order
A	maximum of all $a_{k,i}$ and $b_{k,i}$
$a_{k,i}$	numerator of $w_{k,i}$
B	basis in the definition of the unified weight function W $B := 2nA^2(\frac{d^2}{2}+d)^{2^{n-1}}$
$b_{k,i}$	denominator of $w_{k,i}$
C	vector consisting of the unknowns y_t and $c_{i,t}$
C'	part of C corresponding to the regular minor $\mathcal{F}'$
c_i	i-th coefficient polynomial in the representation of $h - \mathrm{NF}(h)$
$c_{i,t}$	coefficient of c_i belonging to the term t
D	degree bound (from [Her26]) on the coefficients of the representation of $h - \mathrm{NF}(h)$ $D = \deg(h - \mathrm{NF}(h)) + (sd)^{2^n} \leq N + (sd)^{2^n}$
d	bound on the degree of the ideal generators
$\mathcal{F}$	matrix consisting essentially of the coefficients $f_{i,t}$
$\mathcal{F}'$	maximal regular minor of $\mathcal{F}$

f_i	i-th generating polynomial
$f_{i,t}$	coefficient of f_i belonging to the term t
G	unique reduced Gröbner basis for I w.r.t. $\prec$
H	vector of the coefficients of h
H'	part of H corresponding to the regular minor $\mathcal{F}'$
h	the polynomial to be reduced
h_t	coefficient of h belonging to the term t
I	the ideal generated by $f_1, \ldots, f_s$
K	bound on the numerators and denominators of the coefficients of h and the f_i
M	bound on the format of $\mathcal{F}$. $M = N^n + s(d+D)^n$
N	bound on the degree of the normal form of h. $N = ((2n(\frac{d^2}{2} + d)^{2^{n-1}})^n A^{2n} \deg(h))^{n+1}$
n	number of indeterminates in the polynomial ring
$\mathrm{NF}(f)$	normal form (w.r.t. $\prec$ and I) of a polynomial f
$\mathbb{Q}$	the set of all rational numbers
s	number of generators of I
size	number of bits required to write down the input
T	the set of all terms or power products
W	unified weight function, defined by $W(u) = \sum_{i=1}^{n} B^{i-1} W_i(u)$
W_k	k-th weight function, defined by $W_k({x_1}^{u_1} \ldots {x_n}^{u_n}) = \sum_{i=1}^{n} w_{k,i} u_i$
$w_{k,i}$	i-th weight of the k-th weight function
x_i	i-th indeterminate of the polynomial ring
y_t	coefficient of $\mathrm{NF}(h)$ belonging to the term t