J. Symbolic Computation (2001) **31**, 307–313
doi:10.1006/jsco.2000.1575
Available online at http://www.idealibrary.com on IDEAL®

Counting and Gröbner Bases

K. KALORKOTI†

School of Computer Science, University of Edinburgh, Edinburgh, Scotland EH9 3JZ, U.K.

We show how the complexity of counting relates to the well known phenomenon that computing Gröbner bases under a lexicographic order is generally harder than total degree orders. We give simple examples of polynomials for which it is very easy to compute their Gröbner basis using a total degree order but for which exponential time is required for a lexicographic order. It follows that conversion algorithms do not help in such cases.

1. Introduction

Gröbner bases were introduced by Buchberger (1965) and are now firmly established as a tool in Commutative Algebra and other areas. The reader is referred to Buchberger (1985), Cox, Little and O'Shea (1992) or Becker and Weispfenning (1993) for more information. Eisenbud (1995) places Gröbner bases within the context of more advanced Commutative Algebra.

The ingredients for a Gröbner basis are a finite set G of multivariate polynomials (usually with coefficients from $\mathbb{Q}$) and a suitable total order on the power products. It is a well known observation that, for a given set G, the runtime for a total degree order (i.e. power products are sorted first according to degree and then by some other criterion, especially reverse lexicographic) is usually better than for a lexicographic one and frequently it is dramatically better. See Bayer and Stillman (1987) or Eisenbud (1995) for special properties of the reverse lexicographic order. In this note we show that, for a class of examples, this behaviour is explained by a conjecture in Complexity Theory. These also serve as examples for which basis conversion methods such as those of Faugére *et al.* (1993) or of Collart, Kalkbrenner and Mall (1997) do not help.

It is an easy exercise to encode NP-complete problems in terms of Gröbner bases. For example, given an instance of SATISFIABILITY we can produce a set of equations such that the given formula is satisfiable if and only if the equations have a common zero in some algebraically closed field (in fact the encoding ensures that any solution will have components from $\{0, 1\}$). We test the last condition by computing a Gröbner basis for the polynomials and checking to see if it has a nonzero constant (see Buchberger, 1985). Although this gives us a hint that in the worst case Gröbner bases will be hard to compute, such an approach does not help to explain the difference in runtimes between total degree and lexicographic orders. This suggests that we should consider problems for which solutions are known to exist but for which some other property is believed

†E-mail: kk@dcs.ed.ac.uk

0747–7171/01/030307 + 07 $35.00/0

to be intractable. In this note we focus on #P-complete problems; see Papadimitriou (1994) for background. Although this class includes the counting versions of NP-complete problems (e.g. SATISFIABILITY), it also includes very restricted versions of #MONOTONE SATISFIABILITY (prefixing a decision problem with # indicates that we are considering its counting version). We show how to encode efficiently one of these problems in such a way that finding the Gröbner basis under a total degree order costs no more than the encoding, while even partial information about the Gröbner basis under a lexicographic order would amount to solving the #P-complete problem. In fact, even without any assumptions on #P, it is quite easy to produce examples where the difference in runtimes is exponential in the size of the input (the second basis is exponentially larger than the first).

Becker and Weispfenning (1993) included a brief discussion on complexity issues in an Appendix. Here we note that Möller and Mora (1984) and Huynh (1986) show that in the worst case Gröbner bases have polynomials whose degree is $\Omega(d^{2^n})$ where d is the maximum of the degrees of the inputs and n is the number of indeterminates; their proofs are based on work of Mayr and Meyer (1982). Moreover, Huynh (1986) proved that the same holds for the cardinality of Gröbner bases. Heintz and Morgenstern (1993) discussed matters in relation to the fundamental problems of elimination theory. For zero-dimensional ideals (i.e. ones with finitely many zeros) the situation is not so bad. Lakshman (1991) showed that for polynomials with rational coefficients with finitely many common zeros the cost of computing their Gröbner basis under any admissible ordering is bounded by a polynomial in d^n where d, n are as above. The ideals we use are all zero dimensional and indeed it is easy to see how to obtain their Gröbner basis in $\mathbf{O}(2^n)$ time for the orderings under consideration.

2. Algebraic Preliminaries

Throughout k will be a field and $X = \{ x_1, \ldots, x_n \}$ a nonempty set of distinct indeterminates over k. For each $f \in k[X]$ we set $\overline{f} = 1 - f$ and

$$\mathcal{R} = \{y_1 y_2 \cdots y_n | y_i \in \{ x_i, \overline{x_i} \}, \text{ for } 1 \leq i \leq n\},$$
$$S = \{ x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n \}.$$

Let I be an ideal of $k[X]$ that contains S as a subset. Since $x_i^2 - x_i = \overline{x}_i^2 - \overline{x}_i = x_i \overline{x}_i$ it is clear that for all $m_1, m_2 \in \mathcal{R}$ we have

$$m_1 m_2 \equiv \begin{cases} m_1 \pmod{I}, & \text{if } m_1 = m_2; \\ 0 \pmod{I}, & \text{if } m_1 \neq m_2. \end{cases}$$

It is now easy to see that the members of $\mathcal{R}$ are linearly independent over k (consider their images in $k[X]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$). Moreover, every power product $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ when considered modulo I can be written as a unique linear combination of the members of $\mathcal{R}$ (if $e_i > 1$ then $x_i^{e_i} \equiv x_i \pmod{I}$, while if $e_i = 0$ then multiply by $x_i + \overline{x}_i$ and expand).

LEMMA 2.1. *Let I be an ideal of $k[X]$ that contains S as a subset. Let $f \in k[X]$ and set $f \equiv \sum_{i=1}^{r} a_i m_i \pmod{I}$ where each $a_i \in k^*$ and $m_i \in \mathcal{R}$. Then $f \in I$ if and only if $m_i \in I$ for $1 \leq i \leq m$.*

PROOF. Suppose that $f \in I$. Then for each i we have $a_i^{-1} m_i f \in I$. However $a_i^{-1} m_i f = m_i$. The converse is immediate. □

LEMMA 2.2. *Let I be an ideal of $k[X]$ that contains S as a subset. Then I is a radical ideal, i.e. $f^s \in I$ for some $s > 0$ if and only if $f \in I$.*

PROOF. Set $f \equiv \sum_{i=1}^{r} a_i m_i \pmod{I}$ where each $a_i \in k^*$ and $m_i \in \mathcal{R}$. Then, from the observations made above, we have $f^s \equiv \sum_{i=1}^{r} a_i^s m_i \pmod{I}$ and the result follows from the preceding lemma. □

Suppose now that k has characteristic 0 so that it contains $\mathbb{Q}$ as a subfield. Let α be the endomorphism of $k[X]$ induced by $x_1 \mapsto x_1 - 2x_2 - 2^2 x_3 - \cdots - 2^{n-1} x_n$ and $x_i \mapsto x_i$, for $2 \leq i \leq n$. Clearly α is an automorphism of $k[X]$.

LEMMA 2.3. *Let I be an ideal of $k[X]$ that contains S as a subset and assume that k has characteristic 0. Then $\alpha(I)$ is a radical ideal of $k[X]$. Furthermore, if $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ are zeros of $\alpha(I)$ with $a_1 = b_1$, then $a_i = b_i$ for $2 \leq i \leq n$.*

PROOF. The fact that α is an automorphism implies that $\alpha(I)$ is an ideal. Now $f^s \in \alpha(I)$ if and only if $\alpha^{-1}(f)^s \in I$ and so $\alpha(I)$ is radical by Lemma 2.2.

The last part follows from the observation that $(c_1, c_2, \ldots, c_n) \in \{0, 1\}^n$ is a zero of I if and only if $(c_1 + 2c_2 + \cdots + 2^{n-1} c_n, c_2, \ldots, c_n)$ is a zero of $\alpha(I)$. □

In the following we will use $\mathbf{V}(I)$ to denote the set of common zeros of an ideal I. The next lemma draws together some well known facts about zero-dimensional radical ideals, e.g. see Becker and Weispfenning (1993, Chapter 8), (we omit the proof since it follows from the two preceding lemmas by standard arguments).

LEMMA 2.4. *Let I be an ideal of $k[X]$ that contains S as a subset and assume that k has characteristic 0. Then $\alpha(I) \cap k[x_1] \neq 0$. Furthermore, let p_1 be a nonzero monic element of $\alpha(I) \cap k[x_1]$ of minimal degree and set $d = \deg(p)$. Then:*

(1) $|\mathbf{V}(I)| = d$.
(2) $p_1 = (x_1 - \xi_1)(x_1 - \xi_2) \cdots (x_1 - \xi_d)$ *where $\xi_1, \xi_2, \ldots, \xi_d$ are the x_1-coordinates of all the elements of $\mathbf{V}(\alpha(I))$. In particular, p_1 has integer coefficients.*
(3) There are polynomials $p_2, \ldots, p_n \in \mathbb{Q}[x_1]$ such that $x_2 - p_2, \ldots, x_n - p_n \in \alpha(I)$ and either $p_i = 0$ or $\deg(p_i) < d$ for $2 \leq i \leq n$.

From now on let G be a subset of $k[X]$ such that $S \subseteq G$. Define β to be the endomorphism of $k[X]$ induced by $x_1 \mapsto x_1^2$ and $x_i \mapsto x_i$, for $2 \leq i \leq n$. Note that β is a injective but not surjective. The coding given by $\beta\alpha$ is used by Heintz and Morgenstern (1993); see also Weispfenning (1988). Set

$$I = (G), \qquad J = \alpha(I), \qquad K = (\beta(J)).$$

LEMMA 2.5. *Let $I = (G)$ as above and assume that k has characteristic 0. Then $K \cap k[x_1] \neq 0$. Furthermore, let p_1 be a nonzero monic element of $K \cap k[x_1]$ of minimal degree and set $d = \deg(p_1)$. Then:*

(1) $|\mathbf{V}(I)| = d/2$.
(2) $p_1 = (x_1^2 - \xi_1)(x_1^2 - \xi_2)\cdots(x_1^2 - \xi_r)$ *where $\xi_1, \xi_2, \ldots, \xi_r$ are the x_1-coordinates of all the elements of $\mathbf{V}(J)$.*
(3) There are polynomials $p_2, \ldots, p_n \in \mathbb{Q}[x_1^2]$ such that $x_2 - p_2, \ldots, x_n - p_n \in K$ and either $p_i = 0$ or $\deg(p_i) < d - 1$ for $2 \leq i \leq n$.

PROOF. We may assume that k is algebraically closed. Let $\xi_1, \xi_2, \ldots, \xi_r$ be the x_1-coordinates of all the elements of $\mathbf{V}(J)$ and set $q(x_1) = (x_1 - \xi_1)(x_1 - \xi_2)\cdots(x_1 - \xi_r)$. By Lemma 2.4, $q(x_1) \in J$ and so $q(x_1^2) \in K$. Thus $d \leq 2r$.

We claim that $x_1^2 - \xi_i \mid p_1$, for $1 \leq i \leq r$. Consider $(a_1, a_2, \ldots, a_n) \in \{0, 1\}^n$ and set $A = \sum_{i=1}^{n} a_i 2^{i-1}$. Now $(A, a_2, \ldots, a_n)$ is a zero of J if and only if $(B, a_2, \ldots, a_n)$ is a zero of K for all B such that $B^2 = A$. Since k has characteristic 0 and is algebraically closed it follows that each nonzero element of k has exactly two distinct square roots in k. Since p_1 vanishes at each zero of K it follows that $x_1^2 - \xi_i \mid p_1$ whenever $\xi_i \neq 0$. Now if $(0, 0, \ldots, 0)$ is not zero of J then $\xi_i \neq 0$, for $1 \leq i \leq n$, and the proof of the claim is complete. On the other hand, if $(0, 0, \ldots, 0)$ is a zero of J then exactly one ξ_i is equal to 0. However we have $x_1^2 \mid p_1$ since no element of G can have a nonzero constant term and so sending x_i to 0, for $2 \leq i \leq n$, leaves p_1 fixed and sends K to $(x_1^4 - x_1^2)$ or to $(x_1^4 - x_1^2, x_1^2) = (x_1^2)$. Thus $d \geq 2r$ and $p_1 = q(x_1^2)$ as claimed.

The final part follows from the last part of Lemma 2.4. □

Note that K need not be radical, however it is "nearly" so. The next lemma clarifies the situation (we will not need this result subsequently).

LEMMA 2.6. *Suppose that k has characteristic 0. Then:*

(1) K is radical if and only if G contains a polynomial with a nonzero constant term.
(2) Suppose that $f(x_1^2, x_2, \ldots, x_n)^s \in K$ for some $s > 0$. Then $f(x_1^2, x_2, \ldots, x_n) \in K$.

PROOF. For the first part we use a result given by Becker and Weispfenning (1993) as Proposition 8.14 (based on a lemma of Seidenberg): If k is perfect, then a zero-dimensional ideal is radical if and only if it contains a univariate squarefree polynomial in each indeterminate. In our case K contains $x_i^2 - x_i$, for $2 \leq i \leq n$, which are squarefree. Thus K is radical if and only if the generator of $K \cap k[x_1]$ is squarefree, i.e. if and only if the polynomial $p(x_1)$ of Lemma 2.5 is squarefree. This is so if and only if $(0, 0, \ldots, 0)$ is not a zero of J and this is equivalent to the stated condition on G.

For the second part, if $f(x_1^2, x_2, \ldots, x_n)^s \in K$ for some $s > 0$ then there are polynomials $f_1, f_2, \ldots, f_r \in k[X]$ and $g_1, g_2, \ldots, g_r \in G$ such that $f(x_1^2, x_2, \ldots, x_n)^s = f_1\beta(g_1) + \cdots + f_r\beta(g_r)$. Set $f_i = f_{i0} + f_{i1}$, for $1 \leq i \leq r$, where each term of f_{i0} has even degree in x_1 and each term of f_{i1} has odd degree in x_1. Since each term in $\beta(g_i)$, for $1 \leq i \leq r$, has even degree in x_1 it follows that $f(x_1^2, x_2, \ldots, x_n)^s = f_{10}\beta(g_1) + \cdots + f_{r0}\beta(g_r)$. Now replacing x_1 by $x_1^{1/2}$ we see that $f(x_1, x_2, \ldots, x_n)^s \in J$ and so $f(x_1, x_2, \ldots, x_n) \in J$ since J is radical, by Lemma 2.2. Thus $f(x_1^2, x_2, \ldots, x_n) \in K$ as claimed. □

LEMMA 2.7. *Let L be an ideal of $k[X]$ and suppose that there are $p_1, p_2, \ldots, p_n \in k[x_1]$ such that $p_1, x_2 - p_2, \ldots, x_n - p_n \in L$. Then, provided that p_1 is of minimal degree amongst all members of $L \cap k[x_1]$, we have $L = (p_1, x_2 - p_2, \ldots, x_n - p_n)$.*

PROOF. Set $L' = (p_1, x_2 - p_2, \ldots, x_n - p_n)$ and choose $f \in L$. Then $f \equiv q \pmod{L'}$ for some $q \in L \cap k[x_1]$. It follows that $p_1 \mid q$ since $L \cap k[x_1] = (p_1)$, by the assumption on the degree of p_1. Thus $f \equiv 0 \pmod{L'}$ and so $f \in L'$ which means that $L \subseteq L'$. The result follows since $L' \subseteq L$ by assumption. □

3. Counting

Let $y_1, y_2, \ldots, y_N$ be Boolean variables and consider the following problem:

#MONOTONE 2-SAT
INPUT: A Boolean formula $\phi = c_1 \wedge c_2 \wedge \cdots \wedge c_s$ where each c_i is of the form $y_i \vee y_j$ for some i, j with $1 \leq i, j \leq N$.
OUTPUT: The number of satisfying assignments to the given formula.

Valiant (1979) shows that this problem is #P-complete. Note that we may assume that $i \neq j$ for each clause $y_i \vee y_j$ of ϕ and we make this assumption from now on (this just makes the encoding given below a little simpler; see the remark after Lemma 3.1). Let k, X be as in the preceding section where the cardinality n of X is set to $N + 1$. Given a Boolean formula ϕ as above, we can encode it as a set of polynomials G_ϕ in $k[X]$ as follows:

$$\begin{aligned} \textbf{true} &\mapsto 0, \\ \textbf{false} &\mapsto 1, \\ y_i \vee y_j &\mapsto x_{i+1} x_{j+1}. \end{aligned}$$

G_ϕ consists of the encoded clauses of ϕ together with x_1 and the set S but with $x_1^2 - x_1$ omitted. It is clear that there is a 1–1 correspondence between the satisfying assignments of ϕ and the zeros of $I = (G_\phi)$. Set $J = \alpha(I)$ and $K = (\beta(J))$, as in Section 2.

LEMMA 3.1. *Consider any total degree order on the power products of $k[X]$. Then $\beta(\alpha(G_\phi))$ is a Gröbner basis of K.*

PROOF. There is a subset P of $\{2, 3, \ldots, n\}^2$ such that the members of $\beta(\alpha(G_\phi))$ are precisely

$$\begin{aligned} l &= x_1^2 - \sum_{i=2}^{n} 2^{i-1} x_i, \\ f_{ij} &= x_i x_j, \qquad \text{for } (i, j) \in P \\ s_i &= x_i^2 - x_i, \qquad \text{for } 2 \leq i \leq n. \end{aligned}$$

This set is a Gröbner basis if and only if every S-polynomial of each pair of its elements reduces to 0. We make use of Buchberger's first criterion: if the leading power product of g is coprime to that of h then $S(f, g)$ reduces to 0 using g and h. This means that we

do not need to consider l since its leading power product is x_1^2 and x_1 does not appear in any other polynomial of our set. Likewise we do not need to consider $S(s_i, s_j)$. It is also clear that $S(x_i x_j, x_r x_s) = 0$ (this is so for arbitrary power products; S-polynomials are *designed* to do this). Finally, we need only consider $S(x_i x_j, x_i^2 - x_i)$ for $(i, j) \in P$. Recall that $i \neq j$ so that $S(x_i x_j, x_i^2 - x_i) = x_i x_j$ and this reduces to 0 since $x_i x_j$ is in our set. □

We note that if we allow clauses in ϕ of the form $y_i \vee y_i$ then everything works provided such a clause is encoded as x_{i+1} rather than x_{i+1}^2 (we can also omit $x_i^2 - x_i$).

LEMMA 3.2. *Assume that k has characteristic 0 and consider a lexicographic order on the power products of $k[X]$ in which x_1 is the smallest indeterminate. Let $p_1, p_2, \ldots, p_n$ be as in Lemma 2.5 with $K = (\beta(\alpha(G_\phi)))$. Then,*

(1) Every Gröbner basis of K using the preceding order includes a nonzero constant multiple of p_1.

(2) $p_1, x_2 - p_2, \ldots, x_n - p_n$ form a Gröbner basis for K.

PROOF. By Lemma 2.5, $p_1 \in K$ and so this must reduce to 0 under any Gröbner basis for K. This means that the basis must have a member $q \in k[x_1]$ such that $q \mid p_1$ (since we are using a lexicographic order in which x_1 is the smallest indeterminate). But p_1 has minimal degree amongst all nonzero members of $K \cap k[x_1]$. The first part now follows.

For the second part we note that $p_1, x_2 - p_2, \ldots, x_n - p_n$ are certainly a Gröbner basis (under the stated order) for the ideal that they generate; see the remarks in the proof of Lemma 3.1. By Lemma 2.5 and Lemma 2.7 this ideal is K. □

We can now see one way in which the well known differences in runtime for computing Gröbner bases under a total degree order as opposed to a lexicographic one can be linked with Complexity Theory. On the one hand, the Gröbner basis of K under a total degree order is as cheap to compute as possible; it is the same as the input! On the other hand, if we use a lexicographic order with x_1 as the smallest indeterminate then even finding the degree of p_1 amounts to solving a #P-complete problem (in this connection see also Heintz and Morgenstern, 1993, Proposition 13). Moreover, if we fix a ϕ with exponentially many satisfying assignments then the polynomial p_1 in the Gröbner basis of K under a lexicographic order with x_1 as the least indeterminate has exponentially many terms (this follows from a simple argument). Thus the runtime of any algorithm to compute this Gröbner basis is exponential while the Gröbner basis under a total degree order can be computed in linear time. As observed in the Introduction, this provides simple examples for which basis conversion methods such as those of Faugére *et al.* (1993) or of Collart, Kalkbrenner and Mall (1997) do not help.

Acknowledgement

The author is grateful to an anonymous referee for helpful comments and for pointing out relevant references, particularly Heintz and Morgenstern (1993).

References

Bayer, D., Stillman, M. (1987). A theorem on refining division orders by the reverse lexicographic orders. *Duke J. Math.*, **55**, 321–328.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases. A Computational Approach to Commutative Algebra* (in cooperation with H. Kreidel). New York, Springer.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassesringes nach einem nulldimensionallen Polynomideal. Ph.D. Thesis, University of Innsbruck, Austria.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In Bose, N. K. ed., *Recent Trends in Multidimensional Systems Theory*. Dordrecht, Reidel.

Collart, S., Kalkbrenner, M., Mall, D. (1997). Converting bases with the Gröbner walk. *J. Symb. Comput.*, **24**, 465–469.

Cox, D., Little, J., O'Shea, D. (1992). *Ideals Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. New York, Springer.

Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*. New York, Springer.

Faugère, J. C., Gianni, P., Lazard, D., Mora, T. (1993). Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.*, **16**, 329–344.

Heintz, J, Morgenstern, J. (1993). On the intrinsic complexity of elimination theory. *J. Complexity*, **9**, 471–498.

Huynh, D. T. (1986). A superexponential lower bound for Gröbner bases and Church–Rosser commutative Thue systems. *Inf. Control*, **68**, 196–206.

Lakshman, Y. N. (1991). A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals. In Mora, T., Traverso, C. eds, *Effective Methods in Algebraic Geometry*. Boston, Birkhäser.

Mayr, E. W., Meyer, A. R. (1982). The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.*, **46**, 305–329.

Möller, H. M., Mora, T. (1984). Upper and lower bounds for the degree of Gröbner bases. In Fitch, J. ed., *EUROSAM'84, International Symposium on Symbolic and Algebraic Computation*, *LNCS* **174**, Berlin, Springer.

Papadimitriou, C. H. (1994). *Computational Complexity*. Reading, MA, Addison-Wesley.

Valiant, L. G. (1979). The complexity of enumeration and reliability problems. *SIAM J. Comput.*, **8**, 410–421.

Weispfenning, V. (1988). The complexity of linear problems in fields. *J. Symb. Comput.*, **5**, 4–27.

Originally Received 16 January 1996
Accepted 5 July 2000
Published electronically 24 January 2001