A Single Exponential Bound on the Complexity of Computing Gröbner Bases of Zero Dimensional Ideals

LAKSHMAN Y. N.

Introduction

Let $\mathcal{R} = \mathbb{Q}[x_1, x_2, \ldots, x_n]$ denote the ring of polynomials in n variables over the rational numbers $\mathbb{Q}$. Let $f_1, f_2, \ldots, f_r \in \mathcal{R}$, $r \geq n$ with $\deg(f_i) = d_i$ and let $d = \max(d_i)$. Let $\mathcal{I} = (f_1, f_2, \ldots, f_r)$ be the ideal generated by f_i. $\mathcal{I}$ is assumed to be zero–dimensional. Let $\mathcal{Q}_i$, $i = 1, \ldots, k$ be primary ideals with associated primes $\mathcal{P}_i$ such that $\mathcal{I} = \bigcap_{i=1}^{k} \mathcal{Q}_i$.

We describe an algorithm to compute a reduced Gröbner basis for $\mathcal{I}$ under any admissible term ordering. We assume that we are given reduced Gröbner bases for each of the $\mathcal{P}_i$ under some admissible term ordering. We establish an upper bound on the number of arithmetic operations performed by the algorithm that is polynomially bounded by the dimension of the residue class ring $\mathcal{R}/\mathcal{I}$ seen as a rational vector space. This, combined with the upper bounds established in [Lak, LL] on the complexity of constructing reduced Gröbner bases for $\mathcal{P}_i$, implies a bound that is polynomial in d^n on the complexity of constructing reduced Gröbner bases for zero-dimensional polynomial ideals. Previously known bounds are not as strong ($r^3 d^{O(n^3)}$, see [CGH]) and are obtained using entirely different methods. Recent related work can be found in [KL] and [DS].

Our algorithm for constructing a Gröbner basis for $\mathcal{I}$ works in two stages. In the first stage, the algorithm constructs Gröbner bases for each $\mathcal{Q}_i$ separately from the given basis for $\mathcal{I}$ and a Gröbner basis for $\mathcal{P}_i$. In the second stage, the Gröbner bases of $\mathcal{Q}_i$ are put together to obtain a Gröbner basis for $\mathcal{I}$.

This material is based on work supported by the National Science Foundation under Grant No. CCR-87-05363 and under Grant No. CDA-8805910 at Rensslaer Polytechnic Institute, Troy, N. Y. as part of the author's doctoral dissertation.

T. Mora et al. (eds.), *Effective Methods in Algebraic Geometry*

From Primes to Primaries

Our construction is based on the following well known theorem (see [vdW]).

Theorem 1. *If the ideal $\mathcal{I}$ has an isolated primary component $\mathcal{Q}$ whose associated prime $\mathcal{P}$ is maximal, then, if ρ is the index of $\mathcal{Q}$, then, for any $\sigma \geq \rho$,*

$$\mathcal{Q} = (\mathcal{I}, \mathcal{P}^{\sigma}).$$

An algorithm for primary decomposition based on this theorem has been reported by Kredel [Kre]. However, no analysis of the algorithm is provided there.

Let $\mathcal{Q}$ be a zero–dimensional primary ideal in *general position* with associated prime $\mathcal{P}$. Let $\{q_1, q_2, \ldots, q_s\}$ be a basis for $\mathcal{Q}$ with $\varrho = \max\{\deg(q_i)\}$. Since $\mathcal{Q}$ is in *general position*, the reduced Gröbner basis for $\mathcal{P}$ under the purely lexicographic ordering $>_l$ with $x_1 < x_2 < \ldots < x_n$ looks like

$$x_n - g_n(x_1), \ldots, x_2 - g_2(x_1), g_1(x_1)$$

[GTZ]. Let $\deg(g_1(x_1)) = \delta$. We now state the algorithm for computing a reuced Gröbner basis for $\mathcal{Q}$.

Algorithm "Primary Component":

Input: A basis for $\mathcal{I}$ and a reduced Gröbner basis for $\mathcal{P}$, a prime ideal containing $\mathcal{I}$.

Output: A reduced Gröbner basis for $\mathcal{Q}$, the primary component of $\mathcal{I}$ whose associated prime is $\mathcal{P}$.

$\mathcal{C} := \mathcal{P}$;
$\mathcal{B} := \mathcal{GB}(\mathcal{I}, \mathcal{P}^2)$;
while $\mathcal{C} \neq \mathcal{B}$ **do** $\mathcal{C} := \mathcal{B}$; $\mathcal{B} := \mathcal{GB}(\mathcal{I}, \mathcal{P} \cdot \mathcal{B})$ **od**
return $(\mathcal{B})$;

The correctness of the algorithm follows from theorem 1 and the observation that

$$(\mathcal{I}, \mathcal{P}^{j+1}) = (\mathcal{I}, \mathcal{P} \cdot \mathcal{I}, \mathcal{P}^{j+1}) = (\mathcal{I}, \mathcal{P} \cdot (\mathcal{I}, \mathcal{P}^{j})).$$

This observation is crucial for the following analysis.

Procedure $\mathcal{GB}(\mathcal{A}_1, \mathcal{A}_2)$ is very similar to Buchberger's algorithm for finding the reduced Gröbner basis for $(\mathcal{A}_1, \mathcal{A}_2)$ except that the polynomials of the basis $\mathcal{A}_1 \cup \mathcal{A}_2$ are first mutually reduced as much as possible (bounded Gröbner basis reduction). Following lemmas lead to upper bounds on the time complexity of *Primary component*.

Lemma 1. *The sequence* $(\mathcal{I}, \mathcal{P}^i), i = 0, 1, \ldots$ *is strictly increasing until* $i = \rho$, *the index of the primary component of* $\mathcal{I}$ *whose associated prime is* $\mathcal{P}$. *Q. E. D.*

Lemma 2. *If* $\widehat{\mathcal{Q}}$ *is any primary ideal whose associated prime is* $\mathcal{P}$, *then all the lead terms in the reduced Gröbner basis of* $\widehat{\mathcal{Q}}$ *under* $>_l$ *are of the form*

$$z^{i_1} x_2^{i_2} \ldots x_n^{i_n}, \quad i_j \geq 0$$

where $z = x_1^{\delta}$.

Proof: Let f be the polynomial with the smallest lead term among the polynomials in the reduced Gröbner basis of $\widehat{\mathcal{Q}}$ under $>_l$ whose lead terms are not of the form $z^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, $i_j \geq 0$. Let

$$f = x_1^{\gamma} m + m f' + f''$$

where m is a monomial not depending on x_1, $\gamma \bmod \delta \neq 0$, f' depends on only x_1, f'' is not divisible by m and only has terms smaller than $x_1^{\gamma} m$. The univariate polynomial in x_1 in the Gröbner basis of $\widehat{\mathcal{Q}}$ (call it g) has to be a pure power of g_1. Let $g = x_1^{\Gamma} + f_1$ where Γ is some multiple of δ and f_1 has lower terms. Consider the s-polynomial of f and g i.e.,

$$\begin{aligned} x_1^{\Gamma-\gamma} f - mg &= x_1^{\Gamma-\gamma}(mf' + f'') - mf_1 \\ &= m(x_1^{\Gamma-\gamma} f' - f_1) + x_1^{\Gamma-\gamma} f''. \end{aligned}$$

Because of the choice of f, the only polynomial that can be used to reduce $m(x_1^{\Gamma-\gamma} f' - f_1)$ is f (if it is not zero already). Complete reduction of the terms divisible by m leads us to the equation

$$mp(x^{\gamma} + f') = mg$$

where p is a univariate polynomial in x_1. Follows that $x^{\gamma} + f'$ divides g. But g is a power of the irreducible polynomial g_1. Therefore $x^{\gamma} + f'$ is itself some power of g_1 or a constant which implies that $\gamma = 0 \bmod (\delta)$ contradicting the original assumption. Q. E. D.

Lemma 3. *The dimension of the vector space* $\mathcal{R}/\widehat{\mathcal{Q}}$ *(which is the same as the number of reduced monomials with respect to any Gröbner basis for* $\widehat{\mathcal{Q}}$*) is a multiple of* δ.

Proof: Consider any reduced monomial of the form $m = z^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, $i_j \geq 0$. The monomials $x_1^l m, l = 0, 1, \ldots, \delta - 1$ are also reduced by the lemma above. We can identify all these monomials with a class labelled by m. Similarly, every monomial can be identified with a unique class. Each class has exactly δ monomials. The lemma follows. Q. E. D.

Analysis of *Primary Component.*

By lemma 3, the number of reduced monomials with respect to any Gröbner basis for $\mathcal{Q}$ is $\rho\delta, \rho \geq 1$. By lemma 1, the number of reduced monomials with respect to $\mathcal{C}$ is increasing after each iteration of the *while-loop* except the last in algorithm *Primary Component.* Again, by lemma 3, this increase in each step is by a multiple of δ. Therefore, ρ is an upper bound on the number of iterations of the *while-loop* in *Primary Component.* This is a tight bound as the following example demonstrates. Let

$$\mathcal{Q} = (q_1^{\delta_1}, q_2^{\delta_2} - q_1, \ldots, q_n^{\delta_n} - q_{n-1})$$

where $q_1(x_1)$ is an irreducible polynomial in x_1 of degree δ and $q_i(x_i) = x_i - g_i(x_1), i > 1$. $\mathcal{Q}$ is primary with associated prime $\mathcal{P} = (q_1, q_2, \ldots, q_n)$. The above basis for $\mathcal{Q}$ is a reduced Gröbner basis under $>_l$ and the number of reduced monomials with respect to the basis is $\delta\delta_1\delta_2 \ldots \delta_n$. For any $\Delta < \delta_1\delta_2 \ldots \delta_n$, $\mathcal{P}^\Delta \not\subset \mathcal{Q}$ (clear from looking at the normal form of q_n^Δ with respect to $\mathcal{Q}$) while $\mathcal{P}^{\delta_1\delta_2\ldots\delta_n} \subset \mathcal{Q}$. Now, we can bound the main step in the loop, namely, $\mathcal{GB}(\mathcal{I}, \mathcal{P} \cdot \mathcal{B})$, which is essentially this:

Algorithm $\mathcal{GB}(\mathcal{I}, \mathcal{P} \cdot \mathcal{B})$:

1) Mutually reduce all polynomials in $\mathcal{I} \cup \mathcal{P} \cdot \mathcal{B}$ as much as possible. Let I' be the resulting set of normal forms (they need not be unique.)
2) Perform Buchberger's algorithm on I'.

At the end of each iteration of the *while-loop* in *Primary Component*, $\mathcal{B}$ is a reduced Gröbner basis for some primary ideal $\widehat{\mathcal{Q}}$ that divides $\mathcal{Q}$. Therefore, the dimension of the vector space $\mathcal{R}/\widehat{\mathcal{Q}} \leq \rho\delta$.

Bounding the number of *s*-polynomial reductions.

Lemma 4. *The number of reduced monomials and the number of lead terms with respect to the basis $\mathcal{P} \cdot \mathcal{B}$ (which is not a Gröbner basis) are bounded by $(n+1)\rho\delta$ and $n^2\rho$ respectively.*

Proof: If the number of reduced monomials with respect to $\mathcal{B}$ is $k\delta$, for some $k \leq \rho$, they can be put in k classes as before and since the lead monomials can only be *simple multiples* of the class labels (i.e., every lead monomial is of the form zm or $x_j m$ for some $j > 1$ where m is a class label, a consequence of lemma 2), the maximum number of lead terms in $\mathcal{B}$ is nk. In the basis $\mathcal{P} \cdot \mathcal{B}$, the old lead terms become reduced and the number of reduced monomials is therefore bounded by

$$\delta\rho + nk\delta \leq \delta\rho + n\rho\delta = (n+1)\rho\delta \qquad (= D, say).$$

Since $\mathcal{B}$ has atmost nr lead terms and $\mathcal{P}$ has n elements, the basis $\mathcal{P} \cdot \mathcal{B}$ has atmost $n^2k \leq n^2\rho$ lead terms. Q. E. D.

Lemma 5. *The number of s-polynomial reductions in step 2 of* $\mathcal{GB}(\mathcal{I}, \mathcal{P}\cdot\mathcal{B})$ *is* $O((nD+r)^2)$.

Proof: By the previous lemma, the number of lead terms in $(\mathcal{I}, \mathcal{P}\cdot\mathcal{B})$ before starting Buchberger's algorithm is bounded by $n^2\rho + r = T$(say). As usual, consider all possible pairs of lead terms – $\binom{T}{2}$ of them. Create 2 sets, *Tried* and *Untried*. Initially all the pairs are in *Untried*. The algorithm picks pairs from *Untried* and after performing the corresponding s-polynomial reduction, puts that pair in *Tried*. A "Step" is counted as all the action between two s-polynomial reductions that add a new polynomial to the basis. Each s-polynomial reduction, if not a zero reduction, decreases the number of reduced monomials by at least one. The number of reduced monomials is bounded from below by δ. Hence the number of irredundant s-polynomial reductions i.e., the number of "Steps" is no more than $D - \delta$. At the end of a "Step", we have a new polynomial g; augment the basis with it and also add (g, f) to *Untried* for every f in the current basis. We add atmost $T + D - \delta$ new pairs. The algorithm halts when *Untried* is empty. Now,

$$\begin{aligned}
&\max(|\mathit{Untried} \cup \mathit{Tried}|) \\
\leq &\binom{T}{2} + \sum_{1}^{D-\delta}(T+i) \\
\leq &(nD+r)^2 + (nD+r)D + D^2
\end{aligned}$$

which is a bound on the number of s-polynomial reductions performed. Q. E. D.

Bounding the cost of a single s-polynomial reduction.

Lemma 6. *A single s-polynomial reduction can be performed using* $O(D^4 + \varrho t r D^2)$ *field operations.*

Proof: A monomial of degree θ can be completely reduced with respect to $\mathcal{P}\cdot\mathcal{B}$ in $O(\theta D^2)$ steps, regarding each normal form as a vector of length D. If $\mathcal{I}$ has r polynomials each bounded in degree by ϱ and having at most t terms, then the first step in $\mathcal{GB}(\mathcal{I}, \mathcal{P}\cdot\mathcal{B})$ takes $O(\varrho t r D^2)$ steps.

Each s-polynomial reduction in the second step can be regarded as a normal form reduction of a polynomial of degree less than $2D$, and having at most $2D$ terms. A complete reduction takes $O(D^4)$ steps by similar analysis as before. Q. E. D.

Corollary. *The the number of field operations performed by the algorithm* $\mathcal{GB}$ *is* $O((D^4 + \varrho t r D^2)(nD+r)^2)$.

Proof: Immediate from lemmas 5 and 6. Q. E. D.

We can compute reduced Gröbner bases for all the primary components $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$ of $\mathcal{I}$ in this manner. By the above analysis, the cost of computing a reduced Gröbner basis for $\mathcal{Q}_i$ is polynomially bounded by $\dim(\mathcal{R}/\mathcal{Q}_i)$. Noting that $\dim(\mathcal{R}/\mathcal{I}) = \sum_i \dim(\mathcal{R}/\mathcal{Q}_i)$, we have:

Theorem 2. *Given a basis for a zero-dimensional ideal $\mathcal{I}$ and reduced Gröbner bases for all the prime ideals $\mathcal{P}_i$ containing $\mathcal{I}$, reduced Gröbner bases for all the primary ideals containing $\mathcal{I}$ can be constructed in time polynomial in the dimension of the vector space $\mathcal{R}/\mathcal{I}$.*

The next step is to put together the reduced Gröbner basis for $\mathcal{I}$ under the desired term ordering.

From Primaries to the Full Ideal

At this stage, we have computed reduced Gröbner bases for the primary ideals $\mathcal{Q}_1, \mathcal{Q}_2, \ldots, \mathcal{Q}_k$ where $\mathcal{I} = \mathcal{Q}_1 \cap \mathcal{Q}_2 \cap \ldots \cap \mathcal{Q}_k$. Let G_i be the Gröbner basis of $\mathcal{Q}_i$. This step is based on the simple observation that *a polynomial f belongs to $\mathcal{I}$ iff it belongs to each $\mathcal{Q}_i$* and using this observation in conjunction with the change of basis algorithm of Faugère et al [FGLM]. The algorithm proceeds as in the change of basis algorithm, computing normal forms of monomials in the required order with respect to each G_i separately. However, while looking for a linear relation among the normal forms, we look for one that holds simultaneously in each G_i. Precise description follows.

Let $\mathcal{N}_i(m)$ denote the normal form of monomial m with respect to G_i.
NewBasis: Gröbner basis being built.
ReducedMons: Set of monomials that are known to be reduced with respect to *NewBasis*; Initialized to $\{1\}$.
NextMonom: Function that returns the smallest monomial (under the desired admissible term ordering) that is neither in *ReducedMons* nor is a multiple of some lead term in *NewBasis*. Returns false if no such monomial exists.

ReducedMons := $\{1\}$;
NewBasis := $\{\ \}$;
while (m := *NextMonom*()) **do**
  If there exist $m_1, \ldots, m_s$ **in** *ReducedMons*, **and** $\lambda_j \in \mathbb{Q}$
  such that $\mathcal{N}_i(m) + \sum_{j=1}^{s} \lambda_j \mathcal{N}_i(m_j) = 0, \quad i = 1, \ldots, k$ **then,**
    NewBasis := *NewBasis* $\cup \{m + \sum_{j=1}^{s} \lambda_j m_j\}$
  else
    ReducedMons := *ReducedMons* $\cup \{m\}$;
    Save $\mathcal{N}_i(m), \quad i = 1, \ldots, k.$
  fi
  od end;

The total cost is bounded by the cost of finding linear relations among the normal forms. $\mathcal{N}_i(m)$ is a vector of length $\dim(\mathcal{R}/\mathcal{Q}_i)$. Therefore, the time for solving the linear systems required to find elements of *NewBasis* is polynomially bounded by $\dim(\mathcal{R}/\mathcal{I})$. Suppose d is the maximum of the degrees of the polynomials in the initial basis, then $\dim(\mathcal{R}/\mathcal{I}) \leq d^n$. Combining the results of [**Lak**], [**LL**] and the results presented in this paper so far, we have the following theorem.

Theorem 3. *Given a zero dimensional ideal*

$$\mathcal{I} = (f_1, f_2, \ldots, f_r) \subseteq \mathbb{Q}[x_1, x_2, \ldots, x_n]$$

the reduced Gröbner basis of $\mathcal{I}$ *under any admissible term ordering can be computed in time polynomial in* nd^n *where* $d = \max(\deg(f_i))$.

Remark 1: It was helpful for the analysis to assume that the ideal $\mathcal{I}$ is in general position. This however, is not required for the algorithm.

Remark 2: We assumed that we have a complete decomposition of the radical of $\mathcal{I}$ available. This is not necessary, since, if $\mathcal{Q}_1, \mathcal{Q}_2$ are primary components of $\mathcal{I}$ with distinct associated primes $\mathcal{P}_1, \mathcal{P}_2$, then

$$\mathcal{Q}_1\mathcal{Q}_2 = (\mathcal{I}, (\mathcal{P}_1\mathcal{P}_2)^\sigma)$$

where σ is at least as large as the maximum of the indices of $\mathcal{Q}_1$ and $\mathcal{Q}_2$. This might be helpful if one wants to trade factorization for longer lifting.

Remark 3: We have not taken into account the sizes of the rational numbers that arise during the algorithm in our analysis. For theorem 3 to hold while counting the number of bit operations instead of field operations, it is necessary to prove a polynomial bound (in d^n and the sizes of coefficients in the initial basis) on the sizes of numbers arising in the computations.

Conclusion

We have presented a single exponential time algorithm to construct a reduced Gröbner basis for a zero–dimensional ideal. At this time, the bottle neck is actually getting the radical. The methods proposed in [**Lak**], [**LL**] make use of the u-resultant and a change of coordinates which makes the problem *dense*. If these can be avoided, one might have a sparse, more practical algorithm for computing a reduced Gröbner basis for zero–dimensional ideals. We view the efforts described in this paper as a first step towards that goal.

Acknowledgements: I wish to thank my advisor Prof. Erich Kaltofen for several useful discussions and Prof. Daniel Lazard for his encouragement and suggestions.

REFERENCES

[CGH] Caniglia L., Galligo A., Heintz J., *Some New Effectivity Bounds in Computational Geometry*, in "Proc. 6th AAECC," LNCS 357, Springer-Verlag, pp. 131-152..

[DS] Dickenstein A.M., Sessa C., *Duality Methods for Membership Problem*, these proceedings.

[FGLM] Faugère J.C., Gianni P., Lazard D., Mora T., *Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering*, Tech. Report., LITP, Universite Paris, July 1989.

[GTZ] Gianni P., Trager B., Zacharias G., *Gröbner bases and Primary Decomposition of Polynomial Ideals*, Jour. Symb. Comp. **6** (1988), 149–167.

[Kre] Kredel H., *Primary Ideal Decomposition*, in "Proc. EUROCAL '87 Leipzig," LNCS vol.378, Springer-Verlag, 1987, pp. 270–281.

[KL] Krick T., Logar A., *Membership Problem, Representation Problem and the Computation of the Radical for One-dimensional Ideals*, these proceedings.

[Lak] Lakshman Y.N., *On the Complexity of Computing a Gröbner Basis for the Radical of a Zero Dimensional Ideal*, in "Proc. of 22nd ACM Symposium on Theory of Computing (STOC)," May 1990 (to appear).

[LL] Lakshman Y.N., Lazard D., *On the Complexity of Zero-dimensional Algebraic Systems*, these proceedings.

[vdW] van der Waerden B. L.,, "Algebra," vol.2, Frederick Ungar Pub. Co., 1970.

Lakshman Y. N.
Deptartment of Computer and Information Sciences
University of Delaware
103, Smith Hall
Newakk, DE 19716
U. S. A.
lakshman@math.udel.edu