NON-COMMUTATIVE GRÖBNER BASES FOR COMMUTATIVE ALGEBRAS

David Eisenbud, Irena Peeva and Bernd Sturmfels

Abstract. We show that an ideal I in the free associative algebra $k\langle X_1, \ldots, X_n\rangle$ over a field k has a finite Gröbner basis if the algebra defined by I is commutative; in characteristic 0 and generic coordinates the Gröbner basis may even be constructed by lifting a commutative Gröbner basis and adding commutators.

1. Introduction

Let k be a field, let $k[x] = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables and $k\langle X\rangle = k\langle X_1, \ldots, X_n\rangle$ the free associative algebra in n variables. Consider the natural map $\gamma : k\langle X\rangle \to k[x]$ taking X_i to x_i. It is sometimes useful to regard a commutative algebra $k[x]/I$ through its non-commutative presentation $k[x]/I \cong k\langle X\rangle/J$, where $J = \gamma^{-1}(I)$. This is especially true in the construction of free resolutions as in [An]. Non-commutative presentations have been exploited in [AR] and [PRS] to study homology of coordinate rings of Grassmannians and toric varieties. These applications all make use of Gröbner bases for J (see [Mo] for non-commutative Gröbner bases.) In this note we give an explicit description (Theorem 2.1) of the minimal Gröbner bases for J with respect to monomial orders on $k\langle X\rangle$ that are lexicographic extensions of monomial orders on $k[x]$.

Non-commutative Gröbner bases are usually infinite; for example, if $n = 3$ and $I = (x_1x_2x_3)$ then $\gamma^{-1}(I)$ does not have a finite Gröbner basis for any monomial order on $k\langle X\rangle$. (There are only two ways of choosing leading terms for the three commutators, and both cases are easy to analyze by hand.) However, after a linear change of variables the ideal becomes $I' = (X_1(X_1 + X_2)(X_1 + X_3))$, and we shall see in Theorem 2.1 that $X_1(X_1 + X_2)(X_1 + X_3)$ and the three commutators $X_iX_j - X_jX_i$ are a Gröbner basis for $\gamma^{-1}(I')$ with respect to a suitable order. This situation is rather general: Theorems 2.1 and 3.1 imply the following result:

Corollary 1.1. *Let k be an infinite field and $I \subset k[x]$ be an ideal. After a general linear change of variables, the ideal $\gamma^{-1}(I)$ in $k\langle X\rangle$ has a finite Gröbner basis. In characteristic 0, if I is homogeneous, such a basis can be found with degree at most $max\{2, regularity(I)\}$.*

In characteristic 0 the Gröbner basis of $\gamma^{-1}(I)$ in Corollary 1.1 may be obtained by lifting the Gröbner basis of I, but this is not so in characteristic p; see Example

1991 *Mathematics Subject Classification.* Primary: 13P10; Secondary 16S15.

The first and third authors are grateful to the NSF and the second and third authors are grateful to the David and Lucille Packard Foundation for partial support in preparing this paper.

4.2. Furthermore, $\gamma^{-1}(I)$ might have no finite Gröbner basis at all if the field is finite; see Example 4.1.

The behavior of $\gamma^{-1}(I)$ is in sharp contrast to what happens for arbitrary ideals in $k\langle X\rangle$. For example the defining ideal in $k\langle X\rangle$ of the group algebra of a group with undecidable word problem has no finite Gröbner basis. Another example is Shearer's algebra $k\langle a,b\rangle/(ac-ca, aba-bc, b^2a)\rangle$ which has irrational Hilbert series [Sh]. As any finitely generated monomial ideal defines an algebra with rational Hilbert series, the ideal $(ac-ca, aba-bc, b^2a)$ can have no finite Gröbner basis. (Other consequences of having a finite Gröbner basis are deducible from [An] and [Ba]); these are well-known in the case of commutative algebras!)

In the next section we present the basic computation of the initial ideal and Gröbner basis for $J = \gamma^{-1}(I)$. In §3 we give the application to finiteness and liftability of Gröbner bases.

2. The Gröbner basis of $\gamma^{-1}(I)$

Throughout this paper we fix an ideal $I \subset k[x]$ and $J := \gamma^{-1}(I) \subset k\langle X\rangle$. We shall make use of the *lexicographic splitting* of γ which is defined as the k-linear map

$$\delta \;:\; k[x] \longrightarrow k\langle X\rangle\,, \quad x_{i_1}x_{i_2}\cdots x_{i_r} \mapsto X_{i_1}X_{i_2}\cdots X_{i_r} \quad \text{if} \quad i_1 \le i_2 \le \cdots \le i_r.$$

Fix a monomial order $\prec$ on $k[x]$. The *lexicographic extension* $\prec\!\!\prec$ of $\prec$ to $k\langle X\rangle$ is defined for monomials $M, N \in k\langle X\rangle$ by

$$M \prec\!\!\prec N \quad \text{if} \quad \begin{cases} \gamma(M) \prec \gamma(N) & \text{or} \\ \gamma(M) = \gamma(N) & \text{and } M \text{ is lexicographically smaller than } N. \end{cases}$$

Thus for example $X_iX_j \prec\!\!\prec X_jX_i$ if $i<j$.

To describe the $\prec\!\!\prec$-initial ideal of J we use the following construction: Let L be any monomial ideal in $k[x]$. If $m = x_{i_1}\cdots x_{i_r} \in L$ and $i_1 \le \cdots \le i_r$ denote by $\mathcal{U}_L(m)$ the set of all monomials $u \in k[x_{i_1+1}, \ldots, x_{i_r-1}]$ such that neither $u\frac{m}{x_{i_1}}$ nor $u\frac{m}{x_{i_r}}$ lies in L. For instance, if $L = (x_1x_2x_3,\, x_2^d)$ then $\mathcal{U}_L(x_1x_2x_3) = \{\, x_2^j \mid j < d\,\}$.

Theorem 2.1. *The non-commutative initial ideal $in_{\prec\!\!\prec}(J)$ is minimally generated by the set $\{\, X_iX_j \mid j<i\,\}$ together with the set*

$$\{\; \delta(u\cdot m) \mid m \text{ is a generator of } in_{\prec}(I) \text{ and } u \in \mathcal{U}_{in_{\prec}(I)}(m) \;\}.$$

In particular, a minimal $\prec\!\!\prec$-Gröbner basis for J consists of $\{X_iX_j - X_jX_i : j<i\}$ together with the elements $\delta(u\cdot f)$ for each polynomial f in a minimal $\prec$-Gröbner basis for I and each monomial $u \in \mathcal{U}_{in_{\prec}(I)}(in_{\prec}(f))$.

Proof. We first argue that a non-commutative monomial $M = X_{i_1}X_{i_2}\cdots X_{i_r}$ lies in $in_{\prec\!\!\prec}(J)$ if and only if its commutative image $\gamma(M)$ is in $in_{\prec}(I)$ or $i_j > i_{j+1}$ for some j. Indeed, if $i_j > i_{j+1}$ then $M \in in_{\prec\!\!\prec}(J)$ because $X_sX_t - X_tX_s \in J$ has initial term X_sX_t with $s>t$. If on the contrary $i_1 \le \cdots \le i_r$ but $\gamma(M) \in in_{\prec}(I)$ then there exists $f \in I$ with $in_{\prec}(f) = \gamma(M)$. The non-commutative polynomial $F = \delta(f)$ satisfies $in_{\prec\!\!\prec}(F) = M$. The opposite implication follows because γ induces an isomorphism $k[x]/I \simeq k\langle X\rangle/\gamma^{-1}(I)$.

Now let $m' = u \cdot m$, where $m = x_{i_1} \cdots x_{i_r}$ is a minimal generator of $in_{\prec}(I)$ with $i_1 \leq \cdots \leq i_r$. We must show that $\delta(u \cdot m)$ is a minimal generator of $in_{\lll}(J)$ if and only if $u \in \mathcal{U}_{in_{\prec}(I)}(m)$.

For the "only if" direction suppose that $\delta(u \cdot m)$ is a minimal generator of $in_{\lll}(J)$. Suppose that u contains the variable x_j. We must have $j > i_1$ since else, taking j minimal, we would have $\delta(u \cdot m) = X_j \cdot \delta(\frac{u}{x_j} m)$. Similarly $j < i_r$. Thus $u \in k[x_{i_1+1}, \ldots, x_{i_r-1}]$. This implies $\delta(u \cdot m) = X_{i_1} \cdot \delta(u \frac{m}{x_{i_1}}) = \delta(u \cdot \frac{m}{x_{i_r}}) \cdot X_{i_r}$. Therefore neither $\delta(u \frac{m}{x_{i_1}})$ nor $\delta(u \frac{m}{x_{i_r}})$ lies in $in_{\lll}(J)$ and hence neither $u \frac{m}{x_{i_1}}$ nor $u \frac{m}{x_{i_r}}$ lies in $in_{\prec}(I)$.

For the "if" direction we reverse the last few implications. If $u \in \mathcal{U}_{in_{\prec}(I)}(m)$ then neither $\delta(u \frac{m}{x_{i_1}})$ nor $\delta(u \frac{m}{x_{i_r}})$ lies in $in_{\lll}(J)$ and therefore $\delta(u \cdot m)$ is a minimal generator of $in_{\lll}(J)$. □

3. Finiteness and lifting of non-commutative Gröbner bases

We maintain the notation described above. Recall that for a prime number p the *Gauss order* on the natural numbers is described by

$$s \leq_p t \quad \text{if} \quad \binom{t}{s} \not\equiv 0 \pmod{p}.$$

We write $\leq_0 = \leq$ for the usual order on the natural numbers. A monomial ideal L is called *p-Borel-fixed* if it satisfies the following condition: For each monomial generator m of L, if m is divisible by x_j^t but no higher power of x_j, then $(x_i/x_j)^s m \in L$ for all $i < j$ and $s \leq_p t$.

Theorem 3.1. *With notation as in Section 2:*

(a) If $in_{\prec}(I)$ is 0-Borel fixed, then a minimal $\lll$-Gröbner basis of J is obtained by applying δ to a minimal $\prec$-Gröbner basis of I and adding commutators.

(b) If $in_{\prec}(I)$ is p-Borel-fixed for any p, then J has a finite $\lll$-Gröbner basis.

Proof. Suppose that the monomial ideal $L := in_{\prec}(I)$ is p-Borel-fixed for some p. Let $m = x_{i_1} \cdots x_{i_r}$ be any generator of L, where $i_1 \leq \cdots \leq i_r$, and let $x_{i_r}^t$ be the highest power of x_{i_r} dividing m. Since $t \leq_p t$ we have $x_l^t m / x_{i_r}^t \in L$ for each $l < i_r$. This implies $x_l^t m / x_{i_r} \in L$ for $l < i_r$, and hence every monomial $u \in \mathcal{U}_L(m)$ satisfies $deg_{x_l}(u) < t$ for $i_1 < l < i_r$. We conclude that $\mathcal{U}_L(m)$ is a finite set. If $p = 0$ then $\mathcal{U}_L(m)$ consists of 1 alone since $x_l m / x_{i_r} \in L$ for all $l < i_r$. Theorem 3.1 now follows from Theorem 2.1. □

Proof of Corollary 1.1. We apply Theorem 3.1 together with the following results due to Galligo, Bayer-Stillman and Pardue which can be found in [Ei, Section 15.9]: if the field k is infinite, then after a generic change of variables, the initial ideal of I with respect to any order $\prec$ on $k[x]$ is fixed under the Borel group of upper triangular matrices. This implies that $in_{\prec}(I)$ is p-Borel-fixed in characteristic $p \geq 0$ in the sense above. If the characteristic of k is 0 and I is homogeneous then, taking the reverse lexicographic order in generic coordinates, we get a Gröbner basis whose maximal degree equals the regularity of I. □

We call the monomial ideal L *squeezed* if $\mathcal{U}_L(m) = \{1\}$ for all generators m of L or if, equivalently, $m = x_{i_1} \cdots x_{i_r} \in L$ and $i_1 \leq \cdots \leq i_r$ imply $x_l \frac{m}{\ldots} \in L$ or

$x_l \frac{m}{x_{i_r}} \in L$ for every index l with $i_1 < l < i_r$. Thus Theorem 2.1 implies that a minimal $\prec$-Gröbner basis of I lifts to a Gröbner basis of J if and only if the initial ideal $in_{\prec}(I)$ is squeezed. Monomial ideals that are 0-Borel-fixed, and more generally stable ideals (in the sense of [EK]), are squeezed. Squeezed ideals appear naturally in algebraic combinatorics:

Proposition 3.2. *A square-free monomial ideal L is squeezed if and only if the simplicial complex associated with L is the complex of chains in a poset.*

Proof. This follows from Lemma 3.1 in [PRS]. □

4. Examples in characteristic p

Over a finite field Corollary 1.1 fails even for very simple ideals:

Example 4.1. *Let k be a finite field and $n = 3$. If I is the principal ideal generated by the product of all linear forms in $k[x_1, x_2, x_3]$, then $\gamma^{-1}(I)$ has no finite Gröbner basis, even after a linear change of variables.*

Proof. The ideal I is invariant under all linear changes of variables. The $\lll$-Gröbner basis for J is computed by Theorem 2.1, and is infinite. That no other monomial order on $k\langle X\rangle$ yields a finite Gröbner basis can be shown by direct computation as in the example in the second paragraph of the introduction. □

Sometimes in characteristic $p > 0$ no Gröbner basis for a commutative algebra can be lifted to a non-commutative Gröbner basis, even after a change of variables:

Example 4.2. *Let k be an infinite field of characteristic $p > 0$, and consider the Frobenius power*

$$L \ := \ \big((x_1,\ x_2,\ x_3)^3\big)^{[p]} \quad \subset \quad k[x_1, x_2, x_3]$$

of the cube of the maximal ideal in 3 variables. No minimal Gröbner basis of L lifts to a Gröbner basis of $\gamma^{-1}(L)$, and this is true even after any linear change of variables.

Proof. The ideal L is invariant under linear changes of variable, so it suffices to consider L itself. Since L is a monomial ideal, it is its own initial ideal, so by Corollary 3.2 it suffices to show that L is not squeezed, that is, that neither of $x_1^{p-1}x_2^{p+1}x_3^{p}$ and $x_1^{p}x_2^{p+1}x_3^{p-1}$ is in L. This is obvious, since the power of each variable occurring in a generator of L is divisible by p and has total degree $3p$. □

References

[An] D. Anick, *On the homology of associative algebras*, Transactions Amer. Math. Soc. **296** (1986), 641-659.

[AR] D. Anick, G.-C. Rota, *Higher-order syzygies for the bracket algebra and for the ring of coordinates of the Grassmannian*, Proc. Nat. Acad. Sci. U.S.A. **88** (1991), 8087–8090.

[Ba] J. Backelin, *On the rates of growth of the homologies of Veronese subrings.*, Algebra, algebraic topology and their interactions (Stockholm, 1983), Lecture Notes in Math. 1183, Springer-Verlag, NY, 1986, p. 79–100,.

[Ei] D. Eisenbud, *Commutative Algebra With a View Toward Algebraic Geometry*, Springer-

[EK] S. Eliahou, M. Kervaire, *Minimal resolutions of some monomial ideals*, Journal of Algebra **129** (1990) 1–25.
[Mo] T. Mora, *An introduction to commutative and non-commutative Gröbner bases*, Theoretical Computer Science **134** (1994), 131–173.
[PRS] I. Peeva, V. Reiner and B. Sturmfels, *How to shell a monoid*, preprint, 1996.
[Sh] J. B. Shearer, J. Alg. 62 (1980), 228–231..

David Eisenbud, Dept. of Math., Brandeis University, Waltham, MA 02254
eisenbud@math.brandeis.edu

Irena, Peeva, Dept. of Math., University of California, Berkeley, CA 94720
irena@math.berkeley.edu

Bernd Sturmfels, Dept. of Math., University of California, Berkeley, CA 94720
bernd@math.berkeley.edu