ISSN: 1401-5617

An algorithm to determine the Hilbert series for graded associative algebras

Samuel Lundqvist

Research Reports in Mathematics
Number 3, 2005

Department of Mathematics
Stockholm University

Electronic versions of this document are available at
http://www.math.su.se/reports/2005/3

Date of publication: June 9, 2005

Postal address:
Department of Mathematics
Stockholm University
S-106 91 Stockholm
Sweden

Electronic addresses:
http://www.math.su.se/
info@math.su.se

An algorithm to determine the Hilbert series for graded associative algebras

Samuel Lundqvist

June 9, 2005

Abstract

In this paper we present an algorithm to compute the Hilbert series for quotients of the free algebra with homogeneous ideals. We also give a modified version of the algorithm for quotients of the polynomial ring. The algorithms are implemented in a computer program named "aalg" and we compare running times with other computer algebra programs.

1 Introduction

We are considering quotients of the free associative algebra $k\langle X_1, \ldots, X_n\rangle$ with homogeneous two sided ideals. Using the presentation

$$k\langle X_1, \ldots, X_n\rangle/(X_iX_j - X_jX_i)_{1\leq i<j\leq n} \cong k[X_1, \ldots, X_n] \qquad (1)$$

we are also able to study quotients of the polynomial ring. Our goal is to compute the Hilbert series for these quotients and the main idea is to construct spanning sets for the homogeneous components in each degree, then reduce them to a basis using linear algebra. If we introduce orderings on this spanning set in a suitable manner, we obtain, as a side effect, Gröbner bases for the algebras. The extensive use of linear algebra make us believe that the algorithms are well suited for parallel computations.

Based on the algorithms presented in this paper, a (single processor) computer program has been developed. The program is named "aalg" – for **a**ssociative **alg**ebra. With this program in hand, we present some results both for commutative and non-commutative algebras, and compare the running times with other computer algebra programs. In general, the program seems to be more effective in the non-commutative case. But for certain examples in the commutative setting – large monomial ideals and zero-dimensional ideals generated by forms with a large amount of monomials – the program is comparable with the standard computer algebra programs, and sometimes even faster.

The ideas in this paper are very much influenced by a method to compute the Hilbert series for graded Lie algebras, see [12].

2 Notation

Let Λ denote $k\langle X_1,\ldots,X_n\rangle$, where $k\langle X_1,\ldots,X_n\rangle$ is the free associative algebra over a field k, on generators X_i of degree $|X_i| = 1$. By a non-commutative graded algebra we shall mean

$$\Lambda/(f_1,\ldots,f_r),$$

where the f_i's are homogeneous of degree $|f_i| > 1$. We will refer to the f_i's as *the relations* and to an f_i as *a relation.*

Similarly, by a commutative graded algebra, we mean

$$k[X_1,\ldots,X_n]/(f_1,\ldots,f_r),$$

where $k[X_1,\ldots,X_n]$ is the polynomial ring on generators X_i of degree one, and the f_i's are homogeneous of degree $|f_i| > 1$.

When A is a graded algebra, write

$$A = \oplus_{i\geq 0} A_i,$$

where $A_0 = k$, and A_i is the degree i-part of A. By $A_{\geq n}$ we mean $\oplus_{i\geq n} A_i$ and $A_{<n}$ is defined by $A_{<n} = A/A_{\geq n}$ as a graded algebra.

Define the Hilbert series of A, denoted by $\mathrm{Hs}(A, z)$, to be the power series

$$\sum_{i\geq 0} \dim_k(A_i)\cdot z^i$$

and let the Hilbert function $\mathrm{Hf}(A, n)$ be defined by $\mathrm{Hf}(A, n) = \dim_k(A_n)$. We write $\mathrm{Hs}(z)$ and $\mathrm{Hf}(n)$, omitting A, if it is clear from the context which algebra we mean.

To simplify notation, we assume that tensor products always will be over k.

Remark 1. *The reason for grading over the non-negative integers and assuming the generators $\{X_i\}$ to be of degree $|X_i| = 1$, is simplicity. The theory we present can easily be extended to multigradings and arbitrary degrees of the generators.*

3 The main algorithm

Let $A = k\langle X_1,\ldots,X_n\rangle/I$, where the generators X_i are of degree one and $I = (f_1,\ldots,f_r)$. The aim of the algorithm is to produce a basis, degree by degree, for the k-vector spaces A_i. We have $\dim_k(\Lambda_0) = \dim_k(A_0) = 1$, and since the f_i's are of degree greater than one, we also have $\dim_k(\Lambda_1) = \dim_k(A_1) = n$. Let 1 be a basis for A_0 and $\{x_1,\ldots,x_n\}$ a basis for A_1. Identify the elements in Λ_1 with those in A_1 by $X_i \mapsto x_i$.

Now suppose we are given a basis for each degree up to $d-1$, how do we get a basis of degree d? As mentioned in the introduction, the problem is solved by constructing a generating set for the k-space A_d in degree d and then use linear algebra to reduce the span to a basis. We begin by defining a graded

Λ-module $A_{<d} \oplus (A_1 \otimes A_{d-1})$, with $A_1 \otimes A_{d-1}$ as the degree d-part. Let X_i act on elements of degree $< d-1$ by multiplication with the corresponding x_i in A_1. For elements a of degree $d-1$ we let $X_i.a = x_i \otimes a$ (where . denotes the module-operation), and on elements of degree d, Λ acts trivially.

Lemma 3.1. *Let N_d be the subspace of $A_1 \otimes A_{d-1}$ generated by the expressions $\{f_i.a\}$, for all relations f_i, and all homogeneous elements $a \in A_{<d}$ with $|a| + |f_i| = d$. Then*

$$(A_1 \otimes A_{d-1})/N_d \cong A_d$$

as k-vector spaces.

Proof. First, define a map h of k-vector spaces from $A_1 \otimes A_{d-1}$ to A_d by $x \otimes a \mapsto x \cdot a$. Since $A_d \subseteq A_1 A_{d-1}$, this map is surjective.

Suppose $f \in I$, with $|f| \leq d$. Write $f = \sum c(i_1, \ldots, i_{|f|}) X_{i_1} \cdots X_{i_{|f|}}$. Then, if $a \in A_{d-|f|}$,

$$f.a = (\sum c(i_1, \ldots, i_{|f|}) X_{i_1} \cdots X_{i_{|f|}}).a = \sum c(i_1, \ldots, i_{|f|}) x_{i_1} \otimes x_{i_2} \cdots x_{i_{|f|}} \cdot a,$$

so we get

$$h(f.a) = \sum c(i_1, \ldots, i_{|f|}) x_{i_1} \cdot x_{i_2} \cdots x_{i_{|f|}} \cdot a = \overline{f} \cdot a = 0.$$

Thus $N_d \subseteq \ker(h)$, so h induces a surjective map of k-vector spaces $\overline{h} : (A_1 \otimes A_{d-1})/N_d \to A_d$. We can also define a surjective map g of k-vector spaces from Λ_d to $A_1 \otimes A_{d-1}$ by $g : X_{i_1} X_{i_2} \cdots X_{i_n} \mapsto x_{i_1} \otimes x_{i_2} \cdots x_{i_n}$. Since

$$I_d = \sum_{i=0}^{d-|f_1|} \Lambda_i f_1 \Lambda_{d-|f_1|-i} + \sum_{i=0}^{d-|f_2|} \Lambda_i f_2 \Lambda_{d-|f_2|-i} + \cdots + \sum_{i=0}^{d-|f_r|} \Lambda_i f_r \Lambda_{d-|f_r|-i},$$

then if $b \in I_d$, b can be written as a sum $b_1 + \cdots + b_r$, where

$$b_j \in \sum_{i=0}^{d-|f_j|} \Lambda_i f_j \Lambda_{d-|f_j|-i}.$$

Furthermore, each b_j can be written as a sum $b_{j0} + b_{j1}$, where

$$b_{j0} \in f_j \Lambda_{d-|f_j|}$$

and

$$b_{j1} \in \sum_{i=1}^{d-|f_j|} \Lambda_i f_j \Lambda_{d-|f_j|-1} \subseteq \Lambda_1 I_{d-1},$$

so we have $g(b_{j1}) = 0$. On the other hand, $g(b_{j0}) \in N_d$. This shows that g induces a surjective map $\overline{g}$ of k-vector spaces from Λ_d / I_d to $(A_1 \otimes A_{d-1})/N_d$. But $\Lambda_d / I_d = A_d$, so the surjectivity of $\overline{g}$ and $\overline{h}$ shows that the vector spaces have the same dimension. □

Theorem 3.2. *There is an algebra structure on*

$$A_{<d} \oplus (A_1 \otimes A_{d-1})/N_d$$

such that

$$A_{<d} \oplus (A_1 \otimes A_{d-1})/N_d \cong A_{\leq d}$$

as graded algebras.

Proof. Extend $\overline{g}$ to $A_{\leq d}$ by letting it be the identity on elements of degree less than d. Now we can define the multiplication of elements a and b in $A_{<d} \oplus (A_1 \otimes A_{d-1})/N_d$ by $\overline{g}(\overline{g}^{-1}(a) \cdot \overline{g}^{-1}(b))$, which makes $A_{<d} \oplus (A_1 \otimes A_{d-1})/N_d$ become a graded algebra. By construction, $A_{<d} \oplus (A_1 \otimes A_{d-1})/N_d$ and $A_{\leq d}$ are isomorphic. □

The theorem does not give a canonical way to choose the basis elements. For practical purposes, we need *some* method for making this choice. This can be achieved by the following basic, but somewhat technical construction.

Order the set of elements $\{x_i \otimes e_j\}$ in degree d. The k-vector space N_d is spanned by $\{f_i.e \mid e \text{ a basis element in } A_{d-|f_i|}\}$, where each $f_i.e$ is a linear combination of elements in $\{x_i \otimes e_j\}$.

Define $\text{in}(f_i.e)$ to be the leading term with respect to this order (with coefficient one), and $\text{in}(N_d)$ to be the set of leading terms in N_d. Suppose $\text{in}(N_d) = \{x_{i_1} \otimes e_{j_1}, \ldots, x_{i_m} \otimes e_{j_m}\}$. Then, mod N_d, we can write

$$x_{i_k} \otimes e_{j_k} = \sum c(i,j,k) x_i \otimes e_j,$$

where $c(i_h, j_h, k) = 0$ for $1 \leq h \leq m$. Clearly the $n \cdot \dim_k(A_{d-1}) - m$ congruence classes $\{\overline{x_i \otimes e_j} \mid x_i \otimes e_j \notin \text{in}(N_d)\}$ constitute a basis for $(A_1 \otimes A_{d-1})/N_d$.

Assume inductively that the basis in lower degrees has been chosen according to this method. Then, to every basis element e of degree $1 < |e| < d$, there corresponds – under the isomorphism $\overline{g}$, since we assume $e \in A_{<d}$ – an unique element $\overline{x_{i(e)} \otimes \hat{e}}$, $|\hat{e}| = |e| - 1$, such that $x_{i(e)} \otimes \hat{e} \notin \text{in}(N_{|e|})$. If $|e| = 1$, then e is an $x_{i(e)}$.

Define the word function w on the set of basis elements by $w(e) = X_{i(e)}$ if $|e| = 1$ and recursively in higher degrees by $w(e) = X_{i(e)} \cdot w(\hat{e}) \in \Lambda$. Let $\tilde{w}$ be the extension of w to $\{x_i \otimes e_j\}$ by $\tilde{w}(x_i \otimes e_j) = X_i \cdot w(e_j)$. Extend w and $\tilde{w}$ to linear combinations in the obvious way.

This enables us to identify basis elements in $A_{\leq d}$ with words in Λ and we can induce orderings from Λ on $\{x_i \otimes e_j\}$ as follows. Let $\prec$ be any well ordering on the words in Λ. Then we can let the order between elements $x_i \otimes e_k$ and $x_j \otimes e_l$ be defined by the order between $\tilde{w}(x_i \cdot e_k)$ and $\tilde{w}(x_j \cdot e_l)$ given by $\prec$.

Lemma 3.3. *Let $\prec$ be any well ordering on the words in Λ that respects the multiplication. Induce this ordering on the N_i's as above. Then the set*

$$\tilde{w}(\text{in}(N_{\leq d}))$$

generates the initial ideal $\text{in}(I)_{\leq d}$ *of $I_{\leq d}$, with respect to $\prec$.*

Proof. Let

$$S_1 = \{X_{i_1} \cdots X_{i_d} | X_{i_1} \cdots X_{i_d} \notin \mathrm{in}(I)_d\}$$

and

$$S_2 = \{x_i \otimes e_j | x_i \otimes e_j \notin \mathrm{in}(N_d)\}$$

From the theory of Gröbner bases, we have $|S_1| = \dim_k(A_d)$ and from above $|S_2| = \dim_k(A_d)$. Since $\tilde{w}(N_d) \subseteq I$, it follows that $S_1 \subseteq \tilde{w}(S_2)$ and hence

$$S_1 = \tilde{w}(S_2). \tag{2}$$

Now proceed by induction, with trivial base case. Take $X_{i_1} \cdots X_{i_d} \in \mathrm{in}(I)_d$. If $X_{i_2} \cdots X_{i_d} \in \mathrm{in}(I)_{d-1}$, then by the induction assumption, $X_{i_1} \cdots X_{i_d}$ is in the ideal generated by $\tilde{w}(\mathrm{in}(N_{<d}))$. So suppose it is not in $\mathrm{in}(I)_{d-1}$. Then, by (2), there is an unique basis element e such that $w(e) = X_{i_2} \cdots X_{i_d}$. But $x_{i_1} \otimes e \notin \mathrm{in}(N_d)$ implies $\tilde{w}(x_{i_1} \otimes e) = X_{i_1} \cdots X_{i_d} \notin \mathrm{in}(I)_d$, a contradiction, so we must have $x_{i_1} \otimes e \in \mathrm{in}(N_d)$. □

Theorem 3.4. *$\cup_{i \leq d} \tilde{w}(N_i)$ is a Gröbner basis for $I_{\leq d}$ (with respect to $\prec$).*

Proof. Immediate from the lemma. □

Corollary 3.5. *Let e be a basis element. Then, for every subword a of $w(e)$, there exists a basis element e' with $w(e') = a$.*

Example 1. *Let $A = \mathbb{Q}\langle X_1, X_2 \rangle / I$, where I is the two-sided ideal $(X_1X_2 + X_2^2, X_2X_1 - X_2^2)$. We select basis elements using the lexicographical ordering (with $X_1 > X_2$). Let A_0 be spanned as a vector space by $\{1\}$ and A_1 by $\{x_1, x_2\}$. We construct $A_1 \otimes A_1$ and let the two relations act on the module $A_0 \oplus A_1 \oplus (A_1 \otimes A_1)$.*

$$(X_1X_2 + X_2^2).1 = X_1.x_2 + X_2.x_2 = x_1 \otimes x_2 + x_2 \otimes x_2,$$

$$(X_2X_1 - X_2^2).1 = X_2.x_1 - X_2.x_2 = x_2 \otimes x_1 - x_2 \otimes x_2.$$

Now $x_1 \otimes x_2 \succ x_2 \otimes x_2$ and $x_2 \otimes x_1 \succ x_2 \otimes x_2$. Thus, a basis for the quotient space $A_1 \otimes A_1/N_2$ is chosen as $\{\overline{x_1 \otimes x_1}, \overline{x_2 \otimes x_2}\}$. In A_2 we think of the elements written as x_1^2, x_2^2. Applying the word function on N_2, a Gröbner basis for $I_{\leq 2}$ is $\{X_1X_2 + X_2^2, X_2X_1 - X_2^2\}$.

To compute degree three, we use the basis obtained above for A_2 and construct $A_1 \otimes A_2$, which is spanned by $\{x_1 \otimes x_1^2, x_2 \otimes x_1^2, x_1 \otimes x_2^2, x_2 \otimes x_2^2\}$. There are four expressions spanning N_3. We get

$$\begin{aligned}(X_1X_2 + {X_2}^2).x_1 &= X_1.(X_2.x_1) + X_2.(X_2.x_1) \\ &= X_1.({x_2}^2) + X_2.({x_2}^2) = x_1 \otimes {x_2}^2 + x_2 \otimes x_2^2\end{aligned}$$

and

$$\begin{aligned}(X_1X_2 + X_2^2).x_2 &= X_1.(X_2.x_2) + X_2.(X_2.x_2) \\ &= X_1.(x_2^2) + X_2.(x_2^2) = x_1 \otimes x_2^2 + x_2 \otimes x_2^2.\end{aligned}$$

And in a similar manner

$$(X_2X_1 - {X_2}^2).x_1 = x_2 \otimes x_1^2 - x_2 \otimes x_2^2,$$
$$(X_2X_1 - {X_2}^2).x_2 = -2x_2 \otimes x_2^2.$$

In the lexicographical ordered basis $\{x_1 \otimes x_1^2, x_1 \otimes x_2^2, x_2 \otimes x_1^2, x_2 \otimes x_2^2\}$*, a matrix defined by the equations above, whose nullspace is* N_3*, looks like*

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

Row reducing this matrix, we see that $x_1 \otimes x_2^2 = x_2 \otimes x_1^2 = x_2 \otimes x_2^2 = 0$*. Thus* $\mathrm{in}(N_3) = \{x_1 \otimes x_2^2, x_2 \otimes x_1^2, x_2 \otimes x_2^2\}$ *and we choose* x_1^3 *as a basis for* A_3*. A Gröbner basis for* $I_{\leq 3}$ *is* $\{X_1X_2 + X_2^2, X_2X_1 - X_2^2, X_1{X_2}^2, X_2X_1^2, X_2^3\}$*. Notice that the Gröbner basis is not reduced. Both* $X_1X_2^2$ *and* $X_2X_1^2$ *are redundant.*

3.1 Hilbert-driven calculations

If we know a lower bound B of the Hilbert series, that is $B(n) \leq \mathrm{Hf}(A, n)$, for all n, then we can choose a subset N' of N_d and compute the rank r of the matrix defined by this subset. If r satisfies $\dim_k(A_1) \cdot \dim_k(A_{d-1}) - r = B(d)$, then any element in N_d is a linear combination of elements in N', and hence $(A_1 \otimes A_{d-1})/N' \cong A_d$. If $\dim_k(A_1) \cdot \dim_k(A_{d-1}) - r > B(d)$, then we can take more elements from N_d and recompute the rank, and so on.

3.2 Applications

We use the algorithm to study two different problems.

First application. Let $A = \mathbb{C}\langle X_1, \ldots, X_n\rangle/(f_1, \ldots, f_r)$, with the f_i's generic of degree 2. If $r \leq n^2/4$, the Hilbert series of A is

$$\frac{1}{1 - nz + rz^2}.$$

For $r > n^2/4$ the series is not known, but conjectured to be equal to

$$\left[\frac{1}{1 - nz + rz^2}\right],$$

where $[\sum a_i z_i] = \sum b_i z_i$, and

$$b_n = \begin{cases} a_n & \text{if } a_i > 0 \text{ for all } i \leq n \\ 0 & \text{otherwise} \end{cases}$$

Anick proves in [1] that if $g_1, \ldots, g_n$ are any forms and $|g_i| = |f_i|$, then the generic forms minimizes the Hilbert series in the sense that for all degrees d,

$$\mathrm{Hf}(k\langle X_1, \ldots, X_n\rangle/(g_1, \ldots, g_r), d) \leq \mathrm{Hf}(k\langle X_1, \ldots, X_n\rangle/(f_1, \ldots, f_r), d). \quad (3)$$

# variables	# forms of degree 2	time [s]
5	7	22.9
5	≥ 8	< 0.1
6	10	4892.8
6	11	1.6
6	12	0.1
6	≥ 13	< 0.1

Table 1: Runtimes over $\mathbb{Z}_2$ on an AMD Athlon XP 2500+ (1837.5 MHz), with 3 Gb RAM.

Consider $\mathbb{C}\langle X_1, \ldots, X_n\rangle/I$, where I is generated by forms $f_1, \ldots, f_r$ with coefficients in $\mathbb{Z}$. Let p be a prime and let I_p be the ideal generated by the f_i's, but where the coefficients for these generators are taken modulo p. Then

$$\mathrm{Hf}(\mathbb{C}\langle X_1, \ldots, X_n\rangle/I, d) \leq \mathrm{Hf}(\mathbb{Z}_p\langle X_1, \ldots, X_n\rangle/I_p, d). \tag{4}$$

This can be understood by the following reasoning. The dimension of I in degree d as a vector space over $\mathbb{C}$ is the rank of the matrix with columns indexed by the words of degree d and with rows $a_{1ij}f_ja_{2kj}$, for each f_j and all pairs of words (a_{1ij}, a_{2kj}) with $|a_{1ij}| + |f_j| + |a_{2kj}| = d$. But the rank of a matrix is the size m of its biggest minor different from 0. Clearly the size of the biggest minor in the matrix where the coefficients are taken modulo p is at most m, which imposes (4). A similar argument can be applied to (3).

The inequalities (3) and (4) shows that we can prove the conjecture to be true for fixed n and fixed r if we are able to find any example with the conjectured Hilbert series over Z_p, for any prime p. With the implementation of the algorithm, we find the conjecture to be true by constructing examples in $\mathbb{Z}_2$ for all r, when $n \leq 6$. We use $\mathbb{Z}_2$ because the program handles this field very efficiently. See section 5 for details. As far as we know, the previous known result was for $n \leq 4$. The runtimes are presented in Table 1, and the forms used for $n = 6$ and $r = 10$ were
$\{X_1^2 + X_5X_4 + X_6X_4, X_2^2 + X_3X_1 + X_4X_5, X_2X_5 + X_5X_3 + X_5X_6,$
$X_2X_1 + X_2X_4 + X_6X_1, X_1X_3 + X_3X_4 + X_6X_5, X_1X_5 + X_3X_6 + X_4X_6,$
$X_1X_6 + X_3^2 + X_3X_5, X_1X_2 + X_2X_3 + X_5^2 + X_6^2, X_2X_6 + X_3X_2 + X_4X_1 + X_4^2,$
$X_1X_4 + X_3X_1 + X_3X_6 + X_4X_1\}$.

The **second application** is the algebra $\mathcal{C}_5$, which belongs to a family $\{\mathcal{C}_n\}$ of algebras with presentations $\mathbb{C}\langle X_1, \ldots, X_n\rangle/I$, where I is a homogeneous ideal closed under some differential operators. These algebras occur in a tensor product decomposition of algebras from another family $\{\mathcal{E}_n\}$, and one has

$$\mathrm{Hs}(\mathcal{E}_n, z) = \mathrm{Hs}(\mathcal{C}_{n-1}, z) \cdots \mathrm{Hs}(\mathcal{C}_1, z).$$

$\mathcal{E}_n$ was first introduced in [5] and the decomposition was proved in [6].

The claim is that each $\mathcal{C}_i$ (or $\mathcal{E}_i$) is finite dimensional as a vector space and it has recently been verified with the computer algebra program Bergman

[2] for $i \in \{1, 2, 3, 4\}$. For $i = 5$, Bergman suffices to determine the vector space dimension up to degree 12 using Gröbner basis techniques over $\mathbb{Q}$. With our program we have pushed the result forward three steps and we are now considering the Hilbert series for $\mathcal{C}_5$ as
$1 + 5z + 20z^2 + 70z^3 + 220z^4 + 640z^5 + 1751z^6 + 4560z^7 + 11386z^8 + 27425z^9 + 64015z^{10} + 145330z^{11} + 321843z^{12} + 696960z^{13} + 1478887z^{14} + 3080190z^{15} + \cdots$
It should be noted that we have used characteristic 31991 for these calculations. We aim to work more on this problem in the future.

4 The commutative case

As mentioned in the introduction,

$$k\langle X_1, \ldots, X_n\rangle/(X_iX_j - X_jX_i)_{1\le i<j\le n} \cong k[X_1, \ldots, X_n].$$

This enables us to regard the commutators as ordinary relations and use the algorithm described in the preceding chapter to compute vector bases for polynomial rings divided with homogeneous ideals as well. But to get a fast method in the commutative setting, we need to make certain simplifications of the algorithm.

First we show that we only need to operate once with each relation.

Theorem 4.1. *Let C_d^* be the subspace of $A_1 \otimes A_{d-1}$ generated by the expressions $\{(X_iX_j - X_jX_i).a\}$, for all $1 \le i < j \le n$ and all $a \in A_{d-2}$. Let N_d^* be the subspace of $A_1 \otimes A_{d-1}$ generated by the expressions $\{f_i.1\}$, for all relations f_i of degree d. Then*

$$(A_1 \otimes A_{d-1})/(C_d^* + N_d^*) \cong A_d$$

as k-vector spaces.

Proof. It is enough to show that if f is a relation of degree $|f| < d$, then $\overline{f.e} = 0$, for all basis elements $e \in A_{d-|f|}$ in the quotient module $A_{<d} \oplus (A_1 \otimes A_{d-1})/C_d^*$. Write $f = \sum c(i_1, \ldots, i_{|f|})X_{i_1}\cdots X_{i_{|f|}}$ and fix one $X_{i_1}\cdots X_{i_{|f|}}$. Also write $w(e) = X_{w_1}\cdots X_{w_{d-|f|}}$. We make the following calculation in $A_{<d} \oplus A_1 \otimes A_{d-1}$:

$$\begin{aligned} X_{i_1}\cdots X_{i_{|f|}}.e &= X_{i_1}\cdots X_{i_{|f|}}.w(e).1 \\ &= X_{i_1}.w(e).X_{i_2}\ldots X_{i_{|f|}}.1 = X_{i_1}.X_{w_1}\ldots X_{w_{d-|f|}}.X_{i_2}\ldots X_{i_{|f|}}.1. \end{aligned}$$

But in the quotient module $A_{<d} \oplus (A_1 \otimes A_{d-1})/C_d^*$,

$$\begin{aligned} \overline{X_{i_1}.X_{w_1}\ldots X_{w_{d-|f|}}X_{i_2}\ldots X_{i_{|f|}}.1} &= \overline{X_{w_1}.X_{i_1}.X_{w_2}\ldots X_{w_{d-|f|}}.X_{i_2}\ldots X_{i_{|f|}}.1} \\ &= \overline{X_{w_1}\ldots X_{w_{d-|f|}}.X_{i_1}\ldots X_{i_{|f|}}.1} = \overline{w(e).X_{i_1}\ldots X_{i_{|f|}}.1}, \end{aligned}$$

which shows that

$$\overline{f.e} = \overline{w(e).f.1} = \overline{w(e).0} = 0$$

and the theorem follows. □

In general we have $\dim_k(A_d) \ll n \cdot A_{d-1}$, so it would be convenient if we had another k-vector space V, with a surjection to A_d, such that $\dim_k(V)$ is closer to $\dim_k(A_d)$. We accomplish this by introducing a slightly different module structure from the one defined in section 3. The drawback is that we have to fix an ordering on the set of basis elements.

4.1 A smaller span

If a basis has been chosen for $A_{<d}$ using our algorithm and the presentation (1), then for every basis element e we have that $w(e) \in \Lambda$, where w is the word function defined in section 3. Suppose

$$w(e) = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \tag{5}$$

holds in $A_{<d}$. Let $\min(e)$ be the least i such that α_i is nonzero, and let $\min(x_i, e) = \min(i, \min(e))$. By Corollary 3.5, there exists a basis element of degree $|e| - 1$ with corresponding word $X_{\min(e)}^{\alpha_{\min(e)}-1} \cdots X_n^{\alpha_n}$. Denote this element by $\hat{e}$.

Pick a basis element x_i of degree 1. Then $x_i \cdot e = \sum c(x_i, e, j)e_j$, $|e_j| = |e|+1$. If

$$\min(x_i, e) \leq \min(e_j), \text{for all } j \text{ with } c(x_i, e, j) \text{ non-zero,} \tag{6}$$

and condition (5) holds, then we say that the basis for $A_{<d}$ is *good*. We will later prove the existence of good bases.

Form a subspace V_d of $A_1 \otimes A_{d-1}$ spanned by the set

$$V_d = \{x_i \otimes e \mid i \leq \min(e)\}.$$

If $A_{<d}$ has a good basis, it is possible to define a Λ-module structure on $A_{<d} \oplus V_d$, by

$$X_i.e = \begin{cases} x_i \cdot e & \text{if } |e| < d-1 \\ x_i \otimes e & \text{if } |e| = d-1 \text{ and } i \leq \text{min}(e) \\ x_{\min(e)} \otimes (x_i \cdot \hat{e}) & \text{if } |e| = d-1 \text{ and } i > \text{min}(e) \\ 0 & \text{if } |e| \geq d. \end{cases} \tag{7}$$

That $x_{\min(e)} \otimes (x_i \cdot \hat{e}) \in V_d$ when $|e| = d-1$ and $i > \min(e)$ follows from (6).

Remark 2. *If the ideal is* 0*, then* $\dim_k(V_d) = \dim_k(A_d)$.

Lemma 4.2. *Suppose $A_{<d}$ has a good basis. Let N_d be the subspace of V_d generated by the expressions $\{f_i.1\}$, for f_i of degree d. Let C_d be the subspace of V_d generated by the commutators $\{(X_iX_j - X_jX_i).a\}, |a| = d-2$. Then $V_d/(C_d + N_d) \cong A_d$ as k-vector spaces.*

Proof. By Theorem 4.1, we have $A_d \cong (A_1 \otimes A_{d-1})/(C_d^* + N_d^*)$, The projection $\pi : A_1 \otimes A_{d-1} \to V_d/(C_d + N_d), x_i \otimes e \mapsto X_i.e$ is surjective. If $s = s_1 \cdot \hat{s}$ is a word and e a basis element such that $|s| + |e| = d$, then in the module $A_{<d} \oplus (A_1 \otimes A_{d-1})$, $s.e = s_1 \otimes \hat{s}e$, so $\pi(s.e) = s_1.\hat{s}.e = s.e$, where the dots to

the right indicates operation in $A_{<d} \oplus V_d$. This shows that $\pi(C_d^*) = C_d$ and $\pi(N_d^*) = N_d$, so π extends to a surjective map

$$\overline{\pi} : (A_1 \otimes A_{d-1})/(C_d^* + N_d^*) \to V_d/(C_d + N_d).$$

A_d is generated by $A_1 A_{d-1}$. Let e be a basis element in A_{d-1} and x_i any generator such that $i > \min(e)$. Then, by the commutativity and (6),

$$x_i \cdot e = x_i \cdot x_{\min(e)}\hat{e} = x_{\min(e)} \cdot x_i\hat{e} = \sum c(x_i, \hat{e}, j)x_{\min(e)} \cdot e_j,$$

where $\min(x_i, \hat{e}) \leq \min(e_j)$. Since $\min(e) \leq \min(x_i, \hat{e})$, every element in A_d can be expressed as a linear combination of elements $x_i \cdot e$, where $i \leq \min(e)$. Hence we also have a natural surjective map h of vector spaces from V_d to A_d. Suppose f is a relation (e.g. it might be a commutator). Then, in $A_{<d} \oplus V_d$,

$$f.a = (\sum c(i_1, \ldots, i_{|f|})X_{i_1} \cdots X_{i_{|f|}}).a = \sum c(i_1, \ldots, i_{|f|})X_{i_1}.(x_{i_2} \cdots x_{i_{|f|}} \cdot a).$$

Now, every $x_{i_2} \ldots x_{i_{|f|}}.a$ can be written as a linear combination of elements $\{e_j\}$ of degree $d-1$. Fix one e_j. If $i_1 \leq \min(e_j)$, then $X_{i_1}.e_j = x_{i_1} \otimes e_j \mapsto x_{i_1} \cdot e_j$, by h. Otherwise $X_{i_1}.e_j = x_{\min(e_j)} \otimes x_{i_1}\hat{e}_j \mapsto x_{\min(e_j)} \cdot x_{i_1}\hat{e}_j = x_{i_1} \cdot x_{\min(e_j)}\hat{e}_j = x_{i_1} \cdot e_j$ Thus every $f.a$ maps to $f \cdot a$, so h extends to a surjective map $\overline{h}$ from $V_d/(C_d + N_d)$ to A_d. The lemma follows from surjectivity of $\overline{\pi}$ and $\overline{h}$. □

Theorem 4.3. *$A_{<d} \oplus V_d/(C_d + N_d)$ is an algebra and isomorphic to $A_{\leq d}$. Furthermore, a good basis can be chosen for $A_{\leq d}$.*

Proof. As in the non-commutative case, $A_{<d} \oplus V_d/(C_d + N_d)$ becomes an algebra if we let multiplication be defined by the corresponding multiplication in $A_{\leq d}$ and then use the isomorphism to go back to $A_{<d} \oplus V_d/(C_d + N_d)$. This shows the isomorphism part.

Suppose that the basis for A_{d-1} is good. Order the elements in V_d by the lexicographical ordering and choose basis elements as $\{\overline{x_i \otimes e_j} \mid x_i \otimes e_j \notin \text{in}(N_d \cup C_d)\}$, according to section 3. Then, in $V_d/(N_d + C_d)$, every $\overline{x_k \otimes e_h}$ can be written as a linear combination of elements $\{\overline{x_i \otimes e_j}\}$ such that $x_k \otimes e_h \succeq x_i \otimes e_j$. By the property of V_d, $\min(x_k, e_h) = k$, so if we let e_{ij} be the element in A_d corresponding to $\overline{x_i \otimes e_j} \in V_d/(C_d + N_d)$, then $\min(e_{ij}) = i$. Since $x_k \otimes e_h \succeq x_i \otimes e_j \Leftrightarrow X_k w(e_h) \succeq X_i w(e_j)$, and $\prec$ is lex, it follows that $k \leq i$ and hence the basis is good. The second part of theorem hence follows by induction. □

Theorem 4.4. *$\cup_{i \leq d}(w(C_i) \cup w(N_i))$ is a Gröbner basis in lex for $I_{\leq d}$.*

Proof. Identical to the non-commutative case. □

It will be convenient to think of $w(e) = X_1^{\alpha_i} \cdots X_n^{\alpha_n} \in \Lambda$ as a monomial in the polynomial ring, so we write $\text{mon}(w(e))$ to denote the *monomial* $X_1^{\alpha_i} \cdots X_n^{\alpha_n}$.

Corollary 4.5. *Let e be a basis element. Then, for every monomial m such that $m|mon(w(e))$, there exists an unique basis element e' such that* $\mathrm{mon}(w(e')) = m$.

Before we illustrate the algorithm with an example, we give two lemmas that reduces the calculations.

Lemma 4.6. *Let e be a basis element of degree $d-1$, and suppose* $\min(e) = i$. *Then $(X_jX_i - X_iX_j).\hat{e} = 0$ in V_d, for all $j \geq i$.*

Proof. If $j = i$, it is clear. Suppose $j > i$. Then $X_jX_i.\hat{e} = X_j.(x_i\hat{e}) = X_j.e = x_i \otimes (x_j\hat{e}) = X_iX_j.\hat{e}$. □

Lemma 4.7. *Let C_d^i be the submodule generated by all expressions $\{(X_iX_j - X_jX_i).a\}$, for all j and all a of degree $d-2$. Suppose e is a basis element of degree $d-2$ and that $X_i|\,\mathrm{mon}(w(e))$. Then $\overline{(X_kX_j - X_jX_k).e} = 0$, for all j and all k in the submodule $A_{<d} \oplus V_d/C_d^i$.*

Proof. Write $w(e) = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. Let $b = X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}} X_i^{\alpha_i - 1} X_{i+1}^{\alpha_{i+1}} \cdots X_n^{\alpha_n}$. Then

$$\begin{aligned}\overline{X_kX_j.e} &= \overline{X_kX_j.X_i.b.1} = \overline{X_kX_i.X_j.b.1} = \overline{X_iX_k.X_j.b.1}\\ &= \overline{X_iX_j.X_k.b.1} = \overline{X_jX_i.X_k.b.1} = \overline{X_jX_k.X_i.b.1} = \overline{X_jX_k.e}.\end{aligned}$$

□

This gives us the following method to get the span for C_d. Add all expressions $(X_1X_i - X_iX_1).e$. Then add all expressions $(X_2X_i - X_iX_2).e$, for all $i > 2$ and all e such that $X_1 \nmid \mathrm{mon}(w(e))$. Continue to add $(X_3X_i - X_iX_3).e$, for all $i > 3$ and all e such that neither X_1 nor X_2 divides $\mathrm{mon}(w(e))$, and so on.

Example 2. *Suppose $I = (X_1X_2, X_2X_3 - X_3^2) \subseteq \mathbb{Q}[X_1, X_2, X_3]$ and put $A = \mathbb{Q}[X_1, X_2, X_3]/I$. We let 1 and $\{x_1, x_2, x_3\}$ span A_0 and A_1 respectively. Now V_2 is spanned by $\{x_1 \otimes x_1, x_1 \otimes x_2, x_2 \otimes x_2, x_1 \otimes x_3, x_2 \otimes x_3, x_3 \otimes x_3\}$. The relations operating on $A_0 \oplus A_1 \oplus V_2$ gives:*

$$\begin{gathered}X_1X_2.1 = X_1.x_2 = x_1 \otimes x_2\\ (X_2X_3 - X_3^2).1 = X_2.x_3 - X_3.x_3 = x_2 \otimes x_3 - x_3 \otimes x_3.\end{gathered}$$

By Lemma 4.6, the commutators operate as zero. A Gröbner basis in lex for $I_{\leq 2}$ is of course $\{X_1X_2, X_2X_3 - X_3^2\}$.

In V_2/N_2, $\overline{x_2 \otimes x_3} = \overline{x_3 \otimes x_3}$. Since $X_2X_3 \succ X_3^2$, we let A_2 be spanned by $\{x_1^2, x_2^2, x_1x_3, x_3^2\}$. In degree three, V_3 is spanned by following seven elements:

$$\{x_1 \otimes x_1^2, x_1 \otimes x_2^2, x_2 \otimes x_2^2, x_1 \otimes x_1x_3, x_1 \otimes x_3^2, x_2 \otimes x_3^2, x_3 \otimes x_3^2\}.$$

There are no f_i's of degree 3, so $N_3 = 0$.

To get C_3, we follow the procedure described above. In the first step we add $\{(X_1X_2 - X_2X_1).x_1, (X_1X_3 - X_3X_1).x_1, (X_1X_2 - X_2X_1).x_2, (X_1X_3 - X_3X_1).x_2, (X_1X_2 - X_2X_1).x_3, (X_1X_3 - X_3X_1).x_3\}$. Since x_1^2 and x_1x_3 are basis elements, *by lemma 4.6, only the third and the fourth expressions are non-zero, and we put*

$$(X_1X_2 - X_2X_1).x_2 = x_1 \otimes x_2^2$$
$$(X_1X_3 - X_3X_1).x_2 = x_1 \otimes x_3^2$$

into our spanning set. In step 2*, the only expression left is*

$$(X_2X_3 - X_3X_2).x_3 = x_2 \otimes x_3^2 - x_3 \otimes x_3^2.$$

Thus, there are three expressions spanning C_3. A a Gröbner basis for $I_{\leq 3}$ in lex is

$$\{X_1X_2, X_2X_3 - X_3^2, X_1X_2^2, X_1X_3^2, X_2X_3^2 - X_3^3\}.$$

As in the non-commutative case, the Gröbner basis is not minimal, since for instance $X_1X_2|X_1X_2^2$. We conclude that A_3 is four dimensional as a $\mathbb{Q}$-vector space and spanned by $\{x_1^3, x_2^3, x_1^2x_3, x_3^3\}$.

Remark 3. *The Λ-module structure (7) on $A_{<d} \oplus V_d$ can be generalized to situations when A is not commutative. It is enough to have $X_iX_j - s(i,j)X_jX_i \in I$, for all i, j, where $s : \{1 \dots n\} \times \{1 \dots n\} \mapsto k$. If we assume the basis to be good (which is possible), then we get a Λ-module structure on $A_{<d} \oplus V_d$ by*

$$X_i.e = \begin{cases} x_i \cdot e & \textit{if } |e| < d-1 \\ x_i \otimes e & \textit{if } |e| = d-1 \textit{ and } i \leq \min(e) \\ s(i, \min(e))x_{min(e)} \otimes (x_i \cdot \hat{e}) & \textit{if } |e| = d-1 \textit{ and } i > \min(e) \\ 0 & \textit{if } |e| \geq d. \end{cases}$$

However, Theorem 4.1 does not hold in general, so we have to stick to a weaker form of Theorem 4.3; operating with the relations in each degree as in section 3. But when $s(i,j)$ is constant, one easily shows that Theorem 4.1 and also Theorem 4.3 holds. So for instance, we can use the method to compute quotients of the exterior algebra.

4.2 Termination of the algorithm

When A is commutative, the algorithm actually gives a closed expression for the Hilbert series of A in a finite number of steps. To prove this, we use results obtained by Macaulay and Gotzmann.

If h and i are positive integers, then h can be uniquely written as a sum

$$h = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j},$$

where

$$n_i > n_{i-1} > \cdots > n_j \geq j \geq 1.$$

See [13] for an easy proof. This sum above is called the binomial expansion of h in base i. Define

$$h^{<i>} = \binom{n_i + 1}{i+1} + \binom{n_{i-1} + 1}{i} + \cdots + \binom{n_j + 1}{j+1}.$$

The following characterizations of quotients of the polynomial ring is due to Macaulay. The proof can be found in for instance [14].

Theorem 4.8 (Macaulay)**.** *The following are equivalent*

(i) There exists a graded commutative algebra A with Hilbert function Hf*.*

(ii) $\mathrm{Hf}(0) = 1$ *and* $\mathrm{Hf}(n+1) \leq \mathrm{Hf}(n)^{<n>}$.

Example 3. *There is no* $A = k[X_1, \dots, X_n]/I$ *with* $\dim_k(A_1) = 3$, $\dim_k(A_2) = 5$, $\dim_k(A_3) = 8$, *since* $5 = \binom{3}{2} + \binom{2}{1}$, *and* $5^{<2>} = \binom{4}{3} + \binom{3}{2} = 7 < 8$.

Theorem 4.9 (Gotzmann's persistence theorem)**.** *If* Hf *is the Hilbert function of* $k[X_1, \dots, X_n]/I$*, for some homogeneous ideal I, and the maximal degree of the generators of I is t, then if* $\mathrm{Hf}(n+1) = \mathrm{Hf}(n)^{<n>}$ *for some $n \geq t$, then* $\mathrm{Hf}(m+1) = \mathrm{Hf}(m)^{<m>}$ *for all $m \geq n$.*

Gotzmann's original proof can be found in [7]. For a more combinatorial approach, see [8].

Write $\langle X_i, \dots, X_n\rangle^d$ for the set of monomials in $\{X_i, \dots X_n\}$ of degree d. A Lex-segment set L on $\{X_1, \dots, X_n\}$ of degree d, is the $|L|$ biggest monomials in $\langle X_1, \dots, X_n\rangle^d$ with respect to the lexicographical ordering. Let L^c be the complement $\langle X_1, \dots, X_n\rangle^d \setminus L$.

Suppose $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is the smallest element in L. Then

$$\begin{aligned} L^c = \big(&X_1^{\alpha_1-1}\langle X_2, \dots, X_n\rangle^{d-(\alpha_1-1)} \sqcup X_1^{\alpha_1-2}\langle X_2, \dots, X_n\rangle^{d-(\alpha_1-2)} \sqcup \cdots \\ &\sqcup \langle X_2, \dots, X_n\rangle^d\big) \sqcup \big(X_1^{\alpha_1}X_2^{\alpha_2-1}\langle X_3, \dots, X_n\rangle^{d-(\alpha_1+\alpha_2-1)} \sqcup \cdots \\ &\sqcup X_1^{\alpha_1}\langle X_3, \dots, X_n\rangle^{d-\alpha_1}\big) \sqcup \cdots \\ &\sqcup \big(X_1^{\alpha_1} \cdots X_{n-2}^{\alpha_{n-2}} X_{n-1}^{\alpha_{n-1}-1}\langle X_n\rangle^{d-(\alpha_1+\cdots+\alpha_{n-1}-1)} \sqcup \cdots \\ &\sqcup X_1^{\alpha_1} \cdots X_{n-2}^{\alpha_{n-2}}\langle X_n\rangle^{d-(\alpha_1+\cdots+\alpha_{n-2})}\big), \end{aligned}$$

where the first parenthesis should be removed if $\alpha_1 = 0$, the second should be removed if $\alpha_2 = 0$ and so on. This implies that $|L^c|$ is equal to

$$\begin{aligned} &\left(\binom{n-1-1+d-\alpha_1+1}{d-\alpha_1+1} + \binom{n-1-1+d-\alpha_1+2}{d-\alpha_1+2} + \cdots \right. \\ &\left. + \binom{n-1-1+d}{d}\right) + \left(\binom{n-2-1+d-\alpha_1-\alpha_2+1}{d-\alpha_1-\alpha_2+1} + \cdots \right. \\ &\left. + \binom{n-2-1+d-\alpha_1}{d-\alpha_1}\right) + \cdots \\ &+ \left(\binom{n-(n-1)-1+d-\alpha_1-\cdots-\alpha_{n-1}+1}{d-\alpha_1-\cdots-\alpha_{n-1}+1} + \cdots \right. \\ &\left. + \binom{n-(n-1)-1+d-\alpha_1-\cdots-\alpha_{n-2}}{d-\alpha_1-\cdots-\alpha_{n-2}}\right), \end{aligned}$$

where again the i'th parenthesis should be removed if $\alpha_i = 0$.

Thus we get the binomial expansion of $|L_c|$ in base d. Of course, this can be used as a proof of the existence of a binomial expansion in a given basis.

If L is a lex-segment, let $\langle X_1, \ldots, X_n \rangle L$ be the set of all monomials m such that $m = X_i \cdot m'$, for some i and $m' \in L$

Lemma 4.10. *If $L \subseteq \langle X_1, \ldots, X_n \rangle^d$ is a lex-segment, then $\langle X_1, \ldots, X_n \rangle L$ is a lex-segment.*

Proof. To get a contradiction, assume that $m = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is the minimal monomial not in $\langle X_1, \ldots, X_n \rangle L$, such that there exists a monomial less than m in $\langle X_1, \ldots, X_n \rangle L$. Write $m = X_{i_1}^{\alpha_{i_1}} \cdots X_{i_k}^{\alpha_{i_k}}$, where all i_j's are nonzero. If $k = 1$ and $i_1 = n$, then e.g. $m = X_n^d$, a contradiction since this is the smallest element with respect to the lexicographical ordering. Otherwise, note that

$$m' = X_{i_1}^{\alpha_{i_1}} \cdots X_{i_{k-1}}^{\alpha_{i_{k-1}}-1} X_{i_k}^{\alpha_{i_k}+1}$$

is the biggest monomial less than m. By the minimal assumption, $m' \in \langle X_1, \ldots, X_n \rangle L$. But this implies that $\frac{m'}{X_{i_l}} \in L$, for some l. Since L is a lex-segment and $\frac{m'}{X_{i_l}} \cdot \frac{X_{i_l}}{X_{i_k}} \geq \frac{m'}{X_{i_l}}$, it follows that $\frac{m'}{X_{i_l}} \cdot \frac{X_{i_l}}{X_{i_k}} = \frac{m'}{X_{i_k}} \in L$. Hence $m = \frac{m'}{X_{i_k}} \cdot X_{i_{k-1}} \in \langle X_1, \ldots, X_n \rangle L$, a contradiction.

□

Proposition 4.11. *Let L be a lex-segment on $\{X_1, \ldots, X_n\}$ in degree d. Let I be the ideal generated by L, and consider $A = k[X_1, \ldots, X_n]/I$, for some field k. Then $\dim_k(A_{d+1}) = \dim_k(A_d)^{<d>}$.*

Proof. We have $\dim_k(A_d) = L^c$. Let $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ be the smallest element in L. Then $X_1^{\alpha_1} \cdots X_n^{\alpha_n+1}$ is the smallest element in $\langle X_1, \ldots, X_n \rangle L$ (which is a lex-segment by the lemma). It follows that the number of elements smaller than $X_1^{\alpha_1} \cdots X_n^{\alpha_n+1}$ is $\dim_k(A_{d+1})$. Note that the expansion of L^c is independent of α_n. Thus, to get the expansion of $\dim_k(A_{d+1})$, we only need to replace d by $d+1$. This proves the proposition.

□

Theorem 4.12. *If A is a graded algebra, then there is a d greater than or equal to the maximal degree m of the ideal generators $\{f_i\}$, such that $\dim_k(A_{t+1}) = \dim_k(A_t)^{<t>}$, for all $t \geq d$.*

Proof. For a lex-segment L, let $I(L)$ be the ideal generated by L. Define $\operatorname{codim}(L)_j = \dim_k(k[X_1, \ldots, X_n]/I(L))_j$. Construct a sequence $L_1, L_2, \ldots$ of lex-segment sets as follows. Let L_1 be a lex-segment set in degree 1 such that $\dim_k(A_1) = \operatorname{codim}(L_1)_1$. Suppose L_i is such that $\dim_k(A_i) = \operatorname{codim}(L_i)_i$. By Macaulay's theorem and Proposition 4.11, $\operatorname{codim}(L_i)_{i+1} - \dim_k(A_{i+1}) = d \geq 0$. $L' = \langle X_1, \ldots, X_n \rangle L_i$ is a lex-segment by Lemma 4.10. Let L_{i+1} be the union of L' and the d biggest element in $\langle X_1, \ldots, X_n \rangle^{i+1} \setminus L'$. Then L_{i+1} is a lex-segment and $\dim_k(A_{i+1}) = \operatorname{codim}(L_{i+1})_{i+1}$.

This gives us a chain of ideals, $I(L_1) \subseteq \cdots \subseteq I(L_m) \subseteq I(L_{m+1}) \subseteq \cdots$ and by the noetherian property, equality must occur in a finite number l of steps. But equality between $I(L_l)$ and $I(L_{l+1})$ is the same as $\operatorname{codim}(L_l)_{l+1} = \dim_k(A_{l+1})$. Thus $\dim_k(A_{l+1}) = \dim_k(A_l)^{<l>}$ by Proposition 4.11. The theorem now follows from the persistence theorem. $\square$

Corollary 4.13. *The algorithm gives a closed expression for the Hilbert series in finite time.*

Remark 4. *The Gotzmann criteria is quite weak in practice. Consider for instance the case when I is one-dimensional. Then the Hilbert function eventually gets constant. But $\mathrm{Hf}(i)^{<i>} = \mathrm{Hf}(i+1)$ is equivalent with*

$$\binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j} = \binom{n_i+1}{i+1} + \binom{n_{i-1}+1}{i} + \cdots + \binom{n_j+1}{j+1},$$

where the left hand side is the binomial expansion of $\mathrm{Hf}(i)$. It is easy to see that equality occurs only if $n_i = i, \forall i \geq j$. But this implies $\mathrm{Hf}(i) = i - j + 1$. It follows that the Gotzmann criteria applies only when $\mathrm{Hf}(i) \leq i$.

So if for $\mathrm{Hs}(A,z) = 1+4z+14z^2+16z^3+14z^4+9z^5+5z^6+6z^7+6z^8+\cdots$, then we can apply the Gotzmann criteria in degree 8 (provided the ideal generators are of lower degrees than 8). But if $\mathrm{Hs}(A,z) = 1 + 5z + 13z^2 + 24z^3 + 35z^4 + 43z^5 + 47z^6 + 48z^7 + 48z^8 + \cdots$, then the Gotzmann criteria would apply for the first time in degree 48.

4.3 Runtimes

As mentioned in the introduction, the program has not proved to be quite as effective in the commutative case. This has much to do with the weakness of the Gotzmann-criteria. For instance, aalg does not terminate in within five minutes for simple examples such as homogeneous cyclic 6-roots (which turns out to be a 2-dimensional ideal). This problem is solved by the standard programs in less than one second.

But we have found two instances of problems were the program is fast compared to three existing computer algebra systems; Cocoa [3], Macaulay2 [9], and Singular [10].

First example. We consider in the first case zero-dimensional ideals generated in degree 2,3 and 4, with dense relations in the sense that they consists of linear combination selected at random, of in average 50 percent of all monomials in the specific degree. The runtimes are presented in table 2.

In Cocoa, we used `Hilbert` and in Macaulay2 `hilbertSeries` to compute the Hilbert series. The monomialorder used in both cases were degrevlex. In Singular we used `std` to compute a `standard`-basis in `dp`-ordering, and `hilb` to determine the Hilbert series.

When I is zero-dimensional, theorem 4.4 shows that the algorithm gives a lexicographical Gröbner basis for I. An algorithm that is known to be fast when computing a lexicographical Gröbner basis for a zero-dimensional ideal is the

# vars	#2	#3	#4	char	aalg	coc.	mac.	sin.	s. fglm
10	9	4	2	2	0.9	25.9	7.4	3.8	6.6
10	9	4	2	31991	79.7	91.0	29.2	11.1	17.7
10	3	5	95	2	1.5	*	51.4	36.6	45.0
10	3	5	95	31991	125.1	*	183.4	103.5	136.1
15	30	30	30	2	6.2	169.0	32.3	21.1	25.5
15	30	30	30	31991	131.5	*	98.4	70.0	74.3
15	20	10	30	2	28.6	*	*	*	*

Table 2: Comparison of runtimes for some computer algebra packages on an AMD Athlon XP 2500+ (1837.5 MHz), with 3 Gb RAM. $*$ indicates that the time used exceeded the time limit of 300 [s]. Columns two, three and four indicates the number of forms in degree two, three and four respectively used to generate the ideal.

fglm-algorithm, see [4]. The idea is to first compute a Gröbner basis in degrevlex, which gives a vector space over k, and then use this space to determine the lexicographical Gröbner basis. The fglm-algorithm is implemented in Singular, and the last column in table 2 shows the time used to compute a Gröbner basis in lex using this implementation. To invoke the fglm-algorithm, we used `lp` as monomialorder and then the command `stdfglm`.

Table 2 indicates that using our algorithm to compute Hilbert series and also Gröbner bases in lex is comparable with the standard methods.

The huge difference between the running times for $\mathbb{Z}_2$ and $\mathbb{Z}_{31991}$ for aalg is explained in section 5.

Second example. Let the ideal $I(m) \subset k[X_1, \ldots, X_n]$ be generated by all monomials X_iX_j such that $i + j \neq 0 \pmod{m}$. When $m > 2n$, $I(m)$ will consist of all elements of degree 2, and so the Hilbert series for $k[X_1, \ldots, X_n]/I$ is simply $1 + nz$. On the other hand, when $m = 1$, the series is $1/(1-z)^n$, since $I(1) = 0$.

In Macaulay2 we used `monomialIdeal` to define the ideal and then `hilbertSeries` to compute the Hilbert series. In Singular we use `ideal` to define the ideal, and `hilb` to compute the Hilbert series (without calling `std`). In Cocoa, `Ideal` was used to define the ideal, and `Hilbert` to compute the Hilbert series.

Table 3 shows that in general, the computational time decreases for aalg when m is large. For the other programs it is the other way around; the computational time increases with m. For some numbers, for instance $n = 100$ and $m = 2$, aalg does not terminate within the time limit (this is also the case when $n = 200$), which seems strange since the termination time for $m = 3$ is almost only 1 second. This has of course to do with the Gotzmann criteria, for if $\dim(I) > 0$, then the algorithm terminates only if $\mathrm{Hf}(A, n+1) = \mathrm{Hf}(A, n)^{<n>}$, for some n, and there is no good rule of thumb for when this equality occurs.

The results shows that our program could be of use also in the case when a Gröbner basis is already known, but where the Hilbert series is not. But the

n	m	aalg	cocoa	macaulay2	singular	gotzmann	dim
100	1	<0.1	<0.1	<0.1	<0.1	2	100
100	2	*	3.8	37.4	2.0	>5	50
100	3	1.1	7.4	73.6	4.2	4	33
100	4	*	9.1	89.1	5.2	>6	25
100	5	0.5	10.3	103.2	6.1	4	20
100	22	1.4	14.3	146.3	8.1	12	5
100	100	0.1	15.2	154.9	9.0	4	1
100	201	<0.1	15.3	158.4	9.3	2	0
200	1	<0.1	0.1	<0.1	<0.1	2	200
200	5	8.2	*	*	199.1	4	40
200	22	*	*	*	268.6	>13	9
200	100	0.9	*	*	272.1	4	2
200	401	0.6	*	*	283.9	2	0

Table 3: Comparison of runtimes for some computer algebra packages on an AMD Athlon XP 2500+ (1837.5 MHz), with 3 Gb RAM. * indicates that the time used exceeded the time limit of 300 [s]. An i in the Gotzmann-column indicates that $\mathrm{Hf}(A,n) = \mathrm{Hf}(A,n-1)^{<n-1>}$ holds for $n = i$ and for no $n < i$.

uncertainty of the termination time is a problem. Maybe it would be a good idea to check the Gotzmann-criteria (which is of almost no cost) in the standard algorithms when computing Hilbert series.

5 Implementation

Aalg is implemented in C++, and is available upon request from the author. The program lets the user define the field to perform the calculations in. At present, we only support the finite fields $\mathbb{Z}_p$, and there is an upper limit of $p = 31991$ (the “Macaulay”-prime).

The most time and memory consuming parts of the algorithms are the row reduction of the matrices specified by the relations and the possible commutators. If at most 10% of the entries in a matrix are non-zero, then the matrix is said to be sparse. When a matrix is sparse, a typical representation of a vector is as a list of pairs, where the first entry in each pair is the index with respect to the basis, and the second is the coefficient. In many of the applications we considered in the development of the algorithms, the number of non-zero elements were less than 10%. This made us implement the row reduction algorithm using sparse methods. But now we have understood that the algorithms could be used also problems which gives dense matrices, and in coming versions we will support dense representation.

However, for $\mathbb{Z}_2$, the current version of the program uses a dense representation, for when the field consists of only two elements, we can store 32 or 64 coefficients in one computer word, depending on the word size of the computer. Since every machine instruction computes one word at a time, this also increases the speed of the calculations by a factor 32 or 64 compared to ordinary dense representation. To save time and memory using sparse methods over $\mathbb{Z}_2$, heuristics indicates that one would need to have at most 1% of the elements non-zero.

The difference in representation explains the behavior of aalg in the first instance of problems in section 4.3. When the field is $\mathbb{Z}_2$, the program shows good running times, but when the field is $\mathbb{Z}_{31991}$, the program is rather slow. This is because the matrices occurring in these examples are dense; and as much as 99% of the entries in the matrices are non-zero. To use sparse methods in these examples, as we do for $\mathbb{Z}_{31991}$, is very ineffective.

Except for the representation, it is of importance that one chooses a good algorithm to perform the row reduction. The algorithm implemented in the program is straight forward Gaussian elimination, and we have reason to believe that a well chosen algorithm and a well written code would increase the speed of the program thoroughly. Unfortunately, there is yet no fast package which row-reduces matrices over finite fields. But there is a package under construction, see [11], which we hope to be able to use in the future.

References

[1] D. Anick, Non-commutative graded algebras and their Hilbert series, Journal of Algebra 78 (1982), 120–140.

[2] J. Backelin et al. , Bergman 0.975, a system for computations in commutative and purely non-commutative graded algebra. `http://www.math.su.se/bergman`.

[3] CoCoATeam, CoCoA 4.3: a system for doing Computations in Commutative Algebra. `http://cocoa.dima.unige.it`.

[4] Faugere, Gianni, Lazard, Mora, Efficient computation of zero dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation 16 (1993), 329–344.

[5] S. Fomin, A. N. Kirillov, Quadratic algebras, Dunkl elements, and Schubert calculus, Advances in geometry 172 (1999), 147–182.

[6] S. Fomin, C. Procesi, Fibered quadratic Hopf algebras related to Schubert calculus, Journal of Algebra 230 (2000), 174–183.

[7] G. Gotzmann, Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes, Math. Z. 158 (1978), 61–70.

[8] M. Green, Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann, Lecture Notes in Math. 1389 (1989), 76–86.

[9] D. Grayson, M. Stillman, Macaulay2 0.92, a system for research in algebraic geometry. `http://www.math.uiuc.edu/Macaulay2.`

[10] G.-M. Greuel, G. Pfister, H. Schönemann. SINGULAR 2.0.4. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2001). `http://www.singular.uni-kl.de`.

[11] LinBox, a C++ template library for exact, high-performance linear algebra computation with dense, sparse, and structured matrices over the integers and over finite fields. Development version available at `http://www.linalg.org`.

[12] C. Löfwall, J.-E. Roos, A nonnilpotent 1-2-presented graded Hopf algebra whose Hilbert series converges in the unit circle, Adv. in Math. 130 (1997), no. 2, 161–200.

[13] L. Robbiano, Introduction to the theory of Hilbert functions, Queen's Papers in Pure and Applied Math., vol. 85 (1991) B1–B26.

[14] R. Stanley, Hilbert Functions of Graded Algebras, Adv. in Math. 28 (1978), 57–83.