Computer Science Journal of Moldova, vol.**3**, no.1(7), 1995

Noncommutative Gröbner basis, Hilbert series, Anick's resolution and BERGMAN under MS-DOS

S.Cojocaru V.Ufnarovski

Abstract

The definition and main results connected with Gröbner basis, Hilbert series and Anick's resolution are formulated. The method of the infinity behavior prediction of Gröbner basis in noncommutative case is presented. The extensions of BERGMAN package for IBM PC compatible computers are described.

1 Main Examples

Let $A =< X|R >$ be a finitely presented associative algebra over field K. Here are the main examples of algebras that will help us to illustrate some following definitions (later we will refer to them as main examples).

Example 1 $A =< x, y|x^2 = 0, xy^2 = 0 >$

Example 2 $A =< x, y|x^2 = y^2 >$

Example 3 $A =< x, y|x^2 - xy >$

Example 4 $A =< e_1, e_2, e_3, ...|[e_i, e_j] = (i - j)e_{i+j} >$, *where*

$$[x, y] = xy - yx$$

Though the last example does not look as finitely presented, it is evident that e_1 and e_2 generate the algebra ($e_{k+1} = \frac{[e_k, e_1]}{k-1}$ for $k \geq 2$ and we assume in this example that the characteristic is zero). Slightly less trivial is the fact that it is sufficient to have only two relations:

$$[e_3, e_2] = e_5;\ \ [e_4, e_3] = e_7$$

(see [6]). Nevertheless, we will use this example in this infinite presentation to give the reader a possibility to see how definitions work in the infinite case (and to conclude that sometimes an infinite presentation is more convenient even from a computational point of view).

This is also an example of an universal enveloping algebra: $A = U(L)$, where L is a Lie algebra with the same sets of generators and relations except that the commutator $[x, y]$ is now interpreted as a Lie product.

2 Hilbert series and global dimension

Note that all algebras in our examples are graded algebras: $A = \oplus A_n$,where all components A_n are finite dimensional and $A_n A_m \subseteq A_{m+n}$. For the last example grading is less trivial: $e_n \in A_n$.

We restrict our attention on graded algebras and introduce the following

Definition 1 *The generating function $H_A = H_A(t) = \sum_1^\infty (\dim A_n) t^n$ is called Hilbert series of an algebra A.*

The Hilbert series of a graded algebra is one of our main object of interest. It is a very useful invariant in the commutative case, but in the noncommutative case it also contains a lot of important information about the algebra. First of all, it plays the role of generalized dimension of an algebra. For example, it has the following trivial properties:

- $H_{A \oplus B} = H_A + H_B; H_{A \otimes B} = H_A H_B$,
- $\frac{1}{H_{A*B}} = \frac{1}{H_A} + \frac{1}{H_B} - 1$,

- If L is a graded Lie algebra, $H_L = \sum_1^\infty a_n t^n$ and $A = U(L)$, then

$$H_A = \prod_1^\infty \frac{1}{(1-t^n)^{a_n}}.$$

Example 5 *If $A = K < X >$ is a free algebra, where generators not necessarily have degree 1, then $H_A = (1-H_X)^{-1}$, where $H_X = \sum t^{\deg x}$ is a generating function for the number of generators of given degree. Of course, in the case of natural grading (where all generators have degree 1), it looks as $(1-dt)^{-1}$, where d is the number of generators.*

Example 6 *If L is a Lie algebra from our main example 4, then*

$$H_L = t + t^2 + t^3 + \cdots \Rightarrow H_A = \prod_1^\infty \frac{1}{1-t^n} = \sum p(n)t^n,$$

where $p(n)$ is the number of partitions. So it is the example with non-rational Hilbert series.

Example 7 *In our main examples 1–3 the Hilbert series is equal to $(1-2t+t^2)^{-1}$. It can be directly checked from the first example, but the next two will be discussed in the sequel.*

Secondly, the following two theorems of D.Anick ([1, 2])shows non-trivial properties of Hilbert series:

Theorem 1 *Let H_R be the generating function of the number of minimal relations of given degree (and R is non-empty). Then*

$$gl.\dim A = 2 \Leftrightarrow H_A = (1 - H_X + H_R)^{-1}.$$

Example 8 *In our main examples the value of $(1-H_X+H_R)$ is equal*

1. $(1-2t+t^2+t^3)$,
2. $(1-2t+t^2)$,
3. $(1-2t+t^2)$,

4. $(1 - t - t^2 + t^5 + t^7)$,

so only the second and third examples are algebras of global dimension 2.

Theorem 2 *For every system of diophantine equations* $S = 0$, *there exists a finitely presented algebra* A *(which can be constructively expressed in terms of the coefficients of the* S*) such that* A *has global dimension 2 if and only if the system* $S = 0$ *has no solutions.*

Moreover this algebra is a Hopf algebra, defined by quadratic relations only. This theorem has important, though unpleasant:

Corollary 1 *One cannot*

- *find an algorithm that takes relations as input and gives the Hilbert series as output. (Even more, one cannot detect in general if the Hilbert series of a given algebra is equal some fixed series)*
- *predict in general the behavior of a Hilbert series, knowing only finitely many of its coefficients.*

3 Normal words and Gröbner basis

Despite pessimistic conclusions in the end of the previous chapter, there is some hope to find the Hilbert series in some important cases. Let us introduce some important definitions.

Let S be the set of the all words in the alphabet X (identifying 1 with the empty word). Consider the following ordering on S :

$f > g$ if either the length of word f is greater than that of g or they have the same length, but f is greater then g lexicographicaly.

(more ingenious, the so called admissible ordering may be considered too, but we restrict our attention only to this case).

Definition 2 *A word* $f \in S$ *is called normal (for* A*) if it cannot be written in* A *as a linear combination of words that are less than* f.

Example 9 *In our first main example the words* $1, x, y, xy, yx, y^2$ *are normal, but* x^2, xy^2 *are not. The same is true for the second main example. Why is* xy^2 *not normal? Because* $xy^2 = x^3 = y^2x$.

In the last main example the words of the form $e_1^{k_1}e_2^{k_2}\cdots e_m^{k_m}$ *are normal according the PBW-theorem, if alphabet and ordering is* $e_1 < e_2 < e_3 \cdots$. *It is much more complicated is to express normal words in the alphabet* e_1, e_2 *only.*

The following evident theorem explains how normal words can be used for the calculation of the Hilbert series

Theorem 3 *The set* N, *consisting of all normal words, forms a basis for the algebra* A.

Its Hilbert series can be calculated as $H_A = \sum_0^\infty d_n t^n$, *where* d_n *is the number of normal words of degree* n.

Following D.Anick, let us introduce

Definition 3 *A word* $f \in S$ *is called an obstruction if* f *is not normal itself, but every proper subword is normal.*

Note that, other expressions (such as "tips", for example) are used instead of "obstruction". We denote the set of all obstructions as F.

Example 10 *In our main examples:*

1. $F = \{x^2, xy^2\}$ *(evidently)*
2. *the same (can be proved, as we'll see later)*
3. $F = \{x^2, xyx, xy^2x, xy^3x, xy^4x, ...\}$ *(see later too).*
4. $F = \{e_je_i | j > i\}$.

Of course, knowing an obstruction set we can easy reconstruct normal words:

Theorem 4 *Let* $B =< X|F >$. *Then algebras* A *and* B *have the same sets of normal words and in particular,* $H_A = H_B$.

Definition 4 *Algebra B from previous theorem is called the monomial algebra, associated with A.*

So, the algebra from our first main example is associated monomial algebra for our second example. Note also, that all universal enveloping algebras for Lie algebras with the same Hilbert series have, according the PBW theorem, the same associated monomial algebra (in some alphabet). Note also that definitions depend on choice the generator set (alphabet) and ordering.

So, the main problem is to find F. Because obstructions are not normal words every $f_i \in F$ can be written as a linear combination of normal words: $f_i = u_i$.

Definition 5 *The set $G = \{f_i - u_i\}$ is called a (reduced) Gröbner basis (for A).*

Example 11 *In our main examples:*

1. $G = \{x^2, xy^2\}$ *(evidently)*
2. $G = \{x^2 - y^2, xy^2 - y^2x\}$. *Those elements we already know, so we need only to understand why we have no more elements. This will be explained later.*
3. $G = \{xy^k - xy^{k+1} | k = 0, 1, 2, \ldots\}$ *Explanations later too.*
4. $G = \{e_je_i - e_ie_j - (j-i)e_{i+j} | j > i\}$

More general a Gröbner basis for any ideal I is its subset G, such that the set of highest terms of elements from G is exactly the set of obstructions for $A = K < X > /I$. Note that the reduced Gröbner basis may be easily obtained from an arbitrary Gröbner basis (by selfreducing) and determined uniquely for a given ordering.

4 Calculating Gröbner basis

Fortunately there exists an algorithm for calculating elements of a Groöbner basis. Unfortunately the Gröbner basis itself is infinite (and that is one of the reasons for pessimistic results above). We describe the algorithm in a slightly untraditional manner, taking into account the future generalization. For traditional approach and extra literature see [7]. First we introduce the important:

Definition 6 *A 2-chain is a word f, containing exactly two obstructions as subwords: one as a prefix of f and second as a suffix. Those obstructions should have non-trivial intersection. The set of obstructions will be denoted C_2.*

Example 12 *In our main examples.*

1. $C_2 = \{xxx, xxyy\}$
2. $C_2 = \{xxx, xxyy\}$,
3. $C_2 = \{xy^kxy^lx | k, l = 0, 1, 2, 3...\}$
4. $C_2 = \{e_je_ie_k | j > i > k\}$.

Example 13 $A =< x|x^3 >, F = \{x^3\}, C_2 = \{x^4\}$, *but x^5 is not 2-chain, because it contains obstructions as subwords in 3 different places!*

Now we describe the algorithm for obtaining all the elements of Gröbner basis. Suppose, that we know all the elements of degree at least n. Then we know all normal words of degree at least n, and can reduce any arbitrary word of degree at least n to its normal form - the linear combination of normal words. So, we can introduce a linear operator R_0, that being applied to any word of length $(n+1)$, reduce its suffix of length n to the normal form. For example, $R_0(xxx) = xyy$ in our second main example.

We also know all 2-chains of degree (n+1). Let f be one of them. Consider the following algorithm:

1. Let us single out all words in $f - R_0f$, beginning with an obstruction.
2. Let us replace each of noted obstructions by its normal form.

3. Apply R_0 to the obtained result.

4. In the so obtained element we again single out all the words, starting with an obstruction.

5. go back to stage 2.

Since the leading words decrease all the time, the process will sooner or later stabilize. If the obtained stabilized element is not zero, it should be (up to coefficient) added to Gröbner basis. In this way we get all elements of Gröbner basis of degree (n+1). Note, that they are not necessary in the reduced form, but the highest terms are correct, and using them we can reduce all to obtain the reduced Gröbner basis (if we need).

Example 14 *In the second main example we have from the very beginning one element of Gröbner basis in degree 2: $xx - yy$. In degree 3 we have the only 2-chain: xxx. Applying our procedure we have:*

1. $\underline{xx}x - xyy$

2. $yyx - xyy$

3. $yyx - xyy$

Stabilization. We need to add new element $xyy - yxx$ to our Gröbner basis. In degree 4 we have now the only 2-chain: $xxyy$.

1. $\underline{xx}yy - \underline{xyy}x$

2. $yyyy - yyxx$

3. $yyyy - yyyy = 0.$

Stabilization on zero. We have not more 2-chains and it means that we have got already the Gröbner basis (exactly in the form as that was written before).

Example 15 *As to our third main example we skip the procedure of getting Gröbner basis from original relations, but simply show that the same procedure works for the checking that a given set is really a Gröbner basis:*

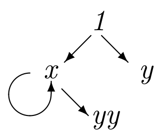
Let $f = xy^kxy^lx$ be any composition. Then

1. $\underline{xy^k}xy^lx - \underline{xy^kx}y^{+l+1}$
2. $xy^{k+l+1}x - xy^{k+l+2}$
3. $\underline{xy^{k+l+1}x} - xy^{k+l+2}$
4. $xy^{k+l+2} - xy^{k+l+2} = 0.$

5 $n-$chains and Poincaré series

The next step is to introduce some homological algebra. Let us consider a graph $\Gamma = (V, E)$, where the set of vertex V consist of union of the unit 1, alphabet X and all proper suffices of the obstructions. Edges E are defined as follows: $1 \to x$ for every $x \in X$ and in other cases $f \to g$ if and only if the word fg contains the only obstruction and this obstruction is its suffix (maybe coinciding with fg).

Example 16 *In our main examples 1 and 2 the graph Γ looks like*



In the third example vertices (except 1 *and* y *have form* y^nx *and are connected each other (including itself),*

It the fourth main example vertices are e_i *and (considering* 1 *as* e_∞*). Every* e_i *is connected with every* e_j *with* $i > j$.

Definition 7 *$n-$chain is a word, that can be read in graph Γ during a path of length $(n+1)$, starting from* 1. *Let C_n be a set of all $n-$chains.*

So,

- The only $-1-$chain is 1 itself: $C_{-1} = 1$.
- The only $0-$chains are letters from the alphabet: $C_0 = X$.
- The only $1-$chains are obstructions: $C_1 = F$.
- The only $2-$chains are ...$2-$chains, as they were defined in the previous section. So, our previous definitions of C_2 coincides with a new one.

Let us enumerate $n-$chains for $n \geq 2$ in some examples

Example 17 *In our first two main examples*

$$C_n = \{x^{n+1}, x^n y^2\}$$

In the third

$$C_n = \{xy^{k_1}xy^{k_2}x \cdots xy^{k_n}x | k_i \geq 0\}.$$

Ih the last main example

$$C_n = \{e_{i_1}e_{i_2} \dots e_{i_{n+1}} | i_1 > i_2 > \cdots i_{n+1}\}.$$

Definition 8 *Monomial Poincaré series for an algebra A is defined as*

$$P_A^{mon}(s,t) = \sum c_{m,n} t^m s^n,$$

where $c_{m,n}$ is the number of $(n+1)-$chains of degree m.

Example 18 *In our first two main examples*

$$P_A^{mon}(s,t) = 1 + 2ts + (t^2 + t^3)s^2 + (t^3 + t^4)s^3 + \cdots.$$

In the third

$$P_A^{mon}(s,t) = 1 + 2ts + \sum_{m \geq n \geq 2} t^m s^n = 1 + 2ts + t^2 s^2 (\sum_{k=0}^{\infty} (t+s)^k.$$

In the fourth main example $c_{m,n}$ is equal the number of partitions of m to n distinct summands.

Let us recall the definition of classical Poincaré series

Definition 9 *A double Poincaré series for an algebra A is defined as a generating function*

$$P_A(s,t) = \dim(Tor^A_{n,m}(K,K))t^m s^n,$$

where $Tor^A_n(K,K)$ *is considered as a graded module.*

From the point of view of calculation of the Hilbert series we can restrict our attention to monomial Poincaré series:

Theorem 5 *If A is monomial algebra, then* $P^{mon}_A(s,t) = P_A(s,t)$*, so* $n-$*chains corresponds to homology of associated monomial algebra.*

Theorem 6
$$H^{-1}_A = P_A(-1,t) = P^{mon}_A(-1,t)$$

Example 19 *In our first two main examples we have*

$$H^{-1}_A = 1 - 2t + t^2 + t^3 - t^3 - t^4 + t^4 + t^5 - \cdots = 1 - 2t + t^2$$

In the third one we have $H^{-1}_A = 1 - 2t + t^2$ *too. The reader can simply interpret himself the connections between partitions, that we have got as a sequence in the last main example.*

6 Anick's resolution

In order to calculate the Poincaré series in general case we construct Anick's resolution ([3]):

$$C_n \otimes A \to C_{n-1} \otimes A \to \cdots C_{-1} \otimes A \to K \to 0$$

It is sufficient to define module homomorphisms $d_n : C_n \otimes A \to C_{n-1} \otimes A$ only for terms $f \otimes 1$. It is convenient to identify $C_n \otimes N$ with $C_n N$. Then the map d_n is defined by induction as

$$d_{n+1}(f) = f - i_n d_n(f)$$

and $i_n : \ker d_{n-1} \to KC_nN$ is defined recursively:

$$i_n(u) = \alpha\hat{u} + i_n(u - \alpha d_n(\hat{u})),$$

where $\hat{u}$ is highest term of u and α is its coefficient.

Note, that:

- d_0 calculate, for every non empty word f, its normal form $\bar{f}$, i_0 acts identically.
- d_1 calculate, for any obstruction, $f - \bar{f}$, i.e. recover the element of Gröbner basis from its obstruction. To apply d_1 for arbitrary word of form fs one need to be more careful: $d_1(fs) = R_0(fs - \bar{f}s)$. (in the general case one need to use the map $R_n : C_{n+1} \to C_n$, that fixed $n-$chain in the beginning and reduce the remaining part to normal form).
- If we collect all the terms that were singled out during the process of constructing the new elements of Gröbner basis that was described above, we get the action of d_2 (if we stabilize on 0. If not, we need first to finish the process, after introducing a new relation).

Example 20 *In our main examples :*

1. $d_n(f) = f$ *for* $f \in C_n$ *and* $d_n(fs) = R_{n-1}(fs)$ *in general. (those formulas are valid for every monomial algebra).*
2. *In tensor language:*

$$d_2 : x^3 \to x^2 \otimes y - xy^2 \otimes 1,$$

$$d_2 : x^2y^2 \otimes 1 \to x^2 \otimes y^2 - xy^2 \otimes x$$

7 Finite state automata and Lie algebras

The main problem in noncommutative case is that Gröbner basis is usually infinite. Nevertheless, using finite state automata we can try to predict the infinity behavior of our Gröbner basis or at least the obstruction set on infinity. The main idea of this approach was described in [8] and can be illustrated here by our third main example: having sufficiently many terms from obstruction set, for example, $x^2, xyx, xy^2x, xy^3x, xy^4x$ man can predict the whole family: xy^nx. This kind of prediction can be formalized in the terms of regular languages (or equivalently, finite state automata). Rather often this prediction gives the correct answer, that can be proved using another arguments. Nevertheless the possibility of prediction are restricted. First of all it is impossible in general case, as we have mentioned in the second section. Second, algebras that have regular obstruction set have also rational Hilbert series and either polynomial or exponential growth. So, the Hilbert series for our fourth main example could not be predicted in this manner after finitely many calculations in terms of only two generators e_1, e_2. But even in a quite nice class of solvable universal enveloping algebras those predictions are impossible, as we see:

Theorem 7 *[5] Let L be a free solvable Lie algebra of solvability length k, $U(L)$ be its universal enveloping algebra. If $k > 2$ then the growth of L and $U(L)$ is almost exponential (it means, that it is less than exponential growth $[2^m]$ but greater than growth $[2^{m^\alpha}]$ for any $\alpha < 1$).*

8 Bergman package under MS-DOS

BERGMAN is en effective program for calculating the Gröbner basis (both for commutative and non-commutative case) and monomial Poincaré series. It was elaborated in Stockholm university (J.Backelin) for SUN-station (and some other types of computers). Main language is PSL. In our implementation on IBM-PC we used the original source of J.Backelin (and his valuable help) ([4]) It can be used under REDUCE only and has some new additional functions:

- possibility to predict the infinite behavior of the set of obstructions basing on in finite part.

- possibility to calculate all Hilbert series using the regular presentation (in original version it can be calculated only up to selected degree).

- the separate effective program for calculating growth of an algebra (calculations of Hilbert series rather often are restricted by huge values of intermediate computations).

- possibility to calculate arbitrary term of Anick's resolution. (implemented by A.Podoplelov).

- shell for more convenient interactive work (implemented by A. Colesnicov and L. Malahova).

The following known commutative examples were compared with Maple 5.2 (that also works under MS-DOS and also has the possibility to work with numbers of arbitrary length) to estimate the effectivity of implementation.
Examples

1. $A_1 =< x, y, u, v|x^2, y^3, x - u + v, y - u - 2v >$

2. $A_2 =< x, y, z, u, t, a|2x^2 + 2y^2 + 2z^2 + 2tt^2 + u^2 - ua, xy + 2yz + 2zt + 2tu - ta, 2xz + 2yt + t^2 + 2zu - za, 2xt + 2zt + 2yu - ya, 2x + 2y + 2z + 2t + u - a >$

3. $A_3 =< a, b, c, d, e, z|a + b + c + d + e, ab + bc + cd + de + ea, abc + bcd + cde + dea + eab, abcd + bcde + cdea + deab + eabc, abcde - z^5 >$

4. $A_4 =< a, b, c, d, e, f, z|a + b + c + d + e + f, ab + bc + cd + de + ef + fa, abc + bcd + cde + def + efa + fab, abcd + bcde + cdef + defa + efab + fabc, abcde + bcdef + cdefa + defab + fabcd, abcdef - z^6 >$

The last variable in all example was added to homogenize the equations (Homogeneous input is the only serious restriction for BERGMAN)

Example	Time	
	BERGMAN	MAPLE
A_1	1 sec.	3.2 sec.
A_2	6 sec.	-
A_3	12 sec.	-
A_4	3 min. 21 sec.	-

486SX 25 MHz IBM PC compatible computer with 4 MB RAM was used. The last three examples could not be calculated by MAPLE.

References

[1] Anick, D., Non-commutative graded algebras and their Hilbert series. J.Algebra, 78, No 1, (1982) 120-140.

[2] Anick, D., Diophantine equations Hilbert series and undecidable spaces. Ann. Math.,II Ser. 122, (1985) 87-112.

[3] Anick, D., On the homology of associative algebras, Trans. Am. Math. Soc.,296, No 2, (1986), 641-659.

[4] J Backelin, J Hollman: Calculating Gröbner bases fast; to appear

[5] Lichtman, A., Ufnarovski V.: On Growth of Lie Algebras. To appear in Algebra Colloquium

[6] Ufnarovskij V.: Poincaré series of graded algebras. Mat.Zametki 27, N0 1 (1980), 21-32. English transl: Math. Notes 27 (1980), 12-18.

[7] Ufnarovski ,V. Combinatorial and Asymptotic Methods in Algebra, *Itogi Nauki Tekh., Ser. Sovrem. Probl. Mat., Fundament. Napravleniya*, **57** (1990), 5–177. English transl.: Encycl. Math. Sci. 57, to appear.

[8] Ufnarovski V., Calculations of growth and Hilbert series by computer, Lect. Notes Pure Appl. Math, 151, (1993) 247–256

S.Cojocaru, V.Ufnarovski,
Institute of Mathematics,
Academy of Sciences of Moldova,
5 Academiei str., Kishinev,
277028, Moldova
e-mail: 22svet@math.moldova.su

Received 3 January, 1995