Computer Science Journal of Moldova, vol.16, no.1(46), 2008

On the Cancellation Rule in the Homogenization

Victor Ufnarovski

Abstract

We consider the possible ways of the homogenization of non-graded non-commutative algebra and show that it should be combined with the cancellation rule to get the mathematically adequate correspondence between graded and non-graded algebras.

1 Introduction

The homogenization is a standard instrument in the commutative algebra. From the computational point of view it is useful because homogeneous algorithms are often more efficient, allowing to save memory (for example cleaning a lot when the current degree is done). In the non-commutative case the situation is much less trivial, because the connection between non-graded algebra and graded algebra obtained by the homogenization is not so obvious as in the commutative case. First of all there are several ways to homogenize. If t is a homogenizing variable and one wants to homogenize a non-commutative polynomial f of the degree k the obvious way is to multiply all the monomials in f that have the degree less than k by the corresponding power of t. But how to do it? From the left? From the right? In the middle?

The answer depends on our aim. Suppose we want to calculate the Gröbner basis G of given non-graded algebra and our goal is to obtain it from the Gröbner basis G^* of the corresponding graded algebra which we get using the homogenization of the relations. It would be nice to get it using the dehomogenization procedure as in the commutative case, i.e. simply putting $t = 1$. Is it possible? Do we really get the Gröbner basis of our non-graded algebra?

An easy example $x^2 = x$ shows that we should be careful about the choice of the ordering: if $t > x$ then $tx > x^2$ and the leading word tx in $tx - x^2$ will be not the leading word after dehomogenization. But suppose that we have solved this problem (and it is not so difficult). Suppose even more that we know that after the dehomogenization we get the correct Gröbner basis. There are still some problems. The first one reflects the fact that 1 commutes with all other variables, but t does not. From the computational point of view it means that the calculating of Gröbner basis G^* may be much more complicated than in the corresponding non-graded algebra. A couple of tests shows that this is the case: almost any non-trivial example creates a huge Gröbner basis G^*, almost always we get infinite Gröbner basis even in the case where the non-graded Gröbner basis is finite. One of the explanation of this phenomena is that though we get Gröbner basis G after dehomogenization, normally it is not minimal, because the reduction works differently in graded and non-graded case. As example, suppose that the leading terms of Gröbner basis in our graded algebra look as txy^kt for all $k > 0$. It is obvious that we get a minimal Gröbner basis G^*. But after dehomogenization we get the set of leading terms xy^k of Gröbner basis G, which is far from being minimal. The term xy alone should be the leading term of the minimal Gröbner basis, but how to avoid the unnecessary calculations of the infinite set in G^*?

One more or less evident attempt to solve this problem is to introduce extra commuting relations: $tx = xt$ for any variable x and demand $tx > xt$. Then all other words in the Gröbner basis of our graded algebra will have the form ft^k, where the word f does not contain t. Words in the example above should be replaced by xy^kt^2 and we can do the reduction already on the level G^*, so xyt^2 be the only leading word term remaining in the minimal Gröbner basis and we achieved our goal in this case. Can we in general hope that the minimal Gröbner basis be still minimal Gröbner basis after dehomogenization? Much more often, but it is still not the case! To see the reason, consider the following example.

Example 1 *The algebra* $A = \langle x, y | x^2 - 1, xy^2 - 1\rangle$ *has the set* $G = \{y^2 - x, x^2 - 1\}$ *as a Gröbner basis if* $y > x$*. If we homogenize the relations using the commuting homogenizing variable* $t > y > x$ *we get the graded algebra*

$$\langle t, x, y | x^2 - t^2, xy^2 - t^3, tx - xt, ty - yt\rangle.$$

Its Gröbner basis is infinite. Even it contains such elements as $y^2t - xt^3, x^2 - t^2$*, which should be sufficient to obtain* G*, it contains also infinitely many other elements, for example, of form*

$$y^2(xy)^{4k-2}t^2 - t^{8k}, k = 1, 2, \ldots$$

The reason for the trouble is the presence of t in the leading word y^2t. Because of it the leading monomials containing y^2 cannot be reduced (as they are in G).

The remedy for this trouble is far from the being trivial and the main aim of this article is to find it. Shortly the idea is that it is not sufficient to homogenize the relations. We should work in another factor-algebra, where leading terms of the corresponding Gröbner basis do not contain t (commutativity relations $tx = xt$ are the only exceptions). We describe this algebra below. Shortly the rule is as follows: during the Gröbner basis calculations cancel t, if it appears in all the terms. The resulting reduced Gröbner basis will be minimal after the dehomogenization. Let us discuss all the details more carefully (but more formally).

2 Homogenization and dehomogenization

Let $K\langle X\rangle$ be a free algebra over the field K and t be an additional (homogenizing) variable. For any homogenous element $u \in K\langle X\rangle$ of the degree k and any $m \geq k$ we define $u^{*(m)} \in K\langle X, t\rangle$ as ut^{m-k}. If $u \in K\langle X\rangle$ is an arbitrary element, written as the sum of its homogeneous components $u = \sum u_i$, and still having degree $k \leq m$ we define $u^{*(m)}$ as $u = \sum u_i^{*(m)}$ and u^* as $u^{*(k)}$. In other words $u^* = \sum u_i t^{k-i}$, if $\deg u_i = i$. So, $u^* = u$ if and only if u is homogeneous.

To dehomogenize some element $v \in K\langle X, t\rangle$ we simply replace all occurrences of t by 1. In other words, if $v = v(X, t)$ we define $v_* = v(X, 1)$.

For example,

$$(x^2 + y)^* = x^2 + yt; (x^2 + y)^{*(3)} = x^2t + yt^2;$$

$$(x^2 + yt)_* = x^2 + y; (tx - xt)_* = 0.$$

The following statement is trivial, but useful.

Lemma 1 *a) The map $v \to v_*$ is a homomorphism from $K\langle X, t\rangle$ to $K\langle X\rangle$.*

b) $(u^*)_* = u$ for any $u \in K\langle X\rangle$. ■

Note that the map $u \to u^*$ is not a homomorphism and in general not always $(v_*)^* = v$. The following definition helps to choose elements that almost have this property.

Definition 1 *A word $g = ft^l$ is canonical, if $l \geq 0$ and f does not contain variable t. A canonical element of $K\langle X, t\rangle$ is a linear combination of some canonical words of the same length.*

Note that canonical elements are by the definition homogeneous. The following lemma shows their importance.

Lemma 2 *a) Every homogeneous element in $K\langle X, t\rangle$ can be uniquely written as a sum of the canonical element and the element belonging to the ideal, generated by the set $S = \{tx - xt | x \in X\}$.*

b) If v is a canonical element then $v = (v_*)^*t^d$, where d is the minimal power of t dividing some word in v. In particular, $v = (v_*)^*$ if and only if v cannot be written as wt.

Proof. a) is evident and is a trivial application of the Gröbner bases theory.

b) is sufficient to check for a canonical word: if $g = ft^i$ and $|g| = k$ then

$$g_* = f, f^{*(m)} = ft^{m-(k-i)} = gt^{m-k}$$

for any $m \geq k - i$. So, if $v = \sum_j \alpha_j g_j = \sum_j \alpha_j f_j t^{i_j}$ is a canonical element of the degree k, then $v_* = \sum_j \alpha_j f_j$ has degree $k - d$, and

$$(v_*)^* = \sum_j \alpha_j g_j t^{(k-d)-k} = vt^{-d}.$$

■

3 Homogenized ideal

Let $A = K\langle X\rangle/I$, where I is some ideal which will be fixed for the rest of this article. In general I (and A) are not graded and our idea is to study A with the help of graded algebra $B = K\langle X, t\rangle/I^*$, where I^* contains all homogenized elements of I and (to be able to work with the canonical elements only) all the commutators $tx-xt$. More formally, I^* is an ideal in $K\langle X, t\rangle$, generated by all homogenized elements $u^*, u \in I$ and the set $S = \{tx - xt | x \in X\}$. We want to prove some elementary properties of I^*.

Lemma 3 *a) If $u \in I$ is homogeneous, then $u \in I^*$.*
b) If $v \in I^*$ then $v_* \in I$.
c) If $v \in K\langle X, t\rangle$ is homogeneous, then $v \in I^* \Leftrightarrow v_* \in I$.
d) If $vt \in I^*$ then $v \in I^*$.

Proof. a) $u = u^*$ and belongs to I^*.
b) Consider a map ϕ which is the composition

$$K\langle X, t\rangle \to K\langle X\rangle \to A = K\langle X\rangle/I,$$

where the first arrow corresponds to the homomorphism $v \to v_*$, and the second is the natural homomorphism. Then $v_* \in I \Leftrightarrow v \in \ker\phi$. Because $S \subset \ker\phi$ and for every $u \in I$, according to Lemma 1, $u^* \in \ker\phi$, we have that $I^* \subset \ker\phi$, which proves b).

c) The implication $v \in I^* \Rightarrow v_* \in I$ follows from b). On the other hand, according to Lemma 2, $v = w+s$, where w is a canonical element and s belongs to the ideal, generated by S. Now $v_* = w_* + s_* = w_*$ so $v_* \in I \Leftrightarrow w_* \in I$ and, according to Lemma 2, $v = w+s = (w_*)^*t^d+s \in I^*$ if $v_* \in I$.

d) follows from c) because I^* is a homogeneous ideal. ■

4 Eliminating ordering

Suppose that $>$ is an admissible ordering on free monoid $\langle X \rangle$ such that $|f| > |g| \Rightarrow f > g$, where $|f|$ is the length of a word f. We will extend it to the eliminating ordering on free monoid $\langle X, t \rangle$, namely for any two words $f, g \in \langle X, t \rangle$ we put

$$f > g \Leftrightarrow \begin{cases} |f| > |g| \\ \quad or \\ |f| = |g|, \quad f_* > g_* \\ \quad or \\ |f| = |g|, \quad f_* = g_*, \quad f >_{lex} g, \end{cases}$$

where $>_{lex}$ is a pure lexicographical ordering, extending $>$ such that the letter t is larger than any letter from X. Note that $t < x$, but $tx > xt$ for any $x \in X$. This ordering is also admissible and has some special properties that we want to use.

Lemma 4 *Let $v \in K\langle X, t \rangle$ be a canonical element, g be its leading word. Then*

a) If $\deg_t g = k$ then $v = wt^k$, for some canonical element w.

b) Leading term of v_* is g_*.

c) If $u \in K\langle X \rangle$ then the leading word of u in $K\langle X \rangle$ is the same as leading word of u^* in $K\langle X, t \rangle$.

Proof. Recall that v is homogeneous.

a) If h is another word in v then $deg_t h \geq \deg_t g$, otherwise $|h_*| > |g_*|$. So, $h = h't^l$ with $l \geq k$ and $v = wt^k$.

b) In the same notations, if $l > k$ then $|g_*| > |h'| = |h_*|$. Otherwise $l = k$ and $g > h \Leftrightarrow g_* > h_*$ (we can cancel t^k).

c) The leading term of u^* does not contain t according to a). Because it depends only on the words of highest length in u we can use b). ■

5 Normal words and Gröbner basis

From now we fix the eliminating ordering. We want to study the relation between the Gröbner basis for I and Gröbner basis for I^*. Let us recall that the subset G of I is its Gröbner basis if for any $u \in I$ there exists an element $g \in G$ such that its leading word (or leading monomial in another terminology) $lm(g)$ is a subword of the leading word $lm(u)$. Words that are not divisible by any $lm(g), g \in G$ (or equivalent by any $lm(u), u \in I$) are called normal and if we denote the set of the normal words by N then $K\langle X\rangle = KN \oplus I$ (direct sum of vector spaces), so N can serve as a basis for factor-algebra $A = K\langle X\rangle/I$ (see e.g. [2] for the details). Suppose that G is a minimal Gröbner basis for I. Our aim is to describe a minimal Gröbner basis G^* for I^* and the corresponding set of normal words N^* in $K\langle X, t\rangle$. Note that N^* is not the same set as $\{n^*|n \in N\}$, which is the same as N.

Theorem 1 *a) A word $f \in \langle X, t\rangle$ is normal relative I^* (i.e $f \in N^*$) if and only if it is canonical and $f_* \in N$.*

b) If G is a minimal Gröbner basis for I then $G^* = S \cup \{g^*|g \in G\}$ is a Gröbner basis for I^*. It is minimal, if G does not contain elements of degree 1 or constants.

c) If $G = \{1\}$ then $\{1\}$ is a minimal Gröbner basis for I^* too.

d) If $Y \subset X$ is the set of leading monomials in G that have degree 1, then to obtain a minimal Gröbner basis for I^* from that one in b) we need only to take away all the commutators $ty - yt, y \in Y$.

Proof. a) Because S is a subset of I^* a normal word should be canonical. Let f be a canonical word, $f = ht^k, f_* = h$.

If f is not normal then it is a leading word of some homogeneous $v \in I^*$ (because I^* is homogeneous). Then by Lemma 3 $v_* \in I$ and according to Lemma 4 h is its leading term, so $f_* = h$ is not normal.

On the other hand if $f_* = h$ is not normal, then h is the leading word of some $u \in I$. According to Lemma 4 $u^* \in I^*$ has h as the leading term, so f is the leading term of $u^*t^k \in I^*$. This conclusion finishes the proof that $f \in N^*$ if and only if $f_* \in N$.

b) Because $g^* \in I^*$ for every $g \in G$ the set G^* is a subset of I^* and it remains to proof that every leading word f of some $u \in I^*$ is divisible by some leading term of G^*. Because f is not normal it is evident for non-canonical words: $tx = lm(tx - xt)$ is a subword for some $x \in X$. If $f = ht^k$ is canonical then, according to a), $h \notin N$ and is divisible by the leading word of some $g \in G$. But $g^* \in G^*$ has the same leading word by Lemma 4 and word is a subword of f too.

If G does not contain any element of degree less then two then no leading term of G^* can be a subword of the leading term of some $s \in S$. Because G is minimal, G^* should be minimal too.

c) is evident and for d) we need only to note that $ty - yt$ can be written in the factor-algebra as linear combination of other commutators and we do not need it. ■

6 Rabbit Strategy in the Calculating of Gröbner basis

Now, when we get the good definition of the homogenization ideal the question is how to get Gröbner basis for the ideal I^* practically, starting from the generating set R for the ideal I? We know, that we need to homogenize the elements in R, we know, that we need to add the commuting relations $xt - tx$ from S, but it is not sufficient to get all the canonical elements in I^*, as Example 1 shows. Fortunately we need only to slightly modify the main algorithm for Gröbner basis calculations to get the desired result.

Definition 2 *The cancellation rule: if $u = vt^k$ is a canonical element and $k \geq 0$ is as maximal as possible then replace u by v. Formally: replace u by $(u_*)^*$.*

Theorem 2 *Let $R \subset K\langle X\rangle$ be the generating set of the ideal I. Consider the eliminating ordering (as above) and the following algorithm. Homogenize R, add $S = \{tx - xt | x \in X\}$ and use the standard Gröbner basis calculation algorithm (Mora's algorithm) with the following modification: every time when we get a new canonical element u that should* *be added to the Gröbner basis add instead the element, obtained by the cancellation rule.*

The resulting set G^* is the Gröbner basis for the ideal I^*. After dehomogenization (setting $t = 1$) we get the Gröbner basis G for the ideal I. Moreover, G^* is minimal if and only if G is minimal. In particular if I has a finite Gröbner basis we get it after finitely many steps.

Proof. Consider the process of calculating the Gröbner basis for I and compare it with the modified algorithm creating G^*. By the construction and according to Lemma 4 all leading monomials from G^* (except those that correspond to S) do not contain t. From this follows that those two processes deal with the same leading monomials. The only possible difference could be in the reduction, but the cancellation rule, commutativity rules for t and ordering are specially designed to take care about this problem: the reduction process looks similar too (see example below). So, for every $g \in G$ we get g^* added to the Gröbner basis. According to the previous theorem we get Gröbner basis for I^* (and no other elements, because we are always inside I^*). Thus G is obtained from G^* using the dehomogenization, which proves all the statements in the theorem. ■

Let us check how this algorithm works in the Example 1. As above we suppose that $y > x > t$, but work in the eliminating ordering. We start from the same set:

$$tx - xt, ty - yt, x^2 - t^2, xy^2 - t^3.$$

Rewriting x^2y^2 in two different ways we get the element

$$x(xy^2 - t^3) - (x^2 - t^2)y^2 = t^2y^2 - xt^3 \to y^2t^2 - xt^3 = u.$$

The main difference now is that we should apply the cancellation rule and add the cancelled element $v = y^2 - xt$ to our Gröbner basis. Now we can throw away the element $xy^2 - t^3$ (it is reduced to zero using v) and we are done: no more new elements appear. The dehomogenization gets the desired result.

The algorithm described in this theorem was used in the Computer Algebra package Bergman (see [3]). Initially Bergman was elaborated for the graded algebras only. This restriction makes it more efficient. To be able to use Bergman in the non-graded situations we introduced so called Rabbit strategy, close to the strategy, described in the last theorem. More exactly, dealing with non-graded algebras, Bergman homogenize them and uses the cancellation rule during the calculations. This means that the calculations cannot be done degree by degree as for graded case, but sometimes (when we used the cancellation rule) we need to go back to the lower degrees. This jumping between the degrees explains the name of the strategy and in fact is organized using three parameters: maximum degree, starting degree and step s. We do all the calculations degree after degree until the maximum degree. But when we pass the starting degree we are ready to jump. We pass s degrees and, if we have found that the cancellation rule was used, we jump back to the corresponding degree and pass next s degrees and so on until the maximum degree will be achieved. In the case we get Gröbner basis completely the dehomogenized set G is the minimal Gröbner basis for our non-graded algebra. If not, the user is informed that obtained set G may be incomplete. The important property of the Rabbit strategy is that if we have a finite Gröbner basis in our non-graded algebra than using sufficiently large maximum degree we will obtain this Gröbner basis and the user will be informed about this.

7 n-chains and Anick resolution

As we have seen above the ideal I^* is the correct way to work with the homogenization. We want to underline this fact even more by showing (without complete proofs) that in fact we can use I^* and G^* to work with the homological properties. For simplicity we restrict ourselves by the case when Gröbner basis G has no elements of the degree less then two, so both G and G^* are minimal. We also suppose that the elements in I have no constant terms, so K be a trivial module both for graded and non-graded algebra. We want to compare Anick resolutions for them.

Let us recall that the sets C_n of n-chains are defined recursively. First of all, $C_{-1} = 1, C_0 = \{X\}$, where X is our alphabet and for every $x \in X$ its tail is x itself.

The set C_{n+1} consists of those words fr with $f \in C_n, 1 \neq r \in N$ which have the following properties:

- If $f = gs$, where s is the tail of f then $sr \notin N$.
- If $r = r'x$, where $x \in X$ then $sr' \in N$.

The normal word r is uniquely determined by the word fr and is its tail.

Recall that the set C_1 is exactly the set of the leading words of any minimal Gröbner basis (and depends on ideal I and ordering only). Now we want to describe the set of n-chains for the ideal I^*.

Theorem 3 *a) The set of n-chains for the ideal I^* is the union of two different sets for $n \geq 0$: $C_n^* = C_n \cup tC_{n-1}$.*

b) Every element of C_n has the same tail as for ideal I.

c) If $f = tg \in tC_{n-1}$ then for $n > 0$ it has the same tail as g and for $n = 0$ the tail is the word t itself.

Proof. Easy induction. Base for $n = 0$ is trivial, for $n = 1$ follows from the Theorem 1. In general, if fr is $(n+1)$-chain for I^* with $n \geq 1$, then $f = gs$ is n-chain for I^* and r, s are normal (for I^*), but sr is not. If $r = r'y, y \in X \cup t$, then sr' is normal. According to Theorem 1 a) we have $y \neq t$ (otherwise sr and sr' are normal simultaneously). Because r is normal r' does not contain t neither. At last, by the induction, the tail s does not contain t. So we decide the question of normality exactly as in I. If $g \in C_n$ we can conclude that $f \in C_{n+1}$, but if $g \in tC_n$, say $g = th, h \in C_{n-1}$, then th and h have the same tale and the fact that ths is $(n+1)$-chain is equivalent to the fact that hs is n-chain for I. ■

Let us recall that n-chains are used for the constructing of Anick resolution (see [1, 2]), namely for the trivial module K over algebra $A = K\langle X\rangle/I$. It looks as

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

The differentials d_n are recursively defined for any n-chain f, which we identify with $f \otimes 1$. The last theorem allow us to see how in fact Anick resolution is lifted from the non-graded algebra A to the graded algebra $B = K\langle X, t\rangle / I^*$. We skip the proof of the technical details of this process, and only formulate its most important properties.

Theorem 4 *If d_n^* are differentials in the Anick resolution for trivial $B-$module K then*
a)If $f \in C_n$ then $d_n^*(f) = (d_n(f))^*$
b)If $f = tg \in tC_{n-1}$ then $d_n^*(tf) = td_{n-1}^*(g) + (-1)^n gt$.
c) $v \in Ker\ d_n^* \Leftrightarrow v_* \in Ker\ d_n$ for any canonical element v.

This and previous theorem gives also some hint how to extract the information about the homology of A from the homology of B. We see for example that in the monomial case the Betti numbers are nothing else than the differences of the corresponding Betti numbers for B, because in the monomial case the Betti numbers are equal to the number of the corresponding n-chains. Of course, we do not need to homogenize monomial algebras, but the last theorem shows that we can calculate the Betti numbers in the similar way in general case. It does not work if we only homogenize the relations. This again shows that the homogenization should be combined with the cancellation rule to get the correct mathematical connection between non-graded and graded algebras.

This article takes its origin from the discussion of the properties of Anick resolution with Ed Green and the author is very grateful to him for all his ideas that have helped to write this article.

References

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

[2] Ufnarovski ,V.: Combinatorial and Asymptotic Methods of Algebra in "Algebra-VI" (A.I.Kostrikin and I.R.Shafarevich, Eds), En-

cyclopaedia of Mathematical Sciences, Vol. 57 , Springer,(1995), pp.5–196.

[3] http://servus.math.su.se/bergman

Victor Ufnarovski,

Received February 19, 2008

Centre for Mathematical Sciences, Mathematics, Lund
Institute of Technology, Lunds University,
P:O. Box 118, SE-22100,
Lund, Sweden
E–mail: *ufn@math.su.se*