Computer Science Journal of Moldova, vol.4, no.3(12), 1996

Constructing the Gröbner basis using Anick's resolution in the noncommutative algebras

A.Podoplelov

Abstract

This article describes the method of construction the Gröbner basis based on the information in the Anick's resolution.

Introduction

Gröbner basis is an important tool to investigate an algebra. For example, it is a base for constructing of so-called Anick's resolution [1]. In this article we show that the resolution itself contains sufficient information to construct the Gröbner basis during the calculation of the differentials.

1 Gröbner basis and $n-$chains

Let $X = \{x_1, x_2, \ldots, x_n\}$ and

$$\mathcal{A} = K < X >$$

be a finitely-generated associative free algebra over a field K. Let $>$ be a degree ordering on the set S of all words in the alphabet X i.e.

- $\deg f < \deg g \Rightarrow f < g$
- $f < g \Rightarrow hfk < hgk, \forall f, g, h, k \in S$

Then for any element of the free algebra it is possible to point out its leading word (term).

Let I be some ideal of the algebra $\mathcal{A}$ which will be fixed in this section.

Definition 1.1 *A word $s \in S$ is called* normal *(modulo the ideal I), if s is not the leading term of any element in I.*

Let us denote by N the linear hull of the set of normal words and call it the *normal complement of the ideal I*. The name is justified by the preposition (see [2]):

$$\mathcal{A} = N \oplus I.$$

In other words any element $u \in \mathcal{A}$ can be represented as $u = n + i, n \in N,\ i \in I$.

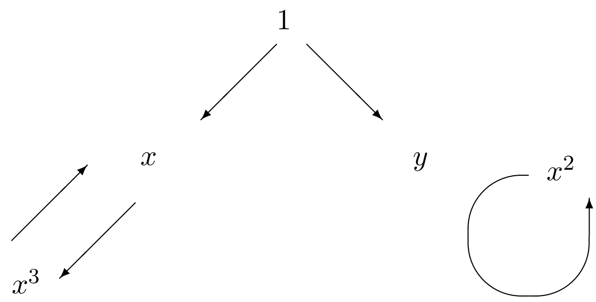
Definition 1.2 *For every $u \in \mathcal{A}$ its* normal form $\overline{u}$ *is defined to be its image by the natural projection $\mathcal{A} \longrightarrow N$. Clearly, $\overline{u} = 0 \Leftrightarrow u \in I$.*

Definition 1.3 *Following [1], we call a word $f \in S$ an* obstruction *if f is the leading term of some of the element of I (i.e. $f \notin N$), but all its proper subwords are normal. We denote by F the set of all the obstructions.*

Definition 1.4 *The subset $G = \{f - \overline{f} | f \in F\}$ of the ideal I is called its* (reduced) Gröbner basis.

Let us define the notion of an *n-chain* using the following *graph of chains $C(F)$*. It is a oriented graph $C(F)$, whose vertices are all proper endings of obstructions (including the empty word $\Lambda = \mathbf{1}$), together with the set of generators X. The edges are defined as follows: there is one edge from the empty word to every generator $\mathbf{1} \to \mathbf{x}$ for $x \in X$. Furthermore $f \to g$ if and only if the word fg contains the only obstruction as a subword and the unique occurrence of the obstruction in the word fg is one of its ends. The $n-$chain is a word, that can be read during a path in $C(F)$ of length $n + 1$, starting with $\mathbf{1}$.

Example. Let $F = \{x^4\}$, $X = \{x, y\}$. Then the graph $C(F)$ is of the following form



-1-chain: 1

0-chains: x, y

1-chain: x^3

2-chain: x^4

3-chain: x^6

...

Note, that every $(n+1)-$chain f can be uniqely presented in the form $f = gt$, where g is $n-$chain (and call t as tail of f).

2 Anick's resolution

Let $A = \mathcal{A}/I$ be a graded finitely-presented algebra. Let us denote all the n-chains by C_n and consider the following resolution, constructed by Anick (see [1]):

$$\dots C_n \otimes A \xrightarrow{d_n} C_{n-1} \otimes A \xrightarrow{d_{n-1}} \cdots C_{-1} \otimes A \xrightarrow{\epsilon} K \to 0$$

The differentials d_n are defined by induction, together with the splitting inverse mapping $i_n : \ker d_{n-1} \to C_n \otimes A$, which unlike d_n will not be homomorphisms of modules. Thus let us set

$$d_0(x \otimes \mathbf{1}) = \mathbf{1} \otimes \mathbf{x},$$

$$i_{-1}(\mathbf{1}) = \mathbf{1} \otimes \mathbf{1},$$

$$i_0(\mathbf{1} \otimes \mathbf{x_{i_1}} \dots \mathbf{x_{i_k}}) = \mathbf{x_{i_1}} \otimes \mathbf{x_{i_2}} \dots \mathbf{x_{i_k}}.$$

Let $f = gt$ be an $(n+1)$-chain with the tail t. We set

$$d_{n+1}(gt \otimes \mathbf{1}) = \mathbf{g} \otimes \mathbf{t} - \mathbf{i_n d_n}(\mathbf{g} \otimes \mathbf{t}),$$

and it remains only to define i_n for $n > 0$. To do this let us note first that, thanks to isomorphism from C_nN to $C_n \otimes N$, the following partial order is defined: $f \otimes t < g \otimes s \Leftrightarrow ft < gs$. In particular, in the definition of d_{n+1}, the first term in $g \otimes t$ will be the leading one and this can also be assumed to be satisfied by induction.

Thus, let $u \in \ker d_{n-1}$ and $f \otimes s$ be the leading term in u, participating in u together with a coefficient $\alpha \neq 0$. Let r be the tail of the $(n-1)$-chain $f = hr$. We know by induction that $d_{n-1}(f \otimes \mathbf{1}) = \mathbf{h} \otimes \mathbf{r} + \dots$ and that $h \otimes r$ is the leading term. $d_{n-1}(f \otimes s) = h \otimes \overline{rs} + \dots$, since d_{n-1} is a homomorphism of A-modules. Note, that $\overline{rs}$ is the normal form of rs. If the word rs were normal, then $h \otimes rs$ would remain the leading word and the element u could not possibly belong to the kernel. Thus, rs contains an obstruction. Choosing its leftmost possible occurrence of the form $rs = abc$, where b is an obstruction, we easily see that $g = hab$ is an n-chain. Consequently $g \otimes c \in C_N \otimes A$. Let us now set

$$i_n(u) = \alpha g \otimes c + i_n(u - \alpha d_n(g \otimes c)),$$

and the matter will be done by one more induction this time on the order $>$, since the parentheses already contain a smaller element.

3 Implementation

The recursive construction, described above, was implemented by author both as a part of the program BERGMAN (elaborated by Jörgen

Backelin in LISP) and as a separate program ANICK (C++) for different computers. We plan to discuss this implementation in the separate article and here restrict our attention by only one aspect of implementation.

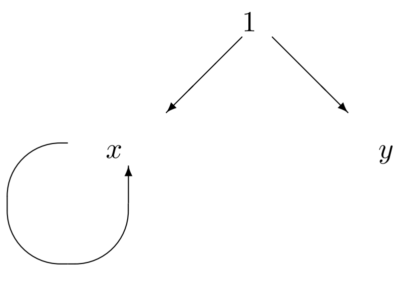
According to the construction, the Gröbner basis should be known (at least up to given degree) to calculate the resolution. Let us suppose we give as input data not complete Gröbner basis, hence the program will have at its disposal only part of the Gröbner basis elements. This means that when the graph of chains is constructed not all the obstructions participated in this process and hence some of the chains could not be obtained from this graph. If in this situation we try to calculate the resolution we will see that there exist such chains to be calculated in the graph that requires these absent chains. So, consequently we get the fact that if we want to have the whole calculated resolution till the degree k, it is necessary to have all the chains till this degree k. But this fact would not be very interesting if it answers only whether we have a complete Gröbner basis or not.

Using the information on the way of the calculations it turned out that it is possible to find in this critical situation a new Gröbner basis element.

Let us consider this on an example. Let $A =< X|R >$ be a finitely-presented graded (associative) algebra over a field K with two generators x and y ($x > y$), and with one element $x^2 - y^2 = 0$, i.e

$$A < x, y \mid x^2 - y^2 >$$

The corresponding graph of chains looks like



Let us try to calculate the differential for 1-chain x^2. Note, that

$$d_0(x \otimes 1) = 1 \otimes x, \text{ and } d_0(y \otimes 1) = 1 \otimes y.$$

So,

$$\begin{gathered}
d_1(x^2 \otimes 1) = x \otimes x - i_0(\overline{d_0(x \otimes 1) * x}) = \\
x \otimes x - i_0(1 \otimes \overline{x^2}) = x \otimes x - i_0(1 \otimes y^2) = \\
x \otimes x - (y \otimes y + i_0(\overline{1 \otimes y^2 - d_0(y \otimes 1) * y})) = \\
x \otimes x - (y \otimes y + i_0(1 \otimes y^2 - 1 \otimes \overline{y^2})) = \\
x \otimes x - (y \otimes y + i_0(1 \otimes y^2 - 1 \otimes y^2)) = \\
x \otimes x - y \otimes y
\end{gathered}$$

And we see that no critical situations occurred while calculating all the i_0. But let us see on the process of the calculation for the 2-chain x^3:

$$\begin{gathered}
d_2(x^3 \otimes 1) = x^2 \otimes x - i_1(\overline{d_1(x^2 \otimes 1) * x}) = \\
x^2 \otimes x - i_1(\overline{(x \otimes x - y \otimes y) * x}) = \\
x^2 \otimes x - i_1(x \otimes \overline{x^2} - y \otimes \overline{yx}) = \\
x^2 \otimes x - i_1(x \otimes y^2 - y \otimes yx) =
\end{gathered}$$

Here the situation appears when to calculate the integral i_1 it is necessary to have an 1-chain xy^2 that for a moment cannot be got from the graph of chains.

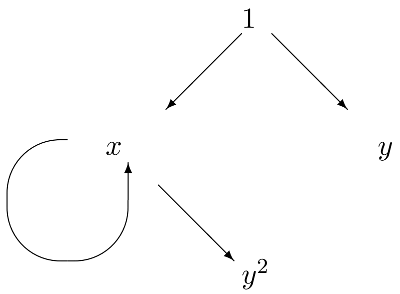
In this situation let us do the following. We replace the tensor product sign in the argument for i_1 with the simple product sign and the result element we add to the Gröbner basis, reconstructing the graph of chains. In our case

$$x \otimes y^2 - y \otimes yx \;\to\; xy^2 - y^2x = 0$$

Hence our new basis will consist already of two elements:

$$x^2 - y^2 = 0, \qquad xy^2 - y^2x = 0.$$

In the graph there will appear the new vertex y^2 and the edge $x \to y^2$, i.e.



Continuing the calculations for the $d_2(x^3 \otimes 1)$ we will get the following result without any critical situations

$$d_2(x^3 \otimes 1) = x^2 \otimes x - xy^2 \otimes 1$$

As we have seen the idea of constructing the Gröbner basis is to calculate in the fixed degree all the 2-chains. After computing these chains in the given degree we get the complete Gröbner basis till this degree. But it remains not minimal so the final stage is to reduce the new Gröbner basis elements.

4 Conclusion

Program is installed in Stockholm university account and is included (together with a package BERGMAN) in the international list of available by ftp Computer Algebra software.

Acknowledgments

I would like to thank Prof. Jan-Erik Roos (Stockholm University, the Department of Mathematics, Sweden), Dr. Victor Ufnarovski (Lund University, Sweden) and Dr. Jörgen Backelin (Stockholm University, the Department of Mathematics, Sweden) for their consultations and support to implement this idea on PC. Also I would like to thank Dr. Svetlana Cojocaru (the Institute of Mathematics of Academy of Sciences of Moldova) for help in resolving all my local problems.

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 in Algebra, Encyclopedia of Mathematical Sciences, v.57, Springer (1995), p.1–196.

A.Podoplelov,
Institute of Mathematics,
Academy of Sciences of Moldova,
5 Academiei str., Kishinev,
MD–2028, Moldova
phone: (373–2) 738073
e–mail: *sandu@math.moldova.su*

Received 3 December, 1996