On linear equations in some non-commutative algebras

Jonas Månsson

The problem of solving linear equations in a non-commutative algebra is in general a highly non-trivial matter. Even in the case of finitely presented algebras, there is no general algorithm for solving seemingly simple equations of the type

$$a\chi = \chi b$$

for some elements a and b.

In this paper we will demonstrate a method by which it is possible to find all the solutions to linear equations in certain factor algebras of the non-commutative polynomial ring. The commutative case reduces to computing syzygy modules, which is treated in Adams [1]. Here we will consider algebras the center of which is sufficiently large, in the sense that the former can be considered a Noetherian module over a subalgebra of its center. We will show that with the aid of Gröbner basis technique, the problem of finding the solutions in the non-commutative setting can be reduced to computing a syzygy module.

1 Basic definitions and notions

Let K be any field and $X = \{x_1, x_2, \ldots, x_k\}$ a finite alphabet. If $H = \{h_1, h_2, \ldots, h_m\}$ is a set of elements in the non-commutative polynomial ring $K\langle X\rangle$ and (H) denotes the two-sided ideal generated by H, we will use the notion $K\langle X|H\rangle$ for the factor algebra $A = K\langle X\rangle/(H)$. From now on it is also assumed that we have an *admissible order* on the set of words of $K\langle X\rangle$. For Gröbner basis calculation we will use a so called *deglex order*, which means

$$f < g \quad\Leftrightarrow\quad \begin{cases} \deg f < \deg g & \text{or} \\ \deg f = \deg g & \text{and f is smaller than g lexicographically} \end{cases}$$

If not otherwise stated the natural order $x_1 < x_2 < \cdots < x_k$ will be used. Now, if f is an element in $K\langle X\rangle$, we can associate to f the *leading term*

$lt(f)$, being the monomial in f containing the largest word. The remaining sum of monomials in f will be denoted by $rt(f)$ (*remaining terms* of f).

If I is an ideal in $K\langle X\rangle$, a word $u \in K\langle X\rangle$ is said to be *normal modulo I* if there is no element f in I such that $lt(f)|u$ (by division we mean division in the non-commutative sense). In case $I = (H)$ for some finite subset H of $K\langle X\rangle$ we write $N_{K\langle X\rangle}(H)$ for the set of normal words modulo I, and if there is no risk of confusion often just N. Furthermore, if we have a set N of normal words, we can also consider the K-span of N, i.e the K-vector space generated by the elements of N, which we will denote by KN. It follows that $K\langle X\rangle = KN \oplus I$ is a direct sum of K-vector spaces (see for instance [2]). Now, if $f \in K\langle X\rangle$, its *normal form* $\overline{f}$ is defined as the image of f by the natural projection $K\langle X\rangle \longrightarrow KN$. If a finite Gröbner basis G can be computed, the normalization procedure is algorithmic, and can be carried out via step-wise reduction by elements in G. By a *reduced Gröbner basis* G we mean a minimal Gröbner basis where $rt(f)$ is in its normal form for all elements f in G. A reduced Gröbner basis can always be computed from a minimal one, just by normalizing all remaining terms with the aid of the basis itself.

If $F = \{f_1, f_2, \ldots, f_n\}$ is a set of elements in $K\langle X|H\rangle$ we will denote by $K\langle F\rangle$ the subalgebra of $K\langle X|H\rangle$ generated by F. We will also repeatedly refer to the center $Z(A)$ of an algebra A, meaning the subalgebra

$$Z(A) = \{f \in A | fg = gf \;\forall g \in A\}$$

2 Main results

In this section we will first introduce the factor algebras of the non-commutative polynomial ring we are interested in. These algebras will be proved to be Noetherian modules over a finitely generated subalgebra of its center. Secondly we will, in some sense, generalize the notion of syzygys to non-commutative algebras and provide a tool by which we can compute these syzygys. This will essentially be the same as determining the solutions to a linear equation. The exact procedure for this will be outlined in the examples in section 3.

Proposition 2.1 *Let $K\langle X|H\rangle$ be a finitely presented algebra over K and $Y = \{y_1, y_2, \ldots, y_n\}$ a finite alphabet. If $H' = \{h'_1, h'_2, \ldots, h'_n\}$ is a finite subset of $K\langle X\rangle$ and $H'_Y = \{y_i - h'_i \,|\, 1 \leq i \leq n\}$ then*

$$K\langle X|H\rangle \backsimeq K\langle X \cup Y | H \cup H'_Y\rangle$$

The isomorphism in 2.1 is really nothing else than giving the elements in H' names by which they can be identified (i.e h'_i is identified with y_i). The advantage of this is that by using a different internal order of the alphabet $X \cup Y$, it is possible to alter the structure of the normal elements to a more desirable form. Returning to the situation in proposition 2.1 we let $A = K\langle X|H\rangle$ be a finitely presented algebra over K and $Y = \{y_1, y_2, \ldots, y_n\}$ a finite alphabet. We assume that we have the internal order $y_1 < y_2 < \cdots < y_n < X$ of the elements in $X \cup Y$.

Proposition 2.2 *If $H' = \{h'_1, h'_2, \ldots, h'_n\}$ is a finite set of elements in $K\langle X\rangle$ such that $\overline{H'} = \{\overline{h'_1}, \overline{h'_2}, \ldots, \overline{h'_n}\}$ is a subset of $Z(A)$, then, for each $f \in K\langle X \cup Y\rangle$, the normal form modulo $(H \cup H'_Y)$ is written*

$$\overline{f} = z_1 n_1 + z_2 n_2 + \cdots + z_l n_l$$

where, for all i, $z_i \in K\langle Y\rangle$ and n_i is a word in $K\langle X\rangle$ which is normal modulo $(H \cup H'_Y)$, i.e $n_i \in N_{K\langle X\cup Y\rangle}(H \cup H'_Y) \bigcap K\langle X\rangle$. Moreover, for all i, each term in z_i is of the form $cy_1^{a_1} y_2^{a_2} \cdots y_n^{a_n}$ for some scalar c and non-negative integers a_j.

Proof Assume that $u \in K\langle X \cup Y\rangle$ is a normal word modulo $(H \cup H'_Y)$. Now, since $x_i h'_j - h'_j x_i$ belongs to the ideal (H) in $K\langle X\rangle$ for all i and j, $x_i y_j - y_j x_i$ must be in the ideal $(H \cup H'_Y)$ in $K\langle X \cup Y\rangle$. Consequently, since $lt(x_i y_j - y_j x_i) = x_i y_j$, u has to be in the form $u = zn$, where z and n are words in $K\langle Y\rangle$ and $K\langle X\rangle$ respectively. Moreover, since $h'_i h'_j - h'_j h'_i$ also belongs to the ideal (H) in $K\langle X\rangle$ for all i and j, the same argument yields that $y_i y_j - y_j y_i \in (H \cup H'_Y)$. Thus, from the internal order of the alphabet Y it follows that $z = y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n}$ for some non-negative integers a_j. By definition, the normal form of an element is a sum of normal monomials, which proves the statement. $\square$

This means we can regard A as a module over a subalgebra generated by some central elements. In particular, if A is finitely generated as a module, it is Noetherian.

Proposition 2.3 *If $N_{K\langle X\cup Y\rangle}(H \cup H'_Y) \cap K\langle X\rangle$ is finite then $A = K\langle X \cup Y|H \cup H'_Y\rangle$ is a Noetherian module over $Z' = K\langle\overline{Y}\rangle \subseteq Z(A)$, i.e the commutative subalgebra of A generated by $\overline{Y} = \{\overline{y_1}, \overline{y_2}, \ldots, \overline{y_n}\}$*

The main problem with linear equations in non-commutative algebras is that multiplication can be carried out on both sides of the unknown variables. Thus, the solution set is not in general a syzygy module, i.e a module over the algebra itself. However, we can still think of it as a module over its center, and in this sense it can be seen as a generalization of the usual notion of syzygys. We will now consider linear homogeneous equations in A defined by the following K-linear maps:

If $F = \{f_{ij}^k \,|\, 1 \leq i \leq s,\, 1 \leq j \leq t_i,\, 1 \leq k \leq 2\}$ is a finite set of elements in a finitely presented algebra $A = K\langle X|H\rangle$ we can define a K-linear map $\phi_F: A^s \longrightarrow A$ by

$$(\chi_1, \chi_2, \ldots, \chi_s) \longmapsto^{\phi_F} \sum_{i=1}^{s} \sum_{j=1}^{t_i} f_{ij}^1 \chi_i f_{ij}^2 \tag{1}$$

In particular, if Z' is a subalgebra of $Z(A)$, ϕ_F becomes a Z'-module homomorphism. The kernel of ϕ_F ($\ker \phi_F$) is then a Z'-submodule of A^s. In case A is commutative the kernel is called a *syzygy module*. For any factor algebra of the commutative polynomial ring the computation of a syzygy module is algorithmic (see for instance Adams [1]). Turning our attention to the non-commutative case again, we notice that if the conditions in proposition 2.3 are fullfilled, the kernel is a Noetherian Z'-module just as in the commutative case. It means there is a possibility to express all the solutions to an equation $\phi_F(\chi_1, \ldots, \chi_s) = 0$ in a fairly simple way, provided we know a way to compute them. We will now consider algebras of this kind, and provide a constructive proof which can be used to reduce a system of linear equations in A to a system of linear equations in the commutative polynomial ring.

Let $A = K\langle X|H\rangle$ be a finitely presented algebra over K, and suppose $H' = \{h_1', h_2', \ldots, h_n'\}$ is a finite set of elements in $K\langle X\rangle$ such that $\overline{H'} \subseteq Z(A)$. Retaining the notation from proposition 2.1 and 2.2

$$K\langle X|H\rangle \backsimeq K\langle X \cup Y | H \cup H_Y'\rangle$$

and, identifying these two algebras, each element f in $K\langle X|H\rangle$ can be written

$$f = z_1 n_1 + z_2 n_2 + \cdots z_l n_l$$

for some $z_i \in K\langle\overline{Y}\rangle$ and $n_j \in N = N_{K\langle X\cup Y\rangle}(H \cup H_Y') \cap K\langle X\rangle$. Suppose further that $N = \{n_1, n_2, \ldots n_l\}$ is a finite set. Proposition 2.3 then says that A is a Noetherian module over $Z' = K\langle\overline{Y}\rangle \subseteq Z(A)$ generated by N.

Let $Z = K[Y]$. Since $Z' \subseteq Z(A)$ we can define a new multiplication $Z \times A \longrightarrow A$ via $(z, f) \longmapsto \overline{z}f$, which we will denote by zf for convenience. This will naturally turn A into a module over Z. Let $\mu: Z^l \longrightarrow A$ be defined by

$$\mu(z_1, z_2, \ldots, z_l) = z_1 n_1 + z_2 n_2 + \cdots + z_l n_l$$

Clearly, μ is a Z-module homomorphism onto A, and moreover, since Z^l is a Noetherian module, $\ker \mu$ is finitely generated. Combining what we already know from this section we can prove the following proposition:

Proposition 2.4 *Assume we have an internal order of the elements of $X \cup Y$ satisfying $Y < X$. If a finite Gröbner basis G for $(H \cup H'_Y)$ can be computed, then a generating set for $\ker \mu$ can be found in finitely many steps.*

Proof As mentioned in section 1 it can be assumed that $G = \{g_1, g_2, \dots, g_r\}$ is reduced, and thus from proposition 2.2 each element $g \in G$ is in the form

$$g = lt(g) + z_1 n_1 + z_2 n_2 + \cdots + z_l n_l$$

for some $z_i \in Z'$. Let M be a subset of Z^l initially set to $\{0\}$.

Let (i, j) be an ordered pair in $\{(i,j) \mid 1 \le i \le r, 1 \le j \le l\}$ such that $lt(g_i) = w n_k$ for some monomial $w \in Z'$ and $n_k \in N$ satisfying $n_j = n_k n'$ for some word $n' \in N$. For each such pair we reduce $rt(g_i)n'$ via G to a sum $z_{ij}^1 n_1 + z_{ij}^2 n_2 + \cdots + z_{ij}^l n_l$ (i.e to its normal form) and add the element

$$m_{ij} = (z_{ij}^1, z_{ij}^2, \dots, z_{ij}^{j-1}, w + z_{ij}^j, z_{ij}^{j+1}, \dots, z_{ij}^l)$$

to the set M.

Now M generates $\ker \mu$. This follows from a pure technical reasoning, using reduction via G. $\square$

3 Examples

In this section we will via a few examples demonstrate how to use the previous results to, for certain noncommutative algebras $K\langle X|H\rangle$, find all the solutions to linear equations of the type

$$\phi_F(\chi_1, \chi_2, \dots, \chi_s) = 0$$

where ϕ_F is a K-linear map defined as in definition (1).

Example 1 Let $A = K\langle x_1, x_2 | x_2^2 - x_1^2\rangle$. Now x_1^2 and $x_2 x_1 + x_1 x_2$ are both elements in $Z(A)$, and proposition 2.1 implies that

$$K\langle x_1, x_2 | x_2^2 - x_1^2\rangle \backsimeq K\langle x_1, x_2, y_1, y_2 | x_2^2 - x_1^2, x_2 x_1 + x_1 x_2 - y_1, x_1^2 - y_2\rangle$$

By using the internal order $y_1 < y_2 < x_1 < x_2$ we obtain a finite Gröbner basis

$$G = \{x_1^2 - y_2, x_2^2 - y_2, x_2 x_1 + x_1 x_2 - y_1, x_2 y_2 - y_2 x_2, x_2 y_1 - y_1 x_2,$$

$$x_1y_2-y_2x_1, x_1y_1-y_1x_1, y_2y_1-y_1y_2\}$$

From this basis we see that $N\cap K\langle X\rangle=\{1,x_1,x_2,x_1x_2\}$. By proposition 2.3, A is a Noetherian module over $Z'=K\langle\overline{y}_1,\overline{y}_2\rangle$, and each element $\chi_i\in A$ can be expressed $\chi_i=z_{i1}+z_{i2}x_1+z_{i3}x_2+z_{i4}x_1x_2$ for some $z_{ij}\in Z'$. Let $\phi: A^2\longrightarrow A$ be the Z'-module homomorphism defined by

$$\phi(\chi_i)=x_2\chi_1+\chi_2x_1$$

After substituting we get

$$\phi(\chi_i)=z_{11}x_2+z_{12}x_2x_1+z_{13}x_2^2+z_{14}x_2x_1x_2+z_{21}x_1+z_{22}x_1^2+z_{23}x_2x_1+z_{24}x_1x_2x_1=$$

$$=(z_{12}y_1+z_{13}y_2+z_{22}y_2+z_{23}y_1)+(z_{21}+z_{24}y_1-z_{14}y_2)x_1+$$

$$+(z_{11}+z_{14}y_1-z_{24}y_2)x_2+(-z_{12}-z_{23})x_1x_2=$$

$$=\mu(z_{12}y_1+z_{13}y_2+z_{22}y_2+z_{23}y_1, z_{21}+z_{24}y_1-z_{14}y_2, z_{11}+z_{14}y_1-z_{24}y_2, -z_{12}-z_{23})$$

From the Gröbner basis G and the proof of proposition 2.4 we deduce that $\ker\mu$ is generated by $M=\{0,y_2y_1-y_1y_2\}=\{0\}$, so

$$\phi(\chi_i)=0\quad\Leftrightarrow\quad\begin{cases} z_{12}y_1+z_{13}y_2+z_{22}y_2+z_{23}y_1=0\\ z_{21}+z_{24}y_1-z_{14}y_2=0\\ z_{11}+z_{14}y_1-z_{24}y_2=0\\ z_{12}+z_{23}=0\end{cases}$$

i.e the problem reduces to computing a syzygy module in $K[Y]$. This is algorithmic since $K[Y]$ is commutative (see [1]). We get the solutions

$$(\chi_1,\chi_2)=z_1'(x_2,-x_1)+z_2'(x_1,-x_2)+z_3'(y_2,x_1x_2-y_1)+z_4'(y_1-x_1x_2,-y_2)=$$

$$=z_1'(x_2,-x_1)+z_2'(x_1,-x_2)+z_3'(x_1^2,-x_2x_1)+z_4'(x_2x_1,-x_1^2)$$

where $z_i'\in Z'$. The set of solutions is a finitely generated module over Z', which is also expected, A^2 being a Noetherian module. □

Example 2 Consider the monomial algebra $A=K\langle x_1,x_2|x_1x_2,x_2x_1^3,x_2^3x_1\rangle$. Here x_1^3 and x_2^3 are elements in the center, and we consider the isomorphic algebra

$$K\langle x_1,x_2,y_1,y_2|x_1x_2,x_2x_1^3,x_2^3x_1,x_1^3-y_1,x_2^3-y_2\rangle$$

and compute a Gröbner basis

$$G=\{y_2x_1,y_1x_2,y_2x_2x_1,y_1y_2,y_2x_2^2x_1,y_2y_1,x_1x_2,x_1^3-y_1,$$

$$x_2^3-y_2,x_2y_1,x_1y_1-y_1x_1,x_1y_2,x_2y_2-y_2x_2\}$$

using the internal order $y_1 < y_2 < x_1 < x_2$, From this basis, proposition 2.2 and 2.3 we conclude that each $\chi \in A$ can be written

$$\chi = z_1 + z_2x_1 + z_3x_2 + z_4x_1^2 + z_5x_2x_1 + z_6x_2^2 + z_7x_2x_1^2 + z_8x_2^2x_1 + z_9x_2^2x_1^2$$

for some $z_i \in Z' = K\langle\overline{y_1}, \overline{y_2}\rangle$. Suppose we want to find all the solutions to $\phi(\chi) = x_1\chi x_1 - x_2\chi x_2 = 0$. After substituting we get

$$\phi(\chi) = z_1(x_1^2 - x_2^2) + z_2(x_1^3 - x_2x_1x_2) + z_3(x_1x_2x_1 - x_2^3) + z_4(x_1^4 - x_2x_1^2x_2) +$$

$$+z_5(x_1x_2x_1^2 - x_2^2x_1x_2) + z_6(x_1x_2^2x_1 - x_2^4) + z_7(x_1x_2x_1^3 - x_2^2x_1^2x_2) + z_8(x_1x_2^2x_1^2 - x_2^3x_1x_2) +$$

$$+z_9(x_1x_2^2x_1^3 - x_2^3x_1^2x_2) = (z_2y_1 - z_3y_2) + z_4y_1x_1 - z_6y_2x_2 + z_1x_1^2 - z_1x_2^2 =$$

$$= \mu(z_2y_1 - z_3y_2, z_4y_1, -z_6y_2, z_1, 0, -z_1, 0, 0, 0)$$

From G we can determine a generating set M for $\ker\mu$. Note that the elements of G which are used in the construction of M have been written in the first six positions. We can easily check that

$$M = \{(y_1)_{r_1}, (y_2)_{r_2}, (y_1y_2)_{r_3} | r_1 = 3, 5, 6, 7, 8, 9; r_2 = 2, 4, 5, 7, 8, 9; 1 \leq r_3 \leq 9\}$$

where $(y)_i$ denotes the element in $K[Y]^9$ having y in the i:th position and 0 everywhere else.

This means that the problem of finding the solutions to the initial equation is reduced to determining the syzygy module of the following system of equations:

$$\begin{cases} z_2y_1 - z_3y_2 + v_1y_1y_2 = 0 \\ z_4y_1 + v_2y_2 + v_3y_1y_2 = 0 \\ -z_6y_2 + v_4y_1 + v_5y_1y_2 = 0 \\ z_1 + v_6y_2 + v_7y_1y_2 = 0 \\ -z_1 + v_8y_1 + v_9y_1y_2 = 0 \end{cases}$$

The solutions to this system (we are only interested in the z_i:s) are

$$(z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8, z_9) = (z_1'y_1y_2, z_2'y_2, z_3'y_1, z_4'y_2, z_5', z_6'y_1, z_7', z_8', z_9')$$

for arbitrary $z_i' \in K[Y]$. Substituting in χ and reducing in A we get

$$\chi = z_5'x_2x_1 + z_7'x_2x_1^2 + z_8'x_2^2x_1 + z_9'x_2^2x_1^2$$

where $z_i' \in Z'$. $\square$

References

[1] Adams, W.W.,Loustaunau, P. (1994): *An Introduction to Gröbner Bases*, American Mathematical Society.

[2] Ufnarovski, V.A. (1995): *Combinatorial and Asymptotic Methods of Algebra*, Algebra-VI (A.I. Kostrikin and I.R. Shafarevich, Eds), Encyclopedia of Mathematical Sciences, Vol. 57, Springer, 5-196.