# On some Basic Applications of Gröbner bases in Non-commutative Polynomial Rings

*Patrik Nordbeck*

Lund Institute of Technology,
Box 118, S-221 00 Lund, Sweden
email: nordbeck@maths.lth.se

**Abstract**

In this paper we generalize some basic applications of Gröbner bases in commutative polynomial rings to the non-commutative case. We define a non-commutative elimination order. Methods of finding the intersection of two ideals are given. If both the ideals are monomial we deduce a finitely written basis for their intersection. We find the kernel of a homomorphism, and decide membership of the image. Finally we show how to obtain a Gröbner basis for an ideal by considering a related homogeneous ideal.

The method of Gröbner bases, introduced by Bruno Buchberger in his thesis (1965), have become a powerful tool for constructive problems in polynomial ideal theory and related domains. Generalizations of the basic ideas to the non-commutative setting was done, as an theoretical instrument, by Bokut (1976) and Bergman (1978). From the constructive point of view, the non-commutative version of *Buchberger's algorithm* was presented by Mora (1986). For some special classes of non-commutative rings, Gröbner bases has been studied in more detail, e.g. solvable algebras by Kandri-Rody and Weispfenning (1990).

As the title indicates, we will here consider Gröbner bases in non-commutative polynomial rings, i.e. free associative algebras (over some field). Most of the results are just easy generalizations of the theory of Gröbner basis in commutative polynomial rings, which can be found e.g. in the textbook by Adams and Loustaunau (1994), or in the original paper by Buchberger (1985).

In section 2 we define an order allowing us to use elimination techniques. Section 3 concerns intersection of ideals. We find a Gröbner basis for the intersection of two ideals. In the special case when both the ideals are monomial, we show how automata can be used to obtain a finitely written basis. The material in section 4, where we find a Gröbner basis for the kernel of a homomorphism, and decide membership of the image, is nearly identical with the commutative case as presented in the textbook mentioned above. As an application we mention the study of subalgebras. Since homogeneous ideals are more comfortable to work with, we will in the last section show how to obtain a Gröbner basis for an ideal by considering a related ideal with homogeneous generators.

All of the Gröbner basis calculations in the examples are performed with the program GROEBNER by Feustel and Green (1992).

The author expresses his thanks to V.A. Ufnarovski for helpful discussions.

# 1 Basic definitions and notations

Let $X = \{x_1, x_2, \ldots, x_n\}$ be a finite alphabet, and let $K\langle X\rangle$ denote the free associative algebra over the arbitrary field $K$. Denote by $S$ the set of all words in $X$, including the empty word $\mathbf{1}$. We will assume that $S$ is given an *admissible order*, i.e. an well-order preserving multiplication: $f < g$ implies $hfk < hgk$ for all $f, g, h, k \in S$, such that the smallest word always is the unity $\mathbf{1}$. As an example we mention the following order called *deglex* (degree lexicographical): If $|u|$ denotes the length of $u \in S$, we let $u > v$ if either $|u| > |v|$ or $|u| = |v|$ but $u$ is larger than $v$ lexicographically.

When we have chosen an admissible order we can with every non-zero element $f \in K\langle X\rangle$ associate its leading word $\hat{f} \in S$.

If $u, v \in S$, and $u$ is a (not necessarily proper) subword of $v$, we write $u \mid v$. A word $u \in S$ is called *normal* modulo an ideal $I \subset K\langle X\rangle$ (always two-sided) if for every $f \in I$, $\hat{f} \nmid u$.

If $N$ denotes the linear hull of the set of normal words (mod $I$), we have $K\langle X\rangle = N \oplus I$ as direct sum of vector spaces (see Ufnarovski 1995).

For every $f \in K\langle X\rangle$, its image by the projection $K\langle X\rangle \longrightarrow N$ will be called its *normal form*, and be denoted $\bar{f}$. Clearly $\bar{f} = 0$ if and only if $f \in I$.

**Definition 1** *A subset $G$ of the ideal $I$ is called a* Gröbner basis *if for every $f \in I$ there is $g \in G$ such that $\hat{g} \mid \hat{f}$.*

A Gröbner basis is *minimal* if no proper subset of it is a Gröbner basis. If, moreover, every element $g \in G$ has the form $\hat{g} - \bar{\hat{g}}$, then the basis is called *reduced*. When an admissible order is selected, every ideal has an unique reduced Gröbner basis.

For the construction of Gröbner bases we refer to (Mora 1986). We point out however that we now, compared to the commutative case, have a great disadvantage caused by non-noetherianity: Even a finitely generated ideal may have no finite Gröbner basis.

However, if we are given a Gröbner basis (possibly infinite) with its leading words sorted by length, then it is not hard to see that the process of *reduction*

$f \to \bar{f}$ described above can be performed in a finite number of steps. This rests on the fact that an admissible order on $S$ by definition is well-founded, i.e. every infinite sequence $u_1 \geq u_2 \geq \dots u_i \geq \dots$ in $S$ stabilizes.

The standard method of constructing a Gröbner basis, using deglex, will for a homogeneous ideal (see section 5) automatically yield a basis sorted as above. Thus the reduction is algorithmic in this case.

# 2 Elimination

For $u \in S$, let $\deg_{x_i} u$ denote the number of different occurrences of $x_i$ in $u$. We will frequently use the following admissible order suggested by Edward Green[1]:

First use the commutative lexicographic order, i.e. if $x_1 < x_2 < \dots < x_n$ we let $u > v$ $(u, v \in S)$ if $\deg_{x_i} u > \deg_{x_i} v$, where $i$ is the highest number such that $\deg_{x_i} u \neq \deg_{x_i} v$. If $\deg_{x_i} u = \deg_{x_i} v$ for all $i$ we use deglex.

We thus have for example $x_3 > x_1 x_2^2$, and more generally, if a word $u \in S$ does not contain any $x_{m+1}, \dots, x_n$, $m < n$, and if $u > v \in S$ in the order above, then $v$ does not contain any $x_{m+1}, \dots, x_n$ either. We will call this order the *elimination order* as motivated by the following theorem.

**Theorem 1** *Let $G$ be a Gröbner basis for the ideal $I$ according to the elimination order with $x_1 < x_2 < \dots < x_n$. Then, for $m \leq n$, $G_m = G \cap K\langle x_1, x_2, \dots, x_m\rangle$ is a Gröbner basis for the ideal $I_m = I \cap K\langle x_1, x_2, \dots, x_m\rangle$ in $K\langle x_1, x_2, \dots, x_m\rangle$.*

*Proof.* If $f \in I_m \subset I$ there is $g \in G$ such that $\hat{g}|\hat{f}$. Then $\hat{g}$ involves only $x_1, \dots, x_m$, so by the remark above every word in $g$ involves only $x_1, \dots, x_m$. Thus there is, for every $f \in I_m$, an element $g \in G_m$ such that $\hat{g}|\hat{f}$. $\square$

More generally, we could in our definition of the elimination order above first used any commutative elimination order (see e.g. Adams and Loustaunau 1994), and then any (non-commutative) admissible order to break ties.

# 3 Intersection

For two ideals $I = (f_1, \dots f_k)$, $J = (g_1, \dots, g_l) \in K\langle X\rangle$, consider the ideal

$$H = (tf_i, (1-t)g_j, tx_m - x_m t | 1 \leq i \leq k, 1 \leq j \leq l, 1 \leq m \leq n) \in K\langle X, t\rangle. \tag{3.1}$$

**Theorem 2** $I \cap J = H \cap K\langle X\rangle$.

[1] Edward L. Green, Virginia Polytechnic Institute and State University, Blacksburg, Virginia USA.

*Proof.* If $F \in I \cap J$, then $F = \sum_{i=1}^{k} p_{i_L} f_i p_{i_R} = \sum_{j=1}^{l} q_{j_L} g_j q_{j_R}$ for some polynomials $p_{i_L}, p_{i_R}, q_{j_L}, q_{j_R} \in K\langle X\rangle$. In $K\langle X, t\rangle$ we can write

$$F = tF + (1-t)F = \sum_{i=1}^{k} p_{i_L} t f_i p_{i_R} + \sum_{j=1}^{l} q_{j_L}(1-t) g_j q_{j_R} + \sum_{m=1}^{n} r_{m_L}(tx_m - x_m t) r_{m_R}$$

with $r_{m_L}, r_{m_R} \in K\langle X, t\rangle$. Here the last sum on the right hand side appears when moving $t$ (and $1-t$) to the generators $f_i$ ($g_j$). We conclude that $F \in H \cap K\langle X\rangle$.

Conversely, assume $F \in H \cap K\langle X\rangle$. $F \in H$ gives

$$F = \sum_{i=1}^{k} p_{i_L} t f_i p_{i_R} + \sum_{j=1}^{l} q_{j_L}(1-t) g_j q_{j_R} + \sum_{m=1}^{n} r_{m_L}(tx_m - x_m t) r_{m_R},$$

where $p_{i_L}, p_{i_R}, q_{j_L}, q_{j_R}, r_{m_L}, r_{m_R} \in K\langle X, t\rangle$. Since also $F \in K\langle X\rangle$, $F$ is independent of the value of $t$. Substituting 1 for $t$ we get $F = \sum p'_{i_L} f_i p'_{i_R} \in I$, where e.g. $p'_{i_L}(X) = p_{i_L}(X, 1) \in K\langle X\rangle$. Similarly $t = 0$ gives $F \in J$, so $F \in I \cap J$ as required. □

As an immediate consequence we get, using Theorem 1:

**Corollary 1** *Let $G$ be a Gröbner basis for $H$ according to the elimination order in $K\langle X, t\rangle$ with $t > X$. Then $G \cap K\langle X\rangle$ is a Gröbner basis for $I \cap J$.*

Even if $I$ and $J$ are given with a finite number of generators, we can not hope to get a finite set of generators for the intersection. As an easy example consider the ideals $I = (x^2, xy^2)$, $J = (xyx) \in K\langle x, y\rangle$. Beginning to calculate a Gröbner basis for $H = (tx^2, txy^2, (1-t)xyx, tx - xt, ty - yt)$ according to deglex with $t > x > y$, we get, considering words up to length 8 and omitting elements containing $t$, the set $\{xyx^2, x^2yx, xyxy^2, xy^2xyx, xy^3xyx, xy^4xyx\}$. We might guess, despite we are using just deglex and not the order in the Corollary, that

$$\{xyx^2, x^2yx, xyxy^2, xy^ixyx | i = 2, 3, \ldots\} \tag{3.2}$$

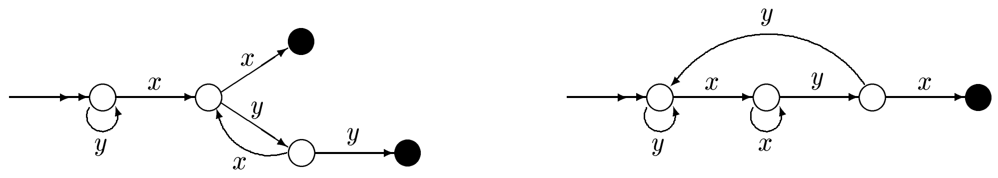
is a Gröbner basis for $I \cap J$. The problem of predicting an infinite basis, knowing a finite subset, is discussed at some extent in (Ufnarovski 1994). We will later in this section see that (3.2) indeed is a basis for $I \cap J$.

We will call an ideal *monomial* if it is generated by finite set of words. It is clear from the definition that any set of generators consisting of words is a Gröbner basis. Obviously a word is in a monomial ideal if and only if it contains one of its generators as a subword. Thus an element is in the intersection of two monomial ideals if and only if it has one generator from each ideal as subwords.

If (as in the example) both $I$ and $J$ are monomial, we can find a finite representation (such as (3.2)) for their intersection using automata. It is easy to see that an element $f \in K\langle X\rangle$ is in a monomial ideal $I$ if and only if all of the words in $f$ are in $I$. Since the same must be true for the intersection of two monomial ideals, it is sufficient to find all words in $I \cap J$.

We begin with constructing, for each ideal, its *ideal automaton*. This is a finite state automaton[2] recognizing the words in the ideal. The construction is similar to the one for the *automata of normal words*, which can be found in (Ufnarovski 1994). An automaton recognizing the words in the intersection

$I = (x^2, xy^2)$ : $\qquad\qquad$ $J = (xyx)$ :




*Ideal automata for $I = (x^2, xy^2)$ and $J = (xyx)$. Paths not leading to accepting states corresponds to the normal words.*

of $I$ and $J$ can now be obtained by simultaneously tracing the two ideal automata (In the language of automata this is called the *direct product* of the automata). A word will then be in the intersection if and only if both of the automata are in accepting states.

To pick out a set of generators for $I \cap J$ we can proceed as follows: For each generator of $I$, find its state in the ideal automaton of $J$. Beginning with these states we now traverse the automaton of $J$, i.e. we look for all possible paths ending with an accepting state. We here have to detect the loops (cycles) in the automaton to get a finite procedure. If we use the same method again, now starting with all the generators of $J$ and traversing the automaton of $I$, we have found all possible words beginning with a generator from one of the ideals, and ending with a generator from the other ideal (Here the generators may of course intersect). Since all words in $I \cap J$ must contain one such word as a subword, we have found a set of generators.

An implementation of the ideas above gives as output, when given $I = (x^2, xy^2)$ and $J = (xyx)$ as in our example, the following result:

*i*) Starting with $xx$ : $\quad xxx^*y(yy^*xx^*y)^*x$
*ii*) Starting with $xyy$ : $\quad xyyy^*xx^*y(yy^*xx^*y)^*x$
*iii*) Starting with $xyx$ : $\quad xyx(yx)^*x$ and
*iiii*) $\quad xyxy(xy)^*y$

[2]For the theory of automata, see e.g. (Howie 1991).

Here $^*$ denotes the usual star operation, $a^* = \{\mathbf{1}, a, a^2, \ldots\}$, and corresponds to the loops the program has detected. The reader can check the result using the automata in Figure 1.

It is easy to see that every element in (3.2) can be obtained by choosing suitable loops in some of the $i) - iiii)$ above. Moreover, however $iii)$ is evaluated, i.e. no matter how many times we run the loop, it will always contain $xyxx$ from (3.2) as a subword. In the same way, $iiii)$ will always contain $xyxyy$, and (although more difficult to see) $i)$ and $ii)$ will contain either $xxyx$ or some $xy^ixyy$ (depending on how the loops are chosen). We conclude that (3.2) and the (infinite) set of elements in $i) - iiii)$ generates the same ideal, so our guess above, that (3.2) was a Gröbner basis for $I \cap J$, was correct.

# 4 Homomorphisms

Let $Y = \{y_1, \ldots, y_m\}$ be another alphabet, and let $\varphi : K\langle Y\rangle \longrightarrow K\langle X\rangle$ be the $K$-algebra homomorphism defined by $\varphi(y_i) = h_i(X)$, $1 \le i \le m$. Consider the ideal

$$H = (y_i - h_i | 1 \le i \le m) \in K\langle X, Y\rangle.$$

We will, for convenience, in the following proofs write $\varphi$ also for its natural extension $\tilde{\varphi} : K\langle X, Y\rangle \longrightarrow K\langle X\rangle$.

**Theorem 3** $\ker(\varphi) = H \cap K\langle Y\rangle$.

*Proof.* If $f \in H \cap K\langle Y\rangle$, then $f(y_1, \ldots, y_m) = \sum_{i=1}^m p_i(y_i - h_i)q_i$ where $p_i, q_i \in K\langle X, Y\rangle$. It follows that $\varphi(f) = f(h_1, \ldots, h_m) = 0$.

Conversely, assume $f \in \ker(\varphi)$. Using that $py_iq = ph_iq + p(y_i - h_i)q$ for all $p, q \in K\langle X, Y\rangle$, we can successively replace all occurrences of the $y_i$ in $f$ by $h_i$ and obtain

$$f(y_1, \ldots, y_m) = f(h_1, \ldots, h_m) + \sum_{i=1}^{m} p_i(y_i - h_i)q_i, \tag{4.1}$$

for some $p_i, q_i \in K\langle X, Y\rangle$. Since $f(h_1, \ldots, h_m) = \varphi(f) = 0$ we conclude that $f \in H$. $\square$

As in the previous section we now use Theorem 1:

**Corollary 2** *Let $G$ be a Gröbner basis for $H$ according to the elimination order in $K\langle X, Y\rangle$ with $X > Y$. Then $G \cap K\langle Y\rangle$ is a Gröbner basis for* $\ker(\varphi)$.

As an example consider the homomorphism $\varphi : K\langle y_1, y_2, y_3\rangle \longrightarrow K\langle x_1, x_2\rangle$ defined by $\varphi(y_1) = x_1 + x_2$, $\varphi(y_2) = x_1^2 + x_1x_2$ and $\varphi(y_3) = x_2^2 + x_2x_1$. Calculating the reduced Gröbner basis for

$$H = (x_1 + x_2 - y_1, x_1^2 + x_1x_2 - y_2, x_2^2 + x_2x_1 - y_3)$$

according to the elimination order $(x_2 > x_1 > y_3 > y_2 > y_1)$ we obtain

$$G = \{x_1y_1 - y_2, y_3 + y_2 - y_1^2, x_2 + x_1 - y_1\}. \tag{4.2}$$

The Corollary now shows that $\ker(\varphi)$ is generated by $y_3 + y_2 - y_1^2$.

We will in the remaining of this section use, as in the Corollary above, the elimination order (in $K\langle X, Y\rangle$) with $X > Y$, so all Gröbner bases and reductions (normal forms) will be with respect to this order.

**Theorem 4** *An element $f \in K\langle X\rangle$ is in $\mathrm{im}(\varphi)$ if and only if $\bar{f} \in K\langle Y\rangle$, where $\bar{f}$ is the normal form of $f$ modulo the ideal $H$ considered above.*

*Proof.* If $f \in \mathrm{im}(\varphi)$, then $f(x_1, \ldots, x_n) = g(h_1, \ldots, h_m)$ for some $g \in K\langle Y\rangle$. Using (4.1) with $f$ replaced by $g$ we see that $f(x_1, \ldots, x_n) = g(y_1, \ldots, y_m) + h, h \in H$. Since h reduces to zero, it is clear that the normal form of $f(x_1, \ldots, x_n)$ is equal to the normal form of $g(y_1, \ldots, y_m)$. But since $Y < X$, the reduction of an element in $K\langle Y\rangle$ yields another element in $K\langle Y\rangle$. Thus $\bar{f} = \bar{g} \in K\langle Y\rangle$.

Conversely, if $\bar{f} \in K\langle Y\rangle$, then, since $f - \bar{f} \in H$,

$$f(x_1, \ldots, x_n) = \bar{f}(y_1, \ldots, y_m) + \sum_{i=1}^{m} p_i(y_i - h_i)q_i,$$

$p_i, q_i \in K\langle X, Y\rangle$. Substituting $h_i$ for $y_i$ we get $f = \bar{f}(h_1, \ldots, h_m) = \varphi(\bar{f})$. □

From the proof we also see that if $f \in \mathrm{im}(\varphi)$, then $f = \varphi(\bar{f})$.

For example, if we normalize $f = x_1^3 + x_1^2x_2 - x_2^3 - x_2^2x_1$ with respect to the basis in (4.2) we get $\bar{f} = y_1y_2 + y_2y_1 - y_1^3$, so the Theorem shows that $f$ is in the image of the homomorphism defined in our example above. The reader can check that $f = \varphi(\bar{f})$.

**Corollary 3** *With the notations above, let $G$ be the reduced Gröbner basis for $H$. Then $\varphi$ is an epimorphism if and only if there exists $f_i = x_i - g_i \in G$, $1 \le i \le n$, with $g_i \in K\langle Y\rangle$.*

*Proof.* Clearly $\varphi$ is an epimorphism if and only if $x_i \in \mathrm{im}(\varphi)$ for all $i$.

Assume $x_i \in \mathrm{im}(\varphi)$. Since $f_i = x_i - \overline{x_i} \in H$ (by the theorem this is not zero), there is a element in $p \in G$ with $\hat{p}|\widehat{f_i} = x_i$, i.e. $\hat{p} = x_i$. Since $G$ is the reduced basis we have $p = x_i - \overline{x_i}$, and $\overline{x_i} \in K\langle Y\rangle$ by the theorem.

Conversely, if $x_i - g_i \in G$, $g_i \in K\langle Y\rangle$, then, again since $G$ is reduced, $\overline{x_i} = g_i \in K\langle Y\rangle$, so by the theorem we have $x_i \in \mathrm{im}(\varphi)$. □

We now see from (4.2) that the homomorphism in the example above is not an epimorphism.

All of the results in this section can be generalized to a homomorphism $\varphi : K\langle Y\rangle/J \longrightarrow K\langle X\rangle/I$. If $\varphi$ is defined as above, and if $I = (f_1, \ldots, f_s)$, we then have to work with the ideal $H = (y_i - h_i, f_j | 1 \leq i \leq m, 1 \leq j \leq s)$, and consider all the elements in $K\langle Y\rangle$ modulo $J$.

To conclude this section, we note that the results above can be used to study subalgebras of $K\langle X\rangle$ (or $K\langle X\rangle/I$). Because if $A$ is the subalgebra of $K\langle X\rangle$ generated by $f_1, \ldots, f_l$, then $A$ can be considered as the image of the homomorphism $\varphi : K\langle y_1, \ldots, y_l\rangle \longrightarrow K\langle X\rangle$ defined by $\varphi(y_i) = f_i$, $1 \leq i \leq l$.

# 5 Homogenization

Most computer programs devoted to non-commutative Gröbner bases works only with homogeneous ideals, i.e. ideals given with a set of homogeneous generators. It is not difficult to see that the elements of the reduced Gröbner basis then also will be homogeneous.

We will here show how to use homogenization techniques to obtain a Gröbner basis for an arbitrary ideal by considering its homogenized counterpart.

The approach below is now implemented in the program ANICK by Podoplelov and Ufnarovski (1997).

For $f \in K\langle X\rangle$, we let $f^* \in K\langle X, t\rangle$ denote the following homogenization of $f$: If $f = f_{(d)} + f_{(d-1)} + \ldots + f_{(0)}$, where $f_{(j)}$ is the homogeneous component of degree $j$, $f_{(d)} \neq 0$, then $f^* = f_{(d)} + tf_{(d-1)} + \ldots + t^d f_{(0)}$. Also, for $g \in K\langle X, t\rangle$, let $g_* = g(X, 1) \in K\langle X\rangle$. We note that $(f^*)_* = f$. Moreover, if $g$ is homogeneous, and if all words in $g$ has all occurrences of $t$ at the beginning, i.e. is of form $t^k w$ for some $k \in \mathbb{N}, w \in K\langle X\rangle$, then $g = t^m (g_*)^*$ for some $m \in \mathbb{N}$ (the highest power of $t$ dividing $g$).

For an ideal $I = (f_1, \ldots, f_s) \subset K\langle X\rangle$, let us consider the ideal

$$J = (f_1^*, \ldots, f_s^*, x_i t - t x_i \mid 1 \leq i \leq n) \subset K\langle X, t\rangle, \tag{5.1}$$

which clearly is homogeneous.

**Theorem 5** *Let $G$ be the reduced Gröbner basis for $J$ according to deglex with $X > t$. Then $G_* = \{g_* \mid g \in G\}$ is a Gröbner basis for $I$ (also w.r.t. deglex).*

For the proof we need a Lemma:

**Lemma 1** *Let $w_i$ and $w_j$ be words in $K\langle X\rangle$, and let $m_i, m_j \in \mathbb{N}$ be such that $|t^{m_i} w_i| = |t^{m_j} w_j|$. Then $w_i > w_j$ w.r.t. deglex in $K\langle X\rangle$ if and only if $t^{m_i} w_i > t^{m_j} w_j$ w.r.t. deglex ($X > t$) in $K\langle X, t\rangle$.*

*Proof.* First assume $|w_i| = |w_j|$. Then $m_i = m_j$, so $w_i > w_j$ lexicographically is equivalent to $t^{m_i} w_i > t^{m_j} w_j$ lexicographically.

If $|w_i| \neq |w_j|$, then $|w_i| > |w_j|$ if and only if $m_i < m_j$, and this is the case if and only if $t^{m_i} w_i$ is larger than $t^{m_j} w_j$ lexicographically. □

*Proof.* (of Theorem) Since $(f_i^*)_* = f_i$ and $(x_i t - t x_i)_* = 0$ we have $G_* \subset I$, so it suffices to find, for arbitrary $f \in I$, an element $g \in G_*$ with $\hat{g} \mid \hat{f}$.

Let $f = \sum_{i=1}^{s} h_{i_L} f_i h_{i_R} \in I$. Since $h_{i_L}^* f_i^* h_{i_R}^*$ is homogeneous for all $i$, we can find $n_i \in \mathbb{N}$, $1 \leq i \leq s$, such that $F = \sum_{i=1}^{s} t^{n_i} h_{i_L}^* f_i^* h_{i_R}^* \in J$ is homogeneous.

After expanding $F$ as a sum of words, we let $F'$ denote the element obtained from $F$ by replacing every word by the corresponding word having all occurrences of $t$ (if any) at the beginning, e.g. $F = x_1 t x_2 t + x_1 t x_2 x_1 + x_2 x_1$ gives $F' = t^2 x_1 x_2 + t x_1 x_2 x_1 + x_2 x_1$. Since $x_i t - t x_i \in J$ for all $i$, we also have $F' \in J$. Writing $f = \sum_{l=1}^{k} c_l w_l$, where the $w_l$ are words in $K\langle X \rangle$, $w_i \neq w_j$ if $i \neq j$, and the $c_l \in K$, we have $F' = \sum_{l=1}^{k} c_l t^{m_l} w_l$ for some $m_l \in \mathbb{N}$. Because if some words cancels in $f$, then, since $F'$ is homogeneous, the corresponding words also cancels in $F'$. Moreover, from the Lemma it follows that if $\hat{f} = w_i$, then $\widehat{F'} = t^{m_i} w_i$, i.e. the leading word of $f$ corresponds to the leading word of $F'$.

There is an element $g \in G$ such that $\hat{g} | \widehat{F'}$. We claim that $\widehat{g_*} | \hat{f}$, which will prove the theorem.

As member of the reduced basis, $g$ is homogeneous and of form $\hat{g} - \bar{g}$. Clearly $\hat{g}$ has all occurrences of $t$ at the beginning ($\hat{g} | \widehat{F'} = t^{m_i} w_i$). The same is true for the words in $\bar{g}$, because they are normal modulo $J$ and thus not divisible by any $x_i t$ (the leading word of $x_i t - t x_i \in J$). It follows that $g_* \neq 0$ (since $g_* = 0$ implies $g = t^m (g_*)^* = 0$), and by the Lemma we see that $\widehat{g_*} = (\hat{g})_*$. Since clearly $\hat{f} = (\widehat{F'})_*$, it is now evident that $\hat{g} | \widehat{F'}$ implies $\widehat{g_*} | \hat{f}$. □

The result above can also be proved for other admissible orders, the essential is that $t$ is less than all the $x_i$. The proof of Theorem 5 need just be modified slightly if we replace deglex with e.g. the elimination order. We can thus find e.g. the intersection of the ideals $I = (f_1, \ldots f_k)$ and $J = (g_1, \ldots, g_l)$, calculating the reduced Gröbner basis for

$$H' = (s f_i, (t-s) g_j, s x_m - x_m s, st - ts, x_m t - t x_m | 1 \leq i \leq k, 1 \leq j \leq l, 1 \leq m \leq n)$$

(compare (3.1) and (5.1)) according to the elimination order with $s > X > t$. Combining Corollary 1 and Theorem 5 we see that it is sufficient to pick out the elements in $H'_*$ (dehomogenized w.r.t. $t$) not containing $s$.

The basis $G_*$ will not in general be minimal. As an example consider the ideal $I = (x^2 - yx, xy - y) \in K\langle x, y \rangle$. Calculating the reduced Gröbner basis for $J = (x^2 - yx, xy - ty, xt - tx, yt - ty)$ according to deglex with $x > y > t$, we get $G = \{y^2 x - tyx, ty^2 - t^2 y, x^2 - yx, xy - ty, xt - tx, yt - ty\}$. By the theorem $G_* = \{y^2 x - yx, y^2 - y, x^2 - yx, xy - y\}$ is a Gröbner basis for $I$, and here the first element is clearly superfluous. The last three elements constitutes the reduced Gröbner basis.

Moreover, $G_*$ can be infinite even if the ideal admits a finite Gröbner basis. An example is the ideal $I = (xy - z, yz - x, zx - y) \in K\langle x, y, z\rangle$ (deglex with $x > y > z$).

## References

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

Bergman, G. (1978): *The Diamond Lemma for Ring Theory*, Advances of Mathematics 29, 178-218.

Bokut, L.A. (1976): *Embeddings in Simple Associative Algebras*, Algebra Logika 15, No. 2, 117-142. English translation: Algebra Logic 15, 73-90 (1977).

Buchberger, B. (1965): *On finding a Vector Space Basis of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal* (German), PhD Thesis, Univ. of Innsbruck, Austria.

Buchberger, B. (1985): *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, Chapter 6 in: Multidimensional Systems Theory (N.K. Bose ed.), 184-232, Reidel Publishing Company, Dodrecht.

Feustel, C.D., Green, E.L. (1992): GROEBNER, C code, available by anonymous ftp from math.vt.edu in the directory: /pub/green.

Howie, J.M. (1991): *Automata and Languages*, Oxford Science Publications.

Kandri-Rody, A., Weispfenning, V. (1990): *Non-commutative Gröbner Bases in Algebras of Solvable Type*, Journal of Symbolic Computation 9, 1-26.

Mora, F. (1986): *Gröbner Bases for Non-commutative Polynomial Rings*, Proc. AAECC-3, Lecture Notes in Computer Science, Vol. 229, Springer, 353-362.

Podoplelov, A., Ufnarovski, V.A. (1997): ANICK, C code, available by anonymous ftp from ftp.riscom.net in the directory: /pub/anick.

Ufnarovski , V.A. (1994): *Calculations of Growth and Hilbert Series by Computer*, Lecture Notes in Pure and Applied Mathematics, Vol. 151, Decker, 247-256.

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