Computer Science Journal of Moldova, vol.**7**, no.1(19), 1999

Canonical bases for subalgebras of factor algebras

P. Nordbeck

Abstract

We introduce canonical bases for subalgebras of quotients of the commutative and non-commutative polynomial ring. The usual theory for Gröbner bases and its counterpart for subalgebras of polynomial rings, also called SAGBI bases, are combined to obtain a tool for computation in subalgebras of factor algebras.

1 Introduction

Canonical bases for subalgebras of the commutative polynomial ring were introduced by Kapur and Madlener (see [5]), and independently by Robbiano and Sweedler ([9]). Some notes on the non-commutative case can be found in [8]. Using the language of Robbiano and Sweedler, we will refer to these "non-quotient" cases as SAGBI bases theory (**S**ubalgebra **A**nalog to **G**röbner **B**ases for **I**deals). In consequence, we will call the canonical bases in our factor algebra setting Factor-SAGBI bases, or simply FS-bases.

SAGBI bases theory is (as the previous parenthesis indicates) strongly influenced by the theory of Gröbner bases, introduced by Bruno Buchberger in his thesis [3]; in e.g. [9] we find the notion of (subalgebra) reduction, the characterization (test) theorem using critical pairs (generalized S-polynomials), and the completion procedure of constructing bases. To make the theory work in our factor algebra setting, we need just complete the SAGBI theory at a few points. We try, as far as possible, to work in the normal complements of the ideals we factor out, so e.g. our subalgebra reduction also includes the usual Gröbner basis reduction (called normalization below). In the test and construction of our bases we are forced to consider, besides critical pairs, one additional type of element.

Some problems concerning subalgebras, e.g. subalgebra membership, can be reduced to Gröbner basis problems. This has been performed for commutative polynomial rings by Shannon and Sweedler ([10]), and generalizations to quotients of polynomial rings and to the non-commutative case are straightforward (see [1] and [7] respectively). In the commutative case, FS-bases, like SAGBI bases, differ from Gröbner bases at one essential point; they may be infinite even for finitely generated subalgebras. This implies that the Factor-SAGBI approach, in contrast to the generalized method of Shannon and Sweedler mentioned above, is not necessarily algorithmic[1]. However, it is easy to provide examples where the FS-basis computation is almost free whereas it is impossible, from the practical point of view, to apply the method of Shannon and Sweedler (due to the high complexity of Gröbner bases). Passing to the non-commutative case, Gröbner bases are no longer in general finite, and we can easily find examples where Factor-SAGBI theory answers questions that would not be algorithmic using the approach of Shannon and Sweedler. Non-commutative FS-bases have also shown to be applicable for solving systems of non-commutative polynomial equations, in an approach under development by Victor Ufnarovski.

Finally we mention that there is a general theory for rewriting modulo congruences, see e.g. [2].

The author expresses his thanks to Victor Ufnarovski for helpful discussions.

2 Basic Definitions and Notation

Let $X = \{x_1, x_2, \ldots, x_n\}$ be a finite alphabet. As usual, $K[X]$ is the commutative polynomial ring and $K\langle X\rangle$ the non-commutative one (i.e.

[1] By an algorithmic problem we will here mean a problem that can be solved by a terminating procedure, assuming that the field-operations in K are effectively computable.

the free associative algebra), both over the arbitrary field K. Since almost all of the theory in the sequel will be the same for the commutative and the non-commutative case, we will denote both $K[X]$ and $K\langle X\rangle$ by $\mathfrak{A}$, meaning that both cases are present. Also, when we speak of the quotient $\mathfrak{A}/I$, we will of course mean that I is an ideal in the respective polynomial ring (always two-sided in the non-commutative case).

Denote by W the set of all words, commuting and non-commuting respectively, in X, including the empty word $\mathbf{1}$. In other words, W is the free (commutative alt. non-commutative) monoid X^* generated by X. We will always in what follows assume that W is given an *admissible order*, i.e. a well-order preserving multiplication: $f < g$ implies $hfk < hgk$ for all $f, g, h, k \in W$ ($hf < hg$ is of course sufficient in the commutative case), such that the smallest word is the unity $\mathbf{1}$. Note that, by definition, every infinite sequence $u_1 \geq u_2 \geq \ldots u_i \geq \ldots$ in W stabilizes.

In the examples below we will use the following admissible order called *deglex* (degree lexicographical): If $|u|$ denotes the length of $u \in W$, we let $u > v$ if either $|u| > |v|$ or $|u| = |v|$ but u is larger than v lexicographically (commutative and non-commutative respectively).

When we have chosen an admissible order we can, if terms with identical words are collected together using the operations over K, with every non-zero element $s \in \mathfrak{A}$ associate its *leading word* $\mathrm{LW}s$. Moreover, the *leading term* $\mathrm{LT}\,s$ of s is the leading word times its coefficient. We also define, for a subset A of $\mathfrak{A}$, $\mathrm{LW}(A) = \{\mathrm{LW}a \mid a \in A\}$.

If $u, v \in W$, and u is a (not necessarily proper) factor of v (in the commutative and non-commutative sense respectively), we write $u \mid v$. A word $u \in W$ is called *normal* modulo an ideal I if for every $f \in I$, $\mathrm{LW}f \nmid u$. If N denotes the K-span of the normal words (mod I), then we have $\mathfrak{A} = N \oplus I$ as direct sum of vector spaces (see e.g. [11]). For every $f \in \mathfrak{A}$, its image by the projection $\mathfrak{A} \to N$ will be called its *normal form*, and be denoted $\bar{f}$. It is now clear that N (together with the multiplication $f * g = \overline{fg}$) is isomorphic to the factor algebra $\mathfrak{A}/I$.

The tools for the *normalization* $f \to \bar{f}$ are Gröbner bases. For the theory of Gröbner bases we refer to [4] in the commutative case, and

[6] for the non-commutative generalization. However, we here give the definition and a few remarks we will need.

Definition 1 *A subset G of the ideal I (in $\mathfrak{A}$) is called a* Gröbner basis *for I if for every $f \in I$, $f \neq 0$, there is $g \in G$ such that* $\mathrm{LW}g \mid \mathrm{LW}f$.

In the commutative case every ideal has (for every order) a finite Gröbner basis. This is unfortunately not true in the non-commutative case. Clearly an element $f \in \mathfrak{A}$ is normal (i.e. $f = \bar{f}$) if and only if none of its words are divisible by any leading word of the Gröbner basis. Finally, the normalization $f \rightarrow \bar{f}$ is always algorithmic when we have a finite Gröbner basis at hand.

Let $H = \{h_1, h_2, \ldots, h_l\}$ be a subset of $\mathfrak{A}$. The subalgebra S of $\mathfrak{A}/I$ generated by H consists of the cosets modulo I of all elements $p(h_1, h_2, \ldots, h_l)$, where p is any polynomial in l commuting alt. non-commuting indeterminates. To be formally correct, we should have used the images in the factor algebra of the h_i. But since we prefer to work in the polynomial ring, we will allow ourselves to use H, or as below, the normal forms of the elements of H (recall that $\mathfrak{A}/I \simeq N$). Since we allow constant polynomials, the image of K lies in S.

For a given subalgebra S of $\mathfrak{A}/I$, the inverse image in $\mathfrak{A}$ of S will be denoted S^c (the *contraction*[2] of S). Clearly an element of $\mathfrak{A}$ belongs to S^c if and only if its image lies in S, and if S is generated by $H = \{h_1, \ldots, h_l\}$, then every element $s \in S^c$ is of form

$$s = p(h_1, \ldots, h_l) + g, \quad g \in I, \tag{1}$$

for some polynomial p. In view of the isomorphism $\mathfrak{A}/I \simeq N$ we also see that $s \in S^c$ represents the zero element in the factor algebra if and only if $\bar{s} = 0$.

Now let $\bar{H} = \{\bar{h_1}, \ldots, \bar{h_l}\}$, i.e. we take the normal form of each element in H. Since $h_i = \bar{h_i} - (\bar{h_i} - h_i)$ and $\bar{h_i} - h_i \in I$, we can, by

[2] Maybe not the most descriptive name in our case, but this is the term used by Atiyah and MacDonald in their classical text-book *Introduction to Commutative Algebra*.

replacing every occurrence of h_i in (1) by $\bar{h_i}$, rewrite (1) as

$$s = p(\bar{h_1}, \ldots, \bar{h_l}) + g' = p(\bar{H}) + g', \quad g' \in I, \tag{2}$$

with the same polynomial p. We conclude that every element $s \in S^c$ can be written in form (2).

We will use $K[\bar{H}]$ ($K\langle \bar{H} \rangle$) to denote the polynomials in the formal commuting (non-commuting) $\bar{H}$-variables. We are particularly interested in the *monomials* in $K[\bar{H}]$ ($K\langle \bar{H} \rangle$), i.e. the monomials in the formal variables $\bar{H}$; the set of these monomials will be denoted $\mathcal{M}$. (So $\mathcal{M} \subset K[\bar{H}]$ alt. $\mathcal{M} \subset K\langle \bar{H} \rangle$. In particular, $\mathcal{M}$ depends on $\bar{H}$.) Contrary to common practice, we will always assume that the coefficient of such a monomial is 1. (So the elements in $\mathcal{M}$ are words in $\bar{H}$, but we want to reserve the name word for W.) Note that the elements in $\mathcal{M}$ are not (in general) words when viewed as elements of $\mathfrak{A}$.

Remark 1 *In the existing literature on commutative SAGBI theory, the role of monomials is played by exponent functions; for a monomial $h_1^{\alpha_1} h_2^{\alpha_2} \cdots h_l^{\alpha_l}$, $\alpha_i \in \mathbb{N}$, we then speak of the exponent vector $\alpha = (\alpha_1, \ldots, \alpha_l)$. Since this approach is not possible in the non-commutative case, and since we want an uniform exposition, we here, as in [8], use monomials.*

When we mention the leading word or term of an element in $K[\bar{H}]$ (alt. $K\langle \bar{H} \rangle$), we will always mean the leading word or term of the element viewed as an element of $K[X]$ ($K\langle X \rangle$), relative to the order here.

Following Robbiano and Sweedler we introduce the notions of height and breadth.

Definition 2 *Let $\sum_{i=1}^{t} k_i m_i(\bar{H})$, $k_i \in K$, $m_i \in \mathcal{M}$, be a K-linear combination of monomials. The* height *of the sum is* $\max\{\mathrm{LW} m_i(\bar{H}) \mid 1 \leq i \leq t\}$*, where the maximum is taken relative to the order in $\mathfrak{A}$. The* breadth *of the sum is the number of i such that* $\mathrm{LW} m_i(\bar{H})$ *is equal to the height.*

Note that the leading word of $s = \sum k_i m_i(\bar{H})$ can be smaller than the height of $\sum k_i m_i(\bar{H})$. This is the case if (and only if) all words larger than LWs cancel in the sum, and the breadth of the sum is then necessarily at least two.

Now to our main definition.

Definition 3 *Let S be a subalgebra of $\mathfrak{A}/I$. A subset $H \subset S^c$ is called a* Factor-SAGBI basis *for S, or simply a* FS-basis *for S, if for every $s \in S^c$ with $\bar{s} \neq 0$ there exists a monomial $m \in \mathcal{M}$ such that* $\mathrm{LW}\bar{s} = \mathrm{LW}m(\bar{H})$.

Remark 2 *Since orders are preserved after multiplication we have, if $m(\bar{H}) = \bar{h}_{i_1}\bar{h}_{i_2}\cdots\bar{h}_{i_t}$, $\bar{h}_{i_j} \in \bar{H}$, $\mathrm{LW}m(\bar{H}) = \mathrm{LW}\bar{h}_{i_1}\mathrm{LW}\bar{h}_{i_2}\cdots\mathrm{LW}\bar{h}_{i_t}$. Thus an equivalent formulation of the definition is that H is a FS-basis for S if $\mathrm{LW}(\bar{S})$ is contained in the (commutative alt. non-commutative) monoid $\mathrm{LW}(\bar{H})^*$ generated by $\mathrm{LW}(\bar{H})$ (here $\bar{S} = \{\bar{s} \mid s \in S^c\}$). We note that in general $\mathrm{LW}(\bar{S}) \neq \mathrm{LW}(\bar{H})^*$.*

In the case $I = \{0\}$ the definition becomes the same as in ordinary SAGBI theory.

Finally we note that, for an arbitrary subalgebra S of $\mathfrak{A}/I$, S^c clearly is a FS-basis for S, so every subalgebra has a FS-basis.

3 IH-reduction

Next we define the process of *IH-reduction*. (We call it IH-reduction since we want to stress the dependence on both I and H.) If $I = \{0\}$, then we can omit step 2 below, and the reduction becomes the same as in [8] and [9].

IH-reduction. *The IH-reduction of $s \in \mathfrak{A}$ with respect to an ideal I and a subset H of $\mathfrak{A}$ is performed as follows:*

1. *$s_0 = s$.*
2. *Compute the normal form $\bar{s_i}$ of s_i (w.r.t. I).*
3. *If $\bar{s_i} = 0$, or if $\mathrm{LW}\bar{s_i} \notin \mathrm{LW}(\bar{H})^*$, then terminate. In case of termination, this $\bar{s_i}$ will be referred as the* result of the IH-reduction.

4. *Find a monomial* $m_i \in \mathcal{M}$ *and* $k_i \in K$ *such that* $\operatorname{LT}\bar{s_i} = \operatorname{LT} k_i m_i(\bar{H})$. *(This is possible since we have not terminated in step 3.) Now let* $s_{i+1} = \bar{s_i} - k_i m_i(\bar{H})$.

5. *Go to step 2* $(i+1 \mapsto i)$.

We note that when step 4 has been performed, then the leading word of s_{i+1} is strictly smaller than the leading word of $\bar{s_i}$ (by the choice of m_i and k_i). Moreover, the normalization in step 2 does not yield a larger leading word (possibly a smaller one though). We conclude, since the order is well-founded, that the IH-reduction always terminates after a finite number of steps.

Having at hand a finite set $\bar{H}$, it is a constructive matter (in both the commutative and the non-commutative case) to determine whether a given word is a product of elements in $\operatorname{LW}(\bar{H})$. It follows that if H is a finite set, and if the normalization $f \to \bar{f}$ is algorithmic (see the discussion after Definition 1), then also the IH-reduction is algorithmic.

If the result of an IH-reduction of s is denoted $\overline{s^{\mathrm{IH}}}$, and if the reduction terminated after t iterations of step 4 above, then it is easy to see that we have, with the notation above,

$$s = \sum_{i=0}^{t-1} k_i m_i(\bar{H}) + g + \overline{s^{\mathrm{IH}}}, \quad g \in I. \tag{3}$$

If $t = 0$, then the right hand side of (3) is of course just $g + \bar{s}$. But if step 4 is performed at least once we have, by above,

$$\operatorname{LW}\bar{s} = \operatorname{LW} m_0(\bar{H}) > \operatorname{LW} m_1(\bar{H}) > \ldots > \operatorname{LW} m_{t-1}(\bar{H}), \tag{4}$$

so the monomial sum in the right hand side of (3) is clearly of breadth one and height equal to $\operatorname{LW}\bar{s}$. *We will use these facts several times in the sequel* (in particular when $\overline{s^{\mathrm{IH}}} = 0$).

There may of course be several different possibilities to choose the m_i in step 4, so the result of the reduction depends (in general) on how we choose these monomials.

We will be particularly interested in the case $\overline{s^{\mathrm{IH}}} = 0$ above. We say that *s IH-reduces to zero weakly* if there exists one IH-reduction (i.e. one choice of the m_i) with $\overline{s^{\text{IH}}} = 0$, and that s *IH-reduces to zero strongly* if every IH-reduction (every choice) yields $\overline{s^{\text{IH}}} = 0$. However, in most cases it does not matter which formulation we use. We will then simply say that s *IH-reduces to zero*, and write $s \xrightarrow{\text{IH}} 0$. Note that $s \xrightarrow{\text{IH}} 0$ if $\bar{s} = 0$, i.e. if the image of s in $\mathfrak{A}/I$ is zero.

As in ordinary SAGBI theory, we can now (having a FS-basis at hand) solve the *Subalgebra Membership Problem.*

Proposition 1 *Let $H \subset \mathfrak{A}$ be a FS-basis for the subalgebra S of $\mathfrak{A}/I$, and let $s \in \mathfrak{A}$. Then $s \in S^c$, i.e. the image of s is in S, if and only if $s \xrightarrow{\text{IH}} 0$.*

Proof. First assume $s \in S^c$. By (3) we have $\overline{s^{\text{IH}}} = s - \sum_{i=1}^{t-1} k_i m_i(\bar{H}) - g$, which is also an element in S^c. The only possibility of termination in step 3 of the IH-reduction is $\overline{s^{\text{IH}}} = 0$. Otherwise, if $\overline{s^{\text{IH}}} \neq 0$ there is, since $\overline{s^{\text{IH}}}$ clearly is normal modulo I, by Definition 3 a monomial $m \in \mathcal{M}$ with $\text{LW}\overline{s^{\text{IH}}} = \text{LW}m(\bar{H})$, and this contradicts the termination.

Conversely, it follows directly from (3) that $\overline{s^{\text{IH}}} = 0$ implies $s \in S^c$.

Corollary 1 *If H is a FS-basis for the subalgebra S of $\mathfrak{A}/I$, then H generates S.*

Proof. Clear from Proposition 1 and (3) (since replacing $\bar{H}$ by H in (3) only yields another element of I).
In view of Corollary 1 we may (and will) simply say that H is a FS-basis, meaning that H is a FS-basis for the subalgebra of $\mathfrak{A}/I$ generated by H.

4 Test and Construction of FS-bases

Proposition 2 *$H \subset S^c$ is a FS-basis for the subalgebra S of $\mathfrak{A}/I$ if and only if every $s \in S^c$ IH-reduces to zero.*

Proof. If H is a FS-basis, then every $s \in S^c$ IH-reduces to zero by Proposition 1.

Conversely, let $s \in S^c$, $\bar{s} \neq 0$, be arbitrary. Since the IH-reduction of s ends up with zero, step 4 in the algorithm must be executed at least once. By (4) we then have $\mathrm{LW}\bar{s} = \mathrm{LW}m_0(\bar{H})$, so H is a FS-basis by Definition 3.
Fortunately we need not check every element of the subalgebra. The following definition is a generalization of one of the cornerstones in Buchberger theory.

Definition 4 *Let I, H, $\bar{H}$ and $\mathcal{M}$ be as above. An I-*critical pair *(m, m') of H is a pair of monomials $m, m' \in \mathcal{M}$ with $\mathrm{LW}m(\bar{H}) = \mathrm{LW}m'(\bar{H})$. If $k \in K$ is such that $\mathrm{LT}\, m(\bar{H}) = \mathrm{LT}\, km'(\bar{H})$, then we define the* T-polynomial[3] *of (m, m') as $T(m, m') = m(\bar{H}) - km'(\bar{H})$.*

Remark 3 *The constant is chosen such that the leading words cancel in $T(m, m')$, and thus we have $\mathrm{LW}T(m, m') < \mathrm{LW}m(\bar{H}) = \mathrm{LW}m'(\bar{H})$. In particular, if $T(m, m') \xrightarrow{\mathrm{IH}} 0$ we get $T(m, m') = \sum k_i m_i(\bar{H}) + g$, $g \in I$, where the height of the monomial sum is less than $\mathrm{LW}m(\bar{H}) = \mathrm{LW}m'(\bar{H})$.*

In SAGBI theory ($I = \{0\}$, $\bar{H} = H$) we now have a proposition saying:

SAGBI Test. *H is a SAGBI basis if and only if the T-polynomials of all (I-)critical pairs of H (I)H-reduce to zero.*

The proof is standard in Buchberger theory, and is included as part of the proof of Theorem 1 below. See also [8] and [9].

In our case when I is arbitrary, the use of critical pairs is not sufficient. We also need to consider the elements in the following definition.

Definition 5 *Let I, H, $\bar{H}$ and $\mathcal{M}$ be as above. We call a monomial $m \in \mathcal{M}$ an* I-monomial *of H if $\mathrm{LW}m(\bar{H}) = \mathrm{LW}g$ for some $g \in I$.*

Remark 4 *Since the leading word of an I-monomial m is not normal we have $\mathrm{LW}\overline{m(\bar{H})} < \mathrm{LW}m(\bar{H})$. If $m(\bar{H}) \xrightarrow{\mathrm{IH}} 0$ we thus get $m(\bar{H}) = \sum k_i m_i(\bar{H}) + g$, $g \in I$, where the height of the monomial sum is less than $\mathrm{LW}m(\bar{H})$ (since the IH-reduction begins with the normalization $m \to \bar{m}$).*

[3] The Gröbner bases term is *S-polynomial*. We here use the T since the counterpart of an I-critical pair in [9] is called a *tête-a-tête.*

Theorem 1 (Test) *H is a FS-basis in $\mathfrak{A}/I$ if and only if all T-polynomials (of all I-critical pairs) and I-monomials of H IH-reduce to zero.*

Proof. Let S be the subalgebra of $\mathfrak{A}/I$ generated by H.

If H is a FS-basis, then, since all T-polynomials and I-monomials of H clearly are elements of S^c, they IH-reduce to zero by Proposition 1.

Conversely, let $s \in S^c$, $\bar{s} \neq 0$, be arbitrary. Since then also $\bar{s} \in S^c$, we can by (2) write (after expanding $p(\bar{H})$ to monomials)

$$\bar{s} = \sum k_i m_i(\bar{H}) + g, \quad k_i \in K,\ m_i \in \mathcal{M},\ g \in I. \tag{5}$$

Now choose, among all representations of form (5), one with minimal height of the sum $\Sigma = \sum k_i m_i(\bar{H})$. Since all T-polynomials IH-reduce to zero we can assume that Σ has breadth one. This follows from Remark 3 since if m_i $(= m_i(\bar{H}))$ and m_j are two of the largest monomials, with $T(m_i, m_j) = m_i - k m_j$, then we can write

$$k_i m_i + k_j m_j = k_i(m_i - k m_j) + (k_j + k_i k) m_j = k_i T(m_i, m_j) + k' m_j,$$

allowing us to reduce the breadth of Σ by (at least) one. (Alternatively, lower the height in the special case when $k' = k_j + k_i k = 0$ and the breadth from the beginning was two.)

If LW$\bar{s}$ = LWΣ, then, since Σ has breadth one, we must have LW$\bar{s}$ = LW$m_j(\bar{H})$ for some monomial (the largest) m_j in Σ. This must clearly be the case when LW$\Sigma >$ LWg, and the case LW$g >$ LWΣ is impossible since it implies LWg = LW$\bar{s}$, contradicting the normality of $\bar{s}$.

The only case remaining is LWΣ = LWg $(>$ LW$\bar{s})$, which as above implies LW$m_j(\bar{H})$ = LWg for the largest monomial m_j in Σ. But this means that m_j is an I-monomial. By Remark 4 we can then write m_j as a monomial sum of height less than LW$m_j(\bar{H})$ (plus an element of I), and this clearly contradicts the minimality of Σ.

We conclude that we must have LW$\bar{s}$ = LW$m_j(\bar{H})$ for some monomial m_j in Σ, and since s was arbitrary, H is a FS-basis by definition 3.

Example 1. Consider the subset $H = \{h_1 = x, h_2 = xy+y\}(= \bar{H})$ of $K[x,y]$ $(x > y)$, and let $I = (x^2 - y^2)$. It is obvious that we do not have any I-critical pairs (except the trivial ones where $m = m'$). But e.g. the I-monomial $m(\bar{H}) = h_1^2 = x^2$ IH-reduces to $y^2 \neq 0$, so H is not a FS-basis in $K[x,y]/(x^2 - y^2)$.

Remark 5 *We see that not even $H = \{x\}$ would be a FS-basis above. This is in strong contrast to ordinary SAGBI theory ($I = \{0\}$) where a singleton element always constitutes a SAGBI basis (in both the commutative and the non-commutative case).*

Since the concept of (I-)critical pairs is the same as in SAGBI theory, we can use the methods in [8] and [9] to obtain them.

In commutative SAGBI theory, the problem of finding critical pairs comes down to solving a system of linear Diophantine equations over the non-negative integers. We can find a finite number of solutions "generating" the set of all solutions. The number of critical pairs is of course in general infinite, but it is possible to show that we in the SAGBI test above only need to consider the critical pairs corresponding to the generating solutions just mentioned. For the details we refer to [9].

The results in [9] allowing us to consider only a finite number of critical pairs can easily be transformed to our factor algebra setting. (Going through the proofs, we need just note that the element $g \in I$ in Remark 3 only will give rise to elements that can be collected in I, thus not affecting the coset belonging). Since the IH-reduction always is algorithmic in the commutative case, we conclude that the part concerning the T-polynomials in Theorem 1 can be taken care of algorithmically.

In the non-commutative case, the algorithmicity of the SAGBI test is left as an open question in [8]. However, partial results, which are valid also in our factor algebra setting, are provided. We also remind that the IH-reduction not necessarily is algorithmic now.

Our factor algebra setting allows us to exclude more T-polynomials from Theorem 1. In both the commutative and the non-commutative case, we do not need to reduce the T-polynomial of an I-critical pair where the two monomials are I-monomials; if these I-monomials can be written as monomial sums of less height (which is the case if they IH-reduce to zero), then the same is clearly true for the T-polynomial. (Recall the proof of Theorem 1.)

It remains to find all I-monomials. Recalling Definition 1, we see that $m \in \mathcal{M}$ is an I-monomial if and only if $\mathrm{LW}g \mid \mathrm{LW}m(\bar{H})$ for some g in the Gröbner basis. Moreover, we need in Theorem 1 only consider those I-monomials that are minimal in the sense that they do not contain any submonomial which is also an I-monomial. This is clear since every I-monomial must contain some minimal I-monomial as a submonomial, and if a submonomial can be written as a sum of smaller monomials, then the same is true for our original monomial. (Again, recall the proof of Theorem 1.) Finally, if the Gröbner basis is finite (which is always possible in the commutative case), then it is easy to see that it is a constructive matter to find all minimal I-monomials.

Summarizing, we conclude that the FS-basis test always is algorithmic in the commutative case, while we may have problems in the non-commutative case. (Even if the non-commutative SAGBI basis test would appear algorithmic, we may still have problem with the normalization.)

As in Buchberger theory, the completion procedure of constructing a FS-basis is now straightforward.

FS-Basis Construction *Let I, H and $\bar{H}$ be as above.*

1. $H_0 = \bar{H}$.

2. *Find the set M_i of all T-polynomials and I-monomials of H_i necessary for the FS-basis test (Theorem 1).*

3. $H_{i+1} = H_i \bigcup \{ \overline{s^{\mathrm{IH}_i}} \mid s \in M_i, \overline{s^{\mathrm{IH}_i}} \neq 0\}$. *Here $\overline{s^{\mathrm{IH}_i}}$ of course denotes a result of reduction w.r.t. H_i (and I).*

4. *If $H_{i+1} \neq H_i$ then go to step 2 $(i+1 \mapsto i)$.*

5. $H_\infty = \bigcup H_i$.

We note that, since every result of a reduction is normal, we have $H_i = \bar{H}_i$ for all i (and thus $H_\infty = \bar{H}_\infty$).

Proposition 3 *H_∞ is a FS-basis for the subalgebra S of $\mathfrak{A}/I$ generated by H.*

Proof. Since $\overline{s^{\mathrm{IH}}} \in S^c$ for every $s \in H = H_0$ we have $H_1 \subset S^c$. By induction is $H_i \subset S^c$ for all i, and thus $H_\infty \subset S^c$.

If $H_i = H_{i+1}$ for some i, then H_i is a FS-basis (by the Test theorem). Otherwise, let s be a T-polynomial or I-monomial of H_∞ necessary for the FS-basis test. Take j so large that all elements of H_∞ occurring in s are in H_j. It is then clear that s reduces to zero (weakly) w.r.t. H_{j+1}, and thus of course also w.r.t. H_∞, so H_∞ is a FS-basis (again by the Test theorem).

Example 2. Continuing Example 1, we let $H_0 = \bar{H} = \{h_1 = x, h_2 = xy + y\}$. Since $I = (x^2 - y^2)$ is principal, its only generator must constitute the Gröbner basis (this is only true in the commutative case). As mentioned before, H_0 does not give rise to any T-polynomial, but we need to consider the minimal I-monomials $h_1^2 = x^2 \xrightarrow{\mathrm{IH}_0} y^2$, $h_1h_2 = x^2y+xy \xrightarrow{\mathrm{IH}_0} y^3+xy$ and $h_2^2 = x^2y^2+2xy^2+y^2 \xrightarrow{\mathrm{IH}_0} y^4+2xy^2+y^2$. But since $y^4 + 2xy^2 + y^2$ reduces to zero over H_0 and y^2, it is easy to see that we can spare this element in step 3 of the algorithm.

We thus get $H_1 = H_0 \cup \{h_3 = y^2, h_4 = y^3 + xy\}$, and the T-polynomials we need to check (the ones not containing I-monomials) are $h_4^2 - h_3^3 = 2xy^4 - x^2y^2 \xrightarrow{\mathrm{IH}_1} 0$, $h_1h_4 - h_2h_3 = x^2y - y^3 \xrightarrow{\mathrm{IH}_1} 0$ and $h_1h_3^2 - h_2h_4 = -x^2y^2 - y^4 - 2xy^2 \xrightarrow{\mathrm{IH}_1} 0$. Since there are no new I-monomials we conclude that $H_1 = H_2$, so H_1 is our FS-basis.

We have, for clarity, written the algorithm without optimizations; in the example above we saw one possibility (the exclusion of $y^4 + 2xy^2 + y^2$). It is also clear that we could have used h_2 to replace $y^3 + xy$ by $y^3 - y$. This would be automatic if we in the "H-part" (step 4) of the IH-reduction considered all words of an element instead of, as in our case, only reducing the leading one (see [8] for further details).

As in SAGBI theory, the construction algorithm will in general not terminate (even for a finite set H). However, our factor algebra setting, where the reduction is also w.r.t. an ideal, imposes new finiteness conditions.

Example 3. In [9] it is shown that the subalgebra of $K[x,y]$ $(x > y)$ generated by $H = \{x, xy - y^2, xy^2\}$ has no finite SAGBI basis. But the reader can check that H is a FS-basis in e.g. $K[x,y]/(y^3 - x^2)$.

One case for which the algorithm always terminates is when I has dimension zero, i.e. when $\mathfrak{A}/I$ is finite dimensional. (In the commutative case, is zero dimensional simply by inspecting the Gröbner we can decide whether an ideal basis.) This rests on the fact that every element added to H_i in step 3 has a leading word not lying in $\mathrm{LW}(H_i)$, so an infinite procedure requires an infinite number of normal words. (Recall that our factor algebra is isomorphic to N, the K-span of normal words.)

Finally we mention that the construction of a "partial" SAGBI basis from a set H of homogeneous elements, described in [8] and [9], applies to our factor algebra setting if also I is generated by homogeneous elements. This means that we can find, for $d \in \mathbb{N}$, a partial FS-basis $H_{(d)} = \{h \in H_\infty | \deg h \leq d\}$ (H_∞ as above), and at least the IH-reduction, and thus the Subalgebra Membership Problem (Proposition 1), is then algorithmic. (See [8] and [9] for the details. In the non-commutative case, we must now also use the fact that the normalization $f \to \bar{f}$ is algorithmic for homogeneous ideals.)

References

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

[2] Bachmair, L., Dershowitz, N. (1989): *Completion for rewriting modulo a congruence*, Theoret. Comput. Sci. 2-3, 173-201.

[3] 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.

[4] Buchberger, B. (1985): *Gröbner bases: An algorithmic method in polynomial ideal theory* in: Multidimensional Systems Theory, Reidel, 184-232.

[5] Kapur, D., Madlener, K. (1989): *A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra* in: Computer and Mathematics (Cambridge MA 1989), Springer, 1-11.

[6] Mora, F. (1986): *Gröbner Bases for Non-commutative Polynomial Rings* in: Proc. AAECC-3 Grenoble 1985, Lecture Notes in Computer Science, Vol. 229, Springer, 353-362.

[7] Nordbeck, P. (1998): *On some Basic Applications of Gröbner Bases in Non-commutative Polynomial Rings* in: Gröbner Bases and Applications, London Math. Soc. Lecture Notes Ser., Vol. 251, Cambridge Univ. Press, 463-472.

[8] Nordbeck, P. (1998): *Canonical Subalgebra Bases in Non-commutative Polynomial Rings* in: Proc. ISSAC'98, ACM Press, 140-146.

[9] Robbiano, L., Sweedler, M. (1990): *Subalgebra bases* in: Proc. Commutative Algebra Salvador 1988 (W. Burns and A. Simis, Eds.), Lecture Notes in Math., Vol. 1430, Springer, 61-87.

[10] Shannon, D., Sweedler, M. (1988): *Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence*, J. Symb. Comp. 6, 267-273.

[11] 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.

Patrik Nordbeck,
Department of Mathematics
Institute of Technology,
S-221 00 Lund, Sweden
phone: 46 46 222-85-66
e-mail: *nordbeck@maths.lth.se*

Received January 5, 1999