Factor-SAGBI Bases: a Tool for Computations in Subalgebras of Factor Algebras

Patrik Nordbeck

Department of Mathematics
Lund Institute of Technology
email: nordbeck@maths.lth.se

We introduce canonical bases for subalgebras of quotients of the commutative and non-commutative polynomial ring. A more complete exposition can be found in [4].

Canonical bases for subalgebras of the commutative polynomial ring were introduced by Kapur and Madlener (see [2]), and independently by Robbiano and Sweedler ([5]). Some notes on the non-commutative case can be found in [3]. 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 [1]; in e.g. [5] 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 of factor algebras, e.g. subalgebra membership, can be reduced to Gröbner basis problems. 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 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 Gröbner bases method mentioned above. Passing to the non-commutative case, Gröbner bases are no longer in general finite, and we can easily find examples where Factor-SAGBI theory solves problems that would not be algorithmic using the Gröbner bases method. 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.

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

Notations

Since most of the theory will be the same for the commutative and non-commutative case, we will let $\mathfrak{A}$ denote both the commutative polynomial ring $K[X]$ and the non-commutative ditto $K\langle X\rangle$ (over the finite alphabet X). We will always assume that the set of words in X is given an admissible order, so we can for every $f \in \mathfrak{A}$ associate its leading word $\mathrm{LW} f$. Moreover, $\mathrm{LT} f$ will be the leading word times its coefficient.

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

We are going to work in the quotient $\mathfrak{A}/I$, where I is an ideal in the respective polynomial ring (always two-sided in the non-commutative case). If N denotes the K-span of the normal words modulo I (in the usual "Gröbner bases sense"), then we have $\mathfrak{A} = N \oplus I$ as direct sum of vector spaces, and $N \simeq \mathfrak{A}/I$. The tools for the normalization $\mathfrak{A} \to N : f \mapsto \bar{f}$ are of course Gröbner bases. The subalgebra S of $\mathfrak{A}/I$ generated by $H = \{h_1, h_2, \ldots, h_l\} \subset \mathfrak{A}$ can be viewed as consisting of the cosets modulo I of all elements $p(h_1, h_2, \ldots, h_l)$, where p is any polynomial.

For a given subalgebra S of $\mathfrak{A}/I$, the inverse image (of the quotient map) in $\mathfrak{A}$ of S will be denoted S^c (the *contraction* 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 it is easy to see that all elements $s \in S^c$ are of form

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

for some polynomial p, now using $\bar{H} = \{\bar{h_1}, \ldots, \bar{h_l}\}$.

We are going to use monomials in the formal $\bar{H}$-variables; the set of these monomials will be denoted $\mathcal{M}$ (we will always assume that the coefficient of such a monomial is 1). We stress that that the elements $m(\bar{H}) \in \mathcal{M}$ are not (in general) monomials in the usual sense, i.e. words, viewed as elements of $\mathfrak{A}$.

We can now define our main objects.

Definition 1. *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* $\mathrm{LW}\bar{s} = \mathrm{LW}m(\bar{H})$.

The Reduction Procedure

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 there is no $m \in \mathcal{M}$ with $\mathrm{LW}m(\bar{H}) = \mathrm{LW}\bar{s}_i$, then terminate.*
4. *For $m_i \in \mathcal{M}$ and $k_i \in K$ with $\mathrm{LT}\bar{s}_i = \mathrm{LT}k_i m_i(\bar{H})$, let $s_{i+1} = \bar{s}_i - k_i m_i(\bar{H})$.*
5. *Go to step 2 ($i + 1 \mapsto i$).*

Since our admissible order is well-founded, it is easy to see that the reduction always terminates after a finite number of step. With standard Buchberger/SAGBI techniques we prove:

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 IH-reduces to zero.*

Test and Construction of FS-bases

We can prove that $H \subset S^c$ *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.* Fortunately, we do not need to check every element of the subalgebra. In Buchberger theory and ordinary SAGBI theory we do well with the so called critical pairs. In our context they look like (with the notations above):

Definition 2. *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 *of (m, m') as $T(m, m') = m(\bar{H}) - km'(\bar{H})$.*

In our factor algebra setting the use of critical pairs is not sufficient. Clearly, we can for every $s \in S^c$ write

$$\bar{s} = \sum k_i m_i(\bar{H}) + g, \quad k_i \in K,\ m_i \in \mathcal{M},\ g \in I. \tag{2}$$

One of the corner-stones in Buchberger theory is the conclusion that the critical pairs, if they reduce to zero, allow us to assume that the monomial sum in the right hand side of (2) has leading word equal to the leading word of some of the monomials. If this word also is the leading word of $\bar{s}$, then s fulfills the condition in Definition 1. If this is not the case, then the leading word of the "largest" m_i must be equal to the leading word of g. (Because otherwise we have $\mathrm{LW}\bar{s} = \mathrm{LW}g$, contradicting the normality of $\bar{s}$.) This motivates the introduction of the following elements.

Definition 3. *We call a monomial $m \in \mathcal{M}$ an* I-monomial *of H if $\mathrm{LW}m(\bar{H}) = \mathrm{LW}g$ for some $g \in I$.*

With a little effort we can now prove:

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

Recalling that $G \subset I$ is a Gröbner basis for I if for every non-zero $f \in I$ there is $g \in G$ with $\mathrm{LW}g \mid \mathrm{LW}f$, 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. We can then (assuming that the Gröbner basis is finite) find a finite set of minimal I-monomials, sufficient for the Test theorem.

In the commutative case, it is not hard to see that we can apply the method in [5] to find a finite sufficient set of critical pairs, and we conclude that the FS-basis test is algorithmic.

As in Buchberger theory, the completion procedure of constructing FS-bases is straightforward; we add to H the remainders of those T-polynomials and I-monomials not reducing to zero, and then start over with our new larger set. Unfortunately, the construction algorithm will not in general terminate. However, our factor algebra setting imposes new finiteness conditions. We give the following example.

Example 1. In [5] 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 we can show that H is a FS-basis in e.g. $K[x, y]/(y^3 - x^2)$.

References

1. 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.
2. 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.
3. Nordbeck, P. (1998): *Canonical Subalgebra Bases in Non-commutative Polynomial Rings* to appear in: Proc. ISSAC'98, ACM Press.
4. Nordbeck, P. (1998): *Canonical Bases for Subalgebras of Factor Algebras*, Preprint, Univ. of Lund, Sweden.
5. 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.