Non-commutative Gröbner Bases Under Composition: A Summary

Patrik Nordbeck

Lund University
Centre for Mathematical Sciences
email: nordbeck@maths.lth.se

In the recent paper [2], Hoon Hong addresses the problem of the behavior of (commutative) Gröbner bases under composition of polynomials. More precisely, let Θ be a set of polynomials, as many as the variables we are working with. The question then is under which conditions on these polynomials it is true that for an arbitrary Gröbner basis G (under some admissible ordering), also the composed set $G \circ \Theta$ is a Gröbner basis (under the same ordering).

Since many of the basic properties of Gröbner bases transfer to the non-commutative polynomial ring, it seems natural to ask under which conditions non-commutative Gröbner bases commutes with composition of a set of (non-commutative) polynomials. In this summary we state the main result in [4]: Composition by Θ commutes with (non-commutative) Gröbner bases computation if and only if the composition is compatible with the ordering, and the set of leading words of Θ is combinatorially free.

1 Definitions and Notation

Let $X = \{x_1, x_2, \dots, x_n\}$ be a finite alphabet, and let $K\langle X\rangle$ denote the free associative algebra over the arbitrary field K. Denote by W the set of all words in X, including the empty word $\mathbf{1}$. We assume that W is given an *admissible ordering*, so that we with every non-zero element $f \in K\langle X\rangle$ can associate its *leading word* $\hat{f} \in W$. We also define, for $F \subset K\langle X\rangle$, $\widehat{F} = \{\hat{f} \mid f \in F\}$.

We will below use the following ordering called *deglex* (degree lexicographical): If $|u|$ denotes the length of $u \in W$, then we let $u > v$ if either $|u| > |v|$, or $|u| = |v|$ but u is larger than v lexicographically with $x_n > \dots > x_1$.

We borrow the following terminology from [1].

Definition 1. *We call a subset* $\{w_1, w_2, \dots\} \subset W$ combinatorially free *if*

1. *whenever* $w_i = u_i v_i$ *and* $w_j = u_j v_j$ *for* $u_i, v_i, u_j, v_j \in W \setminus \{\mathbf{1}\}$ *we have* $v_i \neq u_j$, *and*
2. *no* w_i *is subword of* w_j *for* $i \neq j$.

A pair w_i, w_j *violating one of the conditions above will be called a* combination.

Remark 1. If two words $w_i, w_j \in W$ form a combination, then we have

1. $w_i u = v w_j$ (alt. $u w_i = w_j v$) if w_i, w_j violate the first condition above, or
2. $w_i = u w_j v$ (alt. $u w_i v = w_j$) if the second condition is violated.

Here $u, v \in W$, not equal to $\mathbf{1}$ in case 1, possibly equal to $\mathbf{1}$ in case 2.

For the theory of (non-commutative) Gröbner bases we refer to [3]. We just mention that we will call a pair of polynomials a *critical pair* if their leading words form a combination. From two such polynomials we then form the *S-polynomial*; these are the objects we need to consider to check for the Gröbner bases property.

To state our main theorem we also need the following definitions.

Definition 2. *Let $\Theta = \{\theta_1, \dots, \theta_n\}$ be a subset of $K\langle X\rangle$(=$K\langle x_1, \dots, x_n\rangle$), and let $f \in K\langle X\rangle$. We define the* composition *of f by Θ, written $f \circ \Theta$, as the polynomial obtained from f by replacing each occurrence of the x_i with θ_i. We also define, for $F \subset K\langle X\rangle$, $F \circ \Theta = \{f \circ \Theta \,|\, f \in F\}$.*

Definition 3. *We say that composition by Θ* commutes with Gröbner bases computation *if for every Gröbner basis G, also $G \circ \Theta$ is a Gröbner basis (under the same ordering as G).*

Definition 4. *We say that composition by Θ is* compatible with our given ordering *if for all words $u, v \in W$, $u > v$ implies $u \circ \widehat{\Theta} > v \circ \widehat{\Theta}$.*

2 Comparison with the Commutative Case

The main theorem in Hong's paper [2] is the following, where of course all statements are in a "commutative meaning".

Theorem 1 (Theorem 3.1. in [2]). *Composition by Θ commutes with Gröbner bases computation if and only if both of the following conditions hold:*

1. *Composition by Θ is compatible with the ordering and*
2. *for all monomials (commutative words) $m_1, m_2 \in K[X]$, $m_1 \nmid m_2$ implies $m_1 \circ \widehat{\Theta} \nmid m_2 \circ \widehat{\Theta}$ ($\nmid$ means "do not divide").*

The following example shows that conditions 1 and 2 above are not sufficient in the non-commutative case.

Example 1. We let $G = \{x_2 - x_1\} \subset K\langle x_1, x_2\rangle$ and $\Theta = \{\theta_1 = x_1^2, \theta_2 = x_2^2\}(= \widehat{\Theta})$. It is obvious that G is a Gröbner basis, and that composition by Θ is compatible with the deglex ordering ($x_2 > x_1$). It is also easy to see that (the non-commutative counterpart of) condition 2 is true for Θ. But $G \circ \Theta = \{x_2^2 - x_1^2\}$ is not a Gröbner basis.

3 Main Theorem

We now state our main result.

Theorem 2. *Composition by Θ commutes with Gröbner bases computation if and only if both of the following conditions hold:*

1. *Composition by Θ is compatible with the ordering and*
2. *$\widehat{\Theta}$ is combinatorially free.*

In the proof of the sufficiency, condition 1 is used to obtain $\widehat{f \circ \Theta} = \widehat{f} \circ \widehat{\Theta}$ for all $f \in K\langle X\rangle$. The second condition will ensure that every S-polynomial of $G \circ \Theta$ corresponds to a S-polynomial of G. More precisely:

Lemma 1. *Assume that composition by Θ is compatible with our ordering, and that $\widehat{\Theta}$ is combinatorially free. If $(g \circ \Theta, g' \circ \Theta)$ is a critical pair of $G \circ \Theta$, then (g, g') is a critical pair of G. Moreover, the S-polynomial of $(g \circ \Theta, g' \circ \Theta)$ is $g \circ \Theta\, u \circ \widehat{\Theta} - cv \circ \widehat{\Theta}\, g' \circ \Theta$ (alt. $g \circ \Theta - cu \circ \widehat{\Theta}\, g' \circ \Theta\, v \circ \widehat{\Theta}$), where $gu - cvg'$ ($g - cug'v$) is the S-polynomial of (g, g') ($c \in K, u, v \in W$).*

So if G is a Gröbner basis and we want to prove that the same is true for $G \circ \Theta$, then the idea is, when checking a S-polynomial of $G \circ \Theta$, to compose the corresponding S-polynomial of G. With a little effort we can then prove:

Proposition 1. *If composition by Θ is compatible with the ordering and $\widehat{\Theta}$ is combinatorially free, then composition by Θ commutes with Gröbner bases computation.*

To prove the necessity of the two conditions in Theorem 2 is more complicated. The strategy we have use is clear: Assuming one of the two conditions not true, we need to find a suitable Gröbner basis, contradicting the commutation of Gröbner bases computation.

The first part is easy. (We can actually use the same proof as in the commutative case.)

Proposition 2. *If composition by Θ commutes with Gröbner bases computation, then composition by Θ is compatible with the ordering.*

It is also fairly easy to prove, assuming Θ commuting with Gröbner bases computation, that the leading words of Θ can not form any combinations of the second type in Remark 1. Most difficulties arise when we prove that there can not be any combinations of the first type in Remark 1, and here the hardest part is to exclude the possibility that a leading word of Θ can form a combination with itself. We refer to [4] for the procedure.

When we have excluded all combinations of $\widehat{\Theta}$, we conclude:

Proposition 3. *If composition by Θ commutes with Gröbner bases computation, then $\widehat{\Theta}$ is combinatorially free.*

Thus our main theorem is proved.

4 Compatible Compositions

It is not hard to decide whether $\widehat{\Theta}$ is combinatorially free. But to check the other condition in our main theorem, i.e. if composition by Θ is compatible with the current ordering, is however not a trivial task. In Hong's paper, the following question is left as an open problem.

Does there exist a decision procedure that will determine whether a given composition is compatible with a given term ordering?

We finish this summary by answering this question for our deglex ordering.

Proposition 4. *Composition by Θ is compatible with the deglex ordering if and only if $|\hat{\theta}_i| = |\hat{\theta}_j|$ for all $\theta_i, \theta_j \in \Theta$, and $\hat{\theta}_i > \hat{\theta}_j$ if $x_i > x_j$.*

References

1. Anick, D. J. Noncommutative graded algebras and their Hilbert series. *J. Algebra 78*, 1 (1982), 120–140.
2. Hong, H. Groebner basis under composition. I. *J. Symbolic Comput. 25*, 5 (1998), 643–663.
3. Mora, F. Groebner bases for noncommutative polynomial rings. In *Algebraic algorithms and error correcting codes (Grenoble, 1985)*, vol. 229 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1986, pp. 353–362.
4. Nordbeck, P. Non-commutative Gröbner bases under composition. Tech. rep., Lund University, Centre for Mathematical Sciences, 1999.