An introduction to commutative and non-commutative Gröbner Bases

Teo Mora*

Introduction

In 1965, Buchberger introduced the notion of Gröbner bases for a polynomial ideal and an algorithm (Buchberger Algorithm) for their computation ([**B1**],[**B2**]).

Since the end of the Seventies, Gröbner bases have been an essential tool in the development of computational techniques for the symbolic solution of polynomial systems of equations and in the development of effective methods in Algebraic Geometry and Commutative Algebra.

Bergman ([**Ber**]) was the first to extend Gröbner bases and Buchberger algorithm to ideals in the free non-commutative algebra; later, [**M1**] made precise in which sense Gröbner bases can be "computed" in the free non-commutative algebra: there is a procedure which halts if and only an ideal has a finite Gröbner basis, in which case it returns such a basis; remark that the property of having a finite Gröbner basis is undecidable.

Gröbner bases have been also generalized to various non-commutative algebras, of interest in Differential Algebra (e.g. Weyl algebras, enveloping algebras of Lie algebras).

The aim of this paper is to give an introduction, as elementary as I was able to make it, to both commutative and non-commutative algebras: Gröbner bases are in a sense a finite model of an infinite linear Gauss-reduced basis of an ideal viewed as a vector-space and Buchberger algorithm is the corresponding generalization of the Gaussian Elimination algorithm. This approach is not new (*cf.*[**Ga1**], [**GM**]), but at my knowledge it has never been developed in such a detail and up to a presentation of the algorithm which includes the "useless pair criteria".

While the results surveyed in this paper are fairly standard, some minor points are new: e.g. the detailed presentation of the "useless pair criteria" in the non-commutative case and the final result on the existence and "computability" of Gröbner bases for two-sided ideals in any finitely presented algebra.

Acknowledgements

I would like to thank Masami Ito for his invitation to the Kyoto Workshop, which gave me another occasion to speak of my favourite mathematical subject and a unique occasion to write this survey; Larry Lambe who first induced me to prepare a presentation of this material; Dominique Duval for her invitation and hospitality in Limoges, where most of these notes were written; Joachim Apel, Tatiana Gateva, Maria Grazia Marinari, Volker Weispfenning for commenting on a draft version; Birgit Reinert for having informed me of undecidability of the finite Gröbner basis property.

1 Gröbner Bases

Setup

Our aim is to give algorithmic recipes to deal with finitely presented algebras over a field and with their ideals. A good starting point is then just a semigroup $\mathbf{S}$ which we only require to be endowed with a well-ordering $<$, which is a semigroup ordering, i.e. it is compatible with the product:

$$\text{for each} \quad l, r, t_1, t_2 \in \mathbf{S}, \quad t_1 < t_2 \quad \text{implies} \quad l t_1 r < l t_2 r$$

We consider then the semigroup ring $k\langle\mathbf{S}\rangle$, which has an obvious k-vector space structure, for which $\mathbf{S}$ is a basis. In other words each element of $k\langle\mathbf{S}\rangle$ has a unique representation as a linear combination of elements of $\mathbf{S}$. The well-ordering $<$ gives us something more: each element $f \in k\langle\mathbf{S}\rangle$ has a unique *ordered* representation as a linear combination of elements of $\mathbf{S}$:

$$f = \sum_{i=1}^{s} c_i t_i : c_i \in k \setminus \{0\}, t_i \in \mathbf{S}, t_1 > \cdots > t_s$$

* DIMA and DISI, Università di Genova, Via L.B. Alberti 4, 16132 Genova; E-mail: theomora@dima.unige.it
Partially supported by ESPRIT-BRA 6846 **PoSSo**

So to each non-zero element $f \in k\langle\mathbf{S}\rangle$, we can associate $T(f) := t_1$, the *maximal term* of f, and $lc(f) := c_1$, the *leading coefficient* of f.

Example While at least the beginning of the theory can be stated quite in general, we will develop only two easy cases, and the generalizations we will propose will be in different directions.

First, we take $\mathbf{S} := \langle a_1, \ldots, a_n\rangle$, the free semigroup generated by the n symbols a_i. Each element $t \in \mathbf{S}$ has then a "degree" which is given by the cardinality of symbols composing it, so for instance $deg(a_2a_1a_2) = 3$.

As an ordering we can choose the *deglex* ordering $<$ such that $t_1 < t_2$ if and only if either

$$deg(t_1) < deg(t_2) \quad \text{or} \quad deg(t_1) = deg(t_2) \quad \text{and} \quad t_1 \quad \text{is lexicographically less than} \quad t_2,$$

where we say that t_1 is lexicographically less than t_2 if

$$\text{either there is} \quad r \in \mathbf{S} \quad \text{such that} \quad t_2 = t_1 r$$

$$\text{or there are} \quad l, r_1, r_2 \in \mathbf{S}, \quad a_{j_1}, a_{j_2} \quad \text{with} \quad j_1 < j_2 \quad \text{such that} \quad t_1 = l a_{j_1} r_1, t_2 = l a_{j_2} r_2$$

(the definition depends obviously on an ordering of the generating symbols). The first terms of $\mathbf{S} = \langle a_1, a_2\rangle$ are then:

$$1 < a_1 < a_2 < a_1^2 < a_1a_2 < a_2a_1 < a_2^2 < a_1^3 < a_1^2a_2 < a_1a_2a_1 < a_1a_2^2 < a_2a_1^2 < a_2a_1a_2 < a_2^2a_1 < a_2^3 < \cdots$$

Remark that "lexicographically less" is *not* good, since it is not a well-ordering; in fact $a_1^{j+1}a_2 < a_1^j a_2$.

As a second case, we take $\mathbf{T}$, the commutative free semigroup generated by $a_1, \ldots, a_n$, whose elements are $a_1^{e_1} \cdots a_n^{e_n} : e_i \in \mathbb{N}$. As an ordering we can choose the following one:

$$t_1 := a_1^{e_1} \cdots a_n^{e_n} < a_1^{\eta_1} \cdots a_n^{\eta_n} =: t_2 \quad \text{if and only if either}$$

$$deg(t_1) < deg(t_2) \quad \text{or} \quad deg(t_1) = deg(t_2) \quad \text{and there is} \quad j : e_i = \eta_i, i < j, e_j > \eta_j$$

Remark that, if we consider $\mathbf{T}$ as the subset of $\mathbf{S}$ (the product is different, of course!) consisting of those elements $a_{i_1}a_{i_2}\cdots a_{i_s}$ such that $i_1 \le i_2 \le \cdots \le i_s$, then the ordering on $\mathbf{T}$ agrees with the one in $\mathbf{S}$. For some unfathomable reasons, however, the ordering is known as *degrevlex* (and also as the *total degree* ordering). ∎

With $\mathbf{S}$ and $\mathbf{T}$ defined as above, $k\langle\mathbf{S}\rangle$ is the free k-algebra on $a_1, \ldots, a_n$ and $k\langle\mathbf{T}\rangle$ is the polynomial ring $k[a_1, \ldots, a_n]$.

Using the ordering defined above, we have for instance, for $f := 2a_2^2a_1^2 - 3a_1^2a_2^2 + 4a_2^3 \in k\langle\mathbf{S}\rangle$, $T(f) = a_2^2a_1^2, lc(f) = 2$ and for $f := a_1a_3 + a_2^2 \in k[a_1, \ldots, a_n]$, $T(f) = a_2^2$.

If $I \subset k\langle\mathbf{S}\rangle$ is a (two-sided, left, right) ideal of $k\langle\mathbf{S}\rangle$, the set

$$T(I) := \{T(f) \in \mathbf{S} : f \in I\} \subset \mathbf{S}$$

is a (two-sided, left, right) semigroup ideal of $\mathbf{S}$ and the set

$$O(I) := \mathbf{S} \setminus T(I)$$

is a (two-sided, left, right) *order ideal* of $\mathbf{S}$ i.e.

$$\text{for each} \quad l, r, t \in \mathbf{S}, ltr \in O(I) \quad \text{implies} \quad t \in O(I) \quad \text{(two-sided case)}$$

$$\text{for each} \quad l, t \in \mathbf{S}, lt \in O(I) \quad \text{implies} \quad t \in O(I) \quad \text{(left case)}$$

Example Let us continue the example above, with $n = 3$, i.e. $k\langle\mathbf{S}\rangle = k\langle a_1, a_2, a_3\rangle$ and $k\langle\mathbf{T}\rangle = k[a_1, a_2, a_3]$.

First we consider the two-sided ideal $I_0 \subset k\langle\mathbf{S}\rangle$ generated by $(a_2a_1 - a_1a_2, a_3a_1 - a_1a_3, a_3a_2 - a_2a_3)$, where elements are written so that the first term is their maximal term. It is quite easy (in this example) to realize that $k\langle\mathbf{S}\rangle \,/\, I_0 = k\langle\mathbf{T}\rangle$. As an obvious consequence then, $O(I_0) = \mathbf{T}, T(I_0) = (a_2a_1, a_3a_1, a_3a_2)$

As a second example, we consider the two-sided ideal $I_1 \subset k\langle\mathbf{S}\rangle$ generated by $(a_1a_1 - a_1, a_2a_2 - a_2, a_3a_3 - a_3)$; here it is less easy to convince oneself that $T(I_1) = (a_1a_1, a_2a_2, a_3a_3)$, and that $O(I_1)$ consists of those terms $a_{i_1} \cdots a_{i_t}$ s.t. $a_{i_j} \ne a_{i_{j+1}}$ for each j.

Finally, we consider the ideal $I_2 \subset k\langle\mathbf{T}\rangle$ generated by $(a_1a_1 - a_1, a_2a_2 - a_2, a_3a_3 - a_3)$; again $T(I_2) = (a_1a_1, a_2a_2, a_3a_3)$, however $O(I_2)$ is the finite set $\{1, a_1, a_2, a_3, a_1a_2, a_1a_3, a_2a_3, a_1a_2a_3\}$. ∎

Theorem 1.1 *The following holds:*
1) $k\langle \mathbf{S}\rangle = I \oplus Span_k(O(I))$
2) *There is a* k*-vector space isomorphism between* $k\langle \mathbf{S}\rangle/I$ *and* $Span_k(O(I))$
3) *for each* $f \in k\langle \mathbf{S}\rangle$ *there is a unique* $g := Can(f, I) \in Span_k(O(I))$ *s.t.* $f - g \in I$

Moreover:
a) $Can(f, I) = Can(g, I)$ *if and only if* $f - g \in I$
b) $Can(f, I) = 0$ *if and only if* $f \in I$

Proof: The second and the third statements are just useful rephrasing of the first one; so let us procede to prove (1). The proof that $I \cap Span_k(O(I)) = \{0\}$ is quite easy: if $f \neq 0 \in I \cap Span_k(O(I))$ then $T(f)$ is in both $T(I)$ and $O(I)$ which is an obvious contradiction. A proof that $k\langle \mathbf{S}\rangle = I + Span_k(O(I))$ follows from the following "procedure":

$f_0 := f, \phi_0 := 0, h_0 := 0, i := 0$
while $f_i \neq 0$ **do**
  If $T(f_i) \notin T(I)$ **then**
    $\phi_{i+1} := \phi_i, h_{i+1} := h_i + lc(f_i)T(f_i), f_{i+1} := f_i - lc(f_i)T(f_i)$
  else % $T(f_i) \in T(I)$ %
    choose $g \in I$ **s.t.** $T(g) = T(f_i), lc(g) = 1$
    $\phi_{i+1} := \phi_i + lc(f_i)g_i, h_{i+1} := h_i, f_{i+1} := f_i - lc(f_i)g_i$
  $i := i + 1$
$\phi := \phi_i, h := h_i$

The correctness of the algorithm is based on the easy observations that

$$\forall i \ : \ \phi_i \in I, \ h_i \in Span_k(O(I)), \ f_i + \phi_i + h_i = f.$$

Termination is guaranteed by the easy observation that if $f_n \neq 0$ then $T(f_n) < T(f_{n-1})$ and $<$ is a well-ordering. ▮

Example Let us compute $Can(f, I_0)$ where $f = 2a_3a_2a_1 - 3a_1a_3^2$. We have:

$f_0 = 2a_3a_2a_1 - 3a_1a_3^2 \quad \phi_0 = 0 \quad h_0 = 0$
$T(f_0) = a_3a_2a_1 \in T(I_0), g = a_3(a_2a_1 - a_1a_2)$
$f_1 = 2a_3a_1a_2 - 3a_1a_3^2 \quad \phi_1 = 2a_3a_2a_1 - 2a_3a_1a_2 \quad h_1 = 0$
$T(f_1) = a_3a_1a_2 \in T(I_0), g = (a_3a_1 - a_1a_3)a_2$
$f_2 = -3a_1a_3^2 + 2a_1a_3a_2 \quad \phi_2 = 2a_3a_2a_1 - 2a_1a_3a_2 \quad h_2 = 0$
$T(f_2) = a_1a_3^2 \notin T(I_0)$
$f_3 = 2a_1a_3a_2 \quad \phi_3 = 2a_3a_2a_1 - 2a_1a_3a_2 \quad h_3 = -3a_1a_3^2$
$T(f_3) = a_1a_3a_2 \in T(I_0), g = a_1(a_3a_2 - a_2a_3)$
$f_4 = 2a_1a_2a_3 \quad \phi_4 = 2a_3a_2a_1 - 2a_1a_2a_3 \quad h_4 = -3a_1a_3^2$
$T(f_4) = a_1a_2a_3 \notin T(I_0)$
$f_5 = 0 \quad \phi_5 = 2a_3a_2a_1 - 2a_1a_2a_3 \quad h_5 = -3a_1a_3^2 + 2a_1a_2a_3$

obtaining $Can(f, I_0) = -3a_1a_3^2 + 2a_1a_2a_3$.

The reader is encouraged to check himself that choosing different g's at each step (say $g = (a_3a_2 - a_2a_3)a_1$ for f_0) while changing the intermediate computations would not change the final result. ▮

Remarking that each semigroup ideal in an ordered semigroup has a unique irredundant basis, we immediately obtain:

Proposition 1.1 *If* $I \in k\langle \mathbf{S}\rangle$ *is an ideal, there is a unique set* $G \subset I$ *s.t.*
1) $\{T(g) : g \in G\}$ *is an irredundant basis of* $T(I)$
2) $lc(g) = 1$ *for each* $g \in G$
3) $g = T(g) - Can(T(g), I)$ *for each* $g \in G$.

G *is called the reduced Gröbner basis of* I.

Example So the bases we have given for I_0, I_1, I_2 are reduced Gröbner bases.▮

We can relax the notion above to introduce the following:

Definition *A set $G \subset I$ is called a Gröbner basis of I if $T(G) = T(I)$ where $T(G)$ is the semigroup ideal generated by $\{T(g) : g \in G\}, T(G) := (T(g) : g \in G)$.*

Theorem 1.2 *The following conditions are equivalent:*
1) G is a Gröbner basis of I
2) for each $f \in k\langle \mathbf{S} \rangle$:

$$f = Can(f, I) + \sum_{i=0}^{t} c_i l_i g_i r_i \quad c_i \in k - \{0\},\ l_i, r_i \in \mathbf{S},\ g_i \in G$$

$$T(f) \geq l_1 T(g_1) r_1 > \ldots > l_i T(g_i) r_i > l_{i+1} T(g_{i+1}) r_{i+1} > \ldots$$

3) for each $f \in k\langle \mathbf{S} \rangle$, $f \in I$ if and only if:

$$f = \sum_{i=0}^{t} c_i l_i g_i r_i \quad c_i \in k - \{0\},\ l_i, r_i \in \mathbf{S},\ g_i \in G$$

$$T(f) = l_1 T(g_1) r_1 > \ldots > l_i T(g_i) r_i > l_{i+1} T(g_{i+1}) r_{i+1} > \ldots$$

Such a representation is called a Gröbner representation.

Proof: 1) $\Rightarrow$ 2) The proof is obtained by modifying the procedure in the proof of Theorem 1; we have just to specialize the choice of g in the instruction

choose $g \in I$ **s.t.** $T(g) = T(f_i), lc(g) = 1$

by taking $g = lc(g_i^{-1}) l_i g_i r_i$ where $g_i \in G$ is such that $T(g_i)$ divides $T(f)$ and l_i, r_i in $\mathbf{S}$ are s.t. $T(f) = l_i T(g_i) r_i$ i.e. by substituting it with the instructions

choose $g_i \in G$, $l_i, r_i \in \mathbf{S}$ **s.t.** $l_i T(g_i) r_i = T(f_i)$

$g := lc(g_i^{-1}) l_i g_i r_i$

2) $\Rightarrow$ 3) If f has a Gröbner representation, then it is in the ideal generated by G which is contained in I. Conversely if $f \in I$, then $Can(f, I) = 0$, so the result follows immediately from 2).

3) $\Rightarrow$ 1) Let $t \in T(I)$ and let $f \in I$ be s.t. $t = T(f)$ and let $f = \sum_{i=1}^{t} c_i l_i g_i r_i$ be a Gröbner representation of f. Then $t = T(f) = l_1 T(g_1) r_1$ so that $t \in T(G) = (T(g) : g \in G)$ and $T(G) = T(I)$. ∎

Example So we have $f = Can(f, I_0) + 2a_3 g_{12} + 2g_{13} a_2 + 2a_1 g_{23}$ where $g_{ij} = a_j a_i - a_i a_j$ ∎

Effectiveness of Gröbner Bases

A basic question is, how effective is this procedure?

We cannot forget that undecidability is lurking around, so that there MUST be obstructions to make the above procedure an algorithm. In fact, the above procedure would allow to solve the *ideal membership problem*, i.e.

given $I \in k\langle \mathbf{S} \rangle$, given $f \in k\langle \mathbf{S} \rangle$, decide whether $f \in I$

by applying the procedure above to obtain $Can(f, I)$: then by Theorem 1.1,4), $f \in I$ if and only if $Can(f, I) = 0$

On the other side, it is well known that the *word problem* for a finitely presented semigroup is undecidable. The word problem can be formulated as follows:

Let $\mathbf{S}$ be the free non-commutative semigroup on n symbols; let $\mathcal{R} := \{(l_1, r_1), \ldots, (l_t, r_t)\} \subset \mathbf{S} \times \mathbf{S}$; let $\equiv_{\mathcal{R}}$ be the congruence generated by $\mathcal{R}$.

Given $\mathcal{R}, w_1, w_2 \in \mathbf{S}$ decide whether $w_1 \equiv_{\mathcal{R}} w_2$.

The word problem can be easily reduced to the ideal membership problem as follows:

Let k be any field, let $I_{\mathcal{R}} \subset k\langle \mathbf{S} \rangle$ be the ideal generated by $\{l_i - r_i : (l_i, r_i) \in \mathcal{R}\}$; then:

$$w_1 \equiv_{\mathcal{R}} w_2 \quad \text{if and only if} \quad w_1 - w_2 \in I_{\mathcal{R}}.$$

Therefore if the procedure above were an algorithm, we could solve the ideal membership problem and so the undecidable word problem.

Let us restrict ourselves to the case in which $\mathbf{S} := \langle a_1, \ldots, a_n \rangle$ and discuss what consequences the undecidability of the word problem has on the effectiveness of the reduction procedure. First of all, most steps of the procedure require just arithmetics on $k\langle\mathbf{S}\rangle$: since in order to reduce the word problem to the ideal membership problem we can choose any field we like, non-effectiveness cannot hide here; also it is clear that it is always possible to compare two elements in $\mathbf{S}$ in order to decide whether one divides the other.

It is not obvious that given a semigroup ordering $<$ it is possible to decide which is the maximal term of an element in $k\langle\mathbf{S}\rangle$; but this is surely possible for many orderings, and we are free to choose any ordering we like. An ordering for which this is possible is for instance the deglex ordering. In what follows we will exclude from consideration "undecidable" orderings, i.e. orderings s.t. it is impossible to effectively order a finite set of terms.

This allows to chase undecidability to its last potential refuge, the instruction:

choose $g_i \in G$, $l_i, r_i \in \mathbf{S}$ **s.t.** $l_i T(g_i) r_i = T(f_i)$

There are several reasons why one might not execute it:

- first of all $k\langle\mathbf{S}\rangle$ is not noetherian, so there are ideals which are not finitely generated; even restricting ourselves to finitely generated ideals, we cannot rule out the possibility that such an ideal has infinite Gröbner bases only. In fact, we will see soon that the undecidability of the word problem implies that there are finitely generated ideals all of whose Gröbner bases are infinite (at least for decidable orderings). It is useful to remark that this doesn't chase word problem undecidability to its last refuge: Squier [**S**] proved that there are ideals with decidable ideal membership all of whose Gröbner bases are infinite.
- however infiniteness of Gröbner bases doesn't answer completely our question; in fact to decide whether a given f is in I, we don't need to know a complete Gröbner basis G of I, but just $\{g \in G : T(g) \leq T(f)\}$ which is a finite set at least in case $<$ is a *sequential* ordering, i.e. is s.t. $\forall t \in \mathbf{S}$, $\{u \in \mathbf{S} : u < t\}$ is finite. For instance *deglex* is sequential.

To fix notations let us say that G is a Gröbner basis of I *truncated at* $t \in \mathbf{S}$ if there is a Gröbner basis H of I s.t. $G = \{g \in H : T(g) \leq t\}$

We have reached therefore the following provisional conclusion:

Proposition 1.2 *Given a semigroup $\mathbf{S}$ and an ideal $I \subset k\langle\mathbf{S}\rangle$ for which the ideal membership problem is undecidable, then, for each decidable semigroup well-ordering $<$ which is sequential there is no algorithm s.t. given $t \in \mathbf{S}$ computes a Gröbner basis of I truncated at t.*

Looking at the other side of the coin we can assert the following:

Proposition 1.3 *Given a semigroup $\mathbf{S}$ and an ideal $I \subset k\langle\mathbf{S}\rangle$, if for some decidable semigroup well-ordering $<$ either*

I has a finite Gröbner basis w.r.t. $<$ and there is an algorithm to compute it

or

$<$ is sequential and for each $t \in \mathbf{S}$ there is an algorithm to compute a Gröbner basis of I truncated at t

then:

1. *the ideal membership problem is decidable for I*
2. *the algebra $k\langle\mathbf{S}\rangle/I$ has an effective presentation as $Span_k(O(I))$.*

The aim of the next paragraphs is to show that, restricting to decidable well-orderings, and "nice" semigroups $\mathbf{S}$:

Claim *If $k\langle\mathbf{S}\rangle$ is noetherian then for each ideal I it is possible to compute a Gröbner basis of I.*

If I has a finite Gröbner basis w.r.t. $<$, then there is an algorithm to compute it.

If I is homogeneous and $<$ is a degree-compatible ordering (i.e. $deg(t_1) < deg(t_2)$ implies $t_1 < t_2$), then for each $t \in \mathbf{S}$ it is possible to compute a Gröbner basis truncated at t.

2 Gröbner Bases and Gauss Bases

Canonical Forms and Gaussian Reduction

Before discussing an "algorithm" to compute Gröbner bases, let us go back to the procedure discussed in the previous section and refine our analysis of it. We begin by giving a simplified version of it:

Can(f, I)
where
$f \in k\langle \mathbf{S} \rangle$
$I \subset k\langle \mathbf{S} \rangle$ is an ideal
G is a Gröbner basis of I
$h := 0$
while $f \neq 0$ **do**
If $T(f) \notin T(I)$ **then**
$h := h + lc(f)T(f), f := f - lc(f)T(f)$
else % $T(f) \in T(I)$ %
choose $g \in G$, $l, r \in \mathbf{S}$ **s.t.** $lT(g)r = T(f)$
$f := f - lc(f)lc(g)^{-1}lgr$
$Can(f, I) := h$

It is easy to realize that this is essentially a rephrasing of the classical "complete" Gaussian reduction procedure for vector spaces.

There is also a variant of this procedure which is analogous of "incomplete" Gaussian Reduction, in which the computation is truncated when one either reaches the null vector or a vector whose first coordinate is not among the first coordinates of the current basis elements.

Before writing down explicitly this variant, let us give the following:

Definition *Let $G \subset k\langle \mathbf{S} \rangle$, and denote I the ideal generated by G; let $f \in k\langle \mathbf{S} \rangle$. A normal form of f w.r.t. G is an element $h \in k\langle \mathbf{S} \rangle$ s.t.*
- $g - h \in I$
- either $h = 0$ or $T(h) \notin T(G)$

Example For instance (going back to the previous examples) f_2 is a normal form of f with respect to $G := \{a_2a_1 - a_1a_2, a_3a_1 - a_1a_3, a_3a_2 - a_2a_3\}$. ∎

Proposition 2.1 *G is a Gröbner basis of I if and only if $\forall f \in k\langle \mathbf{S} \rangle$, $\forall h$, a normal form of f:*
- if $h = 0$ then $f \in I$
- if $h \neq 0$ then $f \notin I$

Proof: Assume G is a Gröbner basis of I and let h be a normal form of f. If $f \notin I$, then $h \neq 0$ since $f - h \in I$. If $f \in I$, then $h \in I$ too, so that if $h \neq 0$, $T(h) \in T(I) = T(G)$; therefore $h = 0$.

Conversely if G is not a Gröbner basis of I, then there is $f \in I$ s.t. $T(f) \notin T(G)$; f is then a normal form of f w.r.t. G. ∎

The following procedure (which is effective provided $<$ is a decidable ordering), computes normal forms w.r.t. finite sets G and is a counterpart of incomplete Gaussian reduction:

h := **Normal Form**(f,G)
where
$f \in k\langle \mathbf{S} \rangle$
G is a finite subset of $k\langle \mathbf{S} \rangle$
$h \in k\langle \mathbf{S} \rangle$ is a normal form of f w.r.t. G
$h := f$
while $h \neq 0$ **and** $T(h) \in T(G)$ **do**
choose $g \in G$, $l, r \in \mathbf{S}$ **s.t.** $lT(g)r = T(h)$
$h := h - lc(h)lc(g)^{-1}lgr$

Gaussian Reduction revisited

Because of this analogy, let us therefore discuss in detail the classical Gaussian Reduction Algorithm for finitely dimensional vector spaces.

Let us denote by $T(v)$ the first non-zero coordinate of a vector $v \in k^n$ and, for a set $S \subset k^n$, $T(S) := \{T(v) : v \in S\}$. Let us call *Gauss basis* (resp. *Gauss generating set*) a basis (resp. a generating set) B of a subvectorspace $V \subset k^n$ s.t. $T(B) = T(V)$ and *echelon set* in V a set L of linearly independent elements in V s.t. if $v, w \in L$, $v \neq w$, then $T(v) \neq T(w)$.

The following is then a (non-standard) description of the Gaussian Reduction Algorithm, to compute a Gauss basis B of a subvectorspace $V \subset k^n$, given a basis G of V:

Let B an echelon set extracted from G s.t. $T(B) = T(G)$. For each $v \in G \setminus B$ perform incomplete Gaussian reduction on v w.r.t. B and add the result to B if it is non-zero.

This procedure doesn't give only an algorithm to compute a Gauss basis B of V from a given basis G; it gives also a test whether a generating set is Gauss: denoting B an echelon set extracted from G s.t. $T(B) = T(G)$, G is a Gauss generating set if and only if B is a Gauss basis if and only if each $v \in G \setminus B$ is reduced to zero.

Moreover, denoting $\{e_1, \ldots, e_n\}$ the canonical basis of k^n, the set $\{e_j : j \notin T(B)\}$ is a basis of a subvectorspace of k^n which is isomorphic to k^n/V.

The following remark has probably been used over and over; we need to make it explicit since we will do an essential use of it in the next paragraph. We begin with a definition:

Definition *Let $G = (v_1, \ldots, v_s)$ be a generating set of V. An echelon set B s.t.*
$T(B) = T(G)$
if $v_i \in G, v_j \in B$ are such that $T(v_i) = T(v_j)$,then $i \geq j$
will be called the canonical echelon set extracted from G

Proposition 2.2 *Let $G = (v_1, \ldots, v_s)$ be a generating set of V and let B be the canonical echelon set extracted from G. Then B is a Gauss basis if and only if:*
for each $v_j \in G \setminus B$, there is a (weak) Gauss representation $v_j = c_0 v_{i_0} + \sum_{k=1}^{u} c_i v_{i_k}$ with $v_{i_k} \in G, T(v_j) = T(v_{i_0})$, $i_0 < j$, $T(v_{i_k}) > T(v_j)$ for $k > 0$.

Proof: Of course, B is a Gauss basis if and only if for each v_j in $G \setminus B$, there is a *strong Gauss representation* $v_j = c_0 v_{i_0} + \sum_{k=1}^{u} c_i v_{i_k}$ with $v_{i_k} \in B, T(v_j) = T(v_{i_0})$, $T(v_{i_k}) > T(v_j)$ for $k > 0$

Assume this is false and let $v_j \in G \setminus B$ be an element for which a strong Gauss representation doesn't exist, and which is minimal in the sense that $T(v_j)$ is as high as possible and that v_j has the minimal index among all the counterexamples with $T(v_j)$ as first non-zero coordinate. This means that in the weak Gauss representation $v_j = c_0 v_{i_0} + \sum_{k=1}^{u} c_i v_{i_k}$ all the v_{i_k}'s either are in B or have a strong Gauss representation; substituting each v_{i_k} not in B with its strong Gauss representation, we obtain a strong Gauss representation for v_j too. ▮

To look for an algorithm, which, at least under the restrictive assumptions made in the Claim, allows to compute a Gröbner basis for a finitely generated ideal in $k\langle \mathbf{S} \rangle$, we need to understand the relations between Gröbner bases of an ideal and Gauss bases of a subvectorspace; but this is trivial:

Remark *G is a Gröbner basis for I if and only if $\{lgr : l, r \in \mathbf{S}, g \in G\}$ is a Gauss generating set for I.*

Gröbner Bases for left ideals in $k\langle a_1, \ldots, a_n \rangle$

How much can we generalize Gaussian reduction in order to compute Gröbner bases?

Let us start our discussion with a very simple case in which the Gröbner basis algorithm is just a trivial adaptation of Gaussian Reduction: we take $\mathbf{S} := \langle a_1, \ldots, a_n \rangle$ and we consider finitely generated left ideals in $k\langle \mathbf{S} \rangle$.

Let $I \subset k\langle \mathbf{S} \rangle$ be a finitely generated left ideal and let G be a finite basis of I. Then the set $\{tf : t \in \mathbf{S}, f \in G\}$ is a vector space generating set of I. It is not a Gauss basis if and only if there are two elements in it, $t_1 f_1$, $t_2 f_2$ s.t. $t_1 T(f_1) = t_2 T(f_2)$, which is possible if and only if there are $f, h \in G$, $t \in \mathbf{S}$ s.t. $T(f) = tT(h)$

The following algorithm then allows to compute a Gröbner basis of I:

While there are $f, h \in G$, $t \in \mathbf{S}$ **s.t.** $T(f) = tT(h)$ **do**
  $G := G \setminus \{f\}$
  $g :=$ **Normal Form**(f, G)
  If $g \neq 0$ **then**
    $G := G \cup \{g\}$.

Example Let us consider the left ideal I in $k\langle a,b\rangle$ generated by $f_1 := a^3 - a, f_2 := ab^3 - a, f_3 := b^3 - a$ (here we have identified a with a_1, b with a_2 and we use deglex). So we have:

$G := \{f_1, f_2, f_3\} \quad f := f_2 \quad G := \{f_1, f_3\} \quad$ **NormalForm**$(f_2, G) = a^2 - a =: f_4$

$G := \{f_1, f_3, f_4\} \quad f := f_1 \quad G := \{f_3, f_4\} \quad$ **NormalForm**$(f_1, G) = 0$

$G := \{f_3, f_4\}$

which is a Gröbner basis of I; we have therefore $T(I) = (b^3, a^2)$. ∎

The peculiarity of this case is that the following rather strong assertion holds:

Let G be a finite basis of a finitely generated left ideal $I \subset k\langle\mathbf{S}\rangle$. G is the reduced Gröbner basis of I if and only if $\{tf : t \in \mathbf{S}, f \in G\}$ is a Gauss basis of I.

In general such a strong assertion doesn't hold, for instance when we apply our theory to $k[X_1, \ldots, X_n]$, i.e. $k\langle\mathbf{T}\rangle$, where $\mathbf{T}$ is the free commutative semigroup generated by $\{X_1, \ldots, X_n\}$

In fact, if $G \subset k[X_1, \ldots, X_n]$, then $\{tf : t \in \mathbf{S}, f \in G\}$ is *not* an echelon set, unless G is a singleton: if $g_1, g_2 \in G, g_1 \neq g_2$, $t_1 := T(g_1), t_2 := T(g_2)$, $t, u_1, u_2 \in \mathbf{T}$ are s.t. $t = l.c.m.(t_1, t_2) = u_1 t_1 = u_2 t_2$ then $T(u_1 g_1) = T(u_2 g_2) = t$.

3 Buchberger Algorithm in $k[X_1, \ldots, X_n]$

Partitions of semigroup ideals

In order to compute Gröbner Bases in $k[X_1, \ldots, X_n]$ by some generalization of Gaussian reduction, we must therefore begin by giving some strategy to extract the canonical echelon set from the generating set $\mathcal{G} := \{tf : t \in \mathbf{T}, f \in G\}$.

To do so we must first order it, and we do that by ordering the elements of G as $(g_1, \ldots, g_s)$ and imposing then the following ordering on $\mathcal{G}$:

$$t_1 g_{j_1} < t_2 g_{j_2} \quad \text{if and only if either} \quad t_1 T(g_{j_1}) < t_2 T(g_{j_2}) \quad \text{or} \quad t_1 T(g_{j_1}) = t_2 T(g_{j_2}), j_1 < j_2.$$

Having defined the ordering above on $\mathcal{G}$, it is then consistent with the previous paragraph to say that tg_j has a *(weak) Gauss representation* in terms of G if

$$tg_j = ug_i + \sum_{k=1}^{s} h_k g_k \quad uT(g_i) = tT(g_j) \quad i < j \quad \forall k \; T(h_k g_k) < tT(g_j).$$

We have now to extract the canonical echelon set from $\mathcal{G}$, or, equivalently, to characterize all elements tg_j s.t. there is $u \in \mathbf{T}, i < j$ with $uT(g_i) = tT(g_j)$. It is easy to realize that our problem doesn't really involve polynomials and their arithmetics but only terms and their combinatorics: the problem is in fact to characterize the set $T_j(G) := \left\{t \in \mathbf{T} \text{ s.t. } tT(g_j) \in \left(T(g_1), \ldots, T(g_{j-1})\right)\right\}$, which is clearly an ideal in $\mathbf{T}$.

To avoid cumbersome notation in what follows, let us assume w.l.o.g. that G is s.t. $lc(g_i) = 1 \forall i$ and let us denote:

$T(i) := T(g_i)$

$T(i,j) := l.c.m.(T(i), T(j))$.

Let us also denote:

$T_j(G) := \left\{t \in \mathbf{T} \text{ s.t. } tT(j) \in \left(T(1), \ldots, T(j-1)\right)\right\}$, where $T_1(G) = \emptyset$

$O_j(G) := \left\{t \in \mathbf{T} \text{ s.t. } tT(j) \notin \left(T(1), \ldots, T(j-1)\right)\right\} = \mathbf{T} \setminus T_j(G)$

$E_j(G) := \{tT(j) : t \in O_j(G)\}$

$O(G) := \{t \in \mathbf{T} : t \notin T(G)\}$.

The following results are then obvious:

Lemma 3.1 *$\mathbf{T}$ is the disjoint union of $E_1(G), \ldots, E_s(G), O(G)$*

$O_j(G)$ is an order ideal of $\mathbf{T}$, $T_j(G)$ is an ideal of $\mathbf{T}$ generated by $\{\frac{T(i,j)}{T(j)} : 1 \leq i < j\}$

Proposition 3.1 *$E(G) := \{tg_i : i = 1 \ldots s, t \in O_i(G)\}$ is the canonical echelon set extracted from $\{tg_i : i = 1, \ldots, s, t \in \mathbf{T}\}$.*

G is a Gröbner basis of the ideal I it generates if and only if $E(G)$ is a Gauss basis of I

G is a Gröbner basis of the ideal I it generates if and only if for each j, for each $t \notin O_j(G)$, tg_j has a Gauss representation in terms of G

Proof: It is just an obvious rephrasing of the linear algebra arguments of preceeding paragraph. ▮

Example Consider for instance the polynomial ring $k[X,Y]$ (here we identify X with X_1, Y with X_2 and we use degrevlex). Let $g_1 = X^5 - XY^2, g_2 = X^2Y^2 - 1, g_3 = Y^5 - X^2Y$.

We have:

$T(1) = X^5 \qquad T(2) = X^2Y^2 \qquad T(3) = Y^5$
$T(1,2) = X^5Y^2 \quad T(1,3) = X^5Y^5 \quad T(2,3) = X^2Y^5$
$T_1(G) = \emptyset \quad O_1(G) = \mathbf{T} \quad E_1(G) = \{X^aY^b : a \geq 5\}$
$T_2(G) = (X^3) \quad O_2(G) = \{X^aY^b : 0 \leq a \leq 2\} \quad E_2(G) = \{X^aY^b : 2 \leq a \leq 4, b \geq 2\}$
$T_3(G) = (X^2) \quad O_3(G) = \{X^aY^b : 0 \leq a \leq 1\} \quad E_3(G) = \{X^aY^b : 0 \leq a \leq 1, b \geq 5\}$
$O(G) = \{X^aY^b : 0 \leq a \leq 1, b \leq 4\} \cup \{X^aY^b : 2 \leq a \leq 4, b \leq 1\}$ ▮

Testing for Gauss representations

To test if G is a Gröbner basis, according to Prop. 3.1, we are left with the task of testing the existence of a Gauss representation for the infinitely many elements tg_j, with $t \in T_j(G)$. Luckily, since $T_j(G)$ is a semigroup ideal, we can reduce the problem to the same test for only the finitely many elements tg_j, with t a minimal generator of $T_j(G)$.

Recall that generators of $T_j(G)$ have the special form $\frac{T(i,j)}{T(j)}$, so let us denote, for each j, $MIN(j) \subset \{1,\dots,j-1\}$ a minimal set s.t. $\{\frac{T(i,j)}{T(j)} : i \in MIN(j)\}$ is the minimal basis of $T_j(G)$

Proposition 3.2 *Let $G = (g_1,\dots,g_s)$ be a basis of $I \subset k[X_1,\dots,X_n]$, where $lc(g_i) = 1$, for each i.*

G is a Gröbner basis of I if and only if for each j, for each $i \in MIN(j)$, $\frac{T(i,j)}{T(j)}g_j$ has a Gauss representation in terms of G.

Proof: By Proposition 3.1, to prove that G is a Gröbner basis, we have to prove that for each j, for each $t \notin O_j(G)$, tg_j has a Gauss representation in terms of G.

Let then $t \notin O_j(G)$, so that there are $u \in \mathbf{T}$, $i < j$ s.t. $tT(g_j) = uT(g_i)$, i.e. there is $w \in \mathbf{T}$ s.t. $t = w\frac{T(i,j)}{T(j)}$, $tT(g_j) = wT(i,j)$.

We can w.l.o.g. assume that $i \in MIN(j)$. By assumption, there is then a Gauss representation $\frac{T(i,j)}{T(j)}g_j = ug_\lambda + \sum_{k=1}^s h_k g_k$, so that $tg_j = wug_\lambda + \sum_{k=1}^s wh_k g_k$ is a Gauss representation too. ▮

The usual characterization of Gröbner bases is not in terms of Gauss representations but in terms of reducibility of the so-called *S-polynomials*, which therefore we are going to define:

Definition *The polynomial $S(i,j) := \frac{T(i,j)}{T(j)}g_j - \frac{T(i,j)}{T(i)}g_i$ is called the S-polynomial of g_i, g_j.*

We say that $S(i,j)$ has a weak Gröbner representation if $S(i,j) = \sum_{k=1}^s h_k g_k$, and $T(h_k g_k) < T(i,j) \forall k$

Remark that the the notion of weak Gröbner representation is actually weaker than the one of Gröbner representation: we don't require $T(h_k g_k) \leq T(S(i,j))$ but only $T(h_k g_k) < T(i,j)$. This difference will be crucial in Lemma 3.3 below.

The following result is obvious:

Lemma 3.2 *$\frac{T(i,j)}{T(j)}g_j$ has a Gauss representation $\frac{T(i,j)}{T(j)}g_j = \frac{T(i,j)}{T(i)}g_i + \sum_{k=1}^s h_k g_k$ if and only if $S(i,j)$ has a weak Gröbner representation.*

Theorem 3.1 *Let $G = (g_1,\dots,g_s)$ be a basis of $I \subset k[X_1,\dots,X_n]$, where $lc(g_i) = 1$, for each i.*

G is a Gröbner basis of I if and only if for each j, for each $i \in MIN(j)$, $S(i,j)$ has a weak Gröbner representation.

Proof: By Prop. 3.2, to prove that G is a Gröbner basis, we have to prove that for each j, for each $i \in MIN(j)$, $\frac{T(i,j)}{T(j)}g_j$ has a Gauss representation. This follows immediately by the assumption and Lemma 3.2.

Conversely if G is a Gröbner basis, then for each j, for each $i \in MIN(j)$, $S(i,j) \in I$, so it has a Gröbner representation and a fortiori a weak Gröbner representation. ▮

Useless S-polynomials

We are not yet ready to present Buchberger Algorithm, since some more simplifications are possible, which will allow us to perform only a subset of the tests required by Theorem 3.1.

Lemma 3.3 *If $T(i,j) = T(i)T(j)$, denoting $h_i := g_i - T(g_i)$, $h_j := g_j - T(g_j)$ then $S(i,j) = h_j g_i - h_i g_j$ is a weak Gröbner representation.*

On the basis of Lemma 3.3, we can perform the following construction, to obtain what we may call a *minimal set of obstructions* for g_j:

- consider the set $\{\frac{T(i,j)}{T(j)} : 1 \leq i < j\}$;
- remove from it:
  - all elements which are proper multiples of another element in the set, i.e. all elements which are not minimal generators of $T_j(G)$
  - all elements t which are minimal generators of $T_j(G)$ but s.t. there is $i : t = \frac{T(i,j)}{T(j)}$, $T(i,j) = T(i)T(j)$.
- for all of the remaining terms t choose an index i s.t. $t = \frac{T(i,j)}{T(j)}$ and collect them into a set $OBS(j)$.

Proposition 3.3 *Let $G = (g_1, \ldots, g_s)$ be a basis of $I \subset k[X_1, \ldots, X_n]$, where $lc(g_i) = 1$ for each i.*

G is a Gröbner basis of I if and only if for each j, for each $i \in OBS(j)$, $S(i,j)$ has a weak Gröbner representation.

Proof: Theorem 3.1 doesn't depend on which choice we do for $MIN(j)$; by our construction if $\frac{T(i,j)}{T(j)}$ is a minimal generator of $T_j(G)$ and $i \notin OBS(j)$ then there is k s.t. $\frac{T(i,j)}{T(j)} = \frac{T(k,j)}{T(j)}$ and either $k \in OBS(j)$ or $T(k,j) = T(k)T(j)$.

The conclusion then follows from Theorem 3.1 and Lemma 3.3. ▮

Consideration of more S-polynomials can be avoided in Buchbgerger algorithm by means of:

Lemma 3.4 *Let $i < k < j$ be s.t. $T(i,k)$ is a proper multiple of both $T(i,j)$ and $T(k,j)$ and let $t_i, t_k \in \mathbf{T}$ be s.t. $t_i T(i,j) = T(i,k) = t_k T(k,j)$. Then:*
1) $S(i,k) = t_i S(i,j) - t_k S(k,j)$
2) If $S(k,j)$ and $S(i,j)$ have weak Gröbner representations, then $S(i,k)$ has a weak Gröbner representation.

Buchberger Algorithm

We are finally able to present Buchberger Algorithm to compute the Gröbner basis of an ideal $I \subset k[X_1, \ldots, X_n]$, given a basis F of it; we will assume F to be given as an ordered set $\{g_1, \ldots, g_s\}$ and we will assume $lc(g_i) = 1 \forall i$.

$G :=$ **Gröbner**(F)
where
  $F = (g_1, \ldots, g_s)$ is a basis of an ideal $I \subset k[X_1, \ldots, X_n]$
  G is a Gröbner basis of I
$G = \emptyset$, $OBS = \emptyset$
For $t = 1, \ldots, s$ **do**
  $RED := \{(i,k) \in OBS : T(i,k)$ is a proper multiple of both $T(i,t)$ and $T(k,t)\}$
  $OBS := OBS \setminus RED$
  $G := G \cup \{g_t\}$
  $OBS := OBS \cup \{(i,t) : i \in OBS(t)\}$
While $OBS \neq \emptyset$ **do**
  Choose $(i,j) \in OBS$
  $OBS := OBS \setminus \{(i,j)\}$
  $h :=$ **NormalForm**$(S(i,j), G)$
  If $h \neq 0$ **then**
    $t := t + 1$
    $g_t := h/lc(h)$
    $G := G \cup \{g_t\}$
    $RED := \{(i,k) \in OBS : T(i,k)$ is a proper multiple of both $T(i,t)$ and $T(k,t)\}$
    $OBS := OBS \setminus RED$
    $OBS := OBS \cup \{(i,t) : i \in OBS(t)\}$

Example We are now able to compute a Gröbner basis for the ideal $I := (g_1, g_2, g_3) \subset k[X,Y]$.

The initialization phase gives us the set of S-polynomials to be tested for a weak Gröbner representation: we obtain the set $OBS = \{(1,2),(2,3)\}$; in fact $(1,3) \notin OBS(3)$ because $X^5 = \frac{T(1,3)}{T(3)}$ is not a minimal generator of $T_3(G)$ being multiple of $X^2 = \frac{T(2,3)}{T(3)}$.

We choose then the pair $(1,2)$ from OBS, compute $S(1,2) = Y^2 g_1 - X^3 g_2 = -XY^4 + X^3$, which is a normal form w.r.t. G so we set:

$t = 4 \qquad g_4 = XY^4 - X^3 \qquad G = \{g_1, g_2, g_3, g_4\}$.

Since $T(2,3) = X^2Y^5, T(2,4) = X^2Y^4, T(3,4) = XY^5$, we have $RED = \{(2,3)\}, OBS = \emptyset$. To it we add $OBS(4) = \{(2,4),(3,4)\}$; in fact $X^4 = \frac{T(1,4)}{T(4)}$ is not a minimal generator of $T_4(G)$ being multiple of $X = \frac{T(2,4)}{T(4)}$.

Choosing $(2,4)$, we compute $S(2,4) = Y^2 g_2 - X g_4 = X^4 - Y^2$, a normal form w.r.t. G so we set:

$t = 5 \qquad g_5 = X^4 - Y^2 \qquad G = \{g_1, \ldots, g_5\}$.

Lemma 3.4 doesn't apply so we compute $OBS(5) = \{(1,5),(2,5)\}$ and we have $OBS = \{(3,4),(1,5),(2,5)\}$

Next we compute $S(3,4) = Xg_3 - Yg_4 = 0$, $S(1,5) = g_1 - Xg_5 = 0$, $S(2,5) = X^2 g_2 - Y^2 g_5 = Y^4 - X^2$ and we add the latter element to G:

$t = 6 \qquad g_6 = Y^4 - X^2 \qquad G = \{g_1, \ldots, g_6\}$

and we compute $OBS = OBS(6) = \{(3,6),(4,6)\}$

Finally, since $S(3,6) = g_3 - Yg_6 = 0$, $S(4,6) = g_4 - Xg_6 = 0$, we conclude that $G = \{g_1, \ldots, g_6\}$ is a Gröbner basis of I; we can remove elements whose maximal term is not among the minimal generators of $T(I)$ and we are left with $\{g_2, g_5, g_6\}$. ▮

Termination of the algorithm is guaranteed since, denoting $G_i := (g_1, \ldots, g_i)$, one has for $i > s$, $T(g_i) \notin T(G_{i-1})$, $T(G_{i-1}) \subset T(G_i)$ and because $\mathbf{T}$ is noetherian.

Correctness is guaranteed, since at each step, when (i,j) is extracted from OBS, $S(i,j)$ has a weak Gröbner representation either in terms of $\{g_1, \ldots, g_t\}$ (in case its normal form h is 0), or in terms of $\{g_1, \ldots, g_t, h\}$ (in case its normal form h is not 0). So, at termination, for each $(i,j) \in OBS$, $S(i,j)$ has a weak Gröbner representation in terms of G, while each $(i,j) \in RED$ has a weak Gröbner representation in terms of G, because of Lemma 3.4. Therefore the conditions of Theorem 3.2 are satisfied.

4 Applications of Gröbner bases in $k[X_1, \ldots, X_n]$

Ideals and systems of polynomial equations

Now that we are able to compute Gröbner bases for polynomial ideals, it is natural to ask why one should want to do that, and even why one should want to compute with ideals in the first place.

Polynomial ideals model systems of polynomial equations: let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$, let $\mathbf{k}$ be the algebraic closure of k, let $I := (f_1, \ldots, f_s)$, let $\mathcal{Z} := \{(x_1, \ldots, x_n) \in \mathbf{k}^n : f_i(x_1, \ldots, x_n) = 0\}$. Then if $f \in I$, $f(x_1, \ldots, x_n) = 0$ for each $(x_1, \ldots, x_n) \in \mathcal{Z}$.

Only a weaker converse is true: if $f(x_1, \ldots, x_n) = 0$ for each $(x_1, \ldots, x_n) \in \mathcal{Z}$, then for some r, $f^r \in I$. For instance, if $I = (X^2) \subset k[X]$, so $\mathcal{Z} = \{0\}$, then X vanishes at 0 but is not in I.

The problem is a problem of multiplicities; if the correct notion of multiplicity is given, then one can prove that f vanishes in each $(x_1, \ldots, x_n) \in \mathcal{Z}$ with the proper multiplicity if and only if $f \in I$.

The study of polynomial ideals is therefore the algebraic approach to the study of *algebraic varieties*, which are the sets of zeroes of systems of polynomial equations. Since the zeroes of a system of polynomial equations are actually the zeroes of the corresponding ideal, we will use the notation $\mathcal{Z}(I)$

A computational theory of polynomial ideals was quite developed at the end of last century, but was then forgotten and replaced by abstract algebraic techniques, mainly because of the lack of computing power. After the introduction of Gröbner bases (and of powerful computers, of course), it has been revived and there is today a huge amount of algorithmic research in this field, mostly founded on Gröbner bases. It is obviously impossible to give here a faithful report on the present state of the art, so we will limit to a few glimpses of what can be done by means of Gröbner bases.

Reduction of algebraic problems to combinatorial problems

Theorem 1.1,2) asserts that the vector spaces $k[X_1, \ldots, X_n]/I$ and $Span_k(O(I))$ are isomorphic; since obviously $Span_k(O(I))$ is isomorphic with $k[X_1, \ldots, X_n]/(T(I))$, we have a vector space isomorphism between

$k[X_1,\ldots,X_n]/I$ and $k[X_1,\ldots,X_n]/(T(I))$; beware of brackets: (T(I)) is the polynomial ideal generated by the semigroup ideal T(I).

This isomorphism can be effectively used to reduce questions from the ideal $I \subset k[X_1,\ldots,X_n]$ to the ideal $(T(I)) \subset k[X_1,\ldots,X_n]$, and (since the latter is essentially characterized by the terms it contains) to the semigroup ideal $T(I) \subset \mathbf{T}$.

We already used that in deriving a finite set of conditions for an ideal basis to be Gröbner (Prop. 3.1); among the countless uses to which it has been put, we choose the *postulation problem*:

Given a system of polynomial equations, $f_1 = \cdots = f_s = 0$, how many conditions are to be imposed to a polynomial f of degree at most d, in order that it vanishes in its zeroes, with the proper multiplicity?

Formally we consider the *generic* polynomial $f = \sum_{t\in\mathbf{T}_d} c_t t$, where $\mathbf{T}_d = \{t \in \mathbf{T}, deg(t) \leq d\}$, and c_t are indeterminates, and we ask for f to be in the ideal I, or, what is the same, to be in the vector space $I_d := \{g \in I, deg(g) \leq d\}$. Since f is the generic element of the vector space $k[X_1,\ldots,X_n]_d := \{g \in k[X_1,\ldots,X_n], deg(g) \leq d\}$, the question boils down to linear algebra: how many independent linear conditions are to be satisfied by the c_t's in order for f to be in I_d and the obvious answer is $H_I(d) := dim_k(k[X_1,\ldots,X_n]_d) - dim_k(I_d) = \binom{d+n}{n} - dim_k(I_d)$, which is known as the *Hilbert function* of I.

Its computation amounts to computing $dim_k(I_d)$, which is the same as $dim_k((T(I))_d)$, and the same as the cardinality of the set $\{t \in T(I) : deg(t) \leq d\}$. So $H_I(d) = card\{t \in O(I) : deg(t) \leq d\}$ and the latter function can be computed by combinatorial techniques in very efficient ways; the most recent algorithm for that is [**BRT**].

Elimination

Let $I \subset k[X_1,\ldots,X_n]$ be an ideal and let $I_m \subset k[X_1,\ldots,X_m]$, $m < n$, be the ideal $I_m = I \cap k[X_1,\ldots,X_m]$. One has that $\mathcal{Z}(I_m) \subset \mathbf{k}^m$ is the projection of $\mathcal{Z}(I)$ over the first m coordinates, i.e.:

$$\mathcal{Z}(I_m) = \{(x_1,\ldots,x_m) \subset \mathbf{k}^m : \exists x_{m+1},\ldots,x_n \in \mathbf{k} : (x_1,\ldots,x_n) \in \mathcal{Z}(I)\}$$

(more exactly, it is the *closure* of the projection of $\mathcal{Z}(I)$).

Let us denote by $\mathbf{T}(m)$ the subsemigroup of $\mathbf{T}$ generated by $X_1,\ldots,X_m$ and let us choose an *elimination* ordering, i.e. an ordering s.t. for each $i > m$, for each $t \in \mathbf{T}(m)$, $t < X_i$.

Such an ordering is the *lex* ordering defined by:

$$t_1 := X_1^{e_1}\cdots X_n^{e_n} < X_1^{\eta_1}\cdots X_n^{\eta_n} =: t_2 \quad \text{if and only if there is} \quad j : e_i = \eta_i, i > j, e_j < \eta_j$$

Remark however that there are other elimination orderings, which lead to more efficient computations than *lex*.

Lemma 4.1 *Let $<$ be an elimination ordering and let $g \in k[X_1,\ldots,X_n]$. If $T(g) \in \mathbf{T}(m)$, then $g \in k[X_1,\ldots,X_m]$*

Corollary *Let G be a Gröbner basis of I for an elimination ordering. Then $G \cap k[X_1,\ldots,X_m]$ is a Gröbner basis of $I_m = I \cap k[X_1,\ldots,X_m]$.*

Solving systems of polynomial equations with finitely many solutions

The following classical result:

Theorem 4.1 *Let $I \subset k[X_1,\ldots,X_n]$ be an ideal and $\mathcal{Z}(I)$ its set of zeroes. Then:*

1) $\mathcal{Z}(I) = \emptyset$ if and only if $I = k[X_1,\ldots,X_n]$

2) $\mathcal{Z}(I)$ is finite if and only if $dim_k(k[X_1,\ldots,X_n]/I)$ is finite; in this case the number of zeroes of I, counted with multiplicity, is $dim_k(k[X_1,\ldots,X_n]/I)$.

can be so stated in terms of Gröbner bases:

Corollary *Let $I \subset k[X_1,\ldots,X_n]$ be an ideal, $\mathcal{Z}(I)$ its set of zeroes and G its reduced Gröbner basis w.r.t. to any term-ordering. Then:*

1) $\mathcal{Z}(I) = \emptyset$ if and only if $1 \in G$

2) the following conditions are equivalent:

a) $\mathcal{Z}(I)$ is finite

b) $O(I)$ is finite

c) for each i there is $g \in G$ s.t. $T(g)$ is a power of X_i

In this case the number of zeroes of I, counted with multiplicity, is $card(O(I))$.

Gröbner bases don't only provide a test for detecting finiteness of solutions of a system of polynomial equations, but also allow to present the ideal so to make its solution more feasible. There are essentially two ways of solving such a system by Gröbner bases.

The first one ([**Tr**]) relies on elimination: assume I has finitely many solutions and G is its reduced Gröbner basis w.r.t. *lex*. Because of Lemma 4.1 $G_m := G \cap k[X_1, \ldots, X_m]$ is a Gröbner basis of $I_m := G \cap k[X_1, \ldots, X_m]$. In particular, by Corollary 2.c), G consists of a single polynomial $g \in k[X_1]$.

We consider the elements of G_{m+1} as univariate polynomials in X_{m+1} with coefficients in $k[X_1, \ldots, X_m]$ and denote the leading coefficient of $g \in G_{m+1}$ by $lp(g) \in k[X_1, \ldots, X_m]$, i.e.

$$g = lp(g)(X_1, \ldots, X_m)X_{m+1}^d + h_{d-1}(X_1, \ldots, X_m)X_{m+1}^{d-1} + \cdots + h_0(X_1, \ldots, X_m)$$

Theorem 4.2 *The following holds:*

- *if $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$ then $g(a_1) = 0$*
- *if $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$ then $(a_1, \ldots, a_m) \in \mathcal{Z}(I_m)$*
- *Let $\mathbf{a} := (a_1, \ldots, a_m) \in \mathcal{Z}(I_m)$*

  Let $g_{\mathbf{a}} \in G_{m+1}$ be a polynomial of minimal degree s.t. $lp(g)(a_1, \ldots, a_m) \neq 0$. Then:

  $(a_1, \ldots, a_{m+1}) \in \mathcal{Z}(I_{m+1})$ if and only if $\mathbf{a} := (a_1, \ldots, a_m) \in \mathcal{Z}(I_m)$ and $g_{\mathbf{a}}(a_{m+1}) = 0$

The first two statements are classical; the last one is due to [**Gi,K**].

An easy induction allows therefore to reduce solving polynomial systems of equations with finitely many solutions to solving polynomial equations in one variable.

The second method ([**AS**]) reduces the problem to an eigenvalue problem:

The algebra $A := k[X_1, \ldots, X_n]/I$ has the set $O(I)$ as a linear basis; multiplication in A by an element $g \in Span_k(O(I))$ is a linear morphism; let M_g be the matrix representing it w.r.t. the basis $O(I)$.

Theorem 4.3 *Let $\alpha^{(1)} = (\alpha_1^{(1)}, \ldots, \alpha_n^{(1)}), \ldots, \alpha^{(s)}$ be the zeroes of I. Let $O(I) = \{1, t_2, \ldots, t_s\}$*

Then the eigenvalues of M_g^T are $\lambda_1 := g(\alpha^{(1)}), \ldots, \lambda_s := g(\alpha^{(s)})$.

Moreover, if all of them are distinct (which happens if the zeroes of I are all simple and g is sufficiently generic), then the eigenspace corresponding to λ_j is generated by $(1, t_2(\alpha^{(j)}), \ldots, t_s(\alpha^{(j)}))$.

Example Let $G = \{X^2 - X, XY, Y^2 - Y\}$ which is a lex Gröbner basis of the ideal I it generates. Since $O(I) = \{1, X, Y\}$, I has 3 zeroes. Solving $X^2 - X = 0$ we find $x = 0, 1$. Substituting $x = 0$ in G we get $(Y^2 - Y)$; solving it we get $y = 0, 1$. Substituting $x = 1$ in G we get $(Y, Y^2 - Y) = (Y)$ and so $y = 0$. So the zeroes of I are $(0,0), (0,1), (1,0)$.

The transpose of the matrix representing multiplication by X has a double eigenvalue 0 with eigenspace $\{(a, 0, b) : a, b \in \mathbf{k}\}$ from which the zeroes cannot be read off; and a simple eigenvalue 1 with eigenspace generated by $(1, 1, 0)$, from which we get the zero $(1, 0)$.

The transpose of the matrix representing multiplication by $X + 2Y$ has eigenvalues $0, 1, 2$ and the corresponding eigenspaces are generated by $(1,0,0)$, $(1,1,0)$, $(1,0,1)$ respectively, i.e. the eigenspaces are generated by $(1, X, Y)$ evaluated at $(0,0), (1,0), (0,1)$ and the three zeroes can be read off immediately. ∎

Relations

Given $g_1, \ldots, g_s \in P := k[X_1, \ldots, X_n]$ the set of s-tuples $\{(h_1, \ldots, h_s) \in P^s : \sum h_i g_i = 0\}$ is a finitely generated P-module, whose elements are called *syzygies* of $g_1, \ldots, g_s$.

If $\{g_1, \ldots, g_s\}$ is a Gröbner basis of the ideal it generates, then each $S(i,j)$ has a weak Gröbner representation $S(i,j) = \sum h_k g_k$, which induces a relation $\frac{T(i,j)}{T(j)} g_j - \frac{T(i,j)}{T(i)} g_i - \sum h_k g_k = 0$ and, in turn a syzygy of $g_1, \ldots, g_s$.

It can be proved that the syzygies coming from the pairs $\{(i,j) : i \in MIN(j), j = 1 \ldots s\}$ are a basis for the module of syzygies.

If $\{g_1, \ldots, g_s\}$ is not a Gröbner basis, we can compute a Gröbner basis $\{g_1, \ldots, g_s, g_{s+1}, \ldots, g_t\}$. We obtain at the same time a basis $\mathcal{B}$ for the module of syzygies of $\{g_1, \ldots, g_t\}$ and for each $i > s$ a representation $g_i = \sum_{k=1}^{i-1} p_{ik} g_k$ and therefore a representation $g_i = \sum_{k=1}^{s} q_{ik} g_k$.

If for each syzygy $(h_1, \ldots, h_t) \in \mathcal{B}$, we substitute in $\sum h_k g_k = 0$ each occurrence of $g_i, i > s$ with its representation $g_i = \sum_{k=1}^{s} q_{ik} g_k$, we obtain $\sum_{k=1}^{s}(h_k + \sum_{i=s+1}^{t} h_i q_{ik}) g_k = 0$; the corresponding syzygies are a basis for the module of syzygies of $g_1, \ldots, g_s$.

5 Buchberger Algorithm in $k\langle a_1, \ldots, a_n\rangle$

Setup

Let us move now to Gröbner bases for two-sided ideals in the free non-commutative algebra $k\langle a_1, \ldots, a_n\rangle$. There are obviously two main problems in exporting verbatim Buchberger Algorithm to this setting.

The first problem is that $\mathbf{S} := \langle a_1, \ldots, a_n\rangle$, unlike $\mathbf{T}$, is not noetherian, so termination cannot be proved; we already knew this, because of our discussion on the undecidability of the ideal membership problem; we will postpone termination to the next paragraph and content ourselves for the moment to adapt Buchberger Algorithm to a non-terminating procedure which correctly "computes" Gröbner bases in $k\langle a_1, \ldots, a_n\rangle$.

The second problem is that we don't have even the result that if I is a principal ideal, $I = (g)$, then $\{g\}$ is a Gröbner basis. In fact $\{lT(g)r : l, r \in \mathbf{S}\}$ is no more an echelon set; in other words there are *self-obstructions* as it is immediately shown by the following trivial example: take $t = aba \in \langle a, b\rangle$; then $abt = ababa = tba$.

To obtain a linear generating set from a basis of an ideal, we have in fact to multiply both on the left and on the right by elements of $\mathbf{S}$, so we must use elements of $\mathbf{S} \times \mathbf{S}$. Since there is some algebra on this set, which is the canonical k-basis of the rank 1 free bi-module on $k\langle\mathbf{S}\rangle$, let us use a non-standard notation for it and let us write $\mathbf{S} \otimes \mathbf{S} := \mathbf{S} \times \mathbf{S}$. The algebra we have on this set is:

- a left and a right multiplication with $\mathbf{S}$, which are defined as follows:

$$\text{for each} \quad t \in \mathbf{S}, \quad \text{for each} \quad (l, r) \in \mathbf{S} \otimes \mathbf{S}, \quad t(l, r) = (tl, r), \quad (l, r)t = (l, rt)$$

- for each $t \in \mathbf{S}$ a "convolution" $\phi_t : \mathbf{S} \otimes \mathbf{S} \mapsto \mathbf{S}$ defined by $\phi_t(l, r) = ltr$
- a notion of *ideal* which is a subset $\mathcal{I} \subset \mathbf{S} \otimes \mathbf{S}$ s.t. if $(l, r) \in \mathcal{I}, t \in \mathbf{S}$, then $(tl, r) \in \mathcal{I}, (l, rt) \in \mathcal{I}$; a set of generators for $\mathcal{I}$ is a (not necessarily finite) set $\mathcal{G} \subset \mathcal{I}$ s.t. for each $(l, r) \in \mathcal{I}$ there are $l_1, r_1 \in \mathbf{S}, (w_l, w_r) \in \mathcal{G}$ s.t $l = l_1 w_l$ and $r = w_r r_1$
- a notion of *order ideal* which is a subset $\mathcal{O} \subset \mathbf{S} \otimes \mathbf{S}$ s.t. if $(tl, ru) \in \mathcal{O}$, then $(l, r) \in \mathcal{O}$

Equipped with this algebra, we now adapt to $k\langle\mathbf{S}\rangle$ the approach already used for $k[X_1, \ldots, X_n]$, reducing the problem to linear algebra first and then to a combinatorial problem on $\mathbf{S} \otimes \mathbf{S}$. In this way, we will obtain a minimal set of *S-elements* so that:

- if each of them has a *weak Gröbner representation* (the notion will have to be properly defined of course), then G is a Gröbner basis
- any S-element not having a weak Gröbner representation will give rise to a new element in the Gröbner basis.

This set will then be further reduced by applying analogues of Lemmata 3.3 and 3.4.

As in Section 3, we assume that G is ordered as $(g_1, \ldots, g_s)$, and that $lc(g_i) = 1 \forall i$, and we denote $T(i) := T(g_i)$.

We have to order the generating set $\mathcal{G} = \{lgr : (l, r) \in \mathbf{S} \otimes \mathbf{S}, g \in G\}$ and we do that as follows: $l_1 g_{j_1} r_1 < l_2 g_{j_2} r_2$ if and only if

$$\text{either} \quad l_1 T(j_1) r_1 < l_2 T(j_2) r_2 \quad \text{or}$$

$$l_1 T(j_1) r_1 = l_2 T(j_2) r_2 \quad \text{and either} \quad j_1 < j_2 \quad \text{or} \quad j_1 = j_2, r_2 \quad \text{is a left multiple of} \quad r_1$$

We then say that $lg_j r$ has a *Gauss representation* in terms of G if

$$lg_j r = \lambda g_i \rho + \sum_{k,\mu} c_{k\mu} l_{k\mu} g_k r_{k\mu}$$

$$\lambda T(i) \rho = lT(j) r \quad \forall k, \mu \; l_{k\mu} T(k) r_{k\mu} < lT(j) r$$

$$i < j \quad \text{or} \quad i = j \quad \text{and there is} \quad w \; : \; r = w\rho$$

The combinatorics

First of all, let us face the problem of extracting the canonical echelon set from the generating set $\{lgr : (l,r) \in \mathbf{S} \otimes \mathbf{S}\}$ of a principal ideal (g), i.e. to define self-obstructions of $t \in \mathbf{S}$. Denote:

$SOB(t) := \{(1,r) \in \mathbf{S} \otimes \mathbf{S} : r \neq 1$ and there is $(l,1) \in \mathbf{S} \otimes \mathbf{S} : \phi_t(l,1) = lt = tr = \phi_t(1,r)\}$

$ST(t) \subset \mathbf{S} \otimes \mathbf{S}$ the ideal generated by $SOB(t)$

$SO(t)$ the order ideal $\mathbf{S} \otimes \mathbf{S} \setminus ST(t)$.

We then have:

Lemma 5.1 *If $g \in k\langle\mathbf{S}\rangle$, $t = T(g)$, I the two-sided ideal generated by g, then $\{lgr : (l,r) \in SO(t)\}$ is the canonical echelon set extracted from the generating set $\{lgr : (l,r) \in \mathbf{S} \otimes \mathbf{S}\}$.*

Example Let $g = aba - a$, so $t := T(g) = aba$; then $SOB(t) = \{(1,ba)\} \cup \{(1,wt) : w \in \mathbf{S}\}$, because $tba = ababa = abt$, and for each $w \in \mathbf{S}$, $t(wt) = (tw)t$. Therefore $ST(t)$ is the set of all pairs (l,r), where $l \in \mathbf{S}$ and $r \in \mathbf{S}$ is either a multiple of $t, r = l_1abar_1$, or it is a *right* multiple of $ba, r = bar_1$. Finally $SO(t)$ is the set of all pairs (l,r) with $l \in \mathbf{S}$ and $r \in \mathbf{S}$ neither a multiple of t, nor a right multiple of ba.

Consider with proper awe that $ST(t)$ is *not* finitely generated: in fact set $p_i := (1, a^it), i \geq 0$; then, since a^it is not a right multiple of a^jt for all i,j, $\{p_i\}$ is contained in all minimal sets of generators for $ST(t)$.

We now characterize the order ideals $O_i(G) \subset \mathbf{S}\otimes\mathbf{S}$ s.t. $\{lg_ir : i = 1 \ldots s, (l,r) \in O_i(G)\}$ is the canonical echelon set extracted from $\mathcal{G}$. The proofs which are not explicitly given, are obvious generalizations of the corresponding statements in the previous paragraph; instead of cutting and pasting them, we leave them to the reader.

Denote:

$\phi_j := \phi_{T(j)}$ so that $\phi_j(l,r) = lT(j)r$

$ST(j) := ST(T(j)), \quad SO(j) := SO(T(j))$

$T_j(G) := \{(l,r) : \phi_j(l,r) \in (T(1), \ldots, T(j-1))\} \cup ST(j)$, an ideal in $\mathbf{S} \otimes \mathbf{S}$

$O_j(G) := \{(l,r) : (l,r) \notin T_j(G)\}$, an order ideal in $\mathbf{S} \otimes \mathbf{S}$

$E_j(G) := \{\phi_j(l,r) : (l,r) \in O_j(G)\}$

$O(G) := \{t \in \mathbf{S} : t \notin T(G)\}$.

Example Let us choose $g_1 = aba - b, g_2 := bab - b, G = \{g_1, g_2\}$, so that $T(1) = aba, T(2) = bab$

$SO(1) = O_1(G)$ has been computed above and is the set of all $(l,r) \in \mathbf{S} \otimes \mathbf{S}$ with r neither multiple of aba nor right multiple of ba. $E_1(G)$ is the two-sided ideal generated by aba; in fact if w is a multiple of aba one can write it uniquely as $w = labar$, so that bar is not divisible by aba; this is equivalent to say that r is neither a multiple of aba nor a right multiple of ba. $T_1(G)$ is the set of all pairs (l,r) with r either a multiple of aba or a right multiple of ba, i.e. it is the set $\{(l,r) : l \in \mathbf{S}, r \in R\}$ where R is the union of the two-sided ideal generated by t with the right ideal generated by ba.

In an analogous way $SO(2)$ is the set of all $(l,r) \in \mathbf{S}\otimes\mathbf{S}$ with r neither multiple of bab nor right multiple of ab. To obtain $O_2(G)$, we must remove from $SO(2)$ all elements (l,r) s.t. $lbabr$ is a multiple of aba; we see that we must require that l is neither a multiple of aba, nor a left multiple of a, $l = l_1a$, since in this case $lbabr = l_1aba(br)$, and that r is neither a multiple of aba, nor a right multiple of a. Therefore $T_2(G)$ is the set of all elements $(l,r) \in \mathbf{S} \otimes \mathbf{S}$, with either l multiple of aba, l left multiple of a, r multiple of aba, r right multiple of a. Again consider with proper awe the fact that $T_2(G)$ is not finitely generated since it contains the elements $(abaa^k, 1), k \geq 0$. $E_2(G)$ is the set difference of the two sided ideal (bab) with the two-sided ideal $E_1(G) = (aba)$. ▮

Lemma 5.2 *$\mathbf{S}$ is the disjoint union of $E_1(G), \ldots, E_s(G), O(G)$; $O_j(G)$ is an order ideal of $\mathbf{S} \otimes \mathbf{S}$; $T_j(G)$ is an ideal of $\mathbf{S} \otimes \mathbf{S}$*

Proposition 5.1 *$E(G) := \{lg_ir : i = 1, \ldots, s, (l,r) \in O_i(G)\}$ is the canonical echelon set extracted from $\mathcal{G}$*

G is a Gröbner basis of the ideal I it generates if and only if $E(G)$ is a Gauss basis of I

G is a Gröbner basis of the ideal I it generates if and only if for each j, for each $(l,r) \notin O_j(G)$, lg_jr has a Gauss representation in terms of G

S-elements

We now move to the definition of S-elements: if $(l,r), (\lambda,\rho) \in \mathbf{S} \otimes \mathbf{S}$ are s.t. $\phi_j(l,r) = \phi_i(\lambda,\rho)$ let us denote:

$$S(i,j;l,r;\lambda,\rho) := lg_jr - \lambda g_i\rho$$

and let us say that $S(i,j;l,r;\lambda,\rho)$ has a *weak Gröbner representation* if

$$S(i,j;l,r;\lambda,\rho) = \sum_{k,\mu} c_{k\mu} l_{k\mu} g_k r_{k\mu} \quad \text{for each} \quad k,\mu \quad l_{k\mu} T(g_k) r_{k\mu} < lT(g_j) r$$

Lemma 5.3 *Let $(l,r),(\lambda,\rho) \in \mathbf{S} \otimes \mathbf{S}$ be s.t. $\phi_j(l,r) = \phi_i(\lambda,\rho)$ and moreover $i < j$ or $i = j$ and there is $w : r = w\rho$.*

Then lg_jr has a Gauss representation $lg_jr = \lambda g_i \rho + \sum_{k,\mu} c_{k\mu} l_{k\mu} g_k r_{k\mu}$ if and only if $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation.

As in the commutative case, it is sufficient to test the existence of a weak Gröbner representation, only for an S-element $S(i,j;l,r;\lambda,\rho)$ for each generator (l,r) of $T_j(G)$.

For each j, let us therefore choose a minimal basis of $T_j(G)$, $\mathcal{B}$ (which could as well be infinite); for each $\sigma = (l_\sigma, r_\sigma) \in \mathcal{B}$, we choose $i_\sigma, \lambda_\sigma, \rho_\sigma$ s.t.

$l_\sigma T(j) r_\sigma = \lambda_\sigma T(i_\sigma) \rho_\sigma \qquad i_\sigma < j$ or $i_\sigma = j$ and there is $w : r_\sigma = w\rho_\sigma$
and we let $MIN(j) := \{(i_\sigma, j; l_\sigma, r_\sigma; \lambda_\sigma, \rho_\sigma)\}$.

There is however a problem more with respect to the commutative case, which we had already occasion to remark; given $t_1, t_2 \in \mathbf{S}$ the ideal $\{(l,r) \in \mathbf{S} \otimes \mathbf{S} : lt_2 r \text{ is a multiple of } t_1\}$ is not finitely generated since it contains $\{(t_1 w, 1) : w \in \mathbf{S}\}$. Therefore the restriction outlined above is not sufficient to reduce the tests to be performed to a finite number. A generalization of Lemma 3.3 shows however how to solve this problem :

Lemma 5.4 *Let $g_1, g_2 \in k\langle \mathbf{S} \rangle$, $lc(g_i) = 1$, let $t_i := T(g_i)$, $w \in \mathbf{S}$, $g_i - t_i = \sum_{k=1}^{u_i} c_{ik} t_{ik}$. Then $t_1 w g_2 - g_1 w t_2 = \sum_{k=1}^{u_2} c_{2k} g_1 w t_{2k} - \sum_{k=1}^{u_1} c_{1k} t_{1k} w g_2$ and $t_{1k} w t_2 < t_1 w t_2$, $t_1 w t_{2k} < t_1 w t_2$*

Let us therefore say that $(i,j;l,r;\lambda,\rho) \in MIN(j)$ is *trivial* if there is w s.t. either $l = \lambda T(i) w$ (and so $\rho = wT(j)r$) or $\lambda = lT(j)w$ (and so $r = wT(j)\rho$).

Corollary 5.1 *If $(i,j;l,r;\lambda,\rho) \in MIN(j)$ is trivial, then $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation.*

Moreover $\{(i,j;l,r;\lambda,\rho) \in MIN(j)$ and non trivial$\}$ is finite.

Proof: The first statement is a direct consequence of Lemma 5.4; the second one follows at once, since if $(i,j;l,r;\lambda,\rho)$ is non-trivial, then either

- $\lambda = 1$ and $T(j)$ is a left multiple of ρ
- $\rho = 1$ and $T(j)$ is a right multiple of λ
- $T(j)$ is a multiple of $T(i)$ and so it is a right multiple of λ and a left multiple of ρ.
- $T(i)$ is a multiple of $T(j)$ and so $\lambda = \rho = 1$, $T(i)$ is a right multiple of l and a left multiple of r. ∎

We can now conclude that:

Theorem 5.1 *Let $G = (g_1, \ldots, g_s)$ be a basis of $I \subset k\langle \mathbf{S} \rangle$, where $lc(g_i) = 1$ for each i.*

G is a Gröbner basis of I if and only if for each j, for each non-trivial $(i,j;l,r;\lambda,\rho) \in MIN(j)$, $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation.

On the basis of Theorem 5.1, we need to construct a *minimal set of obstructions* for g_j, i.e. the finite set $OBS(j) = \{(i,j;l,r;\lambda,\rho) \in MIN(j) : (i,j;l,r;\lambda,\rho)$ is not trivial $\}$.

We can do as follows, assuming, w.l.o.g., that $T(j)$ is not multiple of $T(i)$ for $i < j$:

> $OBS(j) = \emptyset$
> **For each** $l, r, w \in \mathbf{S} \setminus \{1\}$ s.t. $T(j) = lw = wr$ **do**
> $OBS(j) = OBS(j) \cup \{(j,j;1,r;l,1)\}$
> **For each** $i < j$ **do**
>   **If** $T(i)$ is multiple of $T(j)$ **then**
>   **For each** $l, r \in \mathbf{S}$ s.t. $T(i) = lT(j)r$ **do**
> $OBS(j) = OBS(j) \cup \{(i,j;l,r;1,1)\}$
>   **For each** $l, r, w \in \mathbf{S} \setminus \{1\}$ s.t. $T(j) = lw, T(i) = wr$ **do**
> $OBS(j) = OBS(j) \cup \{(i,j;1,r;l,1)\}$
>   **For each** $l, r, w \in \mathbf{S} \setminus \{1\}$ s.t. $T(i) = lw, T(j) = wr$ **do**

$OBS(j) = OBS(j) \cup \{(i, j; l, 1; 1, r)\}$
Remove from $OBS(j)$ all elements $(i, j; l, r; \lambda, \rho)$ s.t. (l, r) is not in a minimal basis of $T_j(G)$
Let $\mathcal{S} := \{(l, r) : (i, j; l, r; \lambda, \rho) \in OBS(j)\}$
For each $s = (l, r) \in \mathcal{S}$ **do**
Choose $(i_s, j; l_s, r_s; \lambda_s, \rho_s) \in OBS(j)$ s.t. $l = l_s, r = r_s$
$OBS(j) = \{(i_s, j; l_s, r_s; \lambda_s, \rho_s) : s \in \mathcal{S}\}$

Example We can now go back to our example with the assurance of dealing with finitely many objects only, and the result will be much more easy. Again $g_1 = aba - b, g_2 := bab - b$; we will consider moreover also $g_3 := bb - ab, g_4 := ba - ab, g_5 := aab - b$, and we set $G = \{g_1, g_2, g_3, g_4, g_5\}$, so that

$T(1) = aba, T(2) = bab, T(3) = bb, T(4) = ba, T(5) = aab$

We have:

$OBS(1) = \{(1, 1; 1, ba; ab, 1)\}$ from $abT(1) = ababa = T(1)ba$

$OBS(2) = \{(2, 2; 1, ab; ba, 1), (1, 2; a, 1; 1, b), (1, 2; 1, a; b, 1)\}$ from $baT(2) = babab = T(2)ab$, $T(1)b = abab = aT(2)$ and $bT(1) = baba = T(2)a$
from which we remove $(2, 2; 1, ab; ba, 1)$, since $(1, ab) = (1, a)b$ is a redundant generator of $T_2(G)$

$OBS(3) = \{(3, 3; 1, b; b, 1), (2, 3; 1, ab; b, 1), (2, 3; ba, 1; 1, b)\}$ from $bT(3) = bbb = T(3)b$, $bT(2) = bbab = T(3)ab$ and $T(2)b = babb = baT(3)$

$OBS(4) = \{(1, 4; a, 1; 1, 1), (1, 4; 1, ba; b, 1), (2, 4; 1, b; 1, 1), (2, 4; ba, 1; 1, a), (3, 4; b, 1; 1, a)\}$
from which we remove $(1, 4; 1, ba; b, 1)$ since $(1, ba) = (1, b)a$, and $(2, 4; ba, 1; 1, a)$ since $(ba, 1) = b(a, 1)$

$OBS(5) = \{(1, 5; 1, a; a, 1), (1, 5; ab, 1; 1, ab), (2, 5; 1, ab; aa, 1), (3, 5; 1, b; aa, 1), (4, 5; b, 1; 1, ab), (4, 5; 1, a; aa, 1)\}$
from which we remove $(1, 5; ab, 1; 1, ab), (2, 5; 1, ab; aa, 1)$ since $(ab, 1) = a(b, 1)$ and $(1, ab) = (1, a)b$, and $(4, 5; 1, a; aa, 1)$, because the minimal generator $(1, a)$ is already taken care of by $(1, 5; 1, a; a, 1)$. ∎

Lemma 5.4 has reduced the problem of testing if a finite set is a Gröbner basis to a finite problem, but we still would save unnecessary computations, so we turn to a generalization of Lemma 3.4. Preparing the setting to state it is a bit more complex than in the commutative case, but the test which we will derive, will be as easy.

Lemma 5.5 *Let $i, k < j$, $l, r \in \mathbf{S}$ be s.t. $lT(i) = T(k)r$. Let $w_l \neq 1, w_r \neq 1$ be s.t. $lT(i) = T(k)r = w_lT(j)w_r$. Then either:*

1) there are λ and ρ s.t.$l = w_l\lambda$, $r = \rho w_r$, $\lambda T(i) = T(j)w_r$, $T(k)\rho = w_lT(j)$. In this case:
- *$S(i, k; 1, r; l, 1) = w_lS(i, j; 1, w_r; \lambda, 1) - S(k, j; w_l, 1; 1, \rho)w_r$*
- *If $S(i, j; 1, w_r; \lambda, 1)$ and $S(k, j; w_l, 1; 1, \rho)$ have weak Gröbner representations then $S(i, k; 1, r; l, 1)$ has a weak Gröbner representation.*

2) there are λ and ρ s.t. $w_l = l\lambda$, $r = \rho w_r$, $T(i) = \lambda T(j)w_r$, $T(k)\rho = w_lT(j)$. In this case:
- *$S(i, k; 1, r; l, 1) = lS(i, j; \lambda, w_r; 1, 1) - S(k, j; w_l, 1; 1, \rho)w_r$*
- *If $S(i, j; \lambda, w_r; 1, 1)$ and $S(k, j; w_l, 1; 1, \rho)$ have weak Gröbner representations then $S(i, k; 1, r; l, 1)$ has a weak Gröbner representation.*

3) there are λ and ρ s.t. $l = w_l\lambda$, $w_r = \rho r$, $\lambda T(i) = T(j)w_r$, $T(k) = w_lT(j)\rho$. In this case:
- *$S(i, k; 1, r; l, 1) = w_lS(i, j; 1, w_r; \lambda, 1) - S(k, j; w_l, \rho; 1, 1)r$*
- *If $S(i, j; 1, w_r; \lambda, 1)$ and $S(k, j; w_l, \rho; 1, 1)$ have weak Gröbner representations then $S(i, k; 1, r; l, 1)$ has a weak Gröbner representation.*

4) there are λ and ρ s.t. $w_l = l\lambda$, $w_r = \rho r$, $T(i) = \lambda T(j)w_r$, $T(k) = w_lT(j)\rho$. In this case:
- *$S(i, k; 1, r; l, 1) = lS(i, j; \lambda, w_r; 1, 1) - S(k, j; w_l, \rho; 1, 1)r$*
- *If $S(i, j; \lambda, w_r; 1, 1)$ and $S(k, j; w_l, \rho; 1, 1)$ have weak Gröbner representations then $S(i, k; 1, r; l, 1)$ has a weak Gröbner representation.*

Buchberger Algorithm

As a consequence of the previous results, the following procedure, *if it halts*, computes a Gröbner basis of an ideal $I \subset k\langle\mathbf{S}\rangle$, given a finite basis F of it; we will assume F to be given as an ordered set $\{g_1, \ldots, g_s\}$, s.t. $lc(g_i) = 1$, $\forall i$ and no $T(g_i)$ is multiple of some $T(g_j)$, $j \neq i$.

$G :=$ **Gröbner**(F)

$G = \emptyset$, $OBS = \emptyset$
For $t = 1, \ldots, s$ **do**
  $RED := \{(i,k;l,r;\lambda,\rho) \in OBS : \exists w_l, w_r \in \mathbf{S} \setminus \{1\}$ s.t. $lT(k)r = w_l T(t) w_r\}$
  $OBS := OBS \setminus RED$
  $G := G \cup \{g_t\}$
  $OBS := OBS \cup OBS(t)$
While $OBS \neq \emptyset$ **do**
  Choose $(i,j;l,r;\lambda,\rho) \in OBS$
  $OBS := OBS \setminus \{(i,j;l,r;\lambda,\rho)\}$
  $h :=$ **NormalForm**$(S(i,j;l,r;\lambda,\rho), G)$
  If $h \neq 0$ **then**
    $t := t+1$
    $g_t := h$
    $G := G \cup \{g_t\}$
    $RED := \{(i,k;l,r;\lambda,\rho) \in OBS : \exists w_l, w_r \in \mathbf{S} \setminus \{1\}$ s.t. $lT(k)r = w_l T(t) w_r\}$
    $OBS := OBS \setminus RED$
    $OBS := OBS \cup OBS(t)$

Example We are going to compute here the Gröbner basis of the ideal $I = (g_1, g_2)$. It will turn that the output is $\{g_1, \ldots, g_5\}$ so that the computations we have performed in the last example take care of the combinatorial part of the algorithm (i.e. the computation of OBS). The initialization phase gives the following set of S-elements to be tested:

$OBS = OBS(1) \cup OBS(2) = \{(1,1;1,ba;ab,1),(1,2;a,1;1,b),(1,2;1,a;b,1)\}$
from which we can however remove $(1,1;1,ba;ab,1)$, since $T(1)ba = ababa = aT(2)a$.

We choose $(i,j;l,r;\lambda,\rho) = (1,2;a,1;1,b)$ and compute $S(1,2;a,1;1,b) = ag_2 - g_1 b = bb - ab =: g_3$, which is appended to G.

We update OBS appending $OBS(3)$ to it: we have

$OBS = \{(1,2;1,a;b,1),(3,3;1,b;b,1),(2,3;1,ab;b,1),(2,3;ba,1;1,b)\}$

We choose now $(i,j;l,r;\lambda,\rho) = (1,2;1,a;b,1)$; $S(1,2;1,a;b,1) = g_2 a - bg_1 = bb - ba$; its normal form is $h = -ba + ab$ so we append $g_4 = ba - ab$ to G.

After removing $(2,3;1,ab;b,1)$ from OBS, because $T(3)ab = bbab = bT(4)b$, we append $OBS(4)$ to it, obtaining

$OBS = \{(3,3;1,b;b,1),(2,3;ba,1;1,b),(1,4;a,1;1,1),(2,4;1,b;1,1),(3,4;b,1;1,a)\}$

We choose now $(i,j;l,r;\lambda,\rho) = (3,3;1,b;b,1)$;$S(3,3;1,b;b,1) = g_3 b - bg_3 = bab - aab$ has normal form $b - aab$ so $g_5 = aab - b$ is appended to G and OBS is updated to:

$OBS = \{(2,3;ba,1;1,b),\ (1,4;a,1;1,1),\ (2,4;1,b;1,1),\ (3,4;b,1;1,a),\ (1,5;1,a;a,1),\ (3,5;1,b;aa,1),\ (4,5;b,1;1,ab)\}$

Since the normal forms of all remaining S-elements are 0, a Gröbner basis of I is $\{g_1, \ldots, g_5\}$ and, removing redundant elements, $\{bb - ab, ba - ab, aab - b\}$ ▮

6 Termination of Buchberger Algorithm

As we have already stressed several times, we cannot hope to have a terminating Buchberger Algorithm in $k\langle a_1, \ldots, a_n \rangle$, because this would give a computational solution to the undecidable word problem. The best we can hope for is a procedure, which receiving as input a finite set of elements $\{g_1, \ldots, g_s\} \in k\langle \mathbf{S} \rangle$ defining an ideal I:

- in case I has a finite Gröbner basis, halts returning such a finite Gröbner basis
- otherwise, it produces an infinite sequence of elements $g_1, \ldots, g_s, g_{s+1}, \ldots, g_i, \ldots$ s.t. the infinite set $\{g_i : i \in \mathbb{N}\}$ is a Gröbner basis of I.

One could actually hope for more, e.g. for an algorithm which receiving as input $\{g_1, \ldots, g_s\} \in k\langle \mathbf{S} \rangle$ and $D \in \mathbb{N}$ returns the set $\{g \in G, deg(g) \leq D\}$ where G is the reduced Gröbner basis of I. This hope is however unfounded; in fact this would allow to solve the following problem:

let $<$ be an ordering compatible with the degree (i.e. s.t. $t_1 < t_2$ whenever $deg(t_1) < deg(t_2)$); given $\{g_1, \ldots, g_s\} \in k\langle \mathbf{S} \rangle$ defining an ideal I and $t \in \mathbf{S}$, compute $\{g \in G, T(g) \leq t\}$ where G is the reduced Gröbner basis of I.

just by computing $\{g \in G, deg(g) \leq deg(t)\}$ and this would in turn allow to solve the ideal membership problem; in fact the computation of $Can(f, I)$ doesn't require a whole Gröbner basis of I but only those elements g s.t. $T(g) \leq T(f)$.

There is however an important subcase in which this stronger requirement can be satisfied, the case of *homogeneous* ideals I, i.e. ideals generated by elements $\sum c_i t_i$ s.t. $deg(t_i) = d$ for each i, $c_i \neq 0$.

In our presentation of Buchberger Algorithm, we have never discussed how to perform the instruction **Choose** $(i, j; l, r; \lambda, \rho) \in OBS$; it is clear that, in case the procedure we have described halts, any choice is equally fine to guarantee correctness. In the polynomial ring case (where there is no termination problem), a lot of research has been however dedicated to strategies for implementing this **Choose** instruction, since bad strategies can have a dramatic effect on the time-space performance of the algorithm: the up-to-date state of the algorithm is presented in [**GMNRT**] and it is the basis of all the best implementations. What is a question of efficiency in the polynomial ring case, becomes here a question of survival, as the following example shows:

Example We work on the ring $k\langle a, b, c, d, e, f\rangle$ and the following ordering:

$t_1 < t_2$ if and only if either $wt(t_1) < wt(t_2)$ or $wt(t_1) = wt(t_2)$, t_1 is lexicographically less than t_2 where the ordering on the variables is $a < b < c < d < e < f$ and wt is defined by

$$wt(a) = 3 \quad wt(b) = wt(c) = wt(d) = wt(e) = wt(f) = 1$$

and multiplicatively extended to the semigroup. We will choose the ideal $I = (f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ where

$$f_1 = ca - ac, f_2 = da - ad, f_3 = ba - b^2c, f_4 = be - b, f_5 = bf - b, f_6 = ef - b, f_7 = bcd$$

$$T(f_1) = ca, T(f_2) = da, T(f_3) = ba, T(f_4) = be, T(f_5) = bf, T(f_6) = ef, T(f_7) = bcd$$

A set of minimal obstructions for $\{f_1, \dots, f_7\}$ is given by $\{(4, 6; b, 1; 1, f), (2, 7; 1, a; bc, 1)\}$.

Choosing $(2, 7; 1, a; bc, 1)$; we have:

$S(2, 7; 1, a; bc, 1) = f_7 a - bc f_2 = bcad = bf_1 d + bacd = bf_1 d + f_3 cd + b^2c^2d$

so $f_8 := b^2c^2d$ is a normal form of $S(2, 7; 1, a; bc, 1)$ and is added to the basis, together with the new obstruction $(2, 8; 1, a; b^2c^2, 1)$; if we choose this one, we get:

$S(2, 8; 1, a; b^2c^2, 1) = f_8 a - b^2c^2 f_2 = b^2c^2ad \rightarrow b^2ac^2d = bf_3c^2d + b^3c^3d, f_9 := b^3c^3d$

where we use the notation $t_1 \rightarrow t_2$ to mean that $t_1 - t_2 \in I$, $t_1 > t_2$, i.e. to collapse steps of the normal form computation.

Let us agree that our strategy is to choose the last obstruction in the list; it is then easy to realize that the computation will be infinite and have the following pattern, where $f_{i+6} := b^ic^id$

$OBS = \{(4, 6; b, 1; 1, f), (2, i+6; 1, a; b^ic^i, 1)\}$

$S(2, i+6; 1, a; b^ic^i, 1) = f_{i+6}a - b^ic^if_2 = b^ic^iad \rightarrow b^iac^id = b^{i-1}f_3c^id + b^{i+1}c^{i+1}d, f_{i+7} := b^{i+1}c^{i+1}d$

$OBS = \{(4, 6; b, 1; 1, f), (2, i+7; 1, a; b^{i+1}c^{i+1}, 1)\}$

going on forever without ever computing $S(4, 6; b, 1; 1, f)$ whose computation would give:

$S(4, 6; b, 1; 1, f) = bf_6 - f_4 f = bf - b^2 = f_5 - b^2 + b$

returning $g = b^2 - b$, by which we find $f_{i+7} = f_{i+6} + gb^{i-1}c^{i+1}d$ for each $i \geq 1$.

If we change our strategy so that $S(4, 6; b, 1; 1, f)$ is eventually computed, as remarked above all elements f_{i+7} for $i \geq 1$ are redundant in the Gröbner basis.

The introduction of g requires the computation of the following S-elements: $ga - bf_3$, $ge - bf_4$, $gf - bf_5$, $gcd - bf_7$, $gb^{i-2}c^id - f_{i+7}$ for $i \geq 1$, whose normal forms are all 0, so that the Gröbner basis is actually finite and consisting of $\{f_1, f_2, f_3, f_4, f_5, f_6, f_7, g\}$ ∎

The previous example shows a reason why a computation could go on forever even in the case the minimal Gröbner basis is finite, in which case obviously even the infinite set of elements produced by the algorithm fails to be a Gröbner basis; the reason is simply the indefinite postponing of some computation. It turns out that the remedy to this is just to arrange the computation so that each obstruction which is produced by the algorithm is definitely processed at some finite time. In order to formalize this argument let us add a counter to the algorithm presented in the previous paragraph and let us make a copy of the status of the data each time the counter is updated. So the algorithm will look like:

$G := \textbf{Gröbner}(F)$
$G = \emptyset$, $OBS = \emptyset$
For $t = 1, \ldots, s$ **do**
  $RED := \{(i,k;l,r;\lambda,\rho) \in OBS : \exists w_l, w_r \in \mathbf{S} \setminus \{1\}$ s.t. $lT(k)r = w_l T(t) w_r\}$
  $OBS := OBS \setminus RED$
  $G := G \cup \{g_t\}$
  $OBS := OBS \cup OBS(t)$
* $Count := 0$
While $OBS \neq \emptyset$ **do**
* $Count := Count + 1, OBS_{Count} := OBS, G_{Count} := G$
  Choose $(i,j;l,r;\lambda,\rho) \in OBS$
  $OBS := OBS \setminus \{(i,j;l,r;\lambda,\rho)\}$
  $h := \textbf{NormalForm}(S(i,j;l,r;\lambda,\rho), G)$
  If $h \neq 0$ **then**
    $t := t + 1$
    $g_t := h$
    $G := G \cup \{g_t\}$
    $RED := \{(i,k;l,r;\lambda,\rho) \in OBS : \exists w_l, w_r \in \mathbf{S} \setminus \{1\}$ s.t. $lT(k)r = w_l T(t) w_r\}$
    $OBS := OBS \setminus RED$
    $OBS := OBS \cup OBS(t)$

where we have put a star in front of the two instructions which have been added.

Now let us define: $OBS_\infty := \cup_{i=1}^{\infty} OBS_i$, $G_\infty := \cup_{i=1}^{\infty} G_i$; to make things formally precise, in case the algorithm halts, in which case $Count$ has a maximal value M, we define $G_i := G_M$ and $OBS_i := OBS_M$ for $i > M$. We can then prove the following:

Lemma 6.1 *The following statements are equivalent:*
1) The algorithm halts
2) there is M s.t. $OBS_M = \emptyset$
3) there is N s.t. G_N is a finite Gröbner basis of I

Proof: 1) $\Leftrightarrow$ 2) is just an obvious remark on the behaviour of the algorithm.

1) $\Rightarrow$ 3) is the correctness proof of the previous paragraph.

3) $\Rightarrow$ 2) If G_N is a Gröbner basis of I, then for each $(i,j;l,r;\lambda,\rho) \in OBS_N$, $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation. Therefore for $\epsilon > N$, one has $G_\epsilon = G_N$ and the cardinality of OBS_ϵ is one less than the one of $OBS_{\epsilon-1}$. ▮

Proposition 6.1 *If for each $\sigma \in OBS_\infty$ there is ϵ_σ such that $\sigma \notin OBS_\eta$ for $\eta > \epsilon_\sigma$ then:*
1) G_∞ is a Gröbner basis of I
2) I has a finite Gröbner basis if and only if there is N such that $G_N = G_\infty$ is a Gröbner basis of I in which case the algorithm halts returning G_N.

Proof: 1) Let $\sigma = (i,j;l,r;\lambda,\rho) \in OBS_\infty$; if there is ϵ such that $\sigma \notin OBS_\eta$ for $\eta \geq \epsilon$, then $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation in terms of G_ϵ.

The assumption implies therefore that for each $(i,j;l,r;\lambda,\rho) \in OBS_\infty$, $S(i,j;l,r;\lambda,\rho)$ has a weak Gröbner representation in terms of some G_ϵ and so of G_∞. Because of Theorem 5.1, this implies the thesis.

2) Assume that I has a finite Gröbner basis $G = \{f_1, \ldots, f_k\}$. Since G_∞ is a Gröbner basis of I, by definition for each $j = 1 \ldots k$ there is $h_j \in G_\infty$ s.t. $T(h_j)$ divides $T(f_j)$ and there is N s.t. $h_j \in G_N$ for each $j = 1 \ldots k$. Therefore $T(I) = T(G) \subseteq T(G_N) \subseteq T(G_\infty) = T(I)$, proving that G_N is a Gröbner basis of I. Termination of the algorithm is then guaranteed by Lemma 6.1 ▮

There are plenty of obvious strategies for realizing the **Choose** instruction which guarantee the validity of the assumption of Proposition 6.1; for instance one can choose at each step $(i,j;l,r;\lambda,\rho)$ s.t. j is minimal; in case $<$ is *sequential*, i.e. for each $t \in \mathbf{S}$ the set $\{t' \in \mathbf{S} : t' < t\}$ is finite, one can choose $(i,j;l,r;\lambda,\rho)$ s.t. $lT(j)r = \lambda T(i)\rho$ is minimal.

Assume now that I is homogeneous, so w.l.o.g. we can assume the input $\{g_1, \ldots, g_s\}$ consists of homogeneous elements. Remark that:

- if g_i, g_j are homogeneous, then $h := S(i,j;l,r;\lambda;\rho)$ is homogeneous and $deg(h) = deg(lT(j)r) \geq max(deg(g_i), deg(g_j))$
- if G is a set of homogeneous elements and f is homogeneous, then $h :=$ **NormalForm**(f, G), if not zero, is homogeneous and $deg(h) = deg(f)$.
- the set $\{t \in \mathbf{S} : deg(t) \leq D\}$ is finite for each D.

Therefore for an obstruction $\sigma = (i,j;l,r;\lambda,\rho)$ let us denote $deg(\sigma) := deg(lT(j)r)$; if at each step we choose $\sigma \in OBS$ s.t. $deg(\sigma)$ is minimal and we denote by $D_\epsilon := min(deg(\sigma) : \sigma \in OBS_\epsilon)$ (putting $D_\epsilon := \infty$ if $OBS_\epsilon = \emptyset$), then D_ϵ is a non-decreasing function; therefore for each D there will be M s.t. $D_M > D$. This proves that

Proposition 6.2 *If I is homogeneous, then for each $D \in \mathbb{N}$, it is possible to compute $\{g \in G : deg(g) \leq D\}$, where G is the reduced Gröbner basis of I.*

7 Gröbner Bases in semigroup rings

The aim of this paragraph is to give a sketch of the argument which leads to a proof of the claim at the end of Section 1. Since I don't know any relevant application of Gröbner basis over a semigroup ring $k\langle\mathbf{S}\rangle$ other than polynomial rings and non-commutative free algebras, most of the details will be omitted.

The reader will easily verify that all the arguments developed up to now apply to this more general case, assuming that we are able to provide, given $G := \{g_1, \ldots, g_s\} \subset k\langle\mathbf{S}\rangle$, a minimal set of S-elements so that:

- if each of them has a weak Gröbner representation, then G is a Gröbner basis
- any S-element not having a weak Gröbner representation gives rise to a new element in the Gröbner basis.

This in turn just requires to produce, setting $t_i := T(g_i)$ and assuming $lc(g_i) = 1$, minimal sets of self-obstructions for t_s and minimal sets of obstructions for t_s w.r.t. $t_1, \ldots, t_{s-1}$.

Let us survey the different cases.

Two-sided ideals

Let us define:

$ST(t_j) := \{(\lambda, \rho) : \exists (l,r)\ lt_j r = \lambda t_j \rho, r < \rho\}$ which is an ideal in $\mathbf{S} \otimes \mathbf{S}$.

$T_j := \{(l,r) : lt_j r \in (t_1, \ldots, t_{j-1})\} \cup ST(t_j)$, an ideal in $\mathbf{S} \otimes \mathbf{S}$.

For each generator (l_σ, r_σ) in a minimal basis of T_j, we have to choose $i_\sigma, \lambda_\sigma, \rho_\sigma$ s.t.

$l_\sigma T(j) r_\sigma = \lambda_\sigma T(i_\sigma) \rho_\sigma \qquad i_\sigma < j$ or $i_\sigma = j$ and $\rho_\sigma < r_\sigma$

and to set $MIN(j) := \{(i_\sigma, j; l_\sigma, r_\sigma; \lambda_\sigma, \rho_\sigma)\}$, $\forall (i,j;l,r;\lambda,\rho) \in MIN(j)$, $S(i,j;l,r;\lambda,\rho) := lg_j r - \lambda g_i \rho$

We have moreover to remove *trivial* elements i.e. those $(i,j;l,r;\lambda,\rho) \in MIN(j)$ s.t. there is w s.t. either $l = \lambda T(i) w$ (and so $\rho = wT(j)r$) or $\lambda = lT(j)w$ (and so $r = wT(j)\rho$).

Finally, let us set $\mathcal{S} := \{(i,j;l,r;\lambda,\rho) \in MIN(j), j = 1 \ldots s$ and non trivial$\}$.

Left ideals

Here we define:

$T_j := \{t \in \mathbf{S}$ s.t. $tt_j \in (t_1, \ldots, t_{j-1})\}$, a semigroup ideal

and for each minimal generator t_σ of T_j we choose $\tau_\sigma \in \mathbf{S}, i_\sigma < j$ s.t. $t_\sigma t_j = \tau_\sigma t_{i_\sigma}$. Then we set $MIN(j) := \{(i_\sigma, j; \tau_\sigma, t_\sigma)\}$, and $\forall (i,j;\tau,t) \in MIN(j), S(i,j;\tau,t) := tg_j - \tau g_i$.

I don't know if and how trivial elements can be defined in this case, so let us set $\mathcal{S} := \{(i,j;\tau,t) \in MIN(j), j = 1 \ldots s\}$.

Ideals in commutative semigroups

Here we define:

$T_j := \{t \in \mathbf{S}$ s.t. $tt_j \in (t_1, \ldots, t_{j-1})\}$,a semigroup ideal

and for each minimal generator t_σ of T_j we choose $\tau_\sigma \in \mathbf{S}, i_\sigma < j$ s.t. $t_\sigma t_j = \tau_\sigma t_{i_\sigma}$. Then we set $MIN(j) := \{(i_\sigma, j; \tau_\sigma, t_\sigma)\}$, and $\forall (i,j;\tau,t) \in MIN(j), S(i,j;\tau,t) := tg_j - \tau g_i$.

Trivial elements are those $(i,j;\tau,t)$ s.t. t_i divides t.

Finally let us set $\mathcal{S} := \{(i,j;\tau,t) \in MIN(j), j = 1 \ldots s$ and non trivial$\}$.

Computability of Gröbner bases

Because of the following straightforward generalization of Theorems 3.1 and 5.1

Theorem 7.1 *Let $G = (g_1, \ldots, g_s)$ be a basis of $I \subset k\langle \mathbf{S} \rangle$, where $lc(g_i) = 1$ for each i and let $\mathcal{S}$ be defined as above.*

G is a Gröbner basis of I if and only if for each $\sigma \in \mathcal{S}$, $S(\sigma)$ has a weak Gröbner representation.

with the proper modifications, the algorithm described in Section 5 and with the termination strategy outlined in Section 6, correctly "computes" a Gröbner basis of I, provided the following assumption, which depends only on $\mathbf{S}$, holds:

$\mathcal{S}$ is finite and computable

so that, under this assumption on $\mathbf{S}$:

Theorem 7.2 *If $k\langle \mathbf{S} \rangle$ is noetherian then for each ideal I it is possible to compute a Gröbner basis of I.*

If I has a finite Gröbner basis w.r.t. $<$, then there is an algorithm to compute it.

If $\mathbf{S}$ is graded, I is homogeneous and $<$ is a degree-compatible ordering, then for each $t \in \mathbf{S}$ it is possible to compute a Gröbner basis truncated at t.

8 Gröbner Bases in differential algebras

Weyl Algebras

If we consider partial derivatives $\partial_{X_i} : k[X_1, \ldots, X_n] \mapsto k[X_1, \ldots, X_n]$ and we iterate them we obtain the semigroup of all partial derivatives of any order, which is obviously isomorphic to $\mathbf{T}$, since $\partial_{X_i}\partial_{X_j} = \partial_{X_j}\partial_{X_i}$.

A *differential operator with coefficients in* $k[X_1, \ldots, X_n]$, $\Delta : k[X_1, \ldots, X_n] \mapsto k[X_1, \ldots, X_n]$ is any linear combination of them with coefficients in $k[X_1, \ldots, X_n]$; the set of all such differential operators is obviously a k-vector space, with basis $\{X_1^{a_1} \cdots X_n^{a_n} \partial_{X_1}^{\alpha_1} \cdots \partial_{X_n}^{\alpha_n}\}$ and it is a k-algebra if it is endowed by the product given by composition.

Since, for each $f \in k[X_1, \ldots, X_n]$:

$\partial_{X_i}(X_i f) = X_i \partial_{X_i}(f) + f \quad \partial_{X_i}(X_j f) = X_j \partial_{X_i}(f), j \neq i$

this algebra is isomorphic to $\mathcal{A}_n := k\langle X_1, \ldots, X_n, D_1, \ldots, D_n \rangle / \mathcal{I}$ where $\mathcal{I}$ is the two-sided ideal generated by $\{D_i X_i - X_i D_i - 1 : i = 1 \ldots n\} \cup \{D_i X_j - X_j D_i : i \neq j\} \cup \{X_j X_i - X_i X_j, D_j D_i - D_i D_j : 1 \leq i < j \leq n\}$, which is called *Weyl algebra*.

It is an easy exercise to verify that the above is a Gröbner basis of $\mathcal{I}$ for the *deglex* ordering, so that $O(I) = \{X_1^{a_1} \cdots X_n^{a_n} D_1^{\alpha_1} \cdots D_n^{\alpha_n}\}$, implying the Poincaré-Birkhoff-Witt Theorem, which states that "commutative" terms are a k-basis of $\mathcal{A}_n$.

Enveloping algebras of Lie Algebras

Another ring of interest in differential algebra is the *enveloping algebra of a Lie Algebra*, which is defined as follows; one starts with a finite dimensional Lie Algebra $\mathcal{L}$ i.e. a finite dimensional k-vector space endowed with the *bracket* operator $[\bullet, \bullet]$ which satisfies:

1) $[c_1 v_1 + c_2 v_2, v] = c_1 [v_1, v] + c_2 [v_2, v]$, $\forall c_i \in k, v_i, v \in \mathcal{L}$
2) $[u, v] = -[v, u]$, $\forall u, v \in \mathcal{L}$
3) $[u_1, [u_2, u_3]] - [u_2, [u_1, u_3]] + [u_3, [u_1, u_2]] = 0$, $\forall u_i \in \mathcal{L}$.

Let $\{X_1, \ldots, X_n\}$ be a basis of $\mathcal{L}$ and consider the k-algebra $\mathcal{U}(\mathcal{L}) := k\langle X_1, \ldots, X_n \rangle / \mathcal{I}$ where $\mathcal{I}$ is generated by $\{p_{ji} : 1 \leq i < j \leq n\}$, where $p_{ji} := X_j X_i - X_i X_j - [X_i, X_j]$. Because of 1) and 2), the definition of $\mathcal{U}(\mathcal{L})$ is independent of the choice of a basis of $\mathcal{L}$.

Again, one can prove that the given basis is a Gröbner basis of $\mathcal{I}$ for the *deglex* ordering, so that $O(I) = \{X_1^{a_1} \cdots X_n^{a_n}\}$, implying the Poincaré-Birkhoff-Witt Theorem, which states that "commutative" terms are a k-basis of $\mathcal{U}(\mathcal{L})$.

The proof of that is however less immediate, but another good exercise for the theory developed so far: one has to show that the following S-elements have weak Gröbner representations

$$p_{jk} X_i - X_k p_{ji} = X_k X_i X_j - X_j X_k X_i + X_k [X_i, X_j] - [X_j, X_k] X_i \quad i < j < k$$

An easy computation gives:

$p_{jk} X_i - X_k p_{ji} = X_k X_i X_j - X_j X_k X_i + X_k [X_i, X_j] - [X_j, X_k] X_i =$
$\quad = p_{ik} X_j - X_j p_{ik} + X_i p_{jk} - p_{ij} X_k - [X_k, [X_i, X_j]] + [X_j, [X_i, X_k]] - [X_i, [X_j, X_k]] =$

$= p_{ik}X_j - X_jp_{ik} + X_ip_{jk} - p_{ij}X_k$
since $[X_k, [X_i, X_j]] - [X_j, [X_i, X_k]] + [X_i, [X_j, X_k]] = 0$

Gröbner bases for differential algebras

As vector spaces both $\mathcal{A}_n$ and $\mathcal{U}(\mathcal{L})$ are therefore isomorphic to a polynomial ring $k\langle\mathbf{T}\rangle$, where $\mathbf{T}$ is a free commutative semigroup; however their ring structure is different. Remark however that:

$\forall l, r \in \mathbf{T}, \forall f, T(lfr) = lT(f)r$

where the product on the left-hand side is the one in the algebra, the one on the right-hand side the one in $\mathbf{T}$.

This is a particular instance of the following situation: we consider an ordered semigroup $\mathbf{S}$ (whose product we denote by concatenation) and we endow the k-vector space $R := Span_k(\mathbf{S})$ of a k-algebra structure by defining a product $\star$ s.t. $\forall l, r \in \mathbf{S}, \forall f \in R\ T(l \star f \star r) = lT(f)r$. Let us denote such a ring $k\langle\mathbf{S}, \star\rangle$.

If $\mathbf{S} = \mathbf{T}$, ordered by $<$, then a k-algebra R satisfying the above is isomorphic to $k\langle X_1, \ldots, X_n\rangle/\mathcal{I}$ where $\mathcal{I}$ is generated by $\{g_{ij} : 1 \leq i < j \leq n\}$, $g_{ij} = X_jX_i - c_{ij}X_iX_j - p_{ij}$ with $c_{ij} \in k - \{0\}$ and p_{ij} a linear combination of "commutative" terms $t \in \mathbf{T} \subset \langle X_1, \ldots, X_n\rangle$ s.t. $T(p_{ij}) < X_iX_j$. Moreover $\{g_{ij}\}$ is a Gröbner basis of $\mathcal{I}$ for some ordering $<'$ on $\langle X_1, \ldots, X_n\rangle$ which agrees with $<$ on $\mathbf{T}$ and s.t. $X_iX_j <' X_jX_i\ \forall i < j$. These rings were introduced and their Gröbner basis theory was first studied in [**KR-W**], where they were called *solvable polynomial rings*

It is easy to realize that the whole theory developed until now doesn't require the ring to be the semigroup ring, but that for its correctness it is sufficient to assume the property that $\forall l, r \in \mathbf{S}, \forall f \in R\ T(l \star f \star r) = lT(f)r$. As a consequence, Buchberger algorithm is directly available for the rings $k\langle\mathbf{S}, \star\rangle$.

We can derive immediately the following consequences:

- Buchberger Algorithm for polynomial rings can be applied verbatim for computing Gröbner bases of left ideals in a solvable polynomial ring R, provided the routine for performing multiplication of elements of R is suitably modified
- in particular solvable polynomial rings are left- (and right-) noetherian.
- even when $I \subset R$ is a two-sided ideal, $T(I)$ is a semigroup ideal in the commutative and noetherian semigroup $\mathbf{T}$, so that R is noetherian

Computing Gröbner bases of two-sided ideals in a solvable polynomial ring is a bit more tricky: the ring being non-commutative, obstructions are to be looked for in $\mathbf{T} \otimes \mathbf{T}$; it is easy however to prove that:

Lemma 8.1 *Let R be a solvable polynomial ring. Let $g_1, \ldots, g_s \in R, T(i) := T(g_i) \in \mathbf{T}$. Denote $O_j(G) := \{(l, 1) \in \mathbf{T} \otimes \mathbf{T}, lT(j) \notin (T(1), \ldots, T(j-1))\}$, $T_j(G) := \{(l, r) \in \mathbf{T} \otimes \mathbf{T} : (l, r) \notin O_j(G)\}$. Then:*

a) $\{l \star g_j : (l, 1) \in O_j(G), j = 1 \ldots s\}$ is the canonical echelon set extracted from $\{l \star g_j \star r : (l, r) \in O_j(G), j = 1 \ldots s\}$

b) $T_j(G)$ is generated by $\{(\frac{T(i,j)}{T(j)}, 1) : i < j\} \cup \{(1, X_i) : i = 1 \ldots n\}$

c) G is a Gröbner basis if and only if both $\frac{T(i,j)}{T(j)} \star g_j - \frac{T(i,j)}{T(i)} \star g_i, 1 \leq i < j \leq s$ and $g_j \star X_i - X_i \star g_j, j = 1 \ldots s, i = 1 \ldots n$ have a weak Gröbner representation (obviously, also in this case, useless S-elements can be removed)

Applications

In view of the similarities for Gröbner bases theory of left ideals in a solvable polynomial ring and of ideals in the polynomial ring, many of the applicative algorithms developed for the latter, can be applied to the former too. For instance, [**Ga2**], where Gröbner bases for Weyl Algebras were introduced, discusses syzygy and Hilbert function computations.

Another application ([**AL1**]) is related to enveloping algebras $\mathcal{U}(\mathcal{L})$: because of the fact that $\forall s, t \in \mathcal{U}(\mathcal{L}), \exists u, v \in \mathcal{U}(\mathcal{L}) : us = vt$, the relation $(a, b) \equiv (c, d) \Leftrightarrow \exists u, v : ua = vc, ub = vd$ is an equivalence relation; the equivalence class of (a, b) is denoted $a^{-1}b$.

The set $\mathcal{Q}(\mathcal{L}) := \mathcal{U}(\mathcal{L}) \times \mathcal{U}(\mathcal{L})/\equiv$ can be endowed with a skew field structure, defining:

$a^{-1}b + c^{-1}d = u^{-1}(sb + td)$ where $u = sa = tc$

$a^{-1}bc^{-1}d = (ua)^{-1}(vd)$ where $ub = vc$

Since the map which associates to each $a \in \mathcal{U}(\mathcal{L})$ the equivalence class of $(1, a)$ is an injective morphism, $\mathcal{Q}(\mathcal{L})$ is the skew-field of left fractions of $\mathcal{U}(\mathcal{L})$.

Effective arithmetics in $\mathcal{Q}(\mathcal{L})$ requires the ability to compute, given $a, b \in \mathcal{U}(\mathcal{L})$, elements $u, v \in \mathcal{U}(\mathcal{L})$ s.t. $ua - vb = 0$. This is equivalent to compute left syzygies of a, b, which can be obtained by a partial computation of the Gröbner basis of the left ideal (a, b).

9 Gröbner Bases of finitely presented algebras

A further generalization

We intend here to give a further generalization of the theory developed in Section 1.

So we start with a set $\mathbf{S}$ s.t. $\mathbf{S} \cup \{0\}$ is a semigroup and which is endowed with a well ordering s.t. $\forall l, r, t_1, t_2 \in \mathbf{S}, t_1 < t_2, lt_1r \neq 0, lt_2r \neq 0 \Rightarrow lt_1r < lt_2r$.

We then consider the k-vector space $Span_k(\mathbf{S})$ and we endow it with a ring structure s.t. its product $\star$ satisfies $\forall l, r \in \mathbf{S}, \forall f \in Span_k(\mathbf{S})$, either $lT(f)r = 0$ or $T(l \star f \star r) = lT(f)r$, where $T(\bullet)$ has the same meaning as in Section 1.

We will call such a ring a *twisted semigroup ring* and denote it $k\langle \mathbf{S}, \star \rangle$. Remark that this is a generalization of the rings considered in the previous section and denoted in the same way. Remark also that the theory holds even if $\mathbf{S}$ doesn't have an identity, provided that everywhere the notation $l \star g \star r$ is understood to mean also $l \star g$ and $g \star r$ (and analogously for ltr).

If $I \subset k\langle \mathbf{S}, \star \rangle$ is an ideal, $T(I) = \{T(f) : f \in I\}$ is such that $T(I) \cup \{0\}$ is a semigroup ideal of $\mathbf{S} \cup \{0\}$ and $O(I) = \mathbf{S} - T(I)$ is an order ideal.

Let us call $G \subset I$ a *Gröbner basis* of I if $(T(g) : g \in G) \cup \{0\} = T(I) \cup \{0\}$. Then the following are direct generalizations of Theorems 1.1 and 1.2:

Proposition 9.1 *The following holds:*

a) $k\langle \mathbf{S}, \star \rangle = I \oplus Span_k(O(I))$

b) for each $f \in k\langle \mathbf{S}, \star \rangle$, *there is a unique* $g := Can(f, I) \in Span_k(O(I))$ *s.t.* $f - g \in I$.

c) The following conditions are equivalent:

1) G *is a Gröbner basis of* I

2) for each $f \in k\langle \mathbf{S}, \star \rangle$:

$$f = g + \sum_{i=0}^{t} c_i l_i \star g_i \star r_i \quad g \in Span_k(O(I)),\ c_i \in k - \{0\},\ l_i, r_i \in \mathbf{S},\ g_i \in G,\ l_i T(g_i) r_i \neq 0$$

$$T(f) \geq l_1 T(g_1) r_1 > \ldots > l_i T(g_i) r_i > l_{i+1} T(g_{i+1}) r_{i+1} > \ldots$$

3) for each $f \in k\langle \mathbf{S}, \star \rangle$, $f \in I$ *if and only if:*

$$f = \sum_{i=0}^{t} c_i l_i \star g_i \star r_i \quad c_i \in k - \{0\},\ l_i, r_i \in \mathbf{S},\ g_i \in G,\ l_i T(g_i) r_i \neq 0$$

$$T(f) = l_1 T(g_1) r_1 > \ldots > l_i T(g_i) r_i > l_{i+1} T(g_{i+1}) r_{i+1} > \ldots$$

Therefore the notion of Gröbner basis can be given under such generality; I don't know however a generalization of Buchberger algorithm in this context.

Gröbner bases of quotient rings

Let $R = k\langle \mathbf{S}, \star \rangle$ be a twisted semigroup ring, let $\mathcal{I} \subset R$ be a two sided ideal. The quotient ring $R/\mathcal{I}$ is then isomorphic as a vector space to $Span_k(O(\mathcal{I}))$. If we endow the latter with a product $\bullet$ defined by $f \bullet g := Can(f \star g, \mathcal{I})$, the two rings can be identified. Under this identification the projection $R \mapsto R/\mathcal{I}$ is the morphism $Can : R \mapsto Span_k(O(\mathcal{I}))$. This identification has the further advantage that $R/\mathcal{I}$ can be identified with a subvector space of R.

Moreover $O(\mathcal{I}) \cup \{0\}$ is the quotient of $\mathbf{S} \cup \{0\}$ by the two-sided ideal $T(\mathcal{I}) \cup \{0\}$, so it is a semigroup; the restriction to $O(\mathcal{I})$ of the well ordering on $\mathbf{S}$ satisfies $\forall l, r, t_1, t_2 \in O(\mathcal{I}), t_1 < t_2, lt_1 r \neq 0, lt_2 r \neq 0 \Rightarrow lt_1 r < lt_2 r$, so that $k\langle O(\mathcal{I}), \bullet\rangle$ is a twisted semigroup ring.

Let $g_1, \ldots, g_s \in Span_k(O(\mathcal{I}))$ and let I be the ideal they generate in $k\langle O(\mathcal{I}), \bullet\rangle$ and I_0 the ideal $\mathcal{I} + (g_1, \ldots, g_s)$ in R so that $I_0 = Can^{-1}(I)$ and $Span_k(O(\mathcal{I}))/I = R/I_0$.

Since $\mathcal{I} \subset I_0$, $O(I_0) \subset O(\mathcal{I})$. Moreover since $R/\mathcal{I}$ is identified with the subvector space $Span_k(O(\mathcal{I}))$ of R, one has that $I = I_0 \cap Span_k(O(\mathcal{I}))$. As a consequence we obtain:

Proposition 9.2 *$Span_k(O(\mathcal{I})) = I \oplus Span_k(O(I_0))$; $T(I_0) = T(I) \cup T(\mathcal{I})$*

Proof: By Theorem 1.1 $R = I_0 \oplus Span_k(O(I_0))$, so that

$$Span_k(O(\mathcal{I})) = R \cap Span_k(O(\mathcal{I})) = I_0 \cap Span_k(O(\mathcal{I})) \oplus Span_k(O(I_0)) \cap Span_k(O(\mathcal{I})) = I \oplus Span_k(O(I_0))$$

The second equality is then obvious ▮
which in turn implies:

Proposition 9.3 *Let $\mathcal{F}$ be the reduced Gröbner basis of $\mathcal{I}$, G_0 the reduced Gröbner basis of I_0. Then:*
1) if $g \in G_0$ either $T(g) \in T(\mathcal{I})$ or $g \in Span_k(O(\mathcal{I}))$
2) $G := G_0 \cap Span_k(O(\mathcal{I}))$ is the reduced Gröbner basis of I
3) for each $f \in Span_k(O(\mathcal{I}))$: $Can(f, I) = Can(f, I_0)$
4) $\mathcal{F} \cup G$ is a Gröbner basis of I_0

Proof: 1) is obvious and 3) is an immediate consequence of 2).

Ad 2), let $t \in T(I)$ and let $g \in G_0$ be s.t. $T(g)$ divides t; since $t \in O(\mathcal{I})$, then $T(g) \in O(\mathcal{I})$ too, and by 1), $g \in G$.

Ad 4), $T(I_0) = T(\mathcal{I}) \cup T(I) = T(\mathcal{F}) \cup T(G) = T(\mathcal{F} \cup G)$. ▮

Therefore if Gröbner bases for two-sided ideals can be "computed" (in the sense of Section 6) in $k\langle\mathbf{S}, \star\rangle$ they can be "computed" in any quotient of $k\langle\mathbf{S}, \star\rangle$.

Since each finitely presented algebra is the quotient of a free non-comutative algebra, we can conclude our Gröbner basis theory with the mathematically nice result that:

Theorem 9.1 *Gröbner bases for two-sided ideals can be defined and "computed" in each finitely presented algebra*

The result must however be carefully interpreted; for instance, since $k[a_1, \ldots, a_n]$ is the quotient of $k\langle a_1, \ldots, a_n\rangle$ by the two-sided ideal $(a_2 a_1 - a_1 a_2, \ldots, a_n a_{n-1} - a_{n-1} a_n)$, the theory of this section can be applied to it; however the resulting notion of Gröbner basis is *not* the classical one; it is the one which interprets $k[a_1, \ldots, a_n]$ as a twisted semigroup ring over the semigroup $(\mathbf{T} \cup \{0\}, \circ)$ which is the quotient of $\mathbf{S}$ by the ideal $(a_j a_i : i < j)$, so that e.g. $a_2 \circ a_1 = 0$ and the "Gröbner basis" of $(a_1 a_3)$ is $\{a_1 a_2^i a_3 : i \geq 0\}$. It is however possible to interpret the classical notion of Gröbner basis for $k[a_1, \ldots, a_n]$ by interpreting it as a quotient of $k\langle a_1, \ldots, a_n\rangle$, but this requires a further generalization of the theory, which is detailed in **[M4]**.

This quite contrived example aims to make the point that general Gröbner basis theories (like the very general Theorem 9.1) are probably not so relevant from a computational point of view, and that it is in any case of interest to look for specialized procedures for Gröbner basis computaton in special classes of algebras.

10 Odds and bits

Gröbner bases in special classes of algebras

A procedure for "computing" Gröbner bases of *uniform* ideals in twisted semigroup rings is presented in **[FFG]**. An ideal is uniform if it is generated by uniform elements; f is uniform if $lT(f)r = 0$ implies $l \star f \star r = 0$.

Twisted semigroup rings $k\langle X_1, \ldots, X_n\rangle/\mathcal{I}$ where $\mathcal{I}$ is generated by $\{g_{ij} : 1 \leq i < j \leq n\}$, $g_{ij} = X_j X_i - c_{ij} X_i X_j - p_{ij}$ with $c_{ij} \in k$ and p_{ij} a linear combination of "commutative" terms $t \in \mathbf{T} \subset \langle X_1, \ldots, X_n\rangle$ s.t. $T(p_{ij}) < X_i X_j$ are studied in **[A1, A2, M88]** and a procedure for "computing" Gröbner bases is there. These rings differ from solvable polynomial rings, insofar the conditions that $c_{ij} \neq 0$ and $\{g_{ij}\}$ is a Gröbner basis have been relaxed.

A thorough study of the algebras $k\langle X_1,\dots,X_n\rangle/\mathcal{I}$ where $\mathcal{I}$ is generated by $\{g_{ij} : 1 \le i < j \le n\}$ and $g_{ij} = X_jX_i - a_{ij}X_{i'}X_{j'}$ for some $a_{ij} \in k - \{0\}$ and $i' < j'$ has been performed by Gateva in a series of papers (*cf.* [**GI4-7**]). A generalization of Buchberger algorithm to these algebras is contained in [**GI7**]

Gröbner bases and noetherianity

In a noetherian finitely presented algebra each ideal has a finite Gröbner basis (and an algorithm to compute it) and conversely if each ideal in a ring has a finite Gröbner basis, the ring is necessarily noetherian.

However to have an algorithm for computing Gröbner bases in a finitely presented algebra R , one needs less than noetherianity: one only needs that R satisfies:

Each finitely generated ideal in R has a finite Gröbner basis

Recently Weispfenning ([**W**]) has given an example of a class of algebras which are not noetherian but which satisfy the property above.

Local algebra

Standard bases for ideals I in either $k[[X_1,\dots,X_n]]$ or $k[X_1,\dots,X_n]_0 := \{\frac{f}{1+g} \in k(X_1,\dots,X_n), g(0) = 0\}$ are defined as Gröbner bases in $k[X_1,\dots,X_n]$. They are sets $G \in I$ s.t. $T(G) = T(I)$; however the ordering on $\mathbf{T}$ is such that $t \le 1 \forall t$ so it is a well-ordering no more.

Standard bases have the same kind of applications as Gröbner bases; while the latter are used to perform a "global" study of algebraic varieties, the former are required in the "local" study of an algebraic variety, i.e. near a point or along a subvariety. A variant of Buchberger Algorithm, known as the Tangent Cone Algorithm, allows to compute standard bases in $k[X_1,\dots,X_n]_0$. Details on the algorithm can be found in [**MPT**]; a survey of algebro-geometric applications in [**M5**].

Differential ideals

The differential polynomial ring is the k-algebra generated by a finite set of variables and by all their iterated formal partial derivatives w.r.t. a finite set of derivations. Algebraically it is therefore nothing more than a polynomial ring over countably many variables. In this context one is however interested in *differential* ideals, i.e. in ideals which are closed by derivations.

A Gröbner basis theory can be developed for differential ideals ([**CF3**],[**O1,O2**]), but the algorithmic issues are very complex and not completely clear (at least to me).

Group algebras

There is an unchallenged assumption in this paper: that a semigroup ordering is needed over the semigroup $\mathbf{S}$ in order to derive a Gröbner basis theory for $k\langle\mathbf{S}\rangle$. This rules out a Gröbner basis theory for the obviously interesting case of *group* algebras.

After completion of this paper, a Gröbner basis theory for group algebras was independently provided by Madlener and Reinert [**MR**] and by Rosenmann [**R**], simply by not assuming that the ordering is compatible with product and accordingly modifying the technicalities of the theory.

References

[**A1**] J.Apel, *Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung* (1988) Dissertation, Leipzig

[**A2**] J.Apel, *G-algebras*, Contemporary Mathematics **131** (1992) 195–204

[**AL1**] J.Apel, W.Lassner, *An algorithm for calculations in enveloping fields of Lie Algebras*, Proc. Conf. Comp. Alg., Dubna (1985) 231–241

[**AL2**] J.Apel, W.Lassner, *An extension of Buchberger's algorithm and calculations in envelopping fields of Lie Algebras*, Preprint, Leipzig (1986)

[**AL**] J.Apel, W.Lassner, *An algorithm for calculations in envelopping fields of Lie algebras*, J. Symb. Comp. **6** (1988) 361–370

[**AS**] W. Auzinger, J. Stetter, *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, Int. Ser. Num. Math. **86** (1988), 11 – 30

[**BS**] P. Beckmann, J.Stückrad, *The concept of Gröbner algebras*, J. Symb. Comp. **10** (1990), 465–479

[**Ber**] G. Bergman, *The diamond lemma in ring theory*, Adv. Math **29** (1978), 178–218

[**BRT**] A. Bigatti, L. Robbiano, C. Traverso, *A Divide and Conquer Algorithm for Hilbert-Poincaré Series, Multiplicity and Dimension of Monomial Ideals* Proc. AAECC - 10, Lect. N. Comp. Sci. **673** (1992), 76–88

[**B1**] B.Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph. D. Thesis, Innsbruck, (1965)

[**B2**] B.Buchberger, *Gröbner bases: an algorithmic method in polynomial ideal theory*, in N.K. Bose (ed.) *Recent trends in multidimensional system theory*, Reidel (1985)

[**CF1**] G. Carrà Ferro *Some properties of the lattice points and their applications to differential algebra*, Comm. Alg. 15 (1987), 2625–2632

[**CF2**] G. Carrà Ferro *Some remarks on the differential dimension*, Proc. AAECC-6, Lect. N. Comp. Sci. **357** (1989), 152–163

[**CF3**] G. Carrà Ferro *Gröbner bases and differential algebra*, Proc. AAECC-5, Lect. N. Comp. Sci. **356** (1989), 129–140

[**CG**] G. Carrà Ferro, G. Gallo *A procedure to prove statements in differential geometry*, J. Automated Reasoning **6** (1989), 203–209

[**C1**] F. Castro *Theoreme de division pour les operateurs differentielles et calcul des multiplicites*, These 3me cycle, Paris VII (1984)

[**C2**] F. Castro *Calcul de la dimension et des multiplicites d'un D-module homogene*, C.R. Acad. Sci. Paris **302** (1986), 487–490

[**FFG**] D. Farkas, C. Feustel, E. Green *Synergy in the theories of Gröbner bases and path algebras*, Can. J. Math., to appear

[**Ga1**] A.Galligo *Algorithmes de calcul de bases standard*, Preprint, Nice (1982)

[**Ga2**] A.Galligo *Some algorithmic questions on ideals of differential operators*, Proc. EUROCAL '85 II, Lect. N. Comp. Sci. **204** (1985), 413–421

[**GI1**] T. Gateva-Ivanova, *Algorithmic determination of the Jacobson radical of monomial algebras*, Proc. EUROCAL '87, Lect.Notes Comp.Sci. **378** (1989) 355–364

[**GI2**] T. Gateva-Ivanova, *Algorithmic determination of the global dimension of associative algebras*, Preprint (1988)

[**GI3**] T. Gateva-Ivanova, *Global dimension of associative algebras*, Proc. AAECC-6, Lect. Notes Comp. Sci. **357** (1989) 213–229

[**GI4**] T. Gateva-Ivanova, *On the noetherianity of some associative finitely presented algebras*, J. Alg **138** (1991), 13–35

[**GI5**] T. Gateva-Ivanova, *Noetherian properties and growth of some associative algebras*, Proc. MEGA '90, Birkhauser (1991), 143–158

[**GI6**] T. Gateva-Ivanova, *Noetherian properties of skew polynomial rings with binomial relations*, Tran. Amer. Math. Soc. (to appear)

[**GI7**] T.Gateva-Ivanova, *Gröbner bases in skew polynomial rings*, Reports Dept.Math. Univ. Stockholm, **8** (1992).

[**GL**] T. Gateva-Ivanova, V. Latishev *On recognizable properties of associative algebras*, J. Symb. Comp. **6** (1988) 371–388.

[**GM**] R. Gebauer, H. M. Möller *Buchberger's algorithm and staggered linear bases*, Proc. SYMSAC '86, ACM (1986), 218–221.

[**Gi**] P. Gianni, *Properties of Gröbner bases under specialization*, Proc. EUROCAL '87, Lect. N. Comp. Sci. **378** (1989), 293–297

[**GMNRT**] A.Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, *"One sugar cube, please"; or: Selection strategies in Buchberger algorithm*, Proc. ISSAC '91, ACM (1991), 49–54

[**Go**] E.S. Golod, *Standard bases and homology* Lect. N. Math. **1352** (1988), 88–95

[**K**] M. Kalkbrener, *Solving systems of polynomial equations by using Gróbner bases*, Proc. EUROCAL '87, Lect. N. Comp. Sci. **378** (1989), 282–293

[**KR-W**] A.Kandri-Rody, V.Weispfenning *Non-commutative Gröbner bases in algebras of solvable type*, J. Symb. Comp. **9**, (1990), 1–26

[**Kr**] H. Kredel, *Solvable polynomial rings*, Ph.d. Thesis, Verlag Shaker, Aachen (1993)

[**MR**] K. Madlener, B. Reinert, *Computing Gröbner bases in monoid and group rings*, Proc. ISSAC '93, ACM (1993)

[**M1**] F. Mora *Gröbner bases for non-commutative polynomial rings*, Proc. AAECC 3 Lect. N. Comp. Sci. **229** (1986), 353–362

[**M2**] T. Mora *Standard bases and non-noetherianity: non commutative polynomial rings*, Proc. AAECC 4 Lect. N. Comp. Sci. **307** (1988), 98–109

[**M3**] T. Mora, *Gröbner bases for non-commutative algebras*, Proc. ISSAC 88, Lect. N. Comp. Sci. **358** (1989), 150–161

[**M4**] T.Mora, *Seven variations on standard bases*, Preprint **45**, Dip. Mat. Genova (1988)

[**M5**] T. Mora *La queste del saint* $Gr_a(A_L)$, Proc. AAECC-7, Disc. Appl. Math. **33** (1991), 161–190

[**MPT**] T. Mora, G. Pfister, C. Traverso *An introduction to the tangent cone algorithm*, in C.Hoffmann Ed. *Issues in robotics and non-linear geometry*, JAI Press, Greenwich Conn. (1992), 199–270

[**O1**] F. Ollivier, *Le problème de l'identifiabilité: approche théorique, méthodes effectives et étude de complexité*, Ph. D. Thesis, École Polytechnique (1990)

[**O2**] F. Ollivier, *Standard bases of differential ideals*, Proc. AAECC-8, Lect. Notes Comp. Sci. **508** (1990), 304–321

[**R**] A. Rosenmann, *An Algorithm for constructing Gröbner and free Schreier bases in free group algebras*, Preprint (1992)

[**S**] C. Squier, *Word problems and a homological finiteness condition for monoids*, J. Pure Appl. Algebra **49** (1987), 201–217

[**Tr**] W. Trinks, *Über Buchbergers Verfahren, Systeme für algebraischen Gleighungen zu lösen*, J. Number Th. **10** (1978), 475–488

[**W**] V. Weispfenning, *Finite Gróbner bases in non-noetherian skew polynomial rings*, Proc. ISSAC '92, ACM (1992), 329–334