GRÖBNER BASES

AND THE WORD PROBLEM

TEO MORA

> every solution of the word problem for a class of presentations is a triumph over nature.
> MAGNUS-KARRASS-SOLITAR *Combinatorial group theory*

INTRODUCTION

This is an informal preliminary report on a research on the interrelationship between the undecidability of the word problem and the technique of solution for such problems provided by Buchberger method of Gröbner bases [BUC1,BUC2,BUC3], that I am pursuing since Summer 1985 and on whose leading ideas I first related in my communication at the Grenoble AAECC3 meeting.
As it is known, Buchberger gave an algorithm to solve the ideal membership problem for polynomial rings, and so the word problem for commutative semigroups.

A proposal to extend Buchberger's techniques to non-commutative ring theory was first put forward by Bergman [BER], which also introduced the generalisation of the concept of Gröbner bases to non-commutative polynomial rings and proposed a completion technique to compute them. While looking for a suitable setting to understand the behaviour of Gröbner and standard bases in a non-noetherian situation, I also was led to consider the theory of Gröbner bases for non-commutative polynomial rings [MOR].

Bergman showed that the knowledge of a finite Gröbner basis for a (two-sided) ideal I in a non-commutative polynomial ring allows to solve the ideal membership problem for I; therefore the undecidability of ideal membership problems can either mean, for a fixed ordering, that there are finitely generated ideals whose Gröbner basis is infinite, or that there are finitely generated ideals whose Gröbner basis is finite, but not computable.

The main result of [MOR] was to rule out the second possibility (which is apparently allowed by the original completion technique by Bergman), giving a variant of the Buchberger-Bergman procedure which is guaranteed to halt returning a finite Gröbner basis of a finitely

generated ideal (w.r.t. a fixed ordering), if and only if such a basis exists.

Therefore, given a two-sided ideal I, one can choose a semigroup ordering, apply the procedure described above to (hopefully) get a finite Gröbner basis of I; in case of success, one is able to solve the ideal membership problem for I.

However, since the semigroup orderings on a free semigroup are infinitely many, and since such an approach restricts the choice to, at most, finitely many orderings, it can be scarcely interpreted as a "powerful" technique to attack ideal membership and word problems; in my opinion, it is not superior to any "trial-and-error" approach.

The scenario would be different, however, if one could apply the procedure above, in some parallel way, to try to compute Gröbner bases for an ideal with respect to infinitely many orderings. The idea is not so paradoxical as it could seem, in view of the results which Robbiano and myself were developing at the same time, about the so-called Gröbner fan of an ideal in a (commutative) polynomial ring [M-R], which actually allow to produce an algorithm to compute the Gröbner bases of an ideal w.r.t. all the (infinitely many) orderings.

This was the starting point of my research, which is two-fold.

One of its aims is to give a "powerful" procedure, using Gröbner-basis techniques, to attack the ideal membership problem for non-commutative polynomial rings.

In this direction, I was able to devise a procedure, which, given a finite basis of an ideal I in the non-commutative polynomial ring, halts if and only if I has a finite Gröbner basis w.r.t. some ordering in a set **O**, which satisfies the following property FDR:

> there is an algorithm to decide, given a finite set D of inequalities in a free semigroup, if there is an ordering in **O**, satisfying all inequalities in D.

(in the following I will refer to this procedure as the "Gröbner procedure").

It is not difficult to prove the existence of infinite sets of orderings satisfying the FDR property, so that the power of the proposed method is only limited by the ability of producing larger and larger sets satisfying the FDR property.

However, notwithstanding how powerful this method can become, word problems are still undecidable.

I have the following picturesque interpretation of this: while you can try hard to make your Gröbner tool for solving word problems sharper and sharper, so to become able to dispose of more and more word problems, there is, lurking somewhere, an "undecidability bug" which

eventually will make your tool a rusty, useless one.

The second, and still largely unsuccessful, aim of my research is to hunt the undecidability bug.

My 1985 result is surely a first step of this hunt: if an ideal has a finite Gröbner basis w.r.t. some ordering < which is computable in the sense that, given two words, it is possible to decide which is larger w.r.t. <, then its ideal membership problem is solvable. In fact, this suggests a possible hide for the undecidability bug: are there non-computable orderings?

However, the Gröbner procedure seems to have the useful feature of bypassing questions of computability for the orderings involved. By analogy with the commutative case, one realizes that in order to get all finite Gröbner bases of a finitely generated ideal, one does not need to deal with all orderings, but just with a subset which is dense in some topological sense. So we spot another place where undecidability could lie: is there a dense set of orderings which still has the FDR-property?

Assume the answer is positive. Then, with no regard to computability questions on orderings, we could conclude that if an ideal has unsolvable memebership problem, then necessarily all its Gröbner bases are infinite. This seems to imply (quite unbelievably) the existence of a purely algebraic interpretation of undecidability as a consequence of non-noetherianity. This is not true however, since, to reach such a result, one should be willing to go a step further and actually assume not only the existence of a set which is dense and satisfies the FDR property, but also that the Gröbner procedure is universal, in the sense that:

if an ideal has solvable ideal membership problem, then its membership problem is solvable by the Gröbner procedure

Otherwise, one is still left with the problem of recognizing those ideals with infinite Gröbner bases but solvable ideal membership problem, from the ones with infinite Gröbner bases and unsolvable ideal membership problem.

Part I of the report deals with the Gröbner procedure to attack ideal membership and word problems in the non-commutative case.
The basic notions on semigroup orderings are reviewed in section 1; the ones on Gröbner bases in section 2; the procedure devised in [MOR] is presented in Section 3. Section 4 is devoted to show that also infinite Gröbner bases can be used to solve ideal membership problem (this shaking somewhat the possibility that the Gröbner procedure be universal). Section 5 shows that computing a Gröbner basis for just one ordering is sufficient to solve the ideal membership problem for 0-dimensional ideals, giving also an application to regular languages; the ideal membership problem for 0-dimensional ideals translates to the word

problem for finite semigroups, for which a Todd-Coxeter procedure is already known.
Finally Section 6 presents the Gröbner procedure, allowing to compute finite Gröbner bases for a set satisfying the FDR-property.

Part II deals with the hunt of the undecidability bug and reports on the few conjectural results already discussed above.

Both parts of the report clearly point out that a better knowledge of orderings on a free semigroup is required. The few things I know on the subject are listed in the final part of the report.

Namely, Section 1 shows that all archimedean orderings are refinements of partial orderings obtained by imposing a degree on the variables; then we present an infinite set satisfying the FDR property. Section 2 deals with the few non-archimedean orderings I know of.

ACKNOWLEDGMENTS

I had many discussions on this topic with some colleagues which helped me with suggestions, comments and encouragements, helping me to give a shape to my ideas.

Among them, I'm indebted to Aldo De Luca, Alessandro Logar, Hans Michael Möller, Lorenzo Robbiano, Volker Weisspfenning.

In particular Giuseppa Carrà Ferro made me realize I knew the Gröbner semidecision procedure described in I.3.9; Moss Sweedler asked about the regular language application and suggested the question whether an ideal with unsolvable membership problem necessarily has infinite Gröbner bases only; Alfredo Ferro suggested the question about the universality of the Gröbner procedure.

I A GRÖBNER BASIS PROCEDURE FOR THE WORD PROBLEM

1 ORDERINGS ON A FREE SEMIGROUP

1.1 Let S denote a free semigroup generated by a finite alphabet A.
If m,n are in S, we will say m is a multiple of n (n divides m) iff there are l,r in S s.t. $m = lnr$.
We will say m is contained in n (n contains m) iff there are $u_1,\dots,u_k$, $w_0,\dots,w_k \in S$ s.t. $m = u_1\dots u_k$, $n = w_0u_1w_1\dots u_kw_k$.

1.2 A semigroup ordering $<$ on S is a total ordering s.t.:
for all m,m_1,m in S, $m_1 < m_2$ implies $m\,m_1 < m\,m_2$ and $m_1\,m < m_2\,m$.
A semigroup ordering will be called positive iff $1 \le m$ for all m in S or equivalently iff $m \le mn$ and $m \le nm$ for all m,n in S.

1.3 In contrast with the commutative case, Dickson's Lemma [DIC] doesn't hold in S; namely, the following is an infinite sequence $(m_i : i > 0)$ of elements in the free semigroup generated by $\{a,b\}$, such that for all i,j, $i \neq j$, m_i is not a multiple of m_j: let $s := ab$, $t := ba$, $u := bb$ and let $m_i := s^i t^i u$.
However, a weaker version of Dickson's Lemma, which holds in a more general algebraic setting, is true; it is known as Kruskal's Theorem [KRU], but probably it is to be attributed to Newman [NEW].

1.4 LEMMA If $m_1,\dots,m_i,\dots$ is an infinite sequence of elements of S, there is N s.t. for every $j > N$, there is $i < N$ s.t. m_i is contained in m_j.

1.5 COROLLARY If $<$ is a semigroup ordering, the following conditions are equivalent:
i) $<$ is a well-ordering
ii) $<$ is positive
iii) for all $m,n \in S$, if m is contained in n, then $m \le n$
Proof: i)⇒ii) Assume there is $n \in S$ s.t. $n < 1$. Then $n,n^2,\dots,n^i,n^{i+1},\dots$ is an infinite decreasing sequence.
ii)⇒iii) Assume $m,n \in S$ are s.t. m is contained in n.
Therefore there are $u_1,\dots,u_k$, $w_0,\dots,w_k \in S$ s.t. $m = u_1\dots u_k$, $n = w_0u_1w_1\dots u_kw_k$.
Since $w_i \ge 1$ for every i, then $m \le n$.
iii)⇒i) Assume $<$ is not a well-ordering; so there is an infinite sequence $m_1,\dots,m_i,\dots$ s.t. for every $i < j$, $m_i > m_j$. By the Lemma above, there are i,j $i < j$, s.t. m_i is contained in m_j, so $m_i \le m_j$, a contradiction.

2 GRÖBNER BASES FOR NON-COMMUTATIVE POLYNOMIALS

2.1 K[S], K a field, will denote the ring whose elements are finite linear combinations of elements of S, $K[S] := (\Sigma_i c_i m_i : c_i \in K-\{0\}, m \in S)$, with multiplication canonically defined in terms of the semigroup multiplication.
We will call polynomials the elements of K[S], terms the elements of S.
We can interpret K[S] as the set of all applications from S to K which are 0 a.e.; if $f \in K[S]$, $m \in S$, $c(f,m)$ will denote the value at m of the application f, i.e. the coefficient of m in f; Supp(f) will denote $\{m \in S : c(f,m) \neq 0\}$.

2.2 Let $<$ be a semigroup well-ordering on S.
If $f := \Sigma_{i=1,t} c_i m_i$, $c_i \in K-\{0\}$, $m_i \in S$, $m_1 > m_2 > \dots > m_t$, define $M_<(f) := m_1$, $lc(f) := c_1$; $M_<(f)$ is called the maximal term, and $lc(f)$ the leading coefficient, of f w.r.t. $<$.
If $G \subset K[S]$, define $M_<(G) := \{M_<(f) : f \in G-\{0\}\}$, and remark that, if I is a two-sided non-zero ideal of K[S], $M_<(I)$ is a two-sided ideal of S.
For the sake of simplicity, we will write $M(\cdot)$ instead of $M_<(\cdot)$, when there is no risk of confusion.
We say that $f \in K[S]-\{0\}$ has a G-representation in terms of F iff:
1) $f = \Sigma_{i=1,t} a_i l_i f_i r_i$, $a_i \in K-\{0\}$, $l_i, r_i \in S$, $f_i \in F$.
2) $M(f) \ge l_i M(f_i) r_i$ for all i.

2.3 PROPOSITION Denote by N(I) the K-vector space whose basis is $S - M(I)$. Then for all $f \in K[S]$ there is a unique $g \in N(I)$ s.t. $f - g \in I$.
Proof: [MOR] Prop.3.4

2.4 Given an ordered pair of terms, $(m_1,m_2) \in S^2$, the set of matches of (m_1,m_2), denoted by $M(m_1,m_2)$, is the finite set of all 4-tuples $(l_1,l_2,r_1,r_2) \in S^4$ s.t.either:
1) $l_1 = r_1 = 1$, $m_1 = l_2\,m_2\,r_2$
2) $l_2 = r_2 = 1$, $m_2 = l_1\,m_1\,r_1$
3) $l_1 = r_2 = 1$, $l_2 \neq 1$, $r_1 \neq 1$, there is $w \in S$ s.t. $w \neq 1$, $m_1 = l_2\,w$, $m_2 = w\,r_1$
4) $l_2 = r_1 = 1$, $l_1 \neq 1$, $r_2 \neq 1$, there is $w \in S$ s.t. $w \neq 1$, $m_1 = w\,r_2$, $m_2 = l_1\,w$.
If $G \subset K[S]-\{0\}$, the set of S-polynomials of G is the set
$SP(G) := \{ f \in K[S]-\{0\} : f = lc(g_2)\,l_1\,g_1\,r_1 - lc(g_1)\,l_2\,g_2\,r_2$, for some $(l_1,l_2,r_1,r_2) \in M(M(g_1),M(g_2))$, for some $g_1,g_2 \in G\}$.

2.5 THEOREM Let I be a two-sided ideal of K[S], $G \subset I-\{0\}$. The following conditions are equivalent:

1) M(G) generates M(I)
2) $f \in I-\{0\}$ iff f has a G-representation in terms of G
3) G is a basis of I and for all $f \in SP(G)$, f has a G-representation in terms of G.

A set G satisfying any of these conditions is called a Gröbner basis of I (w.r.t. $<$).

Proof: [MOR] Th.3.3

2.6 Let $f_1,\dots,f_r \in K[S]-\{0\}$. Let $m_1,\dots,m_r \in S$ be such that $m_i \in Supp(f_i)$ for $i = 1\dots r$ and let $c_i := c(f_i,m_i)$.

If $g,h \in K[S]$, we say that g reduces to h w.r.t. $\Gamma := (f_1,\dots,f_r; m_1,\dots,m_r)$, denoted by $g \to_\Gamma h$, iff there exist $l,r \in S$ and $i \in \{1,\dots,r\}$ with $l\,m_i\,r \in Supp(g)$ s.t. $h := g - (1/c_i)\,c(h, l\,m_i\,r)\,l\,f_i\,r$.

Let $\to^*_\Gamma$ denote the transitive-reflexive closure of $\to_\Gamma$; we say $h \in K[S]$ is Γ-irreducible iff $h \to^*_\Gamma g$ implies $g = h$; we say $\to^*_\Gamma$ is noetherian iff for each infinite sequence $(g_0,\dots,g_i,\dots)$ s.t. for each i, $g_{i-1} \to^*_\Gamma g_i$ then, for N sufficiently large, $g_i = g_N$ if $i>N$.

We denote by $RED(f_1,\dots,f_r; m_1,\dots,m_r; g)$ or by $RED(\Gamma; g)$ the set $\{h \in K[S] : h \text{ is } \Gamma\text{-irreducible and } g \to^*_\Gamma h\}$.

2.7 LEMMA Let $f_1,\dots,f_t \in K[S]-\{0\}$; $m_1,\dots,m_t \in S$ be such that $m_i \in Supp(f_i)$. Let $\Gamma := (f_1,\dots,f_t; m_1,\dots,m_t)$, I be the two-sided ideal generated by $(f_1,\dots,f_t)$, $\mathbf{O}$ be the set of all semigroup well-orderings $<$ s.t. $m_i = M_<(f_i)$ for every i, and let $g \in K[S]$. Then the following hold:

1) If $0 \in RED(\Gamma; g)$, then $g \in I$
2) If $0 \neq f \in RED(\Gamma; g)$, then $Supp(f) \cap (m_1,\dots,m_t) = \emptyset$.
3) If $\mathbf{O} \neq \emptyset$, then $\to^*_\Gamma$ is noetherian.

If $\mathbf{O} \neq \emptyset$ and $(f_1,\dots,f_t)$ is a Gröbner basis for I with respect to an ordering in $\mathbf{O}$, then the following hold:

4) for each g, $RED(\Gamma; g)$ contains a unique element which we will denote by $red(\Gamma; g)$
5) $g \in I$ iff $red(\Gamma; g) = 0$
6) $(f_1,\dots,f_t)$ is a Gröbner basis for I with respect to each ordering in $\mathbf{O}$

Proof: 1) and 2) are obvious.

3) Choose an ordering $<$ in $\mathbf{O}$.

Assume there are $g_0,\dots,g_i,\dots \in K[S]$ s.t. for each i, $g_i \to_\Gamma g_{i+1}$. Since $M_<(g_i) \geq M_<(g_{i+1})$ for all i, the assumption implies that there is $N \in \mathbb{N}$, $M_0 \in S$, s.t. $M_<(g_i) = M_0$ for $i > N$. Let then $h_i := g_{i+N} - M_<(g_{i+N})$; it is easy to show that for each i, $h_i \to_\Gamma h_{i+1}$.

By the same argument, there is $N \in \mathbb{N}$, $M_1 \in S$, $M_1 < M_0$, s.t. $M_<(h_i) = M_1$ for $i > N$. This allows to proof the claim by an inductive argument.

Let now $<$ be a fixed well-ordering in $\mathbf{O}$, s.t. $(f_1,\dots,f_t)$ is a Gröbner basis for I w.r.t. $<$.

4) if $h_1,h_2 \in RED(\Gamma; g)$, then $h_1 - h_2 \in I$ and is irreducible; therefore, if $h_1 \neq h_2$, one has $M_<(h_1 - h_2) \notin (m_1,\dots,m_t) = M_<(I)$, a contradiction.

5) If $g \in I$ and $0 \neq h := red(g)$, then $h \in I$. So $M_<(h) \notin (m_1,\dots,m_t) = M_<(I)$, a contradiction.

6) Let $<'$ be a well-ordering in $\mathbf{O}$.
Let $m \in M_<(I)$, $g \in I^*$ be s.t. $M_{<'}(g) = m$.
If, for each i, m is not a multiple of $M_{<'}(f_i)$, then if $h = red(\Gamma; g)$ ($RED(\Gamma; g)$ consists of a unique element because of 4), one has $m \in Supp(h)$, so that $red(\Gamma; g) \neq 0$. This is in contradiction with 5).

2.8 DEFINITION A Gröbner basis G of I w.r.t. $<$, is called reduced, if:

1) $(M_<(g) : g \in G)$ minimally generates $M_<(I)$
2) $lc(g) = 1$ for every $g \in G$
3) $g - M(g) \in N(I)$.

Reduced Gröbner bases of I w.r.t. $<$ are unique.

3 GRÖBNER BASES AND THE WORD PROBLEM

As it is well-known, the word problem for commutative semigroups has been effectively solved by reducing it to the ideal membership problem on the polynomial ring and using Gröbner bases to solve the latter. Analogous statements hold for the non-commutative case, as follows.

3.1 **WORD PROBLEM** Given a free non-commutative semigroup S, a finite subset $E \subset S^2$, $m_1, m_2 \in S$, decide whether (m_1,m_2) is in the congruence generated by E.

3.2 **IDEAL MEMBERSHIP PROBLEM** Given an effective field K, a free non-commutative semigroup S, a finite subset $F \subset K[S]$, $f \in K[S]$, decide whether f is in the ideal generated by F.

3.3 REMARK The word problem is reducible to the ideal membership problem

as follows: let S, $E \subset S^2$, $m_1, m_2 \in S$ be given; let $K := \mathbb{Z}_2$, $F := \{n_1 - n_2 \in K[S] : (n_1,n_2) \in E\}$, $f := m_1 - m_2$. Then (m_1, m_2) is in the congruence generated by E iff f is in the ideal generated by F.

3.4 REMARK Given an effective field K, a free non-commutative semigroup S, a finite subset $F \subset K[S]$, the ideal membership problem is solvable for each $f \in K[S]$, if a finite Gröbner basis G for the ideal generated by F, w.r.t. some well-ordering $<$, is computable, and, moreover, one is able to compute $M_<(g)$ for all $g \in G$.

Namely, once $G = \{g_1,...,g_t\}$ has been computed, let $\Gamma := \{g_1,...,g_t;M(g_1),...M(g_t)\}$ and apply the following algorithm:

$h := f$
While there is $m \in Supp(h)$, $l,r \in S$, $i \in \{1,...,t\}$ s.t. $m = l\,M(g_i)\,r$ **do**
$h := h - c(h,m)(lc(g_i))^{-1}\, l\, g_i\, r$

By the results of Lemma 2.7, this algorithm terminates (since $\rightarrow^*_\Gamma$ is noetherian) and computes $red(\Gamma,f)$; so f is in the ideal generated by F iff $red(\Gamma,f) = 0$.

3.5 However, as it is well-known, the word problem for non-commutative semigroups is undecidable.
This is related with the fact that Dickson's Lemma doesn't hold in S, which implies:

i) the existence of ideals which are not finitely generated, e.g. the ideal generated by $\{m_i : i > 0\}$, where m_i is defined as in 1.2.

2) and so the non-noetherianity of K[S]

3) the impossibility to rule the existence of finitely generated ideals I whose Gröbner basis for a fixed ordering is infinite, i.e. s.t. M(I) is not finitely generated.

Actually, one can produce examples of finitely generated ideals I s.t. for some orderings $<$, $M_<(I)$ is finitely generated, while for other orderings $<'$, $M_{<'}(I)$ is not finitely generated ([MOR] Ex.3.12; cf. also Section 4).

Going back to Remark 3.4 we can conclude, by the undecidability of the word problem, that there are finite sets F s.t. for <u>any</u> well-ordering $<$ it is impossible to compute a finite Gröbner basis, w.r.t. $<$, of the ideal generated by F.

Once $<$ is fixed, if $<$ is <u>computable</u>, (by which we mean that given $m,n \in S$, it is possibile to decide whether $m < n$), this could happen because of two very different reasons:

1) there are finitely generated ideals which have finite, however not computable, Gröbner bases.

2) while finite Gröbner bases are computable, there are finitely generated ideals which don't have finite Gröbner bases.
The following Lemma allows to rule out the first case.

3.6 LEMMA Let $I \subset K[S]$ be a two-sided ideal, $<$ a semigroup well-ordering; let $G_1 \subset G_2 \subset ... \subset G_i \subset ...$ be a sequence of finite sets, $G_i \subset I-\{0\}$, G_1 (and so each G_i) a basis of I s.t. for each n, for each $f \in SP(G_n)$, f has a G-representation in terms of G_{n+1}.
Then for each $f \in I$, there is u s.t. f has a G-representation in terms of G_u.
<u>Proof</u>: cf. the proof of [MOR] Lemma 3.6

3.7 COROLLARY Under the same assumptions of Lemma 3.6, if I has a finite Gröbner basis w.r.t. $<$, then there is n s.t. G_n is a finite Gröbner basis of I w.r.t. $<$.
<u>Proof</u>: cf. [MOR] Lemma 3.6.

3.8 Given a finite set $F \subset K[S]$, and a computable semigroup well-ordering $<$, the following procedure terminates iff the ideal generated by F has a finite Gröbner basis w.r.t. $<$, in which case it returns such a basis G (cf. [MOR] 3.8):

$n := 1$; $H_1 := F$; $G_1 := F$
While $H_n \neq \emptyset$ **do**
$B_n := \{(f,g,l_1,r_1,l_2,r_2) : (l_1,r_1,l_2,r_2) \in M(M(f),M(g)),\ f \in G_n,\ g \in H_n\}$
$H_{n+1} := \emptyset$
While $B_n \neq \emptyset$ **do**
Choose $(f_1,f_2,l_1,r_1,l_2,r_2) \in B_n$
$B_n := B_n - \{(f_1,f_2,l_1,r_1,l_2,r_2)\}$
$f := lc(f_2)\, l_1\, f_1\, r_1 - lc(f_1)\, l_2\, f_2\, r_2$
While there is $m \in Supp(f)$, $l,r \in S$, $g \in G_n \cup H_{n+1}$
s.t. $m = l\,M(g)\,r$ **do**
$f := f - c(f,m)(lc(g))^{-1}\, l\, g\, r$
If $f \neq 0$ **then**
$H_{n+1} := H_{n+1} \cup \{f\}$
$G_{n+1} := G_n \cup H_{n+1}$
$n := n+1$

3.9 REMARK Another consequence of Lemma 3.6. is that there is a

semidecision procedure which, given a finite set $G = \{g_1,...,g_r\}$ and a polynomial f, halts if and only if f is in the ideal generated by G. Without entering in detail, it can be described as follows:

Choose a computable semigroup well-ordering $<$
$G_0 := G$
$n := 0$
While f has no G-representation in terms of G_n **do**
  compute G_{n+1} s.t. for all $f \in SP(G_n)$, f has a G-representation in terms of G_{n+1}
  $n := n+1$.

Obviously, there is another semidecision procedure for the same problem, namely:

$F := \{f\}$
While $0 \notin F$ **do**
  $H := F$
  $F := \emptyset$
  While $H \neq \emptyset$ **do**
    Choose $h \in H$
    $H := H - \{h\}$
    For all $t \in Supp(h)$, $g \in G$, $m \in Supp(g)$ **do**
     If there are $l,r \in S$: $t = l\,m\,r$ **then**
       $h' := h - c(h,t)\,c(g,m)^{-1}\,l\,g\,r$
       $F := F \cup \{h'\}$

So it could be interesting to compare the performances of both procedures on some examples.

4 SOLVING WORD PROBLEMS WITH INFINITE GRÖBNER BASES

The following is a variation of [MOR] Ex.3.12, which we use both to show an application of the results in 3.6-3.8 and to prove the claim of 3.5. It is more complex than the original result, in order to be an instance not only of an ideal membership problem but also of a word problem.

4.1 Let $A=\{a,b,c,d,e,f\}$, S be the free semigroup generated by A, I be the ideal in K[S] generated by $\{f_1,...,f_6\}$, where $f_1 := adc - e$, $f_2 := cb - bc$, $f_3 := db - bd$, $f_4 := ab - aad$, $f_5 := ac - f$, $f_6 := fb - ae$.
Let $deg: S \to \mathbb{N}$ be defined by
$deg(a) := deg(c) := deg(d) := deg(e) := deg(f) := 1$, $deg(b) := 2$,

and, inductively, if $w \in S$, $w = w'x$, with $w' \in S$, $x \in A$,
$deg(w) := deg(w') + deg(x)$.
Let $<$ be the total ordering defined by:
$m < n$ iff $deg(m) < deg(n)$ or $deg(m) = deg(n)$ and m is lexicographically less than n.
It is clear then that $<$ is a semigroup well-ordering and that $M(f_1) = adc$, $M(f_2) = cb$, $M(f_3) = db$, $M(f_4) = ab$, $M(f_5) = ac$, $M(f_6) = fb$.

4.2 Let $g_i := a^{i+1}d^{i+1}c - eb^i$, for $i \geq 1$; then $M(g_i) = a^{i+1}d^{i+1}c$.
Let $G_0 := \{f_1,...,f_6\}$, $G_n := G_0 \cup \{g_i : 1 \leq i \leq n\}$, $G := G_0 \cup \{g_i : i \geq 1\}$.
Remark that $M(M(f_2),M(f_5)) = \{(a,1,1,b)\}$, $M(M(f_2),M(f_1)) = \{(ad,1,1,b)\}$, $M(M(f_2),M(g_n)) = \{(a^{i+1}d^{i+1},1,1,b)\}$, for $n \geq 1$, while the other sets of matches are empty.
Also the following equalities are easy to check:

$$a f_2 - f_5 b = fb - abc = f_6 + ae - abc = f_6 - f_4 c + ae - aadc = f_6 - f_4 c - a f_1$$

$$ad f_2 - f_1 b = eb - adbc = -a f_3 c + eb - abdc = -a f_3 c - f_4 dc + eb - a^2d^2c =$$
$$= -a f_3 c - f_4 dc - g_1$$

$$a^{n+1}d^{n+1} f_2 - g_n b = eb^{n+1} - a^{n+1}d^{n+1}bc$$

$$a^{n+1}d^{n+1}bc = a^{n+1}d^n f_3 c - a^{n+1}d^n bdc = \Sigma_{i=0...n} a^{n+1}d^i f_3 d^{n-i}c + a^{n+1}bd^{n+1}c$$

$$a^{n+1}bd^{n+1}c = a^n f_4 d^{n+1}c + a^{n+2}d^{n+2}c$$

so that

$$a^{n+1}d^{n+1} f_2 - g_n b = -\Sigma_{i=0...n} a^{n+1}d^i f_3 d^{n-i}c - a^n f_4 d^{n+1}c - g_{n+1}.$$

Therefore we can conclude that each element in $SP(G_n)$ has a G-representation in terms of G_{n+1}; also each element in SP(G) has a G-representation in terms of G, so that G is an (infinite) Gröbner basis of I.

4.3 Let $m \in S$, $d := deg(m)$, $G(d) := (g \in G : deg(g) \leq d)$; it is obvious that the unique element m_0 in N(I) s.t. $m - m_0 \in I$, can be obtained by reducing m using only the basis elements in G(d).
Therefore, once an infinite set is proved to be a Gröbner basis, under suitable assumptions it is possible to use a finite subset of it to solve word problems by the technique of 3.4.
The example however is not conclusive, since it is easy to produce a different semigroup well-ordering, w.r.t. which I has a finite Gröbner basis.

4.4 In fact, let $<$ be the total ordering defined by:
$m < n$ iff $length(m) < length(n)$ or $length(m) = length(n)$ and m is antilexicographically less than n.

It is clear then that $<$ is a semigroup well-ordering and that $M(f_1) = adc$, $M(f_2) = bc$, $M(f_3) = bd$, $M(f_4) = aad$, $M(f_5) = ac$, $M(f_6) = ae$.
Also, all the sets of matches are empty, except $M(M(f_1),M(f_4)) = \{(a,1,1,c)\}$; since $a\,f_1 - f_4\,c$ has a G-representation in terms of G_0, then G_0 is a Gröbner basis of I.

5 THE ZERO DIMENSIONAL CASE AND AN APPLICATION TO REGULAR LANGUAGES

There is a case in which the word problem is known to be solvable, the one of finite semigroups, in which for instance a word-problem algorithm dependent on the Todd-Coxeter algorithm for finite semigroups [T-C,NEU] can be easily devised.
In ideal theoretical terms, this corresponds to solve the ideal membership problem for a 0-dimensional ideal I, i.e. an ideal s.t. K[S]/I is a finite dimensional K-vector space.

5.1 PROPOSITION If I is 0-dimensional, then for every semigroup well-ordering $<$, I has a finite Gröbner basis w.r.t. $<$.
Proof: Because of Prop. 2.3, S-M(I) is a basis of a K-vector space isomorphic to K[S]/I, so it is finite.
Therefore there is d s.t. for all $m \in S$ with length(m)$\geq$d, then $m \in M(I)$.
Therefore M(I) is finitely generated.

5.2. If I is 0-dimensional, then for every semigroup well-ordering $<$, procedure 3.8 terminates returning a finite Gröbner basis of I, w.r.t. $<$.

5.3 There is an interesting application of 5.2 to regular languages.
Let E be a finite set of pairs in S^2, F be the quotient monoid of S with respect to the congruence generated by E, $f: M \to F$ be the canonical projection. Assume F is finite, and let T be a finite subset of S, $U = f(T)$, which is a subset of F, $L = f^{-1}(U)$.
We recall that L is said a regular language.

5.4 PROPOSITION Given $m \in S$, it is possible to decide whether $m \in L$.
Proof: Let $<$ be any (computable) semigroup well-ordering on S and K be an effective field.
Let I be the two sided ideal in K[S] generated by $\{n_1 - n_2 : (n_1,n_2) \in E\}$.
Since F is finite, I is a zero dimensional, so that it has a finite Gröbner basis $\{g_1,\dots,g_t\}$ with respect to $<$, where each g_i is a difference of two elements in S.
Let $\Gamma = (g_1,\dots,g_t;M(g_1),\dots,M(g_t))$, and let $U' = \{red(\Gamma;n) : n \in T\}$.

Then, under the isomorphism between F and S-M(I), U' and U are isomorphic.
Finally let $m \in S$; let $m' = red(\Gamma;m)$; clearly, $m \in L$ if and only if $m' \in U'$.

6 A PARALLEL GRÖBNER BASIS PROCEDURE

Obviously, choosing a fixed well-ordering and applying Procedure 3.8 gives very low chances (actually a zero probability) to solve a word problem, and this doesn't change, if Procedure 3.8 is applied, in parallel, for finitely many well-orderings.
In the commutative case however, the following result holds:

6.1 THEOREM Let I be an ideal in $K[X_1,\dots,X_n]$. Then there are finitely many finite sets $G_1,\dots,G_t$ s.t. for each term-ordering $<$, G_i is a Gröbner basis of I w.r.t. $<$ for some $i \in \{1,\dots,t\}$.
Moreover, given a basis of I, it is possible to compute $G_1,\dots,G_t$, and a partition of the set of term-orderings into disjoint subsets $T_1,\dots,T_t$ s.t. for each i, if $<$ is an ordering in T_i, then G_i is the reduced Gröbner basis of I w.r.t. $<$.
Proof: It is a restatement of the results contained in [M-R].

6.2 In analogy with this result we would like to give a procedure which could be described as a parallel version of infinitely many instances of Procedure 3.8.
In order to do so, we need the following:

6.3 DEFINITION Given a set **O** of semigroup well-orderings, and a finite subset D of S^2, we will denote by FDS(**O**,D) the set of all orderings $<$ in **O** s.t. for every $(m,n) \in D$, $m > n$.
A set **O** of semigroup well-orderings is said to have the FDR property (or to be an FDR-set) if, given a finite subset D of S^2, there is an algorithm which decides whether FDS(**O**,D) is empty.
(FDR doesn't stand for Franklin Delano Roosevelt, as usual, but for finite disequation recognizability)

6.4 LEMMA There exists an infinite FDR-set.
Proof: see III,1.11 and 2.6

6.5 We are now ready to present a procedure which operates over a finite set $\{f_1,\dots,f_s\} \subset K[S]$ and a FDR-set **O** of semigroup well-orderings, halting if and only if the ideal $(f_1,\dots,f_s)$ has a finite Gröbner basis with respect to some (unspecified) ordering $<$ in **O**, in which case it returns

such a Gröbner basis G, and $M_<(g)$ for each $g \in G$.

Such a procedure is a non-commutative variant of the algorithm presented in [M-R], and can be interpreted as running in parallel a finite, however unbounded, number of instances of Procedure 3.8.

6.6 NOTATIONS All over the procedure, the following notations are used:

G and H are finite subsets of $K[S]-\{0\}$,

M is a finite subset of S,

D is a finite subset of S^2,

ψ is a finite subset of $K[S]-\{0\} \times S$, s.t. if $(g,m) \in \psi$, then $m \in Supp(g)$; when we need, we will use a functional notation, denoting $\psi(g)$ the (unique) m s.t. $(g,m) \in \psi$,

B and C are finite subsets of $(K[S]-\{0\})^2 \times S^4$,

L is an array (G,H,M,D,ψ,B,C) with its components of the type specified above,

L is a list of such arrays,

g,f are elements in K[S],

l,r,m,n are elements in S.

6.7 PROCEDURE

```
[INITIALISATION OF THE COMPUTATION LIST]
L := (Ø,Ø,Ø,Ø,Ø,Ø,Ø)
L_new := [L]
For i = 1...s do
    L_old := L_new
    L_new := []
    For (G,Ø,M,D,ψ,B,Ø) ∈ L_old do
        G' := G ∪ {f_i}
        For m ∈ Supp(f_i) do
            M' := M ∪ {m}
            D' := D ∪ {(m,n) : n ∈ Supp(f_i) - {m}}
            ψ' := ψ ∪ {(f_i,m)}
            For g ∈ G do
                For (l_1,l_2,r_1,r_2) ∈ M(ψ(g),m) do
                    B' := B ∪ {(g,f_i;l_1,l_2,r_1,r_2)}
            If FDS(0,D') ≠ Ø then
                L := (G',Ø,M',D',ψ',B',Ø)
                L_new := append(L_new,[L])
```



```
[COMPUTATION OF THE GRÖBNER BASES]
L := L_new
Repeat
    (G,H,M,D,ψ,B,C) := first(L)
    L := rest(L)
    If B ≠ Ø then
        Choose (g_1,g_2;l_1,l_2,r_1,r_2) ∈ B
        B' := B - {(g_1,g_2;l_1,l_2,r_1,r_2)}
        f := lc(g_2) l_1 g_1 r_1 - lc(g_1) l_2 g_2 r_2
        While there is m ∈ Supp(f), l, r ∈ S, g ∈ G ∪ H s.t. m = l ψ(g) r do
            f := f - c(f,m)(c(g,ψ(g)))^-1 l g r
        If f ≠ 0 then
            H' := H ∪ {f}
            For m ∈ Supp(f) do
                M' := M ∪ {m}
                D' := D ∪ {(m,n) : n ∈ Supp(f) - {m}}
                ψ' := ψ ∪ {(f,m)}
                For g ∈ G ∪ H' do
                    For (l_1,l_2,r_1,r_2) ∈ M(ψ(g),m) do
                        C' := C ∪ {(g,f;l_1,l_2,r_1,r_2)}
                If FDS(0,D') ≠ Ø then
                    L := (G,H',M',D',ψ',B',C')
                    L := append(L,[L])
    else [B = Ø]
        if H ≠ Ø then
            G' := G ∪ H
            H' := Ø
            B' := C
            C' := Ø
            L := (G',H',M,D',ψ,B',C')
            L := append(L,[L])
until B = Ø and H = Ø
```

6.8 To prove the correctness of the claim done in 6.5, the following remarks, which the readers can easily prove by themselves, are needed:

1) All over the procedure, for each $(G,H,M,D,\psi,B,C) \in \mathbf{L}$, the following hold:

1.1) G and H are disjoint subsets of $K[S]-\{0\}$

1.2) ψ is a bijection between $G \cup H$ and M;

1.3) for all orderings $<$ in FDS(0,D), $\psi(g) = M_<(g)$ holds for all $g \in G \cup H$,

1.4) for each $(g_1,g_2;l_1,l_2,r_1,r_2) \in B$, one has that $g_1,g_2 \in G$ and

$(l_1,l_2,r_1,r_2) \in M(\psi(g_1),\psi(g_2))$

1.5) for each $(g_1,g_2;l_1,l_2,r_1,r_2) \in C$, one has that $g_1 \in G \cup H$, $g_2 \in H$ and $(l_1,l_2,r_1,r_2) \in M(\psi(g_1),\psi(g_2))$

1.6) let $g_1,g_2 \in G$ and $(l_1,l_2,r_1,r_2) \in M(\psi(g_1),\psi(g_2))$ be s.t. $(g_1,g_2;l_1,l_2,r_1,r_2) \notin B$; let $<$ be an ordering in $FDS(\emptyset,D)$; then the polynomial

$$lc(g_2)\, l_1\, g_1\, r_1 - lc(g_1)\, l_2\, g_2\, r_2$$

has a G-representation in terms of $G \cup H$

1.7) therefore if B and H are empty (implying C is empty too), for all orderings $<$ in $FDS(\emptyset,D)$, one has that each polynomial in $SP(G)$ has a G-representation in terms of G, i.e. G is a Gröbner basis

2) At any call of the **repeat**-loop, for each ordering $<$ in D, there is a unique $(G,H,M,D,\psi,B,C) \in L$, s.t. $<$ is in $FDS(\emptyset,D)$.

3) Since at any call of the **repeat**-loop, the first element of L is extracted, and new elements are added at the end of the list, termination of the procedure in case of the existence of a finite Gröbner basis is guaranteed.

6.9 REMARK As it was remarked in 3.4, once a finite Gröbner basis G of an ideal w.r.t. a well-ordering $<$ is known, we don't need the computability of $<$ (i.e. that, given $m,n \in S$, we can decide whether $m > n$), but just to be able to compute $M_<(g)$ for all $g \in G$.

Therefore, since procedure 6.7, in case of termination, returns such an information, computability of the orderings in a FDR-set doesn't matter at all.

II CONJECTURES

1 GRÖBNER DECIDABILITY AND ESSENTIALLY INFINITE IDEALS

1.1 DEFINITION Let $F \subset K[S]$ be a finite set, I the ideal generated by F. We say F (or I) is Gröbner decidable if there is a computable semigroup well-ordering $<$ and a finite set G, s.t. G is a finite Gröbner basis for I w.r.t. $<$.

1.2 DEFINITION Let $F \subset K[S]$ be a finite set, I the ideal generated by F. We say F (or I) is <u>essentially infinite</u> if for all semigroup well-orderings $<$, the reduced Gröbner basis of I w.r.t. $<$ is of infinite cardinality.

1.3 LEMMA If F is Gröbner decidable then the ideal membership problem for I is decidable.
<u>Proof</u>: there is a computable semigroup well-ordering $<$ such that the reduced Gröbner basis of I w.r.t. $<$ is finite. So one has just to compute a finite Gröbner basis of I w.r.t. $<$ by procedure 1.3.8 and then apply algorithm 1.3.4

1.4 FACT If all semigroups well-orderings are computable, then a finitely generated ideal with undecidable ideal membership problem, is essentially infinite.
<u>Proof</u>: Assume that I is not essentially infinite and that all semigroup well-orderings $<$ are computable.
Since I is not essentially infinite there is a semigroup well-ordering $<$ and a finite set G, s.t. G is a finite Gröbner basis for I.
Since $<$ is computable, F is Gröbner decidable.

2 DENSE SETS OF ORDERINGS

2.1 As it was remarked in 1.6.9, Procedure 1.6.7 allows to skip questions related to computability of orderings in an FDR-set. One can wonder if a version of 1.4 is possible, where no unproved assumption on computability of well-orderings are required.
By analogy with the commutative setting, it is possible to produce such an assertion, which, however, depends on another unproved assumption. The results of [M-R] in the commutative case can be interpreted as follows:

2.2 THEOREM There is a set T of term-orderings s.t.:
i) given a finite set $F \subset (\mathbb{N}^n)^2$, it is possible to decide whether there is $<$ in T s.t. $m < n$ for all $(m,n) \in F$.

ii) for each ideal I, for each term-ordering $<$, there is a term-ordering $<'$ in $\mathbf{T}$, s.t. the reduced Gröbner basis $\{g_1,...,g_t\}$ of I w.r.t. $<'$, is also the reduced Gröbner basis of I w.r.t. $<$, and $M_<(g_i) = M_{<'}(g_i)$ for all i.

Proof: this is a restatement of the results contained in [M-R]. For the set $\mathbf{T}$, one can choose those term-orderings which are compatible with an assignment of strictly positive integer weights assigned to the variables and where ties are broken by the rev-lex ordering; in other terms, those term-orderings associated to arrays $(\underline{d}, -e_n, ..., -e_1)$ where e_i are the canonical basis vectors and $\underline{d} = (d_1,...,d_n)$ with d_i positive integers.

2.3 DEFINITION A set $\mathbf{O}$ of semigroup well-orderings is said to be dense, if for each ideal I, for each well-ordering $<$, s.t. I has a finite Gröbner basis w.r.t. $<$, there is a well-ordering $<'$ in $\mathbf{O}$, s.t. the (finite) reduced Gröbner basis G of I w.r.t. $<'$ is also the reduced Gröbner basis of I w.r.t. $<$, and $M_<(g) = M_{<'}(g)$ for all $g \in G$.

2.4 FACT If a dense FDR-set $\mathbf{O}$ exists, then a finitely generated ideal with undecidable ideal membership problem is essentially infinite.
Proof: Assume I is a finitely generated ideal, which has a finite Gröbner basis w.r.t. a well-ordering $<$, and let G be the reduced Gröbner basis of I w.r.t. $<$, which is finite.
Since $\mathbf{O}$ is dense there is $<'$ in $\mathbf{O}$ such that G is the finite reduced Gröbner basis of I w.r.t. $<'$, and $M_<(g) = M_{<'}(g)$ for all $g \in G$.
Since $\mathbf{O}$ is an FDR-set, Procedure I.6.7 applied to F and $\mathbf{O}$ will return such a G, which can be used to solve the ideal membership problem of I.

III ORDERINGS

1 ARCHIMEDEAN ORDERINGS

1.1 Let $A_n := \{a_1,...,a_n\}$, S_n be the free semigroup generated by A_n and let $<$ be a well-ordering on S_n; w.l.o.g. we can assume $a_1 < a_2 < ... < a_n$.

1.2 LEMMA The following conditions are equivalent:
1) for each $u, w \in S_n$, there is $d \in \mathbb{N}$ s.t. $u^d < w < u^{d+1}$
2) there is $d \in \mathbb{N}$ s.t. $a_1^d < a_n < a_1^{d+1}$

We say $<$ is an archimedean ordering if any of the conditions above is satisfied.
Proof: 2⇒1 for each k, $1 < k < n$, there is d(k) s.t. $a_1^{d(k)} < a_k < a_1^{d(k)+1}$, since $a_1 < a_k < a_n < a_1^{d+1}$.
Therefore for each w there is $d(w) \in \mathbb{N}$ s.t. $a_1^{d(w)} < w < a_1^{d(w)+1}$.
Let e be s.t. $e(d(u)+1) \le d(w)$; f be s.t. $d(w)+1 \le f\,d(u)$; then $u^e < a_1^{e(d(u)+1)} \le a_1^{d(w)} < w < a_1^{d(w)+1} \le a_1^{f\,d(u)} < u^f$.

1.3 LEMMA If $<$ is archimedean, then for each k, $1 < k \le n$, there is $d(k) \in \mathbb{R}$, s.t. for all $t,s \in \mathbb{N}$:
if $t\,d(k) > s$ then $a_k^t > a_1^s$;
if $t\,d(k) < s$ then $a_k^t < a_1^s$.
Proof: for each $i \in \mathbb{N}$, there is $e(i) \in \mathbb{N}$ s.t. $a_1^{e(i)} < a_k^i < a_1^{e(i)+1}$.
For all i,j, since $a_1^{j\,e(i)} < a_k^{ij} < a_1^{j(e(i)+1)}$ and $a_1^{i\,e(j)} < a_k^{ij} < a_1^{i(e(j)+1)}$ then $j\,e(i) \le i(e(j)+1)$, i.e. $e(i)/i \le (e(j)+1)/j$.
If $d(k) := \lim e(i)/i$, then, for all i,j, $e(i)/i \le d(k) \le (e(j)+1)/j$.
Therefore, if $t\,d(k) > s$ then $e(t) \ge s$ and $a_k^t > a_1^{e(t)} > a_1^s$; and if $t\,d(k) < s$ then $e(t)+1 \le s$ and $a_1^s > a_k^t$.

1.4 If $<$ is archimedean, we can then define a semigroup morphism $\deg : S_n \to (\mathbb{R}^+, +)$, by $\deg(a_1) := 1$, $\deg(a_k) := d(k)$ for $1 < k \le n$.
From now on, we will use the following notations: $<$ will denote both an archimedean ordering to S_n and its restriction to S_{n-1}, and deg will denote both the degree morphism on S_n and its restriction to S_{n-1}; we will denote $b := a_n$, $a := a_1$, $D := d(n) := \deg(a_n)$; for all $t \in \mathbb{N}$, e(t) is s.t. $a_1^{e(t)} < a_n^t < a_1^{e(t)+1}$; bold lower case letters will denote elements in S_{n-1}, bold upper case letters will denote elements in S_n.

1.5 LEMMA Let $\mathbf{U} := \mathbf{u}_0\, b^{k(1)}\, \mathbf{u}_1\, b^{k(2)} \dots b^{k(t)}\, \mathbf{u}_t$, and let $k := \Sigma_{i=1...t}\, k(i)$. Then

there are $\mathbf{u}_{d1}$, $\mathbf{u}_{d2}$, $\mathbf{u}_{u1}$, $\mathbf{u}_{u2}$, s.t., denoting $\mathbf{U}_d := \mathbf{u}_{d1}\, b^k\, \mathbf{u}_{d2}$, $\mathbf{U}_u := \mathbf{u}_{u1}\, b^k\, \mathbf{u}_{u2}$, then $\mathbf{U}_d \le \mathbf{U} \le \mathbf{U}_u$ and $\deg(\mathbf{U}) = \deg(\mathbf{U}_d) = \deg(\mathbf{U}_u)$.

Proof: by induction on t. If $t = 1$, one just takes $\mathbf{U}_d := \mathbf{U}_u := \mathbf{U}$.

If $t \ge 2$, then $\mathbf{U} := \mathbf{u}_0\, b^{k(1)}\, \mathbf{u}_1\, b^{k(2)}\, \mathbf{U}$, and it is sufficient to show the thesis for $\mathbf{u}_0\, b^{k(1)}\, \mathbf{u}_1\, b^{k(2)}$.

If $b\,\mathbf{u}_1 < \mathbf{u}_1\, b$ then define $\mathbf{U}_u := \mathbf{u}_0\, \mathbf{u}_1\, b^{k(1)+k(2)}$ and $\mathbf{U}_d := \mathbf{u}_0\, b^{k(1)+k(2)}\, \mathbf{u}_1$ (otherwise interchange $\mathbf{U}_u$ with $\mathbf{U}_d$).

1.6 THEOREM Let $<$ be an archimedean ordering on S_n, and let deg be defined as in 1.4; then $\deg(\mathbf{U}) < \deg(\mathbf{V})$ implies $\mathbf{U} < \mathbf{V}$.

Proof: We can proceed by induction on n, since the case $n = 1$ is trivial. Assume, by contradiction, that there are $\mathbf{U}, \mathbf{V}$ s.t. $\mathbf{U} < \mathbf{V}$ and $\deg(\mathbf{U}) > \deg(\mathbf{V})$.

Then, by the lemma above, there are $\mathbf{U}_d := \mathbf{u}_{d1}\, b^k\, \mathbf{u}_{d2}$, $\mathbf{V}_u := \mathbf{v}_{u1}\, b^h\, \mathbf{v}_{u2}$ s.t. $\mathbf{U}_d < \mathbf{U} < \mathbf{V} < \mathbf{V}_u$ and $\deg(\mathbf{U}_d) = \deg(\mathbf{U}) > \deg(\mathbf{V}) = \deg(\mathbf{V}_u)$.

Therefore, for some $\varepsilon > 0$:

$$\deg(\mathbf{u}_{d1}) + \deg(\mathbf{u}_{d2}) - \deg(\mathbf{v}_{u1}) - \deg(\mathbf{v}_{u2}) = (h - k)\,D + \varepsilon.$$

So, for some $m \in \mathbb{N}$:

$$m\,(\deg(\mathbf{u}_{d1}) + \deg(\mathbf{u}_{d2})) - m\,(\deg(\mathbf{v}_{u1}) + \deg(\mathbf{v}_{u2})) > m\,(h - k)\,D + 2.$$

Applying Lemma 1.3 to $\mathbf{U}_d^m$ and $\mathbf{V}_u^m$, one obtains

$$\mathbf{U}' := \mathbf{u}_1\, b^{mk}\, \mathbf{u}_2,\quad \mathbf{V}' := \mathbf{v}_1\, b^{mh}\, \mathbf{v}_2,$$

s.t. $\mathbf{U}' < \mathbf{U}_d^m < \mathbf{V}_u^m < \mathbf{V}'$ and $\deg(\mathbf{U}') = \deg(\mathbf{U}^m) > \deg(\mathbf{V}^m) = \deg(\mathbf{V}')$.

If $\mathbf{u} := \mathbf{u}_1\, a^{e(mk)}\, \mathbf{u}_2$, $\mathbf{v} := \mathbf{v}_1\, a^{e(mh)+1}\, \mathbf{v}_2$, then $\mathbf{u} < \mathbf{U}' < \mathbf{V}' < \mathbf{v}$, and, by inductive assumption:

$$m\,(\deg(\mathbf{u}_{d1}) + \deg(\mathbf{u}_{d2})) - m\,(\deg(\mathbf{v}_{u1}) + \deg(\mathbf{v}_{u2})) \le e(m\,h) - e(m\,k) + 1.$$

This in turn implies

$$e(m\,h) - e(m\,k) + 1 > m\,(h - k)\,D + 2$$

i.e.

$$m\,k\,D - e(m\,k) > m\,h\,D - e(m\,h) + 1.$$

However, for all i, $(e(i) + 1)/i \ge D \ge e(i)/i$, and so $1 \ge i\,D - e(i) \ge 0$, giving the desired contradiction.

1.7 Let T_n be the free commutative semigroup generated by A_n and denote by $ab : S_n \to T_n$, the canonical semigroup projection.

Let $\log : T_n \to (\mathbb{N}^n, +)$ be the semigroup isomorphism which to each commutative term associates its vector of exponents; the composition $\log ab : S_n \to \mathbb{N}^n$ will be denoted also by log.

To keep notations simple, in the following, the term "partial ordering on S_n" will always mean a partial positive ordering $<$ on S_n, s.t.

1) for $m', m'', l, r \in S$, $l\,m'\,r < l\,m''\,r$ if and only if $m' < m''$

2) for each $m \in S$, the set $\{m' \in S : m \text{ is not comparable with } m'\}$ is finite.

Also the term "total ordering on S_n" will always mean a total semigroup positive ordering on S_n.

1.8 LEMMA Let $<$ be a partial ordering on S_n and σ an ordering on A_n, define $<_\sigma$ to be the following relation on S_n:

$m' <_\sigma m''$ iff $m' < m''$ or m' is not comparable with m'' and m' is less than m'' under the lexicographical ordering induced by σ.

Then $<'$ is an ordering on S_n.

Proof: The only non trivial fact is that if $l, m', m'', r \in S$ and $m' <_\sigma m''$ then $l\,m'\,r <_\sigma l\,m''\,r$. This is clearly true if $m' < m''$, while, if m' is not comparable with m'', then also $l\,m'\,r$ is not comparable with $l\,m''\,r$, by which the claim follows immediately.

1.9 REMARK By linear programming techniques, given a finite set of vectors $D \subset \mathbb{Z}^n$, it is possible to decide:

1) whether there exists $(u_1,\dots,u_n) \in \mathbb{R}^n$ (resp. $(u_1,\dots,u_n) \in \mathbb{Z}^n$) s.t. $\Sigma u_i\, d_i > 0$, for each $(d_1,\dots d_n) \in D$.

2) whether there exists $(u_1,\dots,u_n) \in \mathbb{R}^n$ (resp. $(u_1,\dots,u_n) \in \mathbb{Z}^n$) s.t. $\Sigma u_i\, d_i \ge 0$, for each $(d_1,\dots d_n) \in D$.

In the latter case, it is also possible to compute a maximal subset $D' \subset D$, s.t. if $\Sigma u_i\, d_i \ge 0$ for each $(d_1,\dots d_n) \in D$, then $\Sigma u_i\, d_i = 0$, for each $(d_1,\dots d_n) \in D'$

1.10 Let $\underline{u} := (u_1,\dots,u_n)$ with $u_i \in \mathbb{R}$ and $u_i > 0$ and let σ be an ordering on A_n; the archimedean ordering $<$ s.t., for $v, w \in S_n$, denoting $(d_1,\dots,d_n) := \log(v) - \log(w)$:

$v > w$ iff $\Sigma u_i\, d_i > 0$ or $\Sigma u_i\, d_i = 0$ and v is greater than w in the lexicographical ordering induced by σ

is denoted $\mathbf{ord}(\underline{u}, \sigma)$

1.11 PROPOSITION The sets of orderings

$$\mathbf{AL} := \mathbf{AL}(A_n) := \{\mathbf{ord}((u_1,\dots,u_n),\sigma) : u_i \in \mathbb{R},\ u_i > 0,\ \sigma \text{ an ordering on } A_n\},$$

$$\mathbf{IL} := \mathbf{IL}(A_n) := \{\mathbf{ord}((u_1,\dots,u_n),\sigma) : u_i \in \mathbb{N},\ u_i > 0,\ \sigma \text{ an ordering on } A_n\}$$

are FDR-sets.

Proof: Denote by e_i, i=1...n, the elements in the canonical basis of $\mathbb{Z}^n$.
Given a finite set $D \subset S_n^2$, let $D' := \{\log(v) - \log(w) : (v,w) \in D\}$,
$D'' := D' \cup \{e_1,...,e_n\}$.
If there is $(u_1,...,u_n)$ in $\mathbb{R}^n$ (resp. $\mathbb{Z}^n$) s.t. $\sum u_i d_i > 0$ for all $(d_1,...,d_n) \in D''$, then, $u_i > 0$ for all i, and, for all σ, $\mathbf{ord}((u_1,...,u_n),\sigma) \in FDS(\mathbf{AL},D)$ (resp. $FDS(\mathbf{IL},D)$)
If there is no $(u_1,...,u_n)$ in $\mathbb{R}^n$ (resp. $\mathbb{Z}^n$) s.t. $\sum u_i d_i \geq 0$ for all $(d_1,...,d_n) \in D''$, then $FDS(\mathbf{AL},D)$ (resp. $FDS(\mathbf{IL},D)$) is empty.
If there is $(u_1,...,u_n)$ in $\mathbb{R}^n$ (resp. $\mathbb{Z}^n$) s.t. $\sum u_i d_i \geq 0$ for all $(d_1,...,d_n) \in D''$, let D''_0 be a maximal subset of D'' s.t. $\sum u_i d_i \geq 0$ for all $(d_1,...,d_n) \in D''$ implies $\sum u_i d_i = 0$ for all $(d_1,...,d_n) \in D''_0$; if $D''_0 \cap \{e_1,...,e_n\} \neq \emptyset$, then $FDS(\mathbf{AL},D)$ (resp. $FDS(\mathbf{IL},D)$) is empty.
Otherwise let $D_0 := \{(v,w) \in D : \log(v) - \log(w) \in D''_0\}$. If there is σ s.t. for all $(v,w) \in D_0$, v is greater than w in the lexicographical ordering induced by σ, then $\mathbf{ord}((u_1,...,u_n),\sigma) \in FDS(\mathbf{AL},D)$ (resp. $FDS(\mathbf{IL},D)$); otherwise $FDS(\mathbf{AL},D)$ (resp. $FDS(\mathbf{IL},D)$) is empty.

1.12 It is possible to produce a larger FDR-set consisting of archimedean orderings, by assigning to each variable a degree array, instead of a degree, and again resolving ties by a lexicographical ordering.

2 SOME NON-ARCHIMEDEAN ORDERINGS

2.1 Let $A := \{a_1,...,a_n\}$, $B := \{b_1,...,b_m\}$ be two disjoint finite alphabets, let S_A be the free semigroup generated by A, S_B be the free semigroup generated by B, S be the free semigroup generated by $A \cup B$.
Let $p : S \to S_B$ be the canonical projection.
Let $<_A$ be an ordering (i.e. a total positive semigroup ordering) on S_A, $<_B$ be an ordering on S_B.

2.2 Define $<_l$, $<_r$, $<_{dl}$, $<_{dr}$ on S to be the following relations:

if $\mathbf{U}, \mathbf{V} \in S$, $\mathbf{U} = u_1 X_1 u_2 X_2 \dots u_r X_r u_{r+1}$, $\mathbf{V} = v_1 Y_1 v_2 Y_2 \dots v_s Y_s v_{s+1}$, with $u_i, v_j \in S_A$, $X_i, Y_j \in B$

then:

if $p(\mathbf{U}) = X_1 X_2 \dots X_r <_B Y_1 Y_2 \dots Y_s = p(\mathbf{V})$ then $\mathbf{U} <_l \mathbf{V}$, $\mathbf{U} <_r \mathbf{V}$, $\mathbf{U} <_{dl} \mathbf{V}$, $\mathbf{U} <_{dr} \mathbf{V}$.

if $p(\mathbf{U}) = p(\mathbf{V})$ (i.e. $r = s$ and $X_i = Y_i$ for all i) then:

$\mathbf{U} <_l \mathbf{V}$ iff there is $i \leq r+1$ s.t. $u_j = v_j$ if $j < i$, $u_i <_A v_i$.

$\mathbf{U} <_r \mathbf{V}$ iff there is $i \leq r+1$ s.t. $u_j = v_j$ if $j > i$, $u_i <_A v_i$.

$\mathbf{U} <_{dl} \mathbf{V}$ iff

$u_1 u_2 \dots u_r u_{r+1} <_A v_1 v_2 \dots v_r v_{r+1}$, or

$u_1 u_2 \dots u_r u_{r+1} = v_1 v_2 \dots v_r v_{r+1}$ and $\mathbf{U} <_l \mathbf{V}$

$\mathbf{U} <_{dr} \mathbf{V}$ iff

$u_1 u_2 \dots u_r u_{r+1} <_A v_1 v_2 \dots v_r v_{r+1}$, or

$u_1 u_2 \dots u_r u_{r+1} = v_1 v_2 \dots v_r v_{r+1}$ and $\mathbf{U} <_r \mathbf{V}$

If $<_A$ is denoted by $\mathbf{o}_A$, $<_B$ is denoted by $\mathbf{o}_B$, then we denote $<_l$, $<_r$, $<_{dl}$, $<_{dr}$ resp., by $\mathbf{l}(\mathbf{o}_A,\mathbf{o}_B)$, $\mathbf{r}(\mathbf{o}_A,\mathbf{o}_B)$, $\mathbf{dl}(\mathbf{o}_A,\mathbf{o}_B)$, $\mathbf{dr}(\mathbf{o}_A,\mathbf{o}_B)$.

2.3 PROPOSITION $<_l$, $<_r$, $<_{dl}$, $<_{dr}$ are orderings on S.

Proof: Let $\mathbf{U},\mathbf{V},\mathbf{W}$ be in S and $\mathbf{U} <_l \mathbf{V}$.
If $p(\mathbf{U}) <_B p(\mathbf{V})$ then both $p(\mathbf{U}\,\mathbf{W}) <_B p(\mathbf{V}\,\mathbf{W})$ and $p(\mathbf{W}\,\mathbf{U}) <_B p(\mathbf{W}\,\mathbf{V})$ so $\mathbf{U}\,\mathbf{W} <_l \mathbf{V}\,\mathbf{W}$ and $\mathbf{W}\,\mathbf{U} <_l \mathbf{W}\,\mathbf{V}$.
If, instead, $p(\mathbf{U}\,\mathbf{W}) = p(\mathbf{V}\,\mathbf{W})$, let $\mathbf{U} = u_1 Y_1 u_2 Y_2 \dots u_k Y_k u_{k+1}$, $\mathbf{V} = v_1 Y_1 v_2 Y_2 \dots v_k Y_k v_{k+1}$, $w = w_1 X_1 w_2 X_2 \dots w_r X_r w_{r+1}$; there is then j s.t. $u_i = v_i$ if $i < j$ and $u_j < v_j$. But then:

$\mathbf{U}\,\mathbf{W} = w_1 X_1 w_2 X_2 \dots w_r X_r (w_{r+1} u_1) Y_1 u_2 Y_2 \dots u_{j-1} Y_{j-1} u_j \dots u_k Y_k u_{k+1}$

$\mathbf{V}\,\mathbf{W} = w_1 X_1 w_2 X_2 \dots w_r X_r (w_{r+1} u_1) Y_1 u_2 Y_2 \dots u_{j-1} Y_{j-1} v_j \dots v_k Y_k v_{k+1}$

so that $\mathbf{U}\,\mathbf{W} <_l \mathbf{V}\,\mathbf{W}$ and

$\mathbf{U}\,\mathbf{W} = u_1 Y_1 u_2 Y_2 \dots u_{j-1} Y_{j-1} u_j \dots u_k Y_k (u_{k+1} w_1) X_1 w_2 X_2 \dots w_r X_r w_{r+1}$

$\mathbf{V}\,\mathbf{W} = u_1 Y_1 u_2 Y_2 \dots u_{j-1} Y_{j-1} v_j \dots v_k Y_k (v_{k+1} w_1) X_1 w_2 X_2 \dots w_r X_r w_{r+1}$ so that $\mathbf{U}\,\mathbf{W} <_l \mathbf{V}\,\mathbf{W}$.

An analogous argument holds for $<_r$, $<_{dl}$ and $<_{dr}$.

2.4 Let A, B be two disjoint alphabets generating the free semigroups S_A, S_B; S be the free semigroup generated by $A \cup B$; $\mathbf{O}_A$, $\mathbf{O}_B$ sets of orderings on S_A, S_B, resp..
Let us denote by:

$\mathbf{L}(\mathbf{O}_A,\mathbf{O}_B) := \{\mathbf{l}(\mathbf{o}_A,\mathbf{o}_B) : \mathbf{o}_A \in \mathbf{O}_A, \mathbf{o}_B \in \mathbf{O}_B\}$,

$\mathbf{R}(\mathbf{O}_A,\mathbf{O}_B) := \{\mathbf{r}(\mathbf{o}_A,\mathbf{o}_B) : \mathbf{o}_A \in \mathbf{O}_A, \mathbf{o}_B \in \mathbf{O}_B\}$,

$\mathbf{DL}(\mathbf{O}_A,\mathbf{O}_B) := \{\mathbf{dl}(\mathbf{o}_A,\mathbf{o}_B) : \mathbf{o}_A \in \mathbf{O}_A, \mathbf{o}_B \in \mathbf{O}_B\}$

$\mathbf{DR}(\mathbf{O}_A,\mathbf{O}_B) := \{\mathbf{dr}(\mathbf{o}_A,\mathbf{o}_B) : \mathbf{o}_A \in \mathbf{O}_A, \mathbf{o}_B \in \mathbf{O}_B\}$

$\mathbf{J}(\mathbf{O}_A,\mathbf{O}_B) := \mathbf{L}(\mathbf{O}_A,\mathbf{O}_B) \cup \mathbf{R}(\mathbf{O}_A,\mathbf{O}_B) \cup \mathbf{DL}(\mathbf{O}_A,\mathbf{O}_B) \cup \mathbf{DR}(\mathbf{O}_A,\mathbf{O}_B)$

If $A^{(1)},...,A^{(n)}$ is a sequence of disjoint finite alphabets; $S^{(j)}$ the free semigroup generated by $A^{(j)}$; S the free semigroup generated by the union of the $A^{(j)}$'s; $\mathbf{O}^{(j)}$ a set of orderings on $S^{(j)}$, denote $\mathbf{J}(\mathbf{O}^{(1)},...,\mathbf{O}^{(n)})$ recursively by:

$$\mathbf{J}(\mathbf{D}^{(1)},\dots,\mathbf{D}^{(k)}) := \mathbf{J}(\mathbf{J}(\mathbf{D}^{(1)},\dots,\mathbf{D}^{(k-1)}),\mathbf{D}^{(k)}).$$

2.5 LEMMA If each $\mathbf{D}^{(j)}$ is a FDR-set, such is $\mathbf{J} := \mathbf{J}(\mathbf{D}^{(1)},\dots,\mathbf{D}^{(n)})$.
Proof: Given a finite $D \subset S^2$, if p_n denotes the projection of S onto $S^{(n)}$, denote $D^{(n)} := \{(p_n(\mathbf{U}),p_n(\mathbf{V})) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) \neq p_n(\mathbf{V})\}$.
Also if $\mathbf{U} = \mathbf{u}_1 Y_1 \mathbf{u}_2 Y_2 \dots \mathbf{u}_k Y_k \mathbf{u}_{k+1}$, let $q_n(\mathbf{U}) := \mathbf{u}_1\mathbf{u}_2\dots\mathbf{u}_k\mathbf{u}_{k+1}$
If $D^{(n)} \neq \emptyset$ and $FDS(\mathbf{D}^{(n)},D^{(n)}) = \emptyset$, then $FDS(\mathbf{J},D) = \emptyset$.
If $D^{(n)} = \emptyset$ or $FDS(\mathbf{D}^{(n)},D^{(n)}) \neq \emptyset$, then for each $(\mathbf{U},\mathbf{V}) \in D$ s.t. $p_n(\mathbf{U}) = p_n(\mathbf{V})$, with $\mathbf{U} = \mathbf{u}_1 Y_1 \mathbf{u}_2 Y_2 \dots \mathbf{u}_k Y_k \mathbf{u}_{k+1}$, $\mathbf{V} = \mathbf{v}_1 Y_1 \mathbf{v}_2 Y_2 \dots \mathbf{v}_k Y_k \mathbf{v}_{k+1}$, denote $\mathbf{l}(\mathbf{U},\mathbf{V}) := (\mathbf{u}_j,\mathbf{v}_j)$, $\mathbf{r}(\mathbf{U},\mathbf{V}) := (\mathbf{u}_i,\mathbf{v}_i)$, $\mathbf{d}(\mathbf{U},\mathbf{V}) := (q_n(\mathbf{U}),q_n(\mathbf{V}))$, where j is the first index s.t. $\mathbf{u}_j \neq \mathbf{v}_j$, i the last index s.t. $\mathbf{u}_i \neq \mathbf{v}_i$.
Let $\mathbf{J}' := \mathbf{J}(\mathbf{D}^{(1)},\dots,\mathbf{D}^{(n-1)})$,

$D_l := \{\mathbf{l}(\mathbf{U},\mathbf{V}) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) = p_n(\mathbf{V})\}$,
$D_r := \{\mathbf{r}(\mathbf{U},\mathbf{V}) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) = p_n(\mathbf{V})\}$,
$D_d := \{\mathbf{d}(\mathbf{U},\mathbf{V}) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) = p_n(\mathbf{V}), q_n(\mathbf{U}) \neq q_n(\mathbf{V})\}$,
$D'_l := \{\mathbf{l}(\mathbf{U},\mathbf{V}) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) = p_n(\mathbf{V}), q_n(\mathbf{U}) = q_n(\mathbf{V})\}$,
$D'_r := \{\mathbf{r}(\mathbf{U},\mathbf{V}) : (\mathbf{U},\mathbf{V}) \in D, p_n(\mathbf{U}) = p_n(\mathbf{V}), q_n(\mathbf{U}) = q_n(\mathbf{V})\}$,
$D_{dl} := D_d \cup D'_l$,
$D_{dr} := D_d \cup D'_r$,

If either $FDS(\mathbf{J}',D_l) \neq \emptyset$ or $FDS(\mathbf{J}',D_r) \neq \emptyset$ or $FDS(\mathbf{J}',D_{dl}) \neq \emptyset$ or $FDS(\mathbf{J}',D_{dr}) \neq \emptyset$ (which can be decided recursively), then $FDS(\mathbf{J},D) \neq \emptyset$; otherwise $FDS(\mathbf{J},D) = \emptyset$.

2.6 Denote by $\mathbf{Part}(A)$ the set of all partitions of the finite set A into a sequence of disjoint non-empty subsets $A^{(1)},\dots,A^{(k)}$.
For $\Pi := (A^{(1)},\dots,A^{(k)}) \in \mathbf{Part}(A)$, let $\mathbf{JAL}(\Pi) := \mathbf{J}(\mathbf{AL}(A^{(1)}),\dots,\mathbf{AL}(A^{(k)}))$, if $k > 1$, $\mathbf{JAL}(\Pi) := \mathbf{AL}(A)$ if $k = 1$; $\mathbf{JIL}(\Pi) := \mathbf{J}(\mathbf{IL}(A^{(1)}),\dots,\mathbf{IL}(A^{(k)}))$, if $k > 1$, $\mathbf{JIL}(\Pi) := \mathbf{IL}(A)$ if $k = 1$.
Let $\mathbf{JAL}(A) := \cup_{\mathbf{Part}(A)} \mathbf{JAL}(\Pi)$, $\mathbf{JIL}(A) := \cup_{\mathbf{Part}(A)} \mathbf{JIL}(\Pi)$.
Then both $\mathbf{JAL}(A)$ and $\mathbf{JIL}(A)$ are FDR-sets.

REFERENCES

[BER] G.M.BERGMAN The diamond lemma in ring theory, Adv. Math. **29** (1978), 178-218

[BUC1] B.BUCHBERGER Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph. D. Thesis, Univ. Innsbruck, 1965

[BUC2] B.BUCHBERGER Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aeq. Math. **4** (1970), 374-383

[BUC3] B.BUCHBERGER Gröbner bases: an algorithmic method in polynomial ideal theory, in N.K.BOSE Ed. Recent trends in multidimensional system theory, Reidel (1985)

[DIC] L.E.DICKSON Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, Am. J. of Math. **35** (1913), 413-426

[KRU] J.B.KRUSKAL Well-quasi-ordering, the tree theorem, and Vaszonyi's conjecture, Tran. AMS **95** (1960), 210-225

[MOR] F.MORA Gröbner bases for non-commutative polynomial rings, L.N.C.S. **229** (1986), 353-362

[M-R] T.MORA, L.ROBBIANO The Gröbner fan of an ideal

[NEU] B.H.NEUMANN Some remarks on semigroup presentations, Can. J. Math. **19** (1967), 1018-1026

[NEW] M.H.A.NEWMAN On theories with a combinatorial definition of "equivalence" Ann. Math. **43** (1942), 223-243

[T-C] J.A.TODD, H.S.M.COXETER A practical method for enumerating cosets of a finite abstract group, Proc. Edinburgh Math. Soc. **2** (1936), 26-34