J. Symbolic Computation (2002) **33**, 163–181
doi:10.1006/jsco.2001.0500
Available online at http://www.idealibrary.com on IDEAL®

Regular Gröbner Bases

JONAS MÅNSSON† AND PATRIK NORDBECK†

Lund University, Centre for Mathematical Sciences, Box 118, SE-221 00 Lund, Sweden

In this paper we introduce the concept of bi-automaton algebras, generalizing the automaton algebras previously defined by Ufnarovski. A bi-automaton algebra is a quotient of the free algebra, defined by a binomial ideal admitting a Gröbner basis which can be encoded as a regular set; we call such a Gröbner basis regular. We give several examples of bi-automaton algebras, and show how automata connected to regular Gröbner bases can be used to perform reduction.

1. Introduction

In Ufnarovski (1989), the concept of automaton algebras is introduced. These are quotients of the non-commutative polynomial ring where the defining ideal allows some Gröbner basis with a regular set of leading words. However, nothing is reflected concerning the whole structure of the Gröbner basis (except of course for monomial algebras).

In this paper we introduce the concept of regular Gröbner bases and bi-automaton algebras. Regular Gröbner bases consist of (pure difference) binomials which can be represented, in an appropriate way, as regular sets. The corresponding finite automata allow us to perform reduction with respect to such (in general) infinite bases. In particular, this enables us to do computations in any factor algebra where the defining ideal admits a regular Gröbner basis; we call such an algebra bi-automaton.

We show that most examples of automaton (binomial) algebras given by Ufnarovski are bi-automaton. Moreover, we construct automata showing that all subalgebras of the free algebra generated by a finite set of words are bi-automaton. As a consequence, we find that all algebras allowing a finite SAGBI basis are automaton.

Since a great part of the motivation for our work is to be able to compute normal forms with respect to binomial ideals, we describe how regular Gröbner bases, or more precisely the corresponding automata, can be used to perform reduction.

In the last section we indicate how a prediction algorithm for regular sets, recently developed by the authors, can be used to find regular Gröbner bases.

The subject of this paper has natural applications in the theory of term rewriting in monoid (and group) rings. If we associate the binomial $u - v$ to every rewrite rule $u \to v$ in the semi-Thue system defining a monoid, then the congruence generated by the semi-Thue system corresponds to the ideal generated by the binomials. It is easy to see that every monoid can be presented by a semi-Thue system, so being able to handle binomial ideals allows us to do computations in monoid rings. The correspondence between binomial Gröbner bases and term rewriting systems has been investigated in

†E-mail: {jonasm,nordbeck}@maths.lth.se

0747–7171/02/020163 + 19 $35.00/0

several papers, for example Heyworth (2000) and Madlener and Reinert (1998). We also mention the textbook Baader and Nipkow (1998), where Chapter 8 is devoted to Gröbner bases.

We stress that some of the ideas on which this paper is built are also used in the theory of automatic groups to find automatic structures (see Epstein *et al.*, 1991, 1992). It should be mentioned that the notion "bi-automaton" is inspired by the terminology of Ufnarovski, and has little to do with the term "bi-automatic" in the theory of automatic groups.

2. Basic Definitions and Notation

Let $X = \{x_1, x_2, \ldots, x_n\}$ be a finite alphabet, and let $K\langle X\rangle$ denote the free associative algebra over the arbitrary field K. We denote by X^* the set of all words in X, including the empty word $\mathbf{1}$. In other words, X^* is the free monoid generated by X, and $\mathbf{1}$ is the unity of X^*. We let $\deg w$ denote the length of $w \in X^*$.

If $u, v \in X^*$, and u is a (not necessarily proper) subword of v, then we write $u \mid v$. A word $u \in X^*$ is said to be *reduced* with respect to a set $S \subset X^*$ if for every $v \in S$ we have $v \nmid u$. Further, $S \subset X^*$ is called reduced if every $u \in S$ is reduced with respect to $S \setminus \{u\}$. Given a set $S \subset X^*$, there is an obvious procedure of reducing S; just remove every word of S that has another word in S as subword. We will write $\mathrm{red}(S)$ for this new reduced set.

By an *ideal* we will always mean a two-sided ideal of $K\langle X\rangle$. If the ideal I is generated by some set $F \subset K\langle X\rangle$ (not necessarily finite), then we write $I = \langle F\rangle$. We will call a binomial a *pure binomial* if it is a difference of two words, i.e. of the form $u - v$ with $u, v \in X^*$. An ideal I will be called a *pure binomial ideal* if it can be generated by pure binomials, and we then say that $K\langle X\rangle/I$ is a *pure binomial algebra*. The alphabet X together with a set of generators for I is called a *presentation* for $K\langle X\rangle/I$. Following common practice, we will sometimes also call the elements of X *generators*, and the generators of I *defining relations* of the algebra.

2.1. Regular sets and automata

We now mention some facts we will use from the theory of languages and automata. For a more complete exposition we refer to Eilenberg (1974).

Given $S_1, S_2 \subset X^*$, we have their product $S_1S_2 = \{uv \mid u \in S_1, v \in S_2\}$. For a subset S of X^* we then define $S^* = \cup_{i=0}^{\infty} S^i$. Thus S^* is the monoid generated by S, and the notion agrees with the previously defined X^*. A subset of X^* is called *regular* if it can be obtained from finite subsets of X^* by finitely many applications of $\cup$ (union), $\cdot$ (multiplication) and $*$ (the above defined star-operator).

Recall that a *finite automaton* is a 5-tuple (Q, Q_i, Q_a, X, δ), where Q is a finite set of *states*, Q_i and Q_a distinguished subsets of Q consisting of the *initial states* and the *accepting states*, respectively, X a finite alphabet and δ the *transition function* from $Q \times X$ into 2^Q (the set of all subsets of Q). We will as usual represent finite automata as directed graphs, the states being the vertices and the transition function defining the edges, i.e. there will be an edge from q to q' $(q, q' \in Q)$ labelled $x \in X$ if and only if $q' \in \delta(q, x)$. The set of words *accepted* by an automaton consists of all words obtained by reading a path starting from an initial state and ending at an accepting state. We will sometimes write $\mathcal{L}(\mathcal{M})$ for the set (language) accepted by the automaton $\mathcal{M}$.

An automaton is called *deterministic* if there is a unique initial state and δ is a function from $Q \times X$ into $Q \cup \{\emptyset\}$, i.e. if for each $q \in Q$ and each $x \in X$ there is at most one edge labelled x going out from q. Given a non-deterministic automaton $\mathcal{M} = (Q, Q_i, Q_a, X, \delta)$, there is an algorithm for constructing a deterministic automaton $\mathcal{M}_D = (Q', q_0, Q'_a, X, \delta')$ accepting the same set as $\mathcal{M}$. The new automaton is obtained using the following classical *powerset construction*:

The states Q' of $\mathcal{M}_D$ will be 2^Q. The (unique) initial state q_0 is Q_i, the new transition function $\delta' : 2^Q \times X \to 2^Q$ is defined by $\delta'(S, x) = \{\delta(q, x) \mid q \in S\}$ and $Q'_a = \{S \mid S \cap Q_a \neq \emptyset\}$. If $\mathcal{M}$ has k states, then $\mathcal{M}_D$ formally has 2^k states. But since we only need to consider states contained in "successful" paths, the automaton $\mathcal{M}_D$ will often have considerably fewer states. Worst case examples are provided in Crochemore and Rytter (1994) and Månsson (2000a).

The regular sets are exactly the sets accepted by automata; this is the content of *Kleene's Theorem*, which can be found in any textbook on automata theory. For later reference, we recall a few well-known facts about regular sets:

LEMMA 1. *If S is a regular set, then the reduced set* $\mathrm{red}(S)$ *is also regular.*

LEMMA 2. *Let $\phi : X^* \to Y^*$ be a monoid morphism. If $S \subset X^*$ is regular, then so is $\phi(S) \subset Y^*$.*

In the sequel we will need examples of non-regular structures. We then use the set

$$S = \{ax^k y^k b \mid k \geq 1\} \subset \{a, b, x, y\}^*$$

or variations thereof. These sets can be shown not to be regular by using, for example, the *Pumping lemma* (Eilenberg, 1974, Proposition 5.1), and we will sometimes refer to such a set as *our standard example of a non-regular set.*

2.2. GRÖBNER BASES

In this section we collect the material we need concerning (non-commutative) Gröbner bases. For an extensive treatment we refer to Mora (1994).

We will always, in what follows, assume that X^* is given an *admissible ordering*, i.e. a well-ordering preserved under multiplication: $w < w'$ implies $uwv < uw'v$ for all $u, v, w, w' \in X^*$. As an example we mention *deglex* (degree lexicographical):

$$w < w' \Leftrightarrow \begin{cases} \deg w < \deg w' \\ \text{or } \deg w = \deg w' \text{ but } w' \text{ is greater than} \\ w \text{ lexicographically.} \end{cases}$$

When an admissible ordering is chosen we can (if terms with identical words are collected together using the operations over K) with every non-zero element $f \in K\langle X\rangle$ associate its *leading word* $\widehat{f} \in X^*$. We also define, for a subset $F \subset K\langle X\rangle$, $\widehat{F} = \{\widehat{f} \mid f \in F\}$. For a (pure) binomial $f = u - v$ with $\widehat{f} = u$, we will sometimes refer to v as the *non-leading word* of f.

A word $u \in X^*$ will be called *normal* modulo an ideal I if u is reduced with respect to $\widehat{I}$, i.e. if for every $f \in I$ we have $\widehat{f} \nmid u$. If N denotes the K-span of all normal words modulo I, then $K\langle X\rangle = N \oplus I$ as direct sum of vector spaces (see, for example, Ufnarovski

(1995, Theorem 2.3)), so the normal words constitute a K-basis for $K\langle X\rangle/I$. For every $f \in K\langle X\rangle$, its image by the projection $K\langle X\rangle \to N$ will be called its *normal form*, and be denoted $\bar{f}$. The map $f \to \bar{f}$ will be referred to as *reduction*. If we define a multiplication on N by $f \cdot g = \overline{fg}$, then N together with this operation is isomorphic to $A = K\langle X\rangle/I$. Thus the possibility to perform reduction allows us to make computations in A. The tool for the reduction is Gröbner bases.

Definition 1. (Gröbner Basis) A subset G of an ideal I in $K\langle X\rangle$ is called a *Gröbner basis* for I if for every $f \in I$, $f \neq 0$, there exists $g \in G$ such that $\widehat{g} \mid \widehat{f}$.

Recall that a Gröbner basis G is called *minimal* if $\widehat{G}$ is reduced, and G is called *reduced* if in addition every $g \in G$ is of the form $g = w - \bar{w}$ where $w = \widehat{g}$.

It can be shown that if G is a Gröbner basis for I, then G generates I. We may (and will) therefore simply say that G is a Gröbner basis, meaning that G is a Gröbner basis for the ideal generated by G.

Bergman's Diamond lemma (Bergman, 1978) provides us with a method for checking whether a given set G is a Gröbner basis. Using the language of Green (1994), we say that $g_i, g_j \in G$ form an *overlap* if $\widehat{g_i} = u\widehat{g_j}v$ or $\widehat{g_i}u = v\widehat{g_j}$ for some $u, v \in X^*$ (in the second case $g_i = g_j$ is allowed if $u, v \neq \mathbf{1}$). An *overlap relation* of g_i, g_j is then defined as $g_i - cug_jv$ or $g_iu - cvg_j$, where $c \in K$ is such that the leading words cancel out. Note that one pair in G can give rise to several overlap relations. The set G can then be shown to be a Gröbner basis if (and only if) all overlap relations arising from G "reduce" to zero using only the elements of G.

The Diamond lemma also naturally induces a procedure for computing a Gröbner basis, starting from a given set of generators G: we enlarge G with the non-zero "reductums" of the overlap relations and start over to apply the Diamond lemma on this new larger set. This procedure will be referred to as Mora's algorithm, and is a generalization of Buchberger's algorithm in the commutative case (see, for example, Buchberger, 1985).

Following Anick (1986), a non-normal word (modulo some ideal I), all of whose proper subwords are normal, will be called an *obstruction*. It is easily seen that the set $\mathcal{O}$ of all obstructions is exactly $\widehat{G}$, where G is any minimal Gröbner basis for I in our given ordering. Moreover, even if a Gröbner basis G is not minimal, $\widehat{G}$ must clearly contain all obstructions, and turning $\widehat{G}$ into a reduced set we obtain $\mathrm{red}(\widehat{G}) = \mathcal{O}$.

3. Automaton Algebras

In this section we recall the concept of automaton algebras, introduced by Ufnarovski (1989). We begin with the definition.

Definition 2. (Automaton Algebra) An algebra $A = K\langle X\rangle/I$ is called an *automaton algebra* if there exists an ordering such that the normal words (modulo I) constitute a regular set.

The regularity of the normal words implies some nice properties of the algebra, e.g. alternativity of the *growth* and rationality of the *Hilbert series*. We refer to Ufnarovski (1989) for terminology and proofs.

Using basic manipulations with regular sets, we can prove

Proposition 1. (Ufnarovski (1989, Theorem 7)) *Given an ideal I of $K\langle X\rangle$ and an ordering, the set of normal words is regular if and only if the set of obstructions is regular.*

We next show that we have an automaton algebra not only if the obstruction set is regular, but also if the leading words of any Gröbner basis form a regular set.

Corollary 1. *Let G be a Gröbner basis for I (in the given ordering). If $\widehat{G}$ is regular, then the set of normal words is also regular.*

Proof. The result follows from Proposition 1 if we show that the obstruction set $\mathcal{O}$ is regular. As could be seen in Section 2.2, $\mathcal{O} = \mathrm{red}(\widehat{G})$, so the regularity of $\mathcal{O}$ follows from Lemma 1. □

In Ufnarovski (1995) it is conjectured that the property of being automaton is dependent on the generators of the algebra. We now give an easy example verifying this fact.

Example 1. We consider the ideal I of $K\langle a, b, x, y\rangle$ generated by

$$G = \{ax^k y^k b \,|\, k \geq 1\}.$$

It is easy to see that G is reduced, and since every set consisting of only words is a Gröbner basis, G is the (only) obstruction set for I. But G is our standard example of a non-regular set, and thus by Proposition 1 we conclude that $K\langle a, b, x, y\rangle/I$ is not automaton in the given presentation.

But if we make the linear change of variables

$$a \to a, \qquad b \to b, \qquad x \to x, \qquad y \to x + y,$$

then our factor algebra is presented as $A = K\langle a, b, x, y\rangle/J$, where J is generated by $G' = \{g_k \,|\, k \geq 1\}$ with

$$g_k = ax^k(x+y)^k b = ax^{2k}b + ax^{2k-1}yb + ax^{2k-2}yxb + ax^{2k-2}y^2b + \cdots + ax^k y^k b.$$

Using deglex with $x > y$ we get $\widehat{G'} = \{ax^{2k}b \,|\, k \geq 1\} = \{ax^2(x^2)^* b\}$ which clearly is regular. We see that $\widehat{G'}$ does not give rise to any overlaps, so G' is a Gröbner basis for J, and A is automaton in the latter presentation by Corollary 1.

This example also shows that it is essential that we are allowed to choose the ordering in Definition 2, since letting $y > x$ yields the non-regular obstruction set $\widehat{G'} = \{ax^k y^k b \,|\, k \geq 1\}$. We thus have proved

Corollary 2. *The regularity of the set of normal words depends both on the choice of ordering and the choice of generators.*

We mention the remarkable fact that the automaton property for a group (as defined in Epstein *et al.*, 1992) does not depend on the choice of generators.

One may wonder if there exist *finitely* presented algebras (I finitely generated) that are not automaton. In Shearer (1980), an example of a finitely presented algebra with non-rational Hilbert series is given, so this algebra cannot be automaton. We next provide

a new simple example of a non-automaton algebra where the ideal is generated by only two defining relations.

EXAMPLE 2. Let I be the ideal in $K\langle a, x, y\rangle$ generated by

$$\{axya - xya, xy - yx\}.$$

Computations show that

$$G = \{ay^i x^i a - y^i x^i a, xy - yx \mid i \geq 1\}$$

is a reduced Gröbner basis for I in any admissible ordering with $xy > yx$. Since clearly $ay^i x^i a > y^i x^i a$ for all i, it follows that the obstruction set is the non-regular set $\widehat{G} = \{ay^i x^i a, xy \mid i \geq 1\}$. An analogous argument holds for the case $yx > xy$, so $A = K\langle a, x, y\rangle / I$ is not automaton for the given set of generators $\{a, x, y\}$. We cannot however exclude the possibility of A being automaton in another presentation.

REMARK 1. We just mention that sets of the form $\{ax^k y^k b \mid k \geq 1\}$ belong to the class of *context-free* sets, and these are exactly the sets accepted by *stack automata*. Thus the algebra in Example 2 may be what we might call a stack automaton algebra. However, by using the idea of Example 2, and adding more generators and commutators in an appropriate way, we can construct ideals with obstruction sets where three (or arbitrary many) exponents are coupled to each other. Since sets of the form $\{ax^k y^k z^k a \mid k \geq 1\}$ are not context-free, we can consequently find examples of "non-stack automaton algebras".

Example 2 shows that algebras with two defining relations may not be automaton. Whether all finitely generated algebras with one defining relation are automaton seems to be an open question. We conjecture that this is the case. The necessary condition, rationality of Hilbert series (in the homogeneous case), was proved in Backelin (1978) using the different approach of distributive lattices. That the problem is not entirely easy is demonstrated by the following example, showing that regularity of the obstruction set is also dependent on the ordering in the one-relation case.

EXAMPLE 3. Let I be the ideal in $K\langle x, y\rangle$ generated by the homogeneous generator $f = xyx - yx^2$. The corresponding factor algebra $A = K\langle x, y\rangle / I$ is automaton since, for example, deglex with $y > x$ implies that f alone constitutes a Gröbner basis. On the other hand, deglex with $x > y$ yields the reduced Gröbner basis

$$G = \{xy^i x^i - y^i x^{i+1} \mid i \geq 1\}$$

and the obstructions $\widehat{G} = \{xy^i x^i \mid i \geq 1\}$, a non-regular set.

4. Regular Gröbner Bases

To motivate our study of the objects soon to be defined, we consider the ideal $I = \langle x^2 - xy\rangle$ of $K\langle x, y\rangle$, using deglex with $x > y$. The initial computations when applying Mora's algorithm on $\{x^2 - xy\}$ yield the sequence

$$x^2 - xy, \qquad xyx - xy^2, \qquad xy^2x - xy^3, \qquad xy^3x - xy^4.$$

We suspect that $G = \{xy^k x - xy^{k+1} \mid k \geq 0\}$ is a Gröbner basis for I, and this is easily verified using the Diamond lemma.

In general, sets where the exponents are coupled to each other (like k and $k+1$ in G) are not regular; the set $\{ax^k y^k b \,|\, k \geq 1\}$ was mentioned earlier. But we will next see that if we in our present example instead consider pairs of letters, then G will be regular in these pairs. More precisely, the binomials in question are identified with elements in $(\{x,y\} \times \{x,y\})^*$ in the following way:

$$xx - xy \leftrightarrow (x,x)(x,y) \text{ and generally } xy^k x - xy^{k+1} \leftrightarrow (x,x)(y,y)^k(x,y).$$

We can then write

$$G = \{xy^k x - xy^{k+1} \,|\, k \geq 0\} = \{(x,x)(y,y)^*(x,y)\},$$

and it follows that G is regular in the alphabet consisting of the three "letters" (x,x), (x,y) and (y,y). Inspired by our success with this example, we will now try to formalize these ideas.

If the elements in G are not homogeneous, then it is clear that we cannot use only pairs in X. We will therefore use as our new alphabet

$$\mathcal{X} = (X \times \{\mathbf{1}\}) \cup (\{\mathbf{1}\} \times X).$$

Define the map $\varphi : \mathcal{X}^* \to K\langle X \rangle$ by

$$\varphi((x_1, x_1') \cdots (x_t, x_t')) = x_1 \cdots x_t - x_1' \cdots x_t', \tag{1}$$

and the "projections" $\varphi_1, \varphi_2 : \mathcal{X}^* \to X^*$ by

$$\varphi_1((x_1, x_1') \cdots (x_t, x_t')) = x_1 \cdots x_t, \qquad \varphi_2((x_1, x_1') \cdots (x_t, x_t')) = x_1' \cdots x_t'. \tag{2}$$

For a set $S \subset \mathcal{X}^*$ we, as usual, write $\varphi(S) = \{\varphi(s) \,|\, s \in S\}$, and analogously for φ_1 and φ_2. Note that every element in the image of φ is a pure binomial.

Remark 2. In some sense, the $\mathbf{1}$ is just a "dummy" variable as long as it is included in a pair above (i.e. an element of $\mathcal{X}$). But we have chosen to use exactly the unity of X^* to get nice formulations of (1) and (2).

We can now define the main object of this paper.

Definition 3. (Regular Gröbner Basis) Let $G \subset K\langle X \rangle$ be a Gröbner basis consisting of pure binomials. Then we say that G is a *regular Gröbner basis* if there exists a regular set $S \subset \mathcal{X}^*$ with $\varphi(S) = G$ and $\varphi_1(S) = \widehat{G}$.

Remark 3. We could, of course, have chosen to use $\mathcal{X}' = (X \cup \{\mathbf{1}\}) \times (X \cup \{\mathbf{1}\})$ instead. However, we note that if we have a regular set $S' \subset \mathcal{X}'^*$, then a corresponding set $S \subset \mathcal{X}$ is obtained by writing all pairs (x,x'), $x, x' \in X$, as $(x,\mathbf{1})(\mathbf{1},x')$ (or $(\mathbf{1},x')(x,\mathbf{1})$). This new set S is also regular by Lemma 2, defining the monoid morphism $\mathcal{X}'^* \to \mathcal{X}^*$ in the obvious way. It is also clear that the set of binomials $\varphi(S)$ is the same as the correspondingly defined $\varphi(S')$, so we cannot have any regular Gröbner bases defined by $\mathcal{X}'$ that we cannot obtain with our approach using $\mathcal{X}$. Moreover, if we by a *factorization* of a (pure) binomial mean the inverse action of φ, then every binomial has a factorization in $\mathcal{X}^*$ that is unique up to the order of the factors. The same is, of course, not true for $\mathcal{X}'^*$.

As mentioned in the introduction, the idea of working with pairs is also used in the theory of automatic groups during the process of computing automatic structures. However,

sometimes only orderings where a longer word always is greater than a shorter one are considered. The shorter word is then "padded" with a dummy symbol \$ (corresponding to our use of $\mathbf{1}$) at the end of the word, and the products of pairs are always of the form, for a (pure) binomial $x_{i_1}\cdots x_{i_s} - x_{j_1}\cdots x_{j_t}$, $s \geq t$,

$$(x_{i_1}, x_{j_1})\cdots(x_{i_t}, x_{j_t})(x_{i_{t+1}}, \$)\cdots(x_{i_s}, \$). \tag{3}$$

We next give an example where the representations in (3) are not sufficient to obtain regularity. We mention that the general case is also considered in the theory of automatic groups in connection with *asynchronous automaticity*; see Epstein *et al.* (1992, Chapter 7).

Example 4. Consider the (reduced) Gröbner basis

$$G = \{g_k = ax^{2k}b - ax^k \mid k \geq 1\} \subset K\langle a, b, x\rangle.$$

The representation of each g_k in form (3) becomes $(a,a)(x,x)^k(x,\$)^k(b,\$)$, so G is represented as $\{(a,a)(x,x)^k(x,\$)^k(b,\$) \mid k \geq 1\}$, which we have seen is not regular. However, using the alphabet $\mathcal{X}$ (with $X = \{a, b, x\}$), it is easy to see that G can be represented as the regular set $\{(a,\mathbf{1})(\mathbf{1},a)((x,\mathbf{1})(x,\mathbf{1})(\mathbf{1},x))^k(b,\mathbf{1})|k \geqslant 1\}$.

We now give the factor algebras corresponding to regular Gröbner bases a name of its own:

Definition 4. (Bi-automaton Algebra) If the ideal $I \subset K\langle X\rangle$ admits a regular Gröbner basis in some ordering (on X^*), then we say that $A = K\langle X\rangle/I$ is a *bi-automaton algebra*.

Just as for automaton algebras, this definition is dependent on the generators of A; a pure binomial ideal may not even be binomial in another presentation.

We next show that the class of automaton algebras contains all bi-automaton algebras.

Proposition 2. *If A is a bi-automaton algebra, then A is also an automaton algebra.*

Proof. Assuming that $A = K\langle X\rangle/I$ is bi-automaton, we need to show that the set of normal words modulo I is regular. By Corollary 1 it is sufficient to find a Gröbner basis G for I with $\widehat{G}$ regular.

Since I admits a regular Gröbner basis, there is a regular set $S \subset \mathcal{X}$ with $\varphi(S) = G =$ a Gröbner basis for I and $\varphi_1(S) = \widehat{G}$. But it is easily seen that φ_1 is a monoid morphism, so the proposition follows from Lemma 2. □

The following proposition shows that there is no lack of generality if we assume that our regular Gröbner bases are minimal. The result follows by the same principle as Proposition 2.2 in Månsson (2000a).

Proposition 3. *If G is a regular Gröbner basis for some ideal $I \subseteq K\langle X\rangle$, then there exists a minimal regular Gröbner basis G_M for I.*

PROOF. Let $S \subseteq \mathcal{X}^*$ be a regular set with $\varphi(S) = G$ and $\varphi_1(S) = \widehat{G}$. We have seen in the proof of Proposition 2 that $\widehat{G}$ is a regular set, so by Lemma 1 it follows that $\mathcal{O} = \mathrm{red}(\widehat{G})$ is regular. Using a slight modification of the standard procedure of constructing product automata, we can, from the automata for S and $\mathcal{O}$, obtain an automaton $\mathcal{M}''$ such that $\mathcal{L}(\mathcal{M}'') \subset S$ and $\varphi_1(\mathcal{L}(\mathcal{M}'')) = \mathcal{O}$; in other words, $G_M = \varphi(\mathcal{L}(\mathcal{M}''))$ is a minimal regular Gröbner basis for I. □

5. Examples of Regular Gröbner Bases

In this section we give examples of bi-automaton algebras. We point out that all the algebras considered are homogeneous, or can be made homogeneous with an appropriate grading on the generators, and the reduction procedure of computing normal forms modulo a homogeneous ideal is algorithmic also using standard Gröbner bases techniques.

5.1. THE AUTOMATON ALGEBRAS OF UFNAROVSKI

As promised in the introduction, we now show that some of the automaton binomial algebras mentioned in Ufnarovski (1989) are bi-automaton as well. The following proposition is taken from the original paper by Ufnarovski.

PROPOSITION 4. (UFNAROVSKI (1989, THEOREM 9)) *The following classes of finitely generated algebras consist of automaton algebras:*

(a) commutative algebras;
(b) algebras defined by two homogeneous relations of degree two;
(c) algebras defined by identifying with zero a finite number of words;
(d) algebras with defining relations determined by the commutativity $([x_i, x_j] = 0)$ *of some generators.*

We will prove that all algebras in *(a)* and *(d)* defined by pure binomials are bi-automaton. We also believe that the binomial algebras in *(b)* can be shown to be bi-automaton by simply checking all relevant cases in a long and tedious procedure. The algebras in *(c)* are not defined by binomials, and are, therefore, of no interest to us.

PROPOSITION 5. *All the* (*pure*) *binomial algebras in Proposition 4(a), (d) are bi-automaton.*

PROOF. *(a)* A commutative algebra can be seen as a quotient of the free algebra, where the defining ideal I contains all commutators. We choose the deglex ordering on $X = \{x_1, \ldots, x_n\}$ with $x_n > \cdots > x_1$, and let C denote the set $\{x_j x_i - x_i x_j \mid 1 \leq i < j \leq n\}$ of all commutators. It is easy to see (for example, by applying Mora's algorithm) that the pure binomial ideal I has a Gröbner basis G consisting of pure binomials. It is also not hard to realize that if H is the set obtained from G by removing all elements where the leading word is not of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, then $H \cup C$ is a Gröbner basis for I. We may also assume that the non-leading words of H are "reduced with respect to C", so every element of H is of the form

$$p = x_1^{\alpha_1} \cdots x_i^{\alpha_i} \cdots x_n^{\alpha_n} - x_1^{\alpha'_1} \cdots x_i^{\alpha'_i} \cdots x_n^{\alpha'_n}. \tag{4}$$

Let $p \in I$ be as in (4). By using the commutators, we also see that

$$x_i p \equiv x_1^{\alpha_1} \cdots x_i^{\alpha_i+1} \cdots x_n^{\alpha_n} - x_1^{\alpha'_1} \cdots x_i^{\alpha'_i+1} \cdots x_n^{\alpha'_n} \in I.$$

Since this procedure can be repeated for every $x_i \in X$ an arbitrary number of times we see, starting from $p \in I$, that the set

$$p^{(*)} = \{x_1^{\alpha_1+i_1} \cdots x_n^{\alpha_n+i_n} - x_1^{\alpha'_1+i_1} \cdots x_n^{\alpha'_n+i_n} \mid i_j \geq 0, 1 \leq j \leq n\}$$

of binomials is contained in I, and this set can be encoded as the regular set

$$s_p^{(*)} = \{(x_1, \mathbf{1})^{\alpha_1}(\mathbf{1}, x_1)^{\alpha'_1}((x_1, \mathbf{1})(\mathbf{1}, x_1))^* \cdots (x_n, \mathbf{1})^{\alpha_n}(\mathbf{1}, x_n)^{\alpha'_n}((x_n, \mathbf{1})(\mathbf{1}, x_n))^*\}.$$

We note that our choice of ordering implies that the leading word is preserved when passing from p to the elements of $p^{(*)}$, i.e. if the leading word of p is $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, then the $x_1^{\alpha_1+i_1} \cdots x_n^{\alpha_n+i_n}$ are the leading words of $p^{(*)}$.

Recall that all words occurring in the elements of H are of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. By Dickson's Lemma (Dickson, 1913), there is a finite subset $W \subset \widehat{H}$ such that for each $w = x_1^{\beta_1} \cdots x_n^{\beta_n} \in \widehat{H}$, there exists $w' = x_1^{\beta'_1} \cdots x_n^{\beta'_n} \in W$ with $\beta'_i \leq \beta_i$ for all i (i.e. w' divides w in the commutative sense). We let $P \subset H$ be the set of binomials corresponding to the leading words W. It is then not hard to see that the set of leading words of $P^{(*)} = \{p^{(*)} \mid p \in P\}$ must contain $\widehat{H}$. It follows that the finite union

$$S = \bigcup_{p \in P} s_p^{(*)} \cup \{x_j x_i - x_i x_j \mid i < j\}$$

is a regular set proving that I admits a regular Gröbner basis.

(d) Choose again a deglex ordering on X, and let P be the set of all ordered pairs x, y of elements in X such that $x > y$ and $xy - yx$ is one of the defining relations. For $y \in X$, further let $c_y = \{z \in X \mid y > z,\ yz - zy = 0\}$. According to the proof of Theorem 9(d) in Ufnarovski (1989), the finite union

$$G = \bigcup_{x,y \in P} \{xwy - yxw \mid w \in c_y^*\}$$

is a Gröbner basis for the ideal generated by the present commutators. The corresponding factor algebra is then bi-automaton, since the regular set

$$S = \bigcup_{x,y \in P} \{(x, \mathbf{1})(\mathbf{1}, y)(\mathbf{1}, x)\{(z, \mathbf{1})(\mathbf{1}, z) \mid z \in c_y\}^*(y, \mathbf{1})\}$$

shows that G is in fact a regular Gröbner basis. □

We showed in Proposition 2 that every bi-automaton algebra is automaton, and we have just seen examples of automaton algebras that are bi-automaton. However, not every automaton algebra defined by pure binomials is bi-automaton, as the following example illustrates.

Example 5. We consider the ideal I of $K\langle a, b, x, y\rangle$ generated by

$$G = \{ax^{2k}b - ax^k y^k b \mid k \geq 1\}.$$

The algebra $K\langle a, b, x, y\rangle/I$ is automaton for the same reason as $K\langle a, b, x, y\rangle/J$ in Example 1. We claim that no matter what admissible ordering we choose, the set of leading words $\widehat{G}$ will be either

$$S_1 = \{ax^{2k}b \mid k \geq 1\} \qquad \text{or} \qquad S_2 = \{ax^k y^k b \mid k \geq 1\}$$

(and no mix between them). Since $x > y$ clearly implies $x^k > y^k$ and $y > x$ implies $y^k > x^k$, our claim follows from the multiplication preserving property for orderings. We also note that there are no overlaps among S_1 or S_2, and these sets are, moreover, reduced. Consequently, G is a Gröbner basis in every ordering, and the set of obstructions is either S_1 or S_2. Since an ordering uniquely determines the obstruction set, S_1 or S_2 is in fact the set of leading words of any minimal Gröbner basis.

Assume now that I admits some regular Gröbner basis G'; by Proposition 3 we can assume that G' is minimal, so $\widehat{G'}$ is either S_1 or S_2. Since S_2 is our standard example of a non-regular set, we must in fact have $\widehat{G'} = S_1$. By an obvious modification of Proposition 2, we also see that the non-leading words $\varphi_2(G')$ must be a regular set. We claim that this set $\varphi_2(G')$ is exactly S_2, contradicting the assumption that $K\langle a, b, x, y\rangle/I$ is bi-automaton. One verifies easily (e.g. by using the Gröbner basis G previously presented) that $ax^k y^k b$ is the only word equal to $ax^{2k}b$ modulo I. It follows that every element of G' must be of the form $ax^{2k}b - ax^k y^k b$, and we are done.

5.2. SUBALGEBRAS FINITELY GENERATED BY WORDS

We will now study presentation ideals (defined later) for finitely generated submonoids of a free monoid. The regularity of the set of relations associated with such a monoid was first proved by Markov (1971/1972), constructing a finite state grammar. Another construction is due to Spehner (1974/75) (see also Lallement, 1979), which also yields an explicit presentation of the set of relations.

In this section we give a new construction for the presentation ideal, adjusting it to the terminology introduced in Section 4. Moreover, we will show how this presentation ideal can be associated with the concept of Gröbner bases, by providing an explicit construction of a regular Gröbner basis for the presentation ideal for any finitely generated submonoid of a free monoid.

Let $U = \{u_1, u_2, \ldots, u_k\}$ be a finite subset of different non-empty words in X^*, and let $Y = \{y_1, y_2, \ldots, y_k\}$ be a finite alphabet of the same cardinality as U. We define the K-algebra homomorphism $\mu : K\langle Y\rangle \to K\langle X\rangle$ by $\mu(y_i) = u_i$ for all i. We can show that the kernel $\ker\mu$ is a pure binomial ideal in $K\langle Y\rangle$ (cf. Sturmfels (1996, Lemma 4.1)), and is homogeneous with the inherited graduation from X^*. Since the subalgebra $K\langle U\rangle$ generated by U is the image of μ, we know that $K\langle U\rangle$ is isomorphic to $K\langle Y\rangle/\ker\mu$. The ideal $\ker\mu$ is called the *presentation ideal* for $K\langle U\rangle$. This presentation ideal can be calculated by standard Gröbner basis techniques using an appropriate ordering:

PROPOSITION 6. *Let $H = \{h_1, h_2, \ldots, h_k\}$ be a set of elements in $K\langle X\rangle$ and $\mu : K\langle Y\rangle = K\langle y_1, \ldots, y_k\rangle \to K\langle X\rangle$ the homomorphism defined by $\mu(y_i) = h_i$ for all i. If G is a Gröbner basis for the ideal $\langle y_i - h_i \mid 1 \le i \le k\rangle \subseteq K\langle X, Y\rangle$ with respect to some elimination ordering with $X > Y$, then $G \cap K\langle Y\rangle$ is a Gröbner basis for* $\ker\mu$.

This method was first presented in Shannon and Sweedler (1988), and the small adjustments required to make it work in the non-commutative case can be found in Nordbeck (1998b). An elimination ordering with $X > Y$ is, loosely speaking, an ordering where a word containing a letter of X is greater than any word containing only the Y-letters.

As we can see, Proposition 6 is valid not only for words u_i, but for arbitrary elements of $K\langle X\rangle$. The major problem with this technique is, of course, that the computation of Gröbner bases need not terminate in our non-commutative setting. However, we will now

show how a regular Gröbner basis for a presentation ideal can be obtained (algorithmically) by constructing an automaton for the set of irreducible relations (see later) arising from a set of words U, and corresponding to the set S in Definition 3.

Recall the sets U and Y, and the map μ defined above. By a *relation* we will in this section mean a pair of different words

$$(w, w') = (y_{i_1} y_{i_2} \cdots y_{i_k},\, y_{j_1} y_{j_2} \cdots y_{j_l}) \in Y^* \times Y^*$$

such that $\mu(w) = \mu(w')$ in U^*. An *irreducible* relation is a relation where no proper left subword of w is equal to, or forms a relation with, a proper left subword of w'. It is clear that if (w, w') is an irreducible relation, then $w - w' \in \ker \mu$, and we can show that the set of all such elements generates $\ker \mu$ as an ideal.

Example 6. Let $U = \{xy, xyx, yx\}$, and consider the monoid U^* generated by U. To find all (irreducible) relations induced by U, it is necessary to detect all words in U^* that can be "factorized" in (at least) two different ways. To build such a pair of different factorizations, we can in our case begin with

$$\begin{array}{l} xyx \\ xy. \end{array}$$

We then continue by adding to the lower line a word beginning with x. Such a segment that should be continued, like x earlier, will be called a *protrusion*. A pair can be ended when we obtain a protrusion equal to a word in U. An example of a complete pair is

$$\begin{array}{l} xyx|yx|yx|yx \\ xy|xy|xy|xyx. \end{array} \tag{5}$$

Defining μ by

$$\mu(y_1) = xy, \qquad \mu(y_2) = xyx, \qquad \mu(y_3) = yx,$$

we see that the pair in (5) corresponds to the relation $(y_2 y_3^3, y_1^3 y_2)$. In fact, it is not hard to see that the set of all irreducible relations arising from U is

$$\{(y_2 y_3^k, y_1^k y_2) \,|\, k \geq 1\}. \tag{6}$$

In our graph $\mathcal{M}$ reflecting all irreducible relations, these relations will be built up using the approach in Example 6. In order to represent the possible protrusions in the construction of $\mathcal{M}$, the states are indexed with right subwords of the elements in U, together with an index indicating which sequence of the pair under construction the new word of U should be added to. All transitions will be of the form $(y, \mathbf{1})$ or $(\mathbf{1}, y)$, the first alternative representing addition of $\mu(y)$ to the upper sequence (when viewed as in (5)), while the latter adds $\mu(y)$ to the lower one. Formally, this construction may be represented as an automaton $\mathcal{M} = (Q, q_0, q_a, \mathcal{Y}, \delta)$ with

$$Q = \{q_0, q_a\} \cup \{q_{y_i} \,|\, y_i \in Y\} \cup \{q_I \,|\, I \in \{1, 2\} \times R(U)\}$$

where $R(U)$ is the set of all right subwords of the words in U, the alphabet $\mathcal{Y} = (Y \times \mathbf{1}) \cup (\mathbf{1} \times Y)$ and the transition function δ defined as follows. In all cases it is

assumed that $w' \neq \mathbf{1}$.

$$\begin{aligned}
\delta(q_0, (y_j, \mathbf{1})) &= q_{y_j} \\
\delta(q_{y_j}, (\mathbf{1}, y_i)) &= q_{(2,w')} \qquad \text{if} \quad \mu(y_j) = \mu(y_i)w' \\
\delta(q_{(1,w)}, (y_i, \mathbf{1})) &= \begin{cases} q_{(1,w')} & \text{if} \quad w = \mu(y_i)w' \\ q_{(2,w')} & \text{if} \quad \mu(y_i) = ww' \\ q_a & \text{if} \quad w = \mu(y_i) \end{cases} \\
\delta(q_{(2,w)}, (\mathbf{1}, y_i)) &= \begin{cases} q_{(2,w')} & \text{if} \quad w = \mu(y_i)w' \\ q_{(1,w')} & \text{if} \quad \mu(y_i) = ww' \\ q_a & \text{if} \quad w = \mu(y_i). \end{cases}
\end{aligned}$$

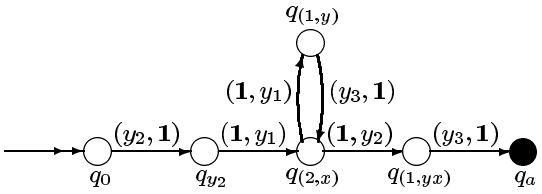
All other transitions are set to empty. The motivation for introducing the states q_{y_i} is to avoid accepting the pairs (y_i, y_i) which are no relations, and moreover to avoid accepting both the (identical) relations (w, w') and (w', w).

If $S \subset \mathcal{Y}$ is the set accepted by $\mathcal{M}$, then the relations corresponding to S are, of course, the set

$$\{(\varphi_1(s), \varphi_2(s)) \mid s \in S\}. \tag{7}$$

To avoid too many technical details, we leave to the reader to convince her/himself that our construction of $\mathcal{M}$ really yields exactly the set of all irreducible relations.

Example 7. For the monoid in Example 6 we get the automaton, after removing superfluous states:



The reader can check that this automaton gives the relations in (6).

We will now construct an ordering such that the relations accepted by our automata $\mathcal{M}$ constitute a regular Gröbner basis. In other words, if $S \subset \mathcal{Y}$ is the set accepted by $\mathcal{M}$, then $G = \varphi(S)$ is a Gröbner basis for $\ker \mu$ with $\widehat{G} = \varphi_1(S)$.

Given an admissible ordering $<_X$ on X^*, we define an admissible ordering $<_Y$ on Y^* in the following way:

$$w <_Y w' \Leftrightarrow \begin{cases} \mu(w) <_X \mu(w') \\ \text{or } \mu(w) = \mu(w') \text{ but} \\ \deg \mu(y) < \deg \mu(y') \end{cases} \tag{8}$$

where y and y' are the two leftmost non-equal letters in the factorizations of w and w', respectively. It is easily checked that the defined ordering $<_Y$ is indeed an admissible ordering on Y^*.

Let f be an arbitrary element of $\ker \mu$, and write $f = c\widehat{f} + c_1 v_1 + \cdots + c_s v_s$ with $\widehat{f} >_Y v_i \in Y^*$ for all i. Since $\mu(f) = c\mu(\widehat{f}) + c_1\mu(v_1) + \cdots + c_s\mu(v_s) = 0$, we see that $\mu(\widehat{f})$

must be equal to some $\mu(v_j)$, i.e. $(\widehat{f}, v_j)$ is a relation. If $(\widehat{f}, v_j)$ is not irreducible, then it is easy to see that $\widehat{f} = uwv$ and $v_j = uw'v'$ for some irreducible relation (w, w'), and $\widehat{f} >_Y v_j$ implies $w >_Y w'$ by our definition of $<_Y$. Summarizing, we have shown that for every $f \in \ker \mu$, there exists an element in the set

$$G = \{g_w = w - w' \mid (w, w') \text{ is an irreducible relation}\} \subset \ker \mu \tag{9}$$

with $\widehat{g}_w \mid \widehat{f}$, and we conclude that G is a Gröbner basis for $\ker \mu$ with respect to $<_Y$. Note that since a Gröbner basis for an ideal generates the ideal, it follows that G generates $\ker \mu$.

If S is the set accepted by $\mathcal{M}$, the "automaton for irreducible relations", then we clearly have $\varphi(S) = G$ (cf. (7) and (9)). Recalling how the transition function δ of $\mathcal{M}$ was defined, it is not hard to see that an element $s \in S$ always begins with $(y_i, \mathbf{1})(\mathbf{1}, y_j)$ where $\deg \mu(y_i) > \deg \mu(y_j)$. It then follows from (8) that $\varphi_1(s) >_Y \varphi_2(s)$, so we also have $\varphi_1(S) = \widehat{G}$. Thus G is a regular Gröbner basis, and we have proved

PROPOSITION 7. *Let $U \subset X^*$ be a finite set of words, and let S be the subalgebra of $K\langle X\rangle$ generated by U. Then S is isomorphic to a bi-automaton algebra.*

5.3. SUBALGEBRAS WITH FINITE SAGBI BASES

We now consider subalgebras of $K\langle X\rangle$ generated by arbitrary elements, i.e. not only words. The concept of SAGBI bases (Subalgebra Analogue to Gröbner Bases for Ideals) was introduced independently by Kapur and Madlener (1989) and Robbiano and Sweedler (1990), and the direct generalization to non-commutative algebras can be found in Nordbeck (1998a). The definition of a Gröbner basis (Definition 1) can be reformulated as: G is a Gröbner basis for $I = \langle G\rangle$ if $\widehat{G}$ generates $\widehat{I}$ as a monoid ideal. In analogue with this, we say that $H \subset K\langle X\rangle$ is a *SAGBI basis* for the subalgebra $S = K\langle H\rangle$ generated by H if $\widehat{H}$ generates $\widehat{S}$ as a monoid.

We next show that every subalgebra which admits a finite SAGBI basis is isomorphic to an automaton algebra. Let, therefore, $H = \{h_1, \ldots, h_k\} \subset K\langle X\rangle$ be a finite SAGBI basis for S with respect to some ordering $<_X$ on X^*. We let $\widehat{H} = \{\widehat{h_1}, \ldots, \widehat{h_k}\} \subset X^*$ play the role of U presented earlier, so μ is defined by $\mu(y_i) = \widehat{h_i}$ and we use the ordering $<_Y$ defined in (8). We further define the homomorphism $\nu : K\langle Y\rangle \to K\langle X\rangle$ by $\nu(y_i) = h_i$ for all i. In analogy, $K\langle H\rangle$ is the image of ν, and $K\langle H\rangle$ is isomorphic to $K\langle Y\rangle / \ker \nu$. To prove that this factor algebra is automaton, we will now construct a Gröbner basis for $\ker \nu$ with a regular set of leading words.

We note that, by the multiplication preserving property for orderings, $\widehat{\nu(w)} = \mu(w)$ for all $w \in Y^*$. In particular, if $(w, w') \in Y^* \times Y^*$ is a relation, then the leading words of $\nu(w)$ and $\nu(w')$ are equal. Such a pair $\nu(w), \nu(w')$ forms a *critical pair* in SAGBI theory, corresponding to the overlaps defined for Gröbner bases. Using the counterpart of reduction, now over the SAGBI basis H, we can then write

$$\nu(w) - c\nu(w') = \sum_i c_i \nu(w_i) \quad \text{(or zero)}, \qquad \widehat{\nu(w_i)} <_X \widehat{\nu(w)} = \widehat{\nu(w')}, \tag{10}$$

for some $c, c_i \in K$ and $w_i \in Y^*$. We refer to Nordbeck (1998a) (or Kapur and Madlener

(1989)/Robbiano and Sweedler (1990)) for the details. If we let

$$g = w - cw' - \sum c_i w_i, \tag{11}$$

then it follows that $\nu(g) = 0$, so $g \in \ker \nu$. We claim that the set G of all such g for all irreducible relations (w, w') is a Gröbner basis for $\ker \nu$ with respect to $<_Y$. As in the previous section we therefore write the arbitrary element $f \in \ker \nu$ as $f = c\widehat{f} + c_1 v_1 + \cdots + c_s v_s$ with $\widehat{f} >_Y v_i \in Y^*$ for all i. By (8) it follows that $\mu(\widehat{f}) \geq_X \mu(v_i)$, and since $\nu(f) = c\nu(\widehat{f}) + c_1\nu(v_1) + \cdots + c_s\nu(v_s) = 0$, it is easy to see that the leading word $\mu(\widehat{f})$ of $\nu(\widehat{f})$ must be equal to some $\mu(v_j)$, i.e. $(\widehat{f}, v_j)$ is a relation. In analogy with the previous section there exists an irreducible relation (w, w') with $w >_Y w'$ and $w \mid \widehat{f}$. We claim that for the element $g \in G$ in (11) constructed from this relation (w, w') we have $\widehat{g} = w$, finally showing that G is a Gröbner basis for $\ker \nu$. But the inequality in (10) is just $\mu(w_i) <_X \mu(w) = \mu(w')$, so according to the definition of $<_Y$ we have $w_i <_Y w$ and $w_i <_Y w'$ for all i, i.e. the greatest of w, w' is the leading word of g, and our claim is proved.

This last claim also shows that the set of leading words of the Gröbner basis G for $\ker \nu$ is the same as the set of leading words for the regular Gröbner basis in (9) constructed for the presentation ideal $\ker \mu$ previously. Earlier we have seen that the set of leading words of a regular Gröbner basis is regular. By Corollary 1 we have then finally proved

Proposition 8. *If the subalgebra $S \subset K\langle X\rangle$ has a finite SAGBI basis, then S is isomorphic to an automaton algebra.*

6. Reduction

In this section we take a closer look at reduction, i.e. the process of turning an element in $K\langle X\rangle$ into normal form modulo some ideal. The reduction with respect to a Gröbner basis G consisting of pure binomials means that we successively look for substrings of the word w to be reduced equal to some $\widehat{g}$ ($g \in G$), and replace by the non-leading word of g. In other words, if $w = u_1\widehat{g}u_2$ for some $g = \widehat{g} - v$, then w "reduces in one step" to $w' = u_1 v u_2$, and we should continue to look for substrings of w'. As always when using a Gröbner basis for reduction, the fact that we are using a well-ordering implies that this procedure will terminate. The major task is to find the substrings equal to the leading words of G, and this is the problem called *string matching*. For an extensive treatment of the well-studied problem of string matching we refer to Crochemore and Rytter (1994). Our main goal in this section is to describe how regular Gröbner bases can be used to perform reduction.

We note that the task of performing reduction with respect to a finite Gröbner basis G is fairly easy. If w is the word to be reduced, then the naive approach is of course to look for the words $\widehat{g}$ ($g \in G$) in w one by one. A more efficient way is to build a tree for $\widehat{G}$; this is the method used in the implementation of the program `MRC` (Monoid Ring Completion) described in Reinert and Zeckzer (1999). Even better is to construct an automaton $\mathcal{M}$ accepting the set of all words, the suffices of which belong to $\widehat{G}$; in this way we do not have to restart the scan on each subsequent letter of w. To get a real efficiency improvement, however, it is important to avoid starting over from the beginning of the word under reduction after each substring replacement. This can be achieved by keeping track of the successive states of $\mathcal{M}$ during the scan, and going back to the state

corresponding to the letter of w just before the replaced string. The latter is the method indicated on p. 403 in Epstein *et al.* (1991).

A major advantage in the finite case is the possibility to have a one-to-one correspondence between words in $\widehat{G}$ and accepting states of $\mathcal{M}$, and thus each such state may contain the corresponding non-leading word. The infinite case gets slightly more complicated, but we will next explain how the automata corresponding to our regular Gröbner bases can be used. We want to mention that a similar method is explained in Section 4 of Epstein *et al.* (1991).

Recall from Section 4 that to each regular Gröbner basis G there was connected a regular set S in the pairs $\mathcal{X}$. We will assume later that we have an automaton $\mathcal{M}_S$ accepting S at hand. Recall that the edges of $\mathcal{M}_S$ are labelled by pairs where the first coordinates form the leading words of G, and the second coordinates the non-leading words. The idea is of course to, while scanning the word w to be reduced, traverse $\mathcal{M}_S$ by following the first coordinate of the pairs. A fairly naive approach would be to simultaneously build up a word with the letters in the second coordinates. However, we must comment on one substantial difference from the finite case: even if $\mathcal{M}_S$ is deterministic, it may not be "deterministic in the first coordinate". Moreover, all edges labelled **1** in the first coordinate should be traversed immediately when reached, without scanning a letter in w; in other words, when considering possible paths from a given state q, the entire ***1**-closure* of q (the set of states reachable from q solely by **1**-transitions) has to be taken in account. We therefore have to work with subsets of states, just as in the powerset construction outlined on page 165, and for each state in such a subset we keep count of the non-leading word built by the second coordinates.

To improve efficiency we now want to, as in the finite case, use an automaton for the set $\widehat{G}_s$ of words with suffices in $\widehat{G}$; we will assume that we have an automaton $\mathcal{M}_{\widehat{G}_s}$ for $\widehat{G}_s$ at hand (for the construction see, for example, Crochemore and Rytter, 1994). In contrast to the finite case, we clearly cannot have one accepting state for each word in $\widehat{G}$. Instead, when we reach an accepting state of $\mathcal{M}_{\widehat{G}_s}$, we start to scan the accepted word backwards in $\mathcal{M}_S$, keeping track of the second coordinates as we go. In this way we can find the relevant non-leading word. Note that we now face the same problems as in the previous paragraph, for example occurrences of **1**s. Finally, we can improve efficiency further if we, just as in the finite case, keep track of visited states of $\mathcal{M}_{\widehat{G}_s}$.

One may object that the construction of the automaton $\mathcal{M}_{\widehat{G}_s}$ is very time consuming, since the number of states may grow exponentially. However, this effort can be sorted under preprocessing and does not effect the performance during reduction.

7. Prediction of Regular Gröbner Bases

In Månsson (2000b) and Månsson and Nordbeck (2001), an algorithm is presented that given a finite set S of words, the longest of length k, produces all regular sets S_i with the following properties:

1. the set of all words in S_i up to length k is exactly S; and
2. S_i can be accepted by an automaton with a number of states that is minimal among all automata accepting sets satisfying property 1.

Thus there are, given S, only a finite number of such S_i, and no other regular sets satisfying the first property can be accepted by automata with strictly fewer states. In

particular, the input S is very rarely among the produced S_i, since given an automaton accepting a finite set S, it is almost always possible to find an automaton with fewer states accepting a set satisfying property 1.

It is also proved in Månsson (2000b) and Månsson and Nordbeck (2001) that, given an automaton accepting a regular set S, we can find a bound k (depending on the number of states) such that words of S up to length k are sufficient to reproduce S. In view of this latter result, it follows that a wanted regular set can always be found provided we have sufficient information of its initial elements. The problem is, of course, that we cannot know in advance (i.e. without knowing the complete regular set) when we have sufficiently many words.

It is now clear how the above mentioned results can help us if we are expecting a (infinite) regular Gröbner basis. Given a finite set of (pure) binomial ideal generators, we apply Mora's algorithm on them for a while, and then use the algorithm in Månsson (2000b) and Månsson and Nordbeck (2001) to obtain a prediction of the infinite basis.

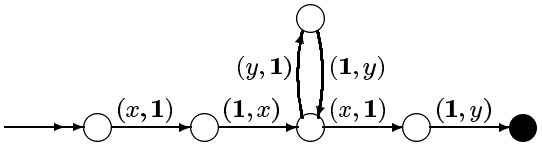
Example 8. Recall from the beginning of Section 4 the ideal $I = \langle x^2 - xy \rangle \subset K\langle x, y\rangle$ and the sequence

$$x^2 - xy, \qquad xyx - xy^2, \qquad xy^2x - xy^3, \qquad xy^3x - xy^4$$

obtained using Mora's algorithm. We write the first two of these elements in our alphabet $\mathcal{X}$ as

$$(x,\mathbf{1})(\mathbf{1},x)(x,\mathbf{1})(\mathbf{1},y), \qquad (x,\mathbf{1})(\mathbf{1},x)(y,\mathbf{1})(\mathbf{1},y)(x,\mathbf{1})(\mathbf{1},y).$$

Given these two words to our prediction algorithm, we obtain the automaton



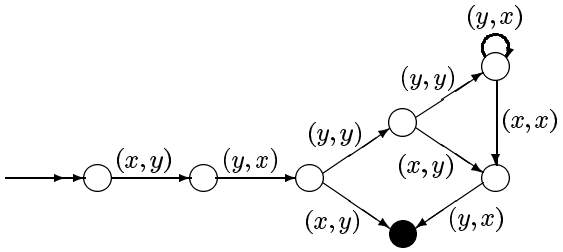
accepting the regular set $\{(x,\mathbf{1})(\mathbf{1},x)((y,\mathbf{1})(\mathbf{1},y))^*(x,\mathbf{1})(\mathbf{1},y)\}$. Applying the map φ from Section 4, we end up with the basis $G = \{xy^kx - xy^{k+1} \mid k \geq 0\}$, which we already have seen is the expected Gröbner basis.

We need, of course, not always use the alphabet $\mathcal{X} = (X \times \{\mathbf{1}\}) \cup (\{\mathbf{1}\} \times X)$. The previous example would be less complicated if we used, as when treated in Section 4, the alphabet $X \times X$. We now give the following less trivial example where it also works to use $X \times X$.

Example 9. We consider the ideal $I = \langle xyx - yxy \rangle \subset K\langle x, y\rangle$ (deglex $x > y$). The initial Gröbner basis computation produces the sequence

$$xyx - yxy,\ xy^2xy - yxy^2x,\ xy^3xy - yxy^2x^2,\ xy^4xy - yxy^2x^3,\ xy^5xy - yxy^2x^4.$$

Encoding this sequence as words in the alphabet $\{x, y\} \times \{x, y\}$ (in the unique way), and giving this corresponding sequence in $(\{x, y\} \times \{x, y\})^*$ to our algorithm, we obtain the automaton



accepting the regular set

$$\{(x,y)(y,x)(x,y),\ (x,y)(y,x)(y,y)(x,y)(y,x),\ (x,y)(y,x)(y,y)^2(y,x)^*(x,x)(y,x)\}.$$

Applying the counterpart of φ (defined on $(X \times X)^*$), we obtain the basis

$$G = \{xyx - yxy,\ xy^2xy - yxy^2x,\ xy^{k+3}xy - yxy^2x^{k+2} \mid k \geq 0\}.$$

Using the Diamond lemma, we can prove that G really is a Gröbner basis for the ideal I.

We have now seen two examples where the prediction algorithm for regular sets was successfully used to find regular Gröbner bases. But we still had to extract the (possible) Gröbner bases from the automata and apply the Diamond lemma "manually". Moreover, the regular Gröbner bases suggested by the algorithm may, of course, in some cases contain elements that are not in the original ideals.

At this point, the authors do not know of any method to "automatically" check for the Gröbner property. (For certain term rewriting systems, this property has been shown undecidable in Ó'Dúnlaing, 1983.) An automaton reflecting all overlaps and overlap relations can be constructed, but how do we perform reduction of the infinite (but regular) set of relations? Moreover, when reducing a regular set, the resulting set need not be regular:

Example 10. Assume that we want to reduce the regular set $\{(xy)^k \mid k \geq 0\}$ using the Gröbner basis $G = \{xy - yx\}$ (deglex $x > y$). It is easy to see that every $(xy)^k$ reduces to y^kx^k via G, so the set of normal forms becomes $\{y^kx^k \mid k \geq 0\}$. This latter set is once again an example of our standard non-regular set.

Also note that it is shown in Otto (1998) that the question whether a finite term rewriting system preserves regularity is undecidable.

We finally want to mention that a different approach of predicting an infinite rewrite system using a finite initial sequence, also based on inductive inference, is presented in Thomas and Jantke (1989).

Acknowledgements

The authors are grateful to the anonymous referees for their valuable comments.

References

Anick, D. J. (1986). On the homology of associative algebras. *Trans. Am. Math. Soc.*, **296**, 641–659.
Baader, F., Nipkow, T. (1998). *Term Rewriting and All That.* Cambridge, Cambridge University Press.
Backelin, J. (1978). La série de Poincaré–Betti d'une algèbre graduée de type fini à une relation est rationnelle. *C. R. Acad. Sci. Paris Sér. A-B*, **287**, A843–A846.

Bergman, G. M. (1978). The diamond lemma for ring theory. *Adv. Math.*, **29**, 178–218.
Buchberger, B. (1985). Groebner bases: an algorithmic method in polynomial ideal theory. In *Multidimensional Systems Theory, Progress, Directions and Open Problems*, pp. 184–232. Dordrecht, Reidel.
Crochemore, M., Rytter, W. (1994). *Text Algorithms*. New York, The Clarendon Press/Oxford University Press, With a preface by Zvi Galil.
Dickson, L. (1913). Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Am. J. Math.*, **35**, 413–426.
Eilenberg, S. (1974). *Automata, Languages, and Machines*, volume A. New York, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers]; *volume 58 of Pure and Applied Mathematics*.
Epstein, D. B. A., Cannon, J. W., Holt, D. F., Levy, S. V. F., Paterson, M. S., Thurston, W. P. (1992). *Word Processing in Groups*. Boston, MA, Jones and Bartlett Publishers.
Epstein, D. B. A., Holt, D. F., Rees, S. E. (1991). The use of Knuth–Bendix methods to solve the word problem in automatic groups. *J. Symb. Comput.*, **12**, 397–414. Computational group theory, Part 2.
Green, E. L. (1994). An introduction to noncommutative Gröbner bases. In *Computational Algebra (Fairfax, VA, 1993)*, pp. 167–190. New York, Dekker.
Heyworth, A. (2000). Rewriting as a special case of non-commutative Gröbner basis theory. In *Computational and Geometric Aspects of Modern Algebra (Edinburgh, 1998)*, pp. 101–105. Cambridge, Cambridge University Press.
Kapur, D., Madlener, K. (1989). A completion procedure for computing a canonical basis for a k-subalgebra. In *Computers and Mathematics (Cambridge, MA, 1989)*, pp. 1–11. New York, Springer.
Lallement, G. (1979). *Semigroups and Combinatorial Applications*, Chichester, John Wiley & Sons; *Pure and Applied Mathematics,* A Wiley-Interscience Publication.
Madlener, K., Reinert, B. (1998). Relating rewriting techniques on monoids and rings: congruences on monoids and ideals in monoid rings. *Theor. Comput. Sci.*, **208**, 3–31. Rewriting techniques and applications (New Brunswick, NJ, 1996).
Månsson, J. (2000a). On the computation of Hilbert series and Poincaré series for algebras with infinite Gröbner bases. *Comput. Sci. J. Moldova*, **8**, 42–63.
Månsson, J. (2000b). A prediction algorithm for rational languages. Combinatorial methods in computer algebra. Licentiate Thesis, Centre for Mathematical Sciences, Lund University.
Månsson, J., Nordbeck, P. (2001). Prediction of rational languages and reconstruction of automata. Report, Department of Computer Science, Lund University.
Markov, A. A. (1971/1972). On finitely generated subsemigroups of a free semigroup. *Semigroup Forum*, **3**, 251–258.
Mora, T. (1994). An introduction to commutative and noncommutative Gröbner bases. *Theor. Comput. Sci.*, **134**, 131–173. Second International Colloquium on Words, Languages and Combinatorics (Kyoto, 1992).
Nordbeck, P. (1998a). Canonical subalgebra bases in non-commutative polynomial rings. In *Proceedings of ISSAC'98*, ACM Press.
Nordbeck, P. (1998b). On some basic applications of Gröbner bases in non-commutative polynomial rings. In *Gröbner Bases and Applications (Linz, 1998)*, pp. 463–472. Cambridge, Cambridge University Press.
Ó'Dúnlaing, C. (1983). Infinite regular Thue systems. *Theor. Comput. Sci.*, **25**, 171–192.
Otto, F. (1998). Some undecidability results concerning the property of preserving regularity. *Theor. Comput. Sci.*, **207**, 43–72. In memoriam of Ronald V. Book.
Reinert, B., Zeckzer, D. (1999). MRC—data structures and procedures for computing in monoid and group rings. *Appl. Algebra Eng. Commun. Comput.*, **10**, 41–78.
Robbiano, L., Sweedler, M. (1990). Subalgebra bases. In *Commutative Algebra (Salvador, 1988)*, volume 1430 of *Lecture Notes in Mathematics*, pp. 61–87. Berlin, Springer.
Shannon, D., Sweedler, M. (1988). Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence. *J. Symb. Comput.*, **6**, 267–273. Computational aspects of commutative algebra.
Shearer, J. B. (1980). A graded algebra with a nonrational Hilbert series. *J. Algebra*, **62**, 228–231.
Spehner, J.-C. (1974/1975). Quelques constructions et algorithmes relatifs aux sous-monoïdes d'un monoïde libre. *Semigroup Forum*, **9**, 334–353.
Sturmfels, B. (1996). *Gröbner Bases and Convex Polytopes*. Providence, RI, American Mathematical Society.
Thomas, M., Jantke, K. P. (1989). Inductive inference for solving divergence in Knuth–Bendix completion. In *Analogical and Inductive Inference (Reinhardsbrunn Castle 1989)*, pp. 288–303. Berlin, Springer.
Ufnarovski, V. A. (1989). On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras. *Mat. Sb.*, **180**, 1548–1560.
Ufnarovski, V. A. (1995). Combinatorial and asymptotic methods in algebra [MR 92h:16024]. In *Algebra,* VI, pp. 1–196. Berlin, Springer.

Received 26 March 2001
Accepted 25 August 2001