Southeast Asian Bulletin of Mathematics (2021) 45: 759–774

Southeast Asian
Bulletin of
Mathematics

Gröbner-Shirshov Bases for Free Idempotent Monoids

Baddi Ul Zaman, Yuqun Chen* and Mingmei Yang
School of Mathematical Sciences, South China Normal University, Guangzhou 510631, China
Email: amath1141@gmail.com; yqchen@scnu.edu.cn; yangmingmeisunny@163.com

Received 23 February 2021
Accepted 30 July 2021

Communicated by L.A. Bokut

Dedicated to the memory of Professor Yuqi Guo (1940–2019)

AMS Mathematics Subject Classification(2000): 16S15, 13P10, 20M05

Abstract. We give a new presentation of free idempotent semigroup (band) in which the set of relations is a Gröbner-Shirshov basis. By using Composition-Diamond lemma for associative algebra, we obtain normal forms of elements of the free idempotent semigroup.

Keywords: Gröbner-Shirshov basis; Normal form; Free idempotent monoid.

1. Introduction

Let A be an alphabet having at least three letters. A square is a word in A^+ of the form uu, with u a nonempty word. A word contains a square if one of its factors is a square, otherwise, the word is called square-free. Then there are infinitely many square-free words in A^*. Consider the semigroup

$$D = sgp\langle A \mid w^2 = 1, w \in A^+\rangle, \quad where\ A^+ = A^* \setminus \{1\}.$$

Each square-free word constitutes an equivalence class modulo this congruence, and the quotient monoid D is infinite.

There is another situation where square-free words can be used. Consider

*Supported by the NNSF of China (11571121, 12071156).

the quotient monoid

$$E = sgp\langle A \mid w^m = w^n, w \in A^+,\ m, n \geq 2\rangle$$

Since each square-free word also defines an equivalence class, the monoid E is infinite. In fact, this result also holds for a two-letter alphabet (Brzozowski, Culik II, and Gabrielian 1971).

These considerations can be placed in the framework of the classical Burnside problem (originally, the Burnside problem was formulated for groups only, but it is easy to state for semigroups also):

Is every finitely generated torsion semigroup finite ? (A torsion semigroup is a semigroup such that each element generates a finite subsemigroup.) We have just seen that the answer is negative in general. But in one special case, surprisingly, the answer is positive.

Let $A = \{a_i \mid i \in I\}$ be a set. The monoid

$$M = sgp\langle A \mid w^2 = w, w \in A^*\rangle$$

is called the free idempotent monoid on A (see [8]).

Theorem 1.1. (Green-Rees [8]) *The free idempotent monoid on A is finite and has exactly*

$$\sum_{k=0}^{n} \binom{n}{k} \prod_{1 \leq i \leq k} (k - i + 1)^{2^i}$$

elements, where $n = Card(A)$.

2. Preliminaries

We first cite some concepts and results from the literature [3, 2, 9] which are related to Gröbner-Shirshov bases for associative algebras.

Let X be a set and F a field, $F\langle X\rangle$ the free associative algebra over F generated by X, and X^* the free monoid generated by X. A well ordering $<$ on X^* is monomial if for any $u, v \in X^*$,

$$u < v \Rightarrow w_1 u w_2 < w_1 v w_2,\ for\ all\ w_1,\ w_2 \in X^*.$$

Let X^+ be the semigroup generated by X. For any $u \in X^*$, denote by $|u|$ the length of u.

A standard example of monomial ordering on X^* is the deg-lex ordering which first compare two words by length and then by comparing them lexicographically, where X is a well ordered set.

Then, for any nonzero polynomial $f \in F\langle X\rangle$, f has the leading (maximal) word $\overline{f}$. We call f *monic* if the coefficient of $\overline{f}$ is 1.

Let $f,\ g \in F\langle X\rangle$ be two monic polynomials and $w \in X^*$.

If $w = \overline{f}b = a\overline{g}$ for some $a, b \in X^*$ such that $|\overline{f}| + |\overline{g}| > |w|$, then $(f, g)_w = fb - ag$ is called the *intersection composition* of f, g relative to w.

If $w = \overline{f} = a\overline{g}b$ for some $a, b \in X^*$, then $(f, g)_w = f - agb$ is called the *inclusion composition* of f, g relative to w. The transformation $f \mapsto f - agb$ is called the elimination of leading word (ELW) of g in f.

In $(f, g)_w$, w is called the *ambiguity* of the composition.

Let $S \subset F\langle X\rangle$ be a monic set. A composition $(f, g)_w$ is called trivial modulo (S, w), denoted by

$$(f, g)_w \equiv 0 \quad mod(S, w)$$

if $(f, g)_w = \sum \alpha_i a_i s_i b_i$, where every $\alpha_i \in F,\ s_i \in S,\ a_i, b_i \in X^*$, and $a_i\overline{s_i}b_i < w$.

Generally, for $f, g \in F\langle X\rangle,\ f \equiv g \quad mod(S, w)$ we mean $f - g = \sum \alpha_i a_i s_i b_i$, where every $\alpha_i \in F,\ s_i \in S,\ a_i, b_i \in X^*$, and $a_i\overline{s_i}b_i < w$.

Recall that S is a *Gröbner-Shirshov basis* if any composition of polynomials from S is trivial modulo S.

Let f and r_1 be two polynomials. Then $f \mapsto f_1$ by ELW of r_1 in f means $f = \alpha_1 a_1 r_1 b_1 + f_1$ where $a_1, b_1 \in X^*,\ \alpha_1 \in F,\ \bar{f} = a_1\overline{r_1}b_1$ and $\bar{f_1} < \bar{f}$ if $f_1 \neq 0$. Generally, $f \mapsto f_1 \mapsto \cdots \mapsto f_n \mapsto r$ means that $f = \sum \alpha_i a_i r_i b_i + r$ where $\bar{f} = a_1\overline{r_1}b_1 > a_2\overline{r_2}b_2 > \cdots > a_n\overline{r_n}b_n > \bar{r}$. If this is the case, we say that f can be reduced to r via $\{r_1, \ldots, r_n\}$.

Clearly, if $(f, g)_w$ can be reduced to zero by ELW of S, then $(f, g)_w \equiv 0 \ \ mod(S, w)$.

The following lemma was first proved by Shirshov [9] for free Lie algebras (with deg-lex ordering) (see also Bokut [3]). Bokut [2] specialized the approach of Shirshov to associative algebras (see also Bergman [1]). For commutative polynomials, this lemma is known as Buchberger's Theorem (see [4, 5]).

Lemma 2.1. (Composition-Diamond Lemma) *Let F be a field, $A = F\langle X|S\rangle = F\langle X\rangle/Id(S)$ and $<$ a monomial ordering on X^*, where $Id(S)$ is the ideal of $F\langle X\rangle$ generated by S. Then the following statements are equivalent:*

1. *S is a Gröbner-Shirshov basis.*
2. *$f \in Id(S) \Rightarrow \bar{f} = a\bar{s}b$ for some $s \in S$ and $a, b \in X^*$.*
3. *$Irr(S) = \{u \in X^* | u \neq a\bar{s}b, s \in S, a, b \in X^*\}$ is an F-basis of the algebra $A = F\langle X|S\rangle$.*

If a subset S of $F\langle X\rangle$ is not a Gröbner-Shirshov basis then one can add all nontrivial compositions of polynomials of S to S. Continuing this process repeatedly, we finally obtain a Gröbner-Shirshov basis S^{comp} that contains S. Such a process is called Shirshov algorithm.

A set S is called *minimal Gröbner-Shirshov basis* if it is a Gröbner-Shirshov basis and there are no inclusion compositions in S.

Let $A = sgp\langle X|S\rangle$ be a semigroup presentation. Then S is also a subset of $F\langle X\rangle$ and we can find Gröbner-Shirshov basis S^{comp}. We also call S^{comp} a Gröbner-Shirshov basis of A. The set $Irr(S^{comp}) = \{u \in S^* | u \neq a\overline{f}b,\ a, b \in$

$S^*,\ f \in S^{comp}\}$ is a linear basis of $F\langle X|S\rangle$ which is also a set of all normal forms of A.

In this chapter, we introduce Burnside problem and Green-Rees theorem. We give a new presentation of free idempotent semigroup in which the set of relations is a Gröbner-Shirshov basis and then a normal form of free idempotent semigroup is obtained by using Composition-Diamond lemma (see Lemma 2.1).

3. Some Properties for Free Idempotent Monoid

Let $A = \{a_i \mid i \in I\}$ be a set. The monoid

$$M = sgp\langle A \mid w^2 = w, w \in A^*\rangle$$

is called the free idempotent monoid on A (see [6, 7, 8]).

For any $w = a_1a_2 \cdots a_n \in A^*$, where $a_1, a_2, \ldots, a_n \in A$, we denote $\text{alph}(w) = \{a_1, a_2, \ldots, a_n\}$, for example, $\text{alph}(aaba) = \{a, b\}$. Let F be a field. $F\langle A\rangle$ is the free associative algebra over F generated by A.

Lemma 3.1. [8] *For any $x, y \in A^*$. If $alph(y) \subseteq alph(x)$, then there exists $u \in A^*$, such that in $F\langle A\rangle$, $xyu - x = \sum a_i(w_i^2 - w_i)b_i$, where $a_i, b_i \in A^*, w_i \in A^+$.*

Proof. Induction on $|y|$.

If $|y| = 0$, then $y = \epsilon$ and let $u = x$.

If $|y| = 1$, then $y = a \in A$. Since $alph(y) \subseteq alph(x)$, there exist $z, z' \in A^*$, such that $x = zaz'$. Let $u = z'$. Then $xyu - x = z[(az')^2 - (az')]$.

For $|y| > 1$, let $y = y'a$, where $a \in A$. Since $\text{alph}(y^{'}) \subseteq \text{alph}(y) \subseteq \text{alph}(x)$, by induction, there exists $u' \in A^*$, such that $xy'u' - x = \sum a_i(w_i^2 - w_i)b_i$. Furthermore, $a \in alph(x)$, whence $x = zaz'$. Let $u = z'y'u'$. Now we have

$$\begin{aligned} xyu - x &= zaz'y'az'y'u' - zaz' \\ &= z[(az'y')^2 - (az'y')]u' + zaz'y'u' - zaz' \\ &= z[(az'y')^2 - az'y']u' + \sum a_i(w_i^2 - w_i)b_i \end{aligned}$$

■

Remark 3.2. Symmetrically, there exists a word v such that in $F\langle A\rangle$, $vyx - x = \sum c_i(t_i^2 - t_i)d_i$, where $c_i, d_i \in A^*, t_i \in A^+$.

For any $x \in A^+$, denote x' the shortest left factor of x such that $\text{alph}(x') = \text{alph}(x)$. Setting $x' = p_xa_x$, where $a_x \in A$, $\text{alph}(p_x) = \text{alph}(x) \setminus \{a_x\}$. Denote x'' the shortest right factor of x such that $\text{alph}(x'') = \text{alph}(x)$. Setting $x'' = b_xq_x$, where $b_x \in A$, we have $\text{alph}(q_x) = \text{alph}(x) \setminus \{b_x\}$. Therefore, for any $x \in A^+$, there exist uniquely p_x, a_x, b_x, q_x which are defined as above.

Lemma 3.3. [8] *For any $x \in A^+$, we have $p_xa_xb_xq_x - x = \sum a_i(w_i^2 - w_i)b_i$, where $a_i, b_i \in A^*, w_i \in A^+$.*

Proof. Let $x = p_x a_x y = z b_x q_x$, where $y, z \in A^*$. Since alph(y) $\subseteq$alph$(p_x a_x)$, there exists $u \in A^*$, such that $p_x a_x - p_x a_x y u = \sum a_i(w_i^2 - w_i)b_i$. Similarly, since alph$(p_x a_x)$ $\subseteq$alph$(b_x q_x)$, there exists $v \in A^*$, such that $v p_x a_x b_x q_x - b_x q_x = \sum c_i(t_i^2 - t_i)d_i$. Since

$$\begin{aligned}
&p_x a_x y u b_x q_x - z v p_x a_x b_x q_x \\
= &[p_x a_x y - (p_x a_x y)^2] u b_x q_x + [(p_x a_x y)^2 u b_x q_x - z v (p_x a_x b_x q_x)^2] \\
&+ z v[(p_x a_x b_x q_x)^2 - p_x a_x b_x q_x] \\
= &[p_x a_x y - (p_x a_x y)^2] u b_x q_x + [(p_x a_x y)^2 u b_x q_x - p_x a_x y p_x a_x b_x q_x] \\
&+ [p_x a_x y p_x a_x b_x q_x - z v (p_x a_x b_x q_x)^2] \\
&+ z v[(p_x a_x b_x q_x)^2 - p_x a_x b_x q_x] \\
= &[p_x a_x y - (p_x a_x y)^2] u b_x q_x + p_x a_x y (p_x a_x y u - p_x a_x) b_x q_x \\
&+ z(b_x q_x - v p_x a_x b_x q_x) p_x a_x b_x q_x + z v[(p_x a_x b_x q_x)^2 - p_x a_x b_x q_x],
\end{aligned}$$

we have

$$\begin{aligned}
&p_x a_x b_x q_x - x \\
= &\ p_x a_x b_x q_x - z b_x q_x \\
= &\ (p_x a_x - p_x a_x y u) b_x q_x + (p_x a_x y u b_x q_x - z v p_x a_x b_x q_x) + z(v p_x a_x b_x q_x - b_x q_x) \\
= &\ (p_x a_x - p_x a_x y u) b_x q_x + [p_x a_x y - (p_x a_x y)^2] u b_x q_x \\
&+ p_x a_x y (p_x a_x y u - p_x a_x) b_x q_x + z(b_x q_x - v p_x a_x b_x q_x) p_x a_x b_x q_x \\
&+ z v[(p_x a_x b_x q_x)^2 - p_x a_x b_x q_x] + z(v p_x a_x b_x q_x - b_x q_x) \\
= &\sum a_i(w_i^2 - w_i) b_i b_x q_x + [p_x a_x y - (p_x a_x y)^2] u b_x q_x \\
&+ \sum p_x a_x y a_i (w_i^2 - w_i) b_i b_x q_x + \sum z c_i (t_i^2 - t_i) d_i p_x a_x b_x q_x \\
&+ z v[(p_x a_x b_x q_x)^2 - p_x a_x b_x q_x] + \sum z c_i (t_i^2 - t_i) d_i.
\end{aligned}$$ ■

For any $u, v \in A^*$, if $u = w_1 w_2$ and $v = w_2 w_3$, where $w_1, w_2, w_3 \in A^*$, we denote cm$(u, v) = w_1 w_2 w_3$.

Definition 3.4. *For any $x \in A^+$, we define $(x)_s$ by induction on $|x|$.*

(1) *For $|x| = 1$, $(x)_s = x$.*
(2) *For $|x| > 1$, by induction $(x)_s = cm((p_x)_s a_x, b_x (q_x)_s)$.*

For example, $x = a_1 a_2 a_2 a_1 a_1 a_2 a_1 \in A^+$. Since $p_x = a_1$, $a_x = a_2$, $b_x = a_2$, $q_x = a_1$, we have $(x)_s = cm(a_1 a_2, a_2 a_1) = a_1 a_2 a_1$.

Lemma 3.5. *For any $x \in A^+$, the word $(x)_s$ is unique.*

Proof. If $|(x)_s| < |(p_x)_s a_x b_x (q_x)_s|$, we suppose that $(x)_s = cm((p_x)_s a_x, b_x (q_x)_s) = v_1 v_2 v_3$, $(x)'_s = cm'((p_x)_s a_x, b_x (q_x)_s) = w_1 w_2 w_3$, where $(p_x)_s a_x =$

$v_1v_2 = w_1w_2$, $b_x(q_x)_s = v_2v_3 = w_2w_3$, $|v_2| \geq 1$, $|w_2| \geq 1$. Suppose $w_2 = cv_2 = b_xd$, where $c, d \in A^*$. If $(x)_s \neq (x)'_s$, then $|c| \geq 1$, $b_x \in$ alph(c), and there exists $t \in A^*$ such that $c = b_xt$. Then $(q_x)_s = tv_2dw_3$ and $b_x \in$alph(v_2) $\subseteq$alph$((q_x)_s)$ which contradicts $b_x \notin$ alph(q_x).

If $|(x)_s| = |(p_x)_sa_xb_x(q_x)_s|$, then $(x)_s = (p_x)_sa_xb_x(q_x)_s$.

This shows that for any $x \in A^+$, $(x)_s$ is unique. ∎

Denote

$$R = \{w^2 - w \mid w \in A^*\},$$
$$S = \{\ paubq - (pabq)_s \mid\ p, q \in A^*,\ a, b \in A,\ (p)_s = p,\ (q)_s = q, a \notin alph(p),$$
$$b \notin alph(q), alph(pa) = alph(bq),\ u \in (alph(pa))^*, |paubq| > |(pabq)_s|\}.$$

Note that $alph(pa) = alph(paubq)$ if $paubq - (pabq)_s \in S$.

Let $(I, <)$ be well-ordered set. Then we order A^* by the deg-lex order. We will use this order in this paper. For any $f \in F\langle A\rangle$, $\overline{f}$ means the leading term of f. Suppose S is a subset of $F\langle A\rangle$. Then we denote Id(S) the ideal of $F\langle A\rangle$ generated by S.

Lemma 3.6. *For any $w \in A^+$, if $(w)_s \neq w$, then there exist $s_1 \in S$, $a, b \in A^*$, such that $w = a\bar{s}_1b$.*

Proof. Induction on Card$(alph(w))$.

For Card$(alph(w)) = 1$, $w = a_i^m$ for some $m \geq 1$. Since $(w)_s \neq w$, we have $m \geq 2$. Setting $s_1 = a_i^2 - a_i$, we have $w = a_i^2a_i^{m-2} = \bar{s}_1a_i^{m-2}$.

Suppose that Card$(alph(w)) > 1$. If $(p_w)_s \neq p_w$ or $(q_w)_s \neq q_w$, by induction, the result holds. If $(p_w)_s = p_w$ and $(q_w)_s = q_w$, then $w = (p_w)_sa_wub_w(q_w)_s$ for some $u \in (alph(pa))^*$ since $(w)_s \neq w$. Now, we have $s_1 = w - (w)_s \in S$ and $w = \overline{s_1}$. ∎

Lemma 3.7. *$Id(R) = Id(S)$ in $F\langle A\rangle$.*

Proof. First we want to prove Id$(S) \subseteq$ Id(R). Clearly, it suffices to show $S \subseteq$ Id(R). For any $paubq - (pabq)_s \in S$, let $x_1 = paubq$ and $x_2 = (pabq)_s$. Since $p_{x_1} = p = p_{x_2}$, $a_{x_1} = a = a_{x_2}$, $b_{x_1} = b = b_{x_2}$, $q_{x_1} = q = q_{x_2}$, by Lemma 3.3, we have

$$\begin{aligned} paubq - (pabq)_s &= (paubq - pabq) + (pabq - (pabq)_s) \\ &= \sum a_i(w_i^2 - w_i)b_i + \sum c_i(v_i^2 - v_i)d_i \in Id(R). \end{aligned}$$

Now we show $R \subseteq$ Id(S). For any $w^2 - w \in R$. There are two cases to consider:

Case 1. Suppose $(w)_s = w$. Since $w = (w)_s = cm((p_w)_sa_w, b_w(q_w)_s) = ((p_w)_sa_wb_w(q_w)_s)_s$, we have $(p_w)_s = p_w, (q_w)_s = q_w$ and there exist $u_1, u_2 \in$

$(alph(w))^*$ such that $w = p_w a_w u_1 = u_2 b_w q_w$. Hence, if $u = u_1 u_2$ then $u \in alph(w))^*$ and

$$\begin{aligned} w^2 - w &= p_w a_w u_1 u_2 b_w q_w - ((p_w)_s a_w b_w (q_w)_s)_s \\ &= (p_w)_s a_w u b_w (q_w)_s - ((p_w)_s a_w b_w (q_w)_s)_s \in S. \end{aligned}$$

Case 2. If $(w)_s \neq w$, then $|w| \geqslant 2$. We will prove this case by induction on $|w|$.

For $|w| = 2$, since $(w)_s \neq w$, we have $w = a_i^2$ and $w^2 - w = a_i^4 - a_i^2 = (a_i^4 - a_i) - (a_i^2 - a_i)$ in $\mathrm{Id}(S)$.

For $|w| > 2$, by Lemma 3.6, there exists $s_1 \in S$ satisfying $(p_{\bar{s_1}})_s = p_{\bar{s_1}}$, $(q_{\bar{s_1}})_s = q_{\bar{s_1}}$ such that $w = c\bar{s_1}d$. Suppose $\bar{s_1} = p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}}$. Then $w = c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d$ and

$$\begin{aligned} & w^2 - w \\ = \ & c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d - c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d \\ = \ & c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d - c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d \\ & + c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d - c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} \\ & q_{\bar{s_1}})_s d + c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s d - c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d \\ = \ & c[p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}} - (p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s]dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})d \\ & + c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc[p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}} - (p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s]d \\ & + c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s d - c(p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s d \\ & - c[p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}} - (p_{\bar{s_1}} a_{\bar{s_1}} u_1 b_{\bar{s_1}} q_{\bar{s_1}})_s]d, \end{aligned}$$

by induction, $c(p_{\bar{s_1}} a_{\bar{s_1}} b_{\bar{s_1}} q_{\bar{s_1}})_s dc(p_{\bar{s_1}} a_{\bar{s_1}} b_{\bar{s_1}} q_{\bar{s_1}})_s d - c(p_{\bar{s_1}} a_{\bar{s_1}} b_{\bar{s_1}} q_{\bar{s_1}})_s d \in Id(S)$. This implies $w^2 - w \in Id(S)$. ∎

4. A Gröbner-Shirshov Basis

By Lemma 3.7, we have $F\langle A \mid S\rangle = F\langle A \mid R\rangle$ which is equivalent to $M = sgp\langle A \mid S\rangle = sgp\langle A \mid R\rangle$.

The following theorem is the main result in this paper.

Theorem 4.1. *With the deg-lex ordering on A^*,*

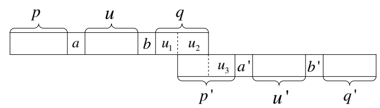
$$\begin{aligned} S = \{\ & paubq - (pabq)_s \mid \ p, q \in A^*,\ a, b \in A,\ (p)_s = p,\ (q)_s = q, a \notin alph(p), \\ & b \notin alph(q),\ alph(pa) = alph(bq), u \in (alph(pa))^*, |paubq| > |(pabq)_s| \} \end{aligned}$$

is a Gröbner-Shirshov basis in $F\langle A\rangle$.

Proof. We will prove that all the compositions in S are trivial. Assume that $f = paubq - (pabq)_s$, $g = p'a'u'b'q' - (p'a'b'q')_s \in S$.

First we prove that all intersection compositions are trivial.

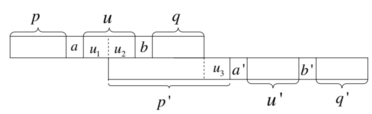
Case 1. No one of $\{a, b, a', b'\}$ is in the intersection, i.e. $q = u_1u_2,\ p' = u_2u_3,\ |u_2| \geq 1,\ w = paubu_1u_2u_3a'u'b'q'$.



There exist $w_1, w_2 \in A^*$ such that $(pabq)_s = w_1bq = w_1bu_1u_2$, $(p'a'b'q')_s = p'a'w_2 = u_2u_3a'w_2$.

$$\begin{aligned}
(f,g)_w &= -(pabq)_s u_3a'u'b'q' + paubu_1(p'a'b'q')_s \\
&= -w_1bu_1u_2u_3a'u'b'q' + paubu_1u_2u_3a'w_2 \\
&\equiv -w_1bu_1(p'a'b'q')_s + (pabq)_s u_3a'w_2 \\
&\equiv -w_1bu_1p'a'w_2 + w_1bqu_3a'w_2 \\
&\equiv -w_1bu_1u_2u_3a'w_2 + w_1bu_1u_2u_3a_{\prime}w_2 \\
&\equiv 0.
\end{aligned}$$

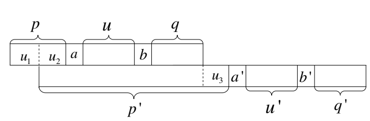
Case 2. One of $\{a, b, a', b'\}$ is in the intersection. We may assume that $u = u_1u_2,\ p' = u_2bqu_3,\ w = paubqu_3a'u'b'q'$.



Clearly, $alph(bqu_3) \subseteq alph(p')$, and $alph(p') = alph(u_2) \cup alph(bqu_3) \subseteq alph(u) \cup alph(bqu_3) = alph(bqu_3)$. We have $alph(bqu_3) = alph(p')$. Then $bqu_3a'u'b'q' - (bqu_3a'b'q')_s \in S$. There exist $w_1, w_2 \in A^*$, such that $(pabq)_s = w_1bq$, $(p'a'b'q')_s = p'a'w_2 = u_2bqu_3a'w_2$, $(bqu_3a'b'q')_s = bqu_3a'w_2$.

$$\begin{aligned}
(f,g)_w &= -(pabq)_s u_3a'u'b'q' + pau_1(p'a'b'q')_s \\
&= -w_1bqu_3a'u'b'q' + pau_1u_2bqu_3a'w_2 \\
&\equiv -w_1(bqu_3a'b'q')_s + (pabq)_s u_3a'w_2 \\
&\equiv -w_1bqu_3a'w_2 + w_1bqu_3a'w_2 \\
&\equiv 0.
\end{aligned}$$

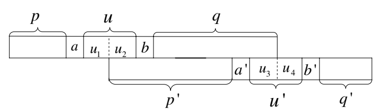
Case 3. Two of $\{a, b, a', b'\}$ is in the intersection. There are three subcases.
(i) $p = u_1u_2,\ p' = u_2aubqu_3,\ w = paubqu_3'u'b'q'$.



Since $alph(u_2a) \subseteq alph(pa) = alph(bq) \subseteq alph(bqu_3)$ and $alph(u) \subseteq alph(bq) \subseteq alph(bqu_3)$, $alph(p') = alph(u_2a) \cup alph(u) \cup alph(bqu_3) = alph(bqu_3)$. So we have $bqu_3a'u'b'q' - (bqu_3a'b'q')_s \in S$. There exist $w_1, w_2 \in A^*$, such that $(pabq)_s = w_1bq$, $(p'a'b'q')_s = p'a'w_2 = u_2aubqu_3a'w_2$, $(bqu_3a'b'q')_s = bqu_3a'w_2$.

$$\begin{aligned}
(f,g)_w &= -(pabq)_s u_3a'u'b'q' + u_1(p'a'b'q')_s \\
&= -w_1bqu_3a'u'b'q' + u_1u_2aubqu_3a'w_2 \\
&\equiv -w_1(bqu_3a'b'q')_s + (pabq)_s u_3a'w_2 \\
&\equiv -w_1bqu_3a'w_2 + w_1bqu_3a'w_2 \\
&\equiv 0.
\end{aligned}$$

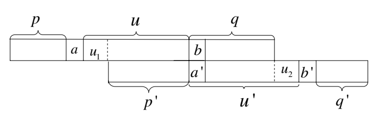
(ii) $u = u_1u_2,\ u' = u_3u_4,\ w = pau_1p'a'u'b'q'$.



Since $alph(u_2) \subseteq alph(bq)$, $alph(u_3) \subseteq alph(p'a')$, $alph(bq) \subseteq alph(p'a'u_3) = alph(p'a') \cup alph(u_3) = alph(p'a')$, $alph(p'a') \subseteq alph(u_2bq) = alph(u_2) \cup alph(bq) = alph(bq)$. Then, $alph(pa) = alph(bq) = alph(p'a') = alph(b'q')$. So $pavb'q' - (pab'q')_s \in S$, where $v \in (alph(pa))^*$. There exist $w_1, w_2 \in A^*$, such that $(pabq)_s = paw_1$, $(p'a'b'q')_s = w_2b'q'$.

$$\begin{aligned}
(f,g)_w &= -(pabq)_s u_4b'q' + pau_1(p'a'b'q')_s \\
&= -paw_1u_4b'q' + pau_1w_2b'q' \\
&\equiv -(pab'q')_s + (pab'q')_s \\
&\equiv 0.
\end{aligned}$$

(iii) $u = u_1p',\ u' = qu_2,\ b = a',\ w = paubqu_2b'q'$.

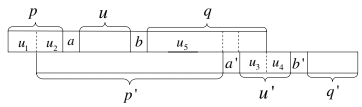


Clearly, $alph(pa) = alph(b'q')$. We have $pavb'q' - (pab'q')_s$, where $v \in (alph(pa))^*$. There exist $w_1, w_2 \in A^*$, such that $(pabq)_s = paw_1$, $(p'a'b'q')_s = w_2b'q'$.

$$\begin{aligned}
(f,g)_w &= -(pabq)_s u_4b'q' + pau_1(p'a'b'q')_s \\
&= -paw_1u_4b'q' + pau_1w_2b'q' \\
&\equiv -(pab'q')_s + (pab'q')_s \\
&\equiv 0.
\end{aligned}$$

Case 4. Three of $\{a, b, a', b'\}$ is in the intersection. There are five subcases.

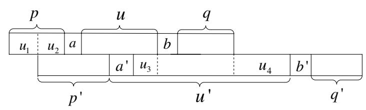
(i) $p = u_1u_2,\ u' = u_3u_4,\ q = u_5a'u_3,\ w = u_1p'a'u'b'q'$.



Clearly, $alph(bq) = alph(p'a')$. There exist $w_1, v_1, v_2, v_3 \in A^*$, such that $(pabq)_s = paw_1$, $(p'a'b'q')_s = v_1v_2v_3$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 b'q' + u_1(p'a'b'q')_s \\ &= -paw_1u_4b'q' + u_1v_1v_2v_3 \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

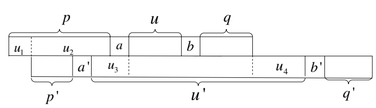
(ii) $p = u_1u_2,\ u' = u_3bqu_4,\ w = paubqu_4b'q'$.



Clearly, we have $alph(bq) = alph(p'a')$. There exists $w_1 \in A^*$, such that $(pabq)_s = paw_1$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 b'q' + u_1(p'a'b'q')_s \\ &= -paw_1u_4b'q' + u_1p'a'u_3b'q' \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

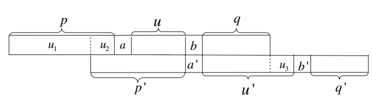
(iii) $pa = u_1p'a'u_3,\ u' = u_3ubqu_4,\ w = paubqu_4b'q'$.



Clearly, we have $alph(bq) = alph(p'a')$. There exists $w_1 \in A^*$, such that $(pabq)_s = paw_1$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 b'q' + u_1(p'a'b'q')_s \\ &= -paw_1u_4b'q' + u_1p'a'u_3b'q' \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

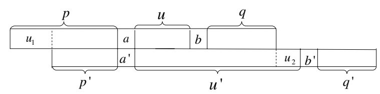
(iv) $pa = u_1u_2,\ u' = qu_3,\ w = paubqu_3b'q'$.



Since $b = a' \notin alph(p')$, $a \in alph(p')$, $a \neq b$. Since $alph(pa) = alph(bq)$, $b \in alph(q)$. Since $alph(q) \subseteq alph(u')$, we have $|alph(u')| \geq 1$. There exists $w_1 \in A^*$, such that $(pabq)_s = paw_1$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_3 b'q' + u_1(p'a'b'q')_s \\ &= -paw_1u_3b'q' + u_1p'a'b'q' \\ &\equiv -(pab'q')_s + paubb'q' \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

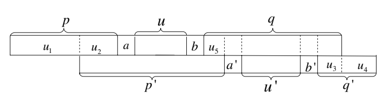
(v) $p = u_1p',\ a = a',\ u' = ubqu_2,\ w = paubqu_2b'q'$.



Clearly, $alph(pa) = alph(b'q')$ and $|alph(u')| \geq 1$. There exists $w_1 \in A^*$, such that $(pabq)_s = paw_1$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_2 b'q' + u_1(p'a'b'q')_s \\ &= -paw_1u_2b'q' + u_1p'a'b'q' \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

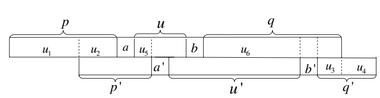
Case 5. All of $\{a, b, a', b'\}$ is in the intersection. There are seven subcases.
(i) $p = u_1u_2,\ q' = u_3u_4,\ p' = u_2aubu_5,\ w = paubqu_4$.



Clearly, $alph(pa) = alph(b'q')$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 + u_1(p'a'b'q')_s \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

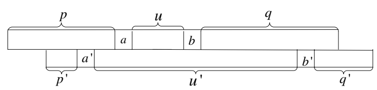
(ii) $p = u_1u_2,\ q' = u_3u_4,\ p' = u_2au_5,\ q = u_6b'u_3,\ w = paubqu_4$.

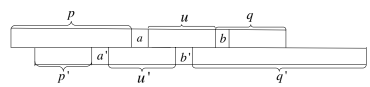


Clearly, $alph(pa) = alph(b'q')$ and $|alph(u)| \geq 1$, $|alph(u')| \geq 1$.

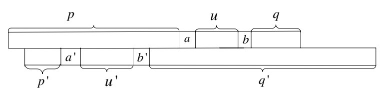
$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 + u_1(p'a'b'q')_s \\ &= -pabqu_4 + u_1 p'a'b'q' \\ &= -pabu_6 b' u_3 u_4 + u_1 u_2 a u_5 a' b' q' \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

Since $a \in alph(u') \subseteq alph(p'a') \subseteq alph(p)$, this contradicts with $a \notin alph(p)$. Then the following two cases will not happen.

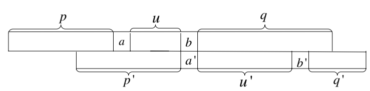




Since $a \in alph(b'q') \subseteq alph(p'a') \subseteq alph(p)$, this contradicts with $a \notin alph(p)$. Then the following case will not happen.



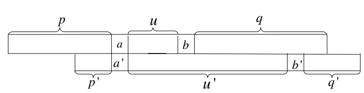
(iii) $p = u_1 u_2, q' = u_3 u_4,\ a' = b,\ w = paubqu_4$.



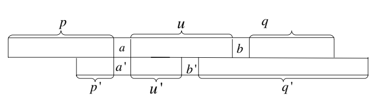
Clearly, $alph(p') = alph(q)$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s u_4 + u_1(p'a'b'q')_s \\ &\equiv -(pab'q')_s + (pab'q')_s \\ &\equiv 0.\end{aligned}$$

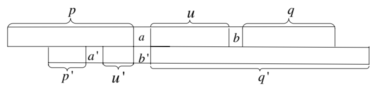
Similarly, we can prove following cases.
(iv) $a = a',\ w = pa'u'b'q'$.



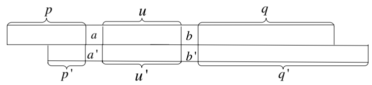
(v) $a = a',\ w = pa'u'b'q'$.



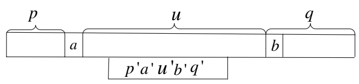
(vi) $a=b',\ w=paq'$.



(vii) $a=a',\ b=b',\ w=paubq'$.

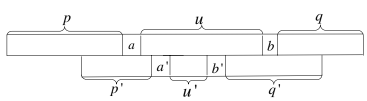


Thus, all intersection compositions in S are trivial.
Now, we prove all inclusion compositions are also trivial.
Case 1. There are three subcases.
(i) $u=u_1\bar{g}u_2,\ w=pau_1p'a'u'b'q'u_2bq$.

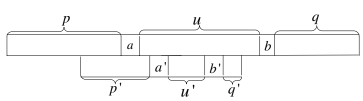


$$\begin{aligned}(f,g)_w &= -(pabq)_s + pau_1(p'a'b'q')_s u_2bq \\ &\equiv -(pabq)_s + (pabq)_s \\ &\equiv 0.\end{aligned}$$

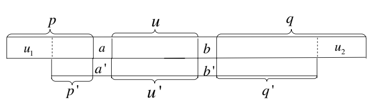
Similarly, we can prove following two cases.
(ii)



(iii)

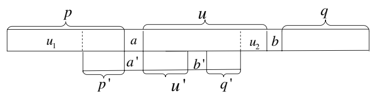


Case 2. $p=u_1p',\ q=q'u_2,\ a=a',\ b=b',\ w=paubq$.



$$\begin{aligned}(f,g)_w &= -(pabq)_s + u_1(p'a'b'q')_s u_2\\ &\equiv -(pabq)_s + (pabq)_s\\ &\equiv 0.\end{aligned}$$

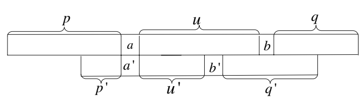
Case 3. There are four subcases.
(i) $p = u_1p',\ u = u'b'q'u_2,\ a = a',\ w = paubq.$



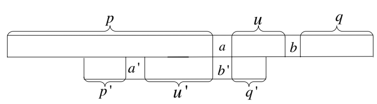
There exists $w_1 \in A^*$ such that $(p'a'b'q')_s = p'a'w_1$.

$$\begin{aligned}(f,g)_w &= -(pabq)_s + u_1(p'a'b'q')_s u_2bq\\ &\equiv -(pabq)_s + u_1p'a'w_1u_2bq\\ &\equiv -(pabq)_s + (pabq)_s\\ &\equiv 0.\end{aligned}$$

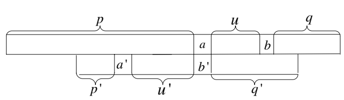
Similarly, we can prove the following three cases.
(ii)



(iii)



(iv)



So all the possible compositions in S are trivial. ■

By Lemma 2.1 and Theorem 4.1, $Irr(S)$ is an F-basis of $F\langle A \mid S\rangle$ which is also a normal form of $sgp\langle A \mid R\rangle$.

We have $Irr(S) = \bigcup_{k=0}^{n} B_k$, where $B_k = \{w \in Irr(S) \mid Card(alph(w)) = k\}$. Now we get B_k by induction on k:

(1) For $k = 0$, $B_0 = \{\epsilon\}$.
(2) For $k = 1$, $B_1 = A$.
(3) For $k > 1$, by induction $B_k^1 = \{ya \mid y \in B_{k-1},\ a \in A \setminus alph(y)\}$, $B_k^2 = \{cm(u,v) \mid u,v \in B_k^1,\ alph(u) = alph(v)\}$ and $B_k = B_k^1 \bigcup B_k^2$.

Noting that by the proof of Lemma 3.5, $cm(u,v)$ is unique in the set B_k^2 in (3).

Corollary 4.2. *The set $\bigcup_{k=0}^{\infty} B_k$ is a normal form of the free idempotent monoid on $A = \{a_i | i \in I\}$, where B_k is defined as above.*

Now, as a special case of Corollary 4.2, we have the following corollary which is due to Green and Rees, see [6].

Corollary 4.3. [6] *The free idempotent monoid on A is finite and has exactly*

$$\sum_{k=0}^{n} \binom{n}{k} \prod_{1 \le i \le k} (k-i+1)^{2^i}$$

elements, where $n = Card(A)$.

Proof. Denote $b_k = Card(B_k)$, where $0 \le k \le n$. Then $b_0 = 1,\ b_1 = n$. If $1 < k \le n$, since $B_k = B_k^1 \bigcup B_k^2$, where $B_k^1 = \{ya \mid y \in B_{k-1},\ a \in A \setminus alph(y)\}$ and $B_k^2 = \{cm(u,v) \mid u,v \in B_k^1,\ alph(u) = alph(v)\}$, we have

$$Card(B_k^1) = b_{k-1} \cdot (n-k+1)$$

and

$$Card(B_k^2) = b_{k-1} \cdot (n-k+1) \cdot [\frac{b_{k-1} \cdot (n-k+1)}{C_n^k} - 1].$$

Then $b_k = \frac{b_{k-1}^2 \cdot (n-k+1)^2}{C_n^k}$. It is easy to get $b_k = \binom{n}{k} \prod\limits_{i=1}^{k} (k-i+1)^{2^i}$. Now we have

$$Card(Irr(S)) = \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} \binom{n}{k} \prod_{1 \le i \le k} (k-i+1)^{2^i}.$$

■

References

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

[2] L.A. Bokut, Imbeddings into simple associative algebras, *Algebra i Logika* **15** (1976) 117–142.

[3] L.A. Bokut, Unsolvability of the word problem, and subalgebras of finitely presented Lie algebras, *Izv. Akad. Nauk. SSSR Ser. Mat.* **36** (1972) 1173–1219.

[4] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal, Ph.D. Thesis, University of Innsbruck, Austria, 1965. (in German)

[5] B. Buchberger, An algorithmical criteria for the solvability of algebraic systems of equations, *Aequationes Math.* **4** (1970) 374–383. (in German)

[6] J.A. Green and D. Rees, On semigroup in which $x^r = x$, *Mat. Proc. Cambridge Phil. Soc.* **48** (1952) 35–40.

[7] J.M. Howie, *Fundamentals of Semigroup Theory*, Cambridge University Press, 2003.

[8] M. Lothaire, *Combinatorics on Words*, Cambridge University Press, 2003.

[9] A.I. Shirshov, Some algorithmic problem for Lie algebras, *Sibirsk. Mat. Z.* **3** (1962) 292–296 (in Russian); English translation in *SIGSAM Bull.* **33** (2) (1999) 3–6.