Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
18 (2002), 1–6
www.emis.de/journals

SUBALGEBRA BASES AND RECOGNIZABLE PROPERTIES

CASAPENKO LOUISA U.

Abstract. The paper considers computer algebra in a non-commutative setting. The theory of Gröbner bases of ideals in polynomial rings gives the possibility of obtaining a series of effective algorithms for symbolic calculations. Recognizable properties of associative finitely presented algebras with the finite Gröbner basis were investigated by V. N. Latyshev, T. Gateva-Ivanova in [1]. While subalgebras may not be as important as ideals, they are the second major type of *subobject* in ring theory. The paper considers recognizable properties of subalgebras with finite standard basis, or *SAGBI*-basis (Subalgebra Analogue to Gröbner Basis for Ideals).

The paper considers computer algebra in a non-commutative setting. The theory of Gröbner bases of ideals in polynomial rings gives the possibility of obtaining a series of effective algorithms for symbolic calculations. Recognizable properties of associative finitely presented algebras with the finite Gröbner basis were investigated by V. N. Latyshev, T. Gateva-Ivanova in [1]. While subalgebras may not be as important as ideals, they are the second major type of *subobject* in ring theory. The paper considers recognizable properties of subalgebras with finite standard basis, or *SAGBI*-basis (Subalgebra Analogue to Gröbner basis for ideals). *SAGBI*-basis in polynomial rings was suggested by L. Robbiano, M. Sweedler in [5] and D. Kapur , K. Madlener in [3]. *SAGBI*-basis of subalgebras in free associative algebras was introduced in [2]. V. N. Latyshev suggested in [4] a general approach to standard bases. It allows to define *SAGBI*-basis of subalgebras in monomial algebras in this article. The paper considers subalgebras with finite *SAGBI*-basis. It is shown that algebraic property such that being finite-dimensional is algorithmically recognizable. It is also recognizable that *SAGBI*-basis generates free subalgebra.

Main Result

In this paper $\mathcal{N}$ denotes the set of the naturals, $\mathcal{K}$ denotes a fixed field, of arbitrary characteristic, and the term $\mathcal{K}$-algebra is used to denote an associative algebra over $\mathcal{K}$. We use the presentation of $\mathcal{K}$-algebra A in the form $A = \mathcal{K}\langle X\rangle/(\mu)$, where $X = \{x_1, \dots, x_n\}$ is a set of indeterminates, $\mathcal{K}\langle X\rangle$ is a free $\mathcal{K}$-algebra on it, and (μ) is an monomial ideal. Let $\mu = \{m_1, \dots, m_M\} \subset \langle X\rangle$ be a generating set for (μ). In this paper, our starting point is a monomial algebra A.

Let $\langle X\rangle$ denote the free semigroup generated by X; we consider the empty word as belonging to $\langle X\rangle$, and denote it by 1. The elements of $\langle X\rangle$ are ordered as follows:

- $x_1 < \ldots < x_n$;
- if $u, v \in \langle X\rangle$ are of the same degree, then $<$ refers to the lexicographic order;
- if $u, v \in \langle X\rangle$ are of degree d_1, d_2 respectively, and $d_1 < d_2$, then $u < v$.

1991 *Mathematics Subject Classification.* 16Z05, 68W30.
Key words and phrases. Standard basis, SAGBI-basis, algorithmically recognizable properties of subalgebras in monomial algebras.

Let E_A denote the $\mathcal{K}$-linear basis of the algebra A

Umirbaev showed unsolvability that the finite subset $G = \{g_1, \dots, g_N\}$ in a free associative algebra generates a free subalgebra (see [8]). This problem is algorithmically solvable for the monomial generating set G (see [6]). We will consider this problem for generating set $G = \{g_1, \dots, g_N\}$ in the monomial algebra A. For this purpose we use a concept of a standard basis.

Let $\overline{f}$ denote the highest term of $f \in A$ which is normal respect to μ.

The product $g_{i_1} \dots g_{i_r}$ of elements $g_{i_1}, \dots, g_{i_r} \in A$ is called essential if $\overline{g_{i_1} \dots g_{i_r}} = \overline{g_{i_1}} \dots \overline{g_{i_r}}$. Otherwise, the product $g_{i_1} \dots g_{i_r}$ is called inessential.

Let $G = \{g_1, \dots, g_N\}$ generates a subalgebra B in the algebra A.

Let the highest coefficients of g_i's are equal to 1.

The generating set G is called standard basis (*SAGBI*-basis) of subalgebra B if for any $b \in B$ exists the essential product $g_{i_1} \dots g_{i_r}$ such that $\overline{b} = \overline{g_{i_1}} \dots \overline{g_{i_r}}$.

Say the equality

$$b = \sum_{(i) \in I} \lambda_{(i)} g_{i_1} \dots g_{i_r}, \tag{1}$$

$b \in B$, $\lambda_{(i)} \in \mathcal{K}$, $g_{i_1}, \dots, g_{i_r} \in G$, is the representation of $b \in B$ if all products $g_{i_1} \dots g_{i_r}$ are essential. The greatest basic vector w among the $\overline{g_{i_1}} \dots \overline{g_{i_r}}$'s is termed a parameter of this representation. If $\overline{b} = w$, then the equality above is called H-representation of $b \in B$.

Let the essential products $g_{i_1} \dots g_{i_r}$, $g_{j_1} \dots g_{j_t}$ have the same highest term $w = \overline{g_{i_1} \dots g_{i_r}} = \overline{g_{j_1} \dots g_{j_t}}$. Then $s = g_{i_1} \dots g_{i_r} - g_{j_1} \dots g_{j_t}$ is called s-element with the initial parameter w.

For any essential product $p(G) = g_{i_1} \dots g_{i_r}$, $u = \overline{g_{i_1} \dots g_{i_r}} \in E_A$ define a reduction $r_{p(G)} : A \to A$, which is a linear transformation on A sending u to the element $r_{p(G)}(u) = u - g_{i_1} \dots g_{i_r}$ and fixing all basic elements from E_A other than u.

Denote $\mathcal{R}_G$ the set of all reductions together with the identity mapping e. Then $(A, \leq, \mathcal{R}_G)$ is a linear scheme of simplification.

We may consider the subalgebra B of the algebra A as a subact of a linear act A over a free monoid $\omega = \langle \Sigma \rangle$, where $\Sigma = \{\sigma_0 = e, \sigma_1 \dots, \sigma_N\}$, $\sigma_i : a \mapsto g_i a$, $i = 1, 2, \dots, N$, $a \in A$. Standard basis of a subact in a linear act is defined by Latyshev in [4]. As a consequence of this work results we obtain the following theorem.

Theorem 1. In the above notation let $B \subset A$ be a subalgebra of the algebra $A = \mathcal{K}\langle X \rangle / I$ and $G = \{g_1, g_2, \dots, g_N\}$ be essential generators of B. Then the following are equivalent.

- **(i):** G is a standard basis.
- **(ii):** Any element b of B is reducible to zero.
- **(iii):** Any element b of B has an H-representation.
- **(iv):** Any s-element has a representation (via G) with a parameter less than its initial parameter.
- **(v):** $(A, \leq, R_G)$ is a linear scheme of simplification with the canonization property.

Let $F(y_1, \dots, y_N)$ be a polynomial in variables $y_1, y_2, \dots, y_N$ such that

$$F(y_1, \dots, y_N) \not\equiv 0$$

in y_i's and $F(g_1, \dots, g_N) \equiv 0$ in x_i's. Then we say that $F(g_1, \dots, g_N) = 0$ is a polynomial relation between $g_1, \dots, g_N$.

Let $G = \{g_1, \dots, g_N\}$ be a *SAGBI*-basis of the subalgebra B.

Then any inessential product $p = g_{i_1} \dots g_{i_r}$ has an H-representation, as an element of the subalgebra B. Let φ be this H-representation. A polynomial relation $p - \varphi = 0$ between $g_1, \dots, g_N$ is called a p-relation.

Any s-element $s = g_{i_1} \dots g_{i_r} - g_{j_1} \dots g_{j_t}$ has an H-representation also. Let δ be this H-representation. A polynomial relation $s - \delta = 0$ between $g_1, \dots, g_N$ is called an s-relation.

Theorem 2. *Any polynomial relation between generators $g_1, \dots, g_N$ is a linear combination of p-,s-relations.*

Theorem 3. *Let $G = \{g_1, g_2, \dots, g_N\}$ be a SAGBI-basis of the subalgebra B of the monomial algebra $A = \mathcal{K}\langle X\rangle/(\mu)$. Then it is a recognizable property that G generates a free subalgebra B.*

Theorem 4. *Let $G = \{g_1, g_2, \dots, g_N\}$ be a SAGBI-basis of the subalgebra B of the monomial algebra $A = \mathcal{K}\langle X\rangle/(\mu)$. Then it is a recognizable property that A is finite dimensional.*

Proofs

Proof of Theorem 2. Let $F(g_1, \dots, g_N) = 0$ be a polynomial relation between generators $g_1, \dots, g_N$.

$$F(g_1, \dots, g_N) = \sum_{(i)\in I} \alpha_{(i)} g_{i_1} \dots g_{i_r} = \sum_{k=1}^{L} F_k = 0.$$

$$F_k = \sum_{(i)\in I_k} \alpha_{(i)} g_{i_1} \dots g_{i_r}.$$

$$\overline{g_{i_1} \dots g_{i_r}} = w_k \quad \forall (i) \in I_k.$$

$$w_1 > w_2 > \dots > w_L.$$

We may regard the monomial w_1 as a parameter of this relation.

(2)

$$F(g_1, \dots, g_N) = \alpha_{(i_1)} g_{i_{11}} \dots g_{i_{1,r(1)}} + \dots + \alpha_{(i_q)} g_{i_{q,1}} \dots g_{i_{q,r(q)}} + \sum_{(i)\in I\setminus I_1} \alpha_{(i)} g_{i_1} \dots g_{i_r}$$

$(i_1), (i_2), \dots, (i_q) \in I_1, |I_1| = q.$

We have $q \geq 2$, $\sum\limits_{(i)\in I_1} \alpha_{(i)} = 0.$

Let $F(g_1, \dots, g_N)$ be not in $Span\{p - \varphi, s - \delta\}$ and it has the minimal parameter w_1 and minimal value $Q = |I_1| = q$ among such polynomial relations.

One can select the following cases.

(1) All products

$$p_1(G) = g_{i_{11}} \dots g_{i_{1,r(1)}}, p_2(G) = g_{i_{21}} \dots g_{i_{2,r(2)}}, \dots, p_q(G) = g_{i_{q1}} \dots g_{i_{q,r(q)}}$$

are inessential.

(2) There exists exactly one essential product among the products

$$p_1(G), p_2(G), \dots, p_q(G).$$

(3) There are at least two essential products among the products

$$p_1(G), \dots, p_q(G).$$

We consider each case in detail.

(1) Subtract the following relation

$$\alpha_{(i_1)}(p_1(G) - \varphi) = 0$$

from the relation (2). $p_1(G) - \varphi = 0$ is a p-relation. Let φ be in the form

$$\varphi = \beta_{(j_1)} g_{j_{11}} \dots g_{j_{1,t(1)}} + \sum_{(j)\in J} \beta_{(j)} g_{j_1} \dots g_{j_t}. \tag{3}$$

$\overline{g_{j_{11}} \dots g_{j_{1,t(1)}}} = \overline{g_{j_{11}}} \dots \overline{g_{j_{1,t(1)}}} > \overline{g_{j_1} \dots g_{j_t}} = \overline{g_{j_1}} \dots \overline{g_{j_t}} \quad \forall (j) \in J.$
Then

$$\alpha_{(i_1)}\beta_{j_1} g_{j_{11}} \dots g_{j_{1,t(1)}} + \alpha_{(i_2)} g_{i_{21}} \dots g_{i_{2,r(2)}} + \dots + \alpha_{(i_q)} g_{i_{q,1}} \dots g_{i_{q,r(q)}} +$$
$$+ \sum_{(i)\in I\setminus I_1} \alpha_{(i)} g_{i_1} \dots g_{i_r} + \sum_{(j)\in J} \alpha_{(i_2)}\beta_{(j)} g_{j_1} \dots g_{j_t} = 0.$$

This polynomial relation is not in $Span\{s-\delta, p-\varphi\}$. Its parameter is equal to w_1. Its value Q is equal to q. But it has exactly one essential product $g_{j_{11}} \dots g_{j_{1,t(1)}}$ with the highest term w_1 (see the case 2).

(2) As $q \geq 2$, there exists an inessential product among them. Let $p_1(G)$ be the essential product, then $p_2(G)$ is not essential. Subtract the following relation

$$\alpha_{(i_2)}(p_2(G) - \varphi) = 0$$

from the relation (2). $p_2(G) - \varphi = 0$ is a p-relation. Let φ be in the form (3). Then

- $$(\alpha_{(i_1)} + \alpha_{(i_2)}\beta_{(j-1)}) g_{i_{11}} \dots g_{i_{1,r(1)}} + \alpha_{(i_3)} g_{i_{31}} \dots g_{i_{3,r(3)}} + \dots +$$
$$+ \alpha_{i_{(q)}} g_{i_{q_1}} \dots g_{i_{q,r(q)}} + \sum_{(i)\in I\setminus I_1} \alpha_{(i)} g_{i_1} \dots g_{i_r} + \sum_{(j)\in J} \alpha_{(i_2)}\beta_{(j)} g_{j_1} \dots g_{j_t} = 0,$$
  if $g_{i_{11}} \dots g_{i_{1,r(1)}}$ is equal to $g_{j_{11}} \dots g_{j_{1,t(1)}}$ lexicographically in g_i's. This polynomial relation is not in $Span\{p-\varphi, s-\delta\}$. It has the parameter w_1. Its value Q is less than q.
$$Q = \begin{cases} q-1, & if \alpha_{(i_1)} + \alpha_{(i_2)}\beta_{(j_1)} \neq 0; \\ q-2, & otherwise. \end{cases}$$
  It contradicts to our assumption.
- $$\alpha_{(i_1)} g_{i_{11}} \dots g_{1,r(1)} + \alpha_{(i_2)}\beta_{j_1} g_{j_{11}} \dots g_{j_{1,t(1)}} + \alpha_{(i_3)} g_{i_{31}} \dots g_{i_{3,r(3)}} + \dots +$$
$$+ \alpha_{(i_q)} g_{i_{q,1}} \dots g_{i_{q,r(q)}} + \sum_{(i)\in I\setminus I_1} \alpha_{(i)} g_{i_1} \dots g_{i_r} + \sum_{(j)\in J} \alpha_{(i_2)}\beta_{(j)} g_{j_1} \dots g_{j_t} = 0,$$
  if $g_{i_{11}} \dots g_{i_{1,r(1)}} \neq g_{j_{11}} \dots g_{j_{1,t(1)}}$ lexicographically in g_i's. This polynomial relation is not in $Span\{p-\varphi, s-\delta\}$. Its parameter is equal to w_1. Its value Q is equal to q. But it has exactly two essential products with the highest term w_1 (see the case 3).

(3) Let $p_1(G), p_2(G)$ be the essential products. Subtract the following relation

$$\alpha_{(i_1)}(p_1(G) - p_2(G) - \delta) = 0$$

from the relation (2). $s = p_1(G) - p_2(G)$ is an s-element. Then

$$(\alpha_{(i_1)} + \alpha_{(i_2)}) p_2(G) + \alpha_{(i_3)} p_3(G) + \ldots + \alpha_{(i_q)} p_q(G) +$$
$$+ \sum_{(i)\in I\setminus I_1} \alpha_{(i)} g_{i_1} \dots g_{i_r} + \alpha_{i_1}\delta = 0,$$
$$\overline{\delta} < w_1 = p_1(\overline{G}) = p_2(\overline{G}).$$

This polynomial relation is not in $Span\{p-\varphi, s-\delta\}$. Its parameter is equal to w_1. The number Q of the products with the highest term w_1 is less than q.

$$Q = \begin{cases} q-1, & if \alpha_{(i_1)} + \alpha_{(i_2)} \neq 0; \\ q-2, & otherwise. \end{cases}$$

It contradicts to our assumption.

Thus, we complete the proof of the theorem. □

Proof of theorem 3. The algebraic dependence of the set $G = \{g_1, g_2, \ldots, g_N\}$ means the existence of a polynomial relation between the generators $g_1, \ldots, g_N$. It is equivalent to the existence of an inessential product or an s-element respect to G. It is a recognizable property that there exists an inessential product for the given finite set G.

Let d_μ denote the maximal degree of monomials $m_1, \ldots, m_M$ in x_i's. We have to check whether a product $\overline{g_{i_1}} \ldots \overline{g_{i_r}}$ is in the ideal (μ) for all $g_{i_1}, \ldots, g_{i_r} \in G$, $r \leq d_\mu$. If such product exists, then $g_{i_1} \ldots g_{i_r}$ is not essential. It means the existence of a p-relation. Then the set G is algebraically dependent. Otherwise, $\overline{g_{i_1}} \ldots \overline{g_{i_r}} \notin (\mu)$ $\forall r \leq d_\mu \quad \forall g_{i_1}, \ldots, g_{i_r} \in G$. Then products $g_{i_1} \ldots g_{i_t} \forall t \in \mathcal{N}$ are essential. There are not any p-relations. Then the existence of an s-element

$$s = p_1(G) - p_2(G) = g_{i_1} \ldots g_{i_r} - g_{j_1} \ldots g_{j_t},$$

$$p_1(\overline{G}) = \overline{g_{i_1}} \ldots \overline{g_{i_r}} = \overline{g_{j_1}} \ldots \overline{g_{j_t}} = p_2(\overline{G}),$$

means the algebraic dependence of the monomial set $\overline{G} = \{\overline{g_1}, \overline{g_2}, \ldots, \overline{g_N}\}$ in a free associative algebra $\mathcal{K}\langle X \rangle$. This property is recognizable for the finite set $\overline{G}$. It was investigated in the code theory (see [7]; [6]). □

Proof of theorem 4. Denote $\mathcal{B} = \{p(G)\}$ the set of all essential products such that $p_1(\overline{G}) \neq p_2(\overline{G})$ in x_i's, $p_1(G) \neq p_2(G)$ in g_i's. $\mathcal{B}$ is a $\mathcal{K}$-linear basis of the subalgebra B.

The set $\mathcal{B}$ is linear independent.

Let

$$\sum_{i=1}^{k} \lambda_i p_i(G) = 0,$$

$$p_i(G) \in \mathcal{B} \quad \forall i = 1, 2, \ldots, k,$$

$$p_1(\overline{G}) < p_2(\overline{G}) < \ldots p_k(\overline{G}) \quad \text{in} \quad x_i' \text{s}.$$

Then

$$\overline{\sum_{i=1}^{k} \lambda_i p_i(G)} = p_k(\overline{G}) \not\equiv 0 \quad (mod(\mu)).$$

That's why

$$\lambda_k = 0 \qquad \sum_{i=1}^{k-1} \lambda_i p_i(G) = 0.$$

Then $\lambda_{k-1} = \ldots = \lambda_1 = 0$.

Any element $b \in B$ is a linear combination of elements of $\mathcal{B}$.

Let b be in the form

$$b = \sum_{i=1}^{k} \lambda_i p_i(G) \tag{4}$$

$\lambda_i \in \mathcal{K}$, $p_i(G)$ is an essential product for all $i = 1, 2, \ldots, k$,
$p_1(\overline{G}) \leq p_2(\overline{G}) \leq \ldots \leq p_k(\overline{G})$ in x_i's.

Let k_0 denote the maximal number such that $p_{k_0}(G) \notin \mathcal{B}$. There exists an essential product $p(G) \in \mathcal{B}$ such that $p_{k_0}(\overline{G}) = p(\overline{G})$ in x_i's. An s-element $s = p_{k_0}(G) - p(G)$ has an H-representation

$$s = \sum_{(i)} \gamma_{(i)} g_{i_1} \ldots g_{i_r}.$$

$g_{i_1}\dots g_{i_r}$ are essential products for all (i). $\overline{g_{i_1}}\dots\overline{g_{i_r}} < p_{k_0}(\overline{G})$. Substitute the equation

$$p_{k_0}(G) = p(G) + \sum_{(i)} \gamma_{(i)} g_{i_1}\dots g_{i_r}$$

to (4). Then we receive the equation with the lesser number of different addendums not belonging to $\mathcal{B}$ and having the highest term $p_{k_0}(\overline{G})$. In consequence by force of d.c.c. we receive the presentation of element $b \in B$ in the form of a linear combination of elements of $\mathcal{B}$.

Let

$$\mathcal{S} = \{p_{1,0}(G), p_{1,1}(G), \dots, p_{1,t(1)}(G), p_{2,0}(G), p_{2,1}(G), \dots, p_{2,t(2)}(G), \dots, \\ p_{R,0}(G), p_{R,1}(G), \dots, p_{R,t(R)}(G), \dots\}$$

denote the set of all essential products. $\mathcal{B} = \{p_{i,0}(G)\} \subset \mathcal{S}$ is a $\mathcal{K}$-linear basis of the subalgebra B.

$$p_{1,0}(\overline{G}) < p_{2,0}(\overline{G}) < \dots < p_{R,0}(G) < \dots \quad \text{in} x_i'\text{s}.$$

$\mathcal{S}(i) = \{p_{i,j}(G)\}_{j=0}^{t(i)}$ is the set of all different essential products such that

$$p_{i,j}(\overline{G}) = p_{i,j'}(\overline{G}) \quad \forall j, j' = 0, 1, \dots, t(i).$$

$t(i) < \infty$ for any i. Construct the auxiliary monomial algebra

$$D = \mathcal{K}\langle y_1, \dots, y_N\rangle/(\eta),$$

where η is a finite monomial set in y_i's. Let the monomial $v = y_{j_1}\dots y_{j_l}$ be in η, $l \le d_\mu$, if and only if $g_{j_1}\dots g_{j_l}$ is an inessential product. Then the monomials $y_{j_1}\dots y_{j_l}$ such that $g_{j_1}\dots g_{j_l}$ is an essential product form a $\mathcal{K}$-linear basis of algebra D. As $t(i) < \infty$ for all i, we receive that the subalgebra B is finite dimensional if and only if D is finite dimensional. It is a recognizable property that D is finite dimensional (see [1]). Thus, we complete the proof of the theorem. □

References

[1] T. Gateva-Ivanova and V. N. Latyshev. On the recognizable properties of associative algebras. In *On comp. aspects comm. algebras*, pages 237–254. Acad. Press., London, 1988.

[2] N. K. Iudu. *Standard basis and the problem subset in subalgebras in free associative algebras.* PhD thesis, Moscow, 1999. in Russian.

[3] D. Kapur and K. Madlener. A completion procedure for computing a canonical basis for a $\mathcal{K}$-subalgebra. In *Computers and Mathematics*, pages 1–11. Cambridge, MA., 1989.

[4] V. N. Latyshev. An improved version of standard bases. In *Proc. of the 12th intern. conf. FPSAC'00 Moscow, June 26-30, 2000.*

[5] L. Robbiano and M. Sweedler. Subalgebra bases. In *Comm. algebra. Proc. of the work-shop held at the Federal Univ. of Bahia, Salvador, 1988.*, volume 1430 of *Lect. notes Math.*, pages 61–87, 1990.

[6] A. Saloma. *Pearles of theory of formal languages.* Mir, 1986. in Russian.

[7] A. Sardinas and G. Patterson. A nesserary and sufficient condition for the unique decomposition of coded messages. IRE Intern. conv. record., 1958. 104–108.

[8] U. U. Umirbaiev. Some algoritmical questions of associative algebras. *Algebra and Logica*, 32(4):450–470, 1993.

Received October 31, 2000.

E-mail address: `acv@aport.ru`

Department of Mechanics and Mathematics (Algebra),
Ulyanovsk State University,
432700 Lev Tolstoy 42, Ulyanovsk, Russia