ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2002 МАТЕМАТИКА № 11 (486)

УДК 519.4

Л.Ю. КАСАПЕНКО

НЕКОТОРЫЕ АЛГОРИТМИЧЕСКИЕ ВОПРОСЫ АССОЦИАТИВНЫХ АЛГЕБР

Введение

Вопрос об алгоритмической распознаваемости алгебраической зависимости конечного семейства элементов свободной ассоциативной алгебры, вообще говоря, решается отрицательно [1]. В теории кодирования существуют эффективные методы распознавания алгебраической зависимости конечного мономиального множества. Старейшим является алгоритм, приведенный в [2]. Описание этого алгоритма также приведено в ([3], с. 59–64). В данной работе рассматриваются так называемые $SAGBI$-базисы (Subalgebra analogue to Gröbner bases for ideals) для подалгебр, являющиеся аналогами стандартных базисов для идеалов. $SAGBI$-базисы первоначально определены для подалгебр алгебры полиномов в [4], [5]. Понятие $SAGBI$-базиса на случай подалгебр свободной ассоциативной алгебры распространено в [6]. Введенное в [7] понятие стандартного базиса подполигона линейного полигона позволило определить понятие $SAGBI$-базиса в подалгебре ассоциативной стандартно конечно-определенной алгебры. В данной работе положительно решен вопрос о распознавании свободной порожденности и конечномерности подалгебры, заданной конечным $SAGBI$-базисом в ассоциативной стандартно конечно-определенной алгебре.

1. Общие определения и обозначения

Пусть $\mathcal{K}$ — поле нулевой характеристики; $X = \{x_1, \dots, x_n\}$ — произвольный алфавит; $\langle X \rangle$ — свободная полугруппа, порожденная множеством X; $\mathcal{K}\langle X \rangle$ — полугрупповая алгебра полугруппы X над полем $\mathcal{K}$, являющаяся алгеброй некоммутативных полиномов или свободной ассоциативной алгеброй ранга n над полем $\mathcal{K}$. Элементы полугруппы $\langle X \rangle$ называются мономами, а элементы $\mathcal{K}\langle X \rangle$ — полиномами.

Полный порядок $x_1 < \dots < x_n$, заданный на алфавите X, продолжается до полной упорядоченности полугруппы $\langle X \rangle$, если из двух мономов разной длины старшим считать более длинный, а мономы одинаковой длины сравнивать лексикографически (степенно-лексикографическая упорядоченность). Такая упорядоченность полугруппы $\langle X \rangle$ удовлетворяет условию обрыва убывающих цепочек descending chain condition (d. c. c.).

В любом ненулевом полиноме p можно выделить старший член, обозначаемый $\overline{p}$. Для монома m из $\langle X \rangle$ через $\deg m$ будем обозначать обычную степень (т. е. длину) соответствующего монома; для полинома p из $\mathcal{K}\langle X \rangle$, представленного в виде несократимой линейной комбинации мономов

$$p = \alpha_1 m_1 + \dots + \alpha_r m_r,$$

положим

$$\deg p = \max_{1 \le i \le r} \deg m_i.$$

Пусть $I = (\phi)$ обозначает идеал в $\mathcal{K}\langle X\rangle$, причем система $\phi = \{f_1, \ldots, f_M\}$ порождающих идеала I образует его базис Гребнера. Фактор-алгебру $A = \mathcal{K}\langle X\rangle/I$ называют стандартно конечно-определенной (с. к. о.) алгеброй [8]. Будем рассматривать распознаваемость некоторых свойств подалгебр с. к. о. алгебры A.

Определение 1 ([7]). Пусть

(i) V — линейное пространство над полем $\mathcal{K}$;

(ii) $E = \{e_\alpha \mid \alpha \in \Lambda\}$ — выделенный базис пространства V, где Λ – упорядоченная полугруппа, в которой полная упорядоченность удовлетворяет d. c. c., базисные элементы сравниваются в соответствии со своими индексами, т. е. $e_\alpha > e_\beta \Leftrightarrow \alpha > \beta$;

(iii) Σ — множество линейных операторов на V, содержащее тождественное отображение, таким образом, всякий элемент $\sigma \in \Sigma$ индуцирует линейное отображение $\sigma : V \to V$;

(iv) некоторые произведения σe_α, $\sigma \in \Sigma$, $e_\alpha \in E$ (включая произведения $ee_\alpha = e_\alpha$), объявлены существенными.

Линейное пространство V называется *линейным полигоном* над свободным моноидом $\omega = \langle\Sigma\rangle$, порожденным операторами из Σ.

Если $\psi = \sigma_1 \ldots \sigma_m \in \omega$, $\sigma_i \in \Sigma$, $x \in V$, то обозначим $\psi_x = \sigma_1(\ldots(\sigma_m x)\ldots)$.

Определение 2 ([7]). Произведение $\sigma_j x$, $\sigma_j \in \Sigma$, $x \in V$, называется *существенным*, если существенным является произведение $\sigma_j\overline{x}$. Символом $\overline{x}$ обозначается базисный вектор (старший член) в представлении $x \in V$ в виде линейной комбинации элементов из E.

Определение 3 ([7]). Произведение ψx, $\psi = \sigma_1 \ldots \sigma_m \in \omega$, $\sigma_i \in \Sigma$, $x \in V$, называется *существенным*, если каждый множитель σ_i действует существенным образом.

Определение 4 ([7]). Линейное подпространство $U \subseteq V$ называется *линейным подполигоном*, если оно является инвариантным относительно операторов из Σ.

Определение 5 ([7]). Будем говорить, что множество элементов $G = \{g_i\} \subset U$ *порождает* U, если U совпадает с линейным пространством $\mathrm{Span}\{\psi g_i \mid \psi \in \omega,\ g_i \in G\}$. Если все произведения ψg_i существенны, то G называется *существенным множеством порождающих.*

Определение 6 ([7]). Множество $G = \{g_i\} \subseteq U$ называется *стандартным базисом* U, если для всякого элемента $x \in U$ существует существенное произведение ψg_i, $\psi \in \omega$, $g_i \in G$, такое, что $\overline{x} = \overline{\psi g_i}$.

Определение 7 ([7]). Пусть $U \subseteq V$ — линейный подполигон и $G = \{g_i\} \subseteq U$ — его множество порождающих. Равенство

$$x = \sum_i \lambda_i \psi_i g_i, \tag{1}$$

$x \in U$, $\lambda_i \in K$, $\psi_i \in \omega$, $g_i \in G$, называется *представлением* $x \in U$, если все произведения $\psi_i g_i$ являются существенными. Старший базисный вектор w среди всех $\overline{\psi g_i}$ называют *параметром представления.* Если $\overline{x} = w$, то представление (1) элемента x называют *H-представлением.*

Символом ${}^0x$ обозначен элемент, полученный из $x \in V$ делением на его старший коэффициент (коэффициент при старшем члене).

Определение 8 ([7]). Пусть существенные произведения $\psi_1 g_i$ и $\psi_2 g_j$, $\psi_1, \psi_2 \in \omega$, $g_i, g_j \in G$, таковы, что $w = \overline{\psi_1 g_i} = \overline{\psi_2 g_j} \in E$. Тогда $s =^0 (\psi_1 g_i) -^0 (\psi_2 g_j)$ называется *s-элементом* с исходным параметром w.

Определение 9 ([7]). Для любого существенного произведения ψg_i, $\psi \in \omega$, $g_i \in G$, $e_\alpha = \overline{\psi g_i}$, назовем *редукцией* $r_{\psi,i} : V \to V$ линейный оператор на V, который элементу e_α сопоставляет элемент $r_{\psi,i}(e_\alpha) = e_\alpha -^0 (\psi g_i)$, а базисные элементы, отличные от e_α, оставляет на месте.

Пусть R_G — множество всех редукций, содержащее тождественное отображение. Тогда $(V, \leq, R_G)$ — линейная схема симплификации.

Теорема 1 ([7]). *Пусть $U \subseteq V$ — линейный подполигон и $G = \{g_i\} \subseteq U$ — существенные порождающие U. Тогда следующие условия эквивалентны*:

(i) G — *стандартный базис*;

(ii) *всякий элемент из U редуцируется к нулю*;

(iii) *всякий элемент из U обладает H-представлением*;

(iv) *всякий s-элемент имеет представление с параметром, меньшим исходного параметра*;

(v) $(V, \leq, R_G)$ — *линейная схема симплификации с канонизацией.*

2. О свободных порождающих подалгебр

В этом параграфе рассматривается вопрос о том, является ли данное конечное семейство элементов в с. к. о. алгебре алгебраически зависимым.

Определим понятие $SAGBI$-базиса подалгебры с. к. о. алгебры A. Пусть $G = \{g_1, \ldots, g_N\} \subset A$ порождает подалгебру B. Без ограничения общности рассуждений можем считать, что старшие коэффициенты элементов g_i равны 1.

В полиноме b из B, представленном в виде несократимой линейной комбинации мономов

$$b = \alpha_1 m_1 + \cdots + \alpha_r m_r,$$

где $m_1, \ldots, m_r \neq u\overline{f}v \ \ \forall u, v \in \langle X \rangle \bigcup 1, \ \ \forall f \in \phi$, можно выделить старший член $\overline{b}$.

Имеем

(i) A — линейное пространство над полем $\mathcal{K}$;

(ii) выделенным базисом E_A являются нормальные мономы относительно идеала I, в качестве полугруппы индексов Λ служит свободная полугруппа $\langle X \rangle$, упорядоченность на E_A наследована с $\langle X \rangle$;

(iii) $\Sigma = \{\sigma_0 = e, \sigma_1 : a \mapsto g_1 a, \ldots, \sigma_N : a \mapsto g_N a \mid a \in A\}$ — множество линейных операторов на A,

$$\sigma_i w = g_i w = \overline{g_i} w - \sum_{j=1}^{k} \beta_j \widetilde{g}_{i,j} w,$$

где $w \in E_A$, $g_i = \overline{g_i} - \sum\limits_{j=1}^{k} \beta_j \widetilde{g}_{ij}$ — представление элемента g_i в виде линейной комбинации базисных векторов, $\beta_j \in \mathcal{K}$, $\widetilde{g}_{ij} \in E_A$,

$$\overline{g_i} w = \begin{cases} \overline{g_i} w, & \text{если } \ \overline{g_i} w \in E_A; \\ \sum\limits_k \alpha_{i,0,k} w_{0,k}, & \text{иначе}; \end{cases}$$

где $\alpha_{i,0,k} \in \mathcal{K}$, $w_{0,k} \in E_A$,

$$\widetilde{g}_{i,j} w = \begin{cases} \widetilde{g}_{i,j} w, & \text{если } \ \widetilde{g}_{ij} w \in E_A; \\ \sum\limits_k \alpha_{i,j,k} w_{j,k}, & \text{иначе}, \end{cases}$$

где $\alpha_{i,j,k} \in \mathcal{K}$, $w_{j,k} \in E_A$;

(iv) произведение $\sigma_i w$ является существенным в том и только том случае, когда $\overline{g_i} w \in E_A$.

Таким образом, A — линейный полигон над свободным моноидом $\omega = \langle \Sigma \rangle$.

Подалгебра $B \subseteq A$, порожденная $G = \{g_1, \ldots, g_N\} \subset A$, является инвариантным подпространством пространства A относительно операторов из Σ, следовательно, B есть линейный подполигон полигона A.

Определение 10. G называется *$SAGBI$-базисом* подалгебры B, если для любого элемента $b \in B$ имеется существенное произведение $g_{i_1} \dots g_{i_r}$, где $g_{i_1}, \dots, g_{i_r} \in G$, такое, что $\overline{b} = \overline{g_{i_1}} \dots \overline{g_{i_r}}$.

Определение 11. Равенство

$$b = \sum_{(i)\in I} \lambda_{(i)} g_{i_1} \dots g_{i_r} \tag{2}$$

называется *представлением* элемента $b \in B$, если произведение $g_{i_1} \dots g_{i_r}$ является существенным для любого $(i) \in I$. *Параметром представления* (2) назовем $w = \max\limits_{(i)\in I} \overline{g_{i_1}} \dots \overline{g}_{i_r}$. Представление (2) называется *H-представлением*, если $\overline{b} = w$.

Определение 12. Элемент $s = g_{i_1} \dots g_{i_r} - g_{j_1} \dots g_{j_t}$, где $\overline{g_{i_1} \dots g_{i_r}} = \overline{g_{i_1}} \dots \overline{g_{i_r}} = \overline{g_{j_1}} \dots \overline{g_{j_t}} = \overline{g_{j_1} \dots g_{j_t}}$, будем называть *$s$-элементом.*

Определение 13. Для каждого существенного произведения $p(G) = g_{i_1} \dots g_{i_r}$ назовем *редукцией* $r_{p(G)} : A \to A$ линейный оператор, действующий на базисных векторах из E_A следующим образом: $r_{p(G)}(u) = u - g_{i_1} \dots g_{i_r}$, если $u = \overline{g_{i_1}} \dots \overline{g_{i_r}}$, и тождественно иначе.

Как следствие из теоремы 1 имеет место

Теорема 2. *Пусть $B \subset A$ — подалгебра с. к. о. алгебры $A = \mathcal{K}\langle X\rangle/I$, $G = \{g_1, \dots, g_N\}$ — существенные порождающие подалгебры B. Тогда следующие условия эквивалентны*:

(i) *G — стандартный базис*;
(ii) *всякий элемент b из B редуцируется к нулю*;
(iii) *всякий элемент b из B обладает H-представлением*;
(iv) *всякий s-элемент имеет представление с параметром, меньшим исходного параметра*;
(v) *$(A, \leq, R_G)$ — линейная схема симплификации с канонизацией.*

В частности, при $I = 0$, $A = \mathcal{K}\langle X\rangle$ получим определение $SAGBI$-базиса подалгебры свободной ассоциативной алгебры, введенное в [6] для решения проблемы вхождения в подалгебру свободной ассоциативной алгебры, порожденной конечным числом однородных элементов.

В дальнейшем будем предполагать, что подалгебра B алгебры A задана своим конечным $SAGBI$-базисом $G = \{g_1, \dots, g_N\}$.

Определение 14. Пусть $0 \not\equiv F(y_1, \dots, y_N) \in \mathcal{K}\langle y_1, \dots, y_N\rangle$ и $F(g_1, \dots, g_N) = 0$ в $\mathcal{K}\langle X\rangle$. Тогда $F(g_1, \dots, g_N) = 0$ называется *полиномиальным соотношением* между элементами $g_1, \dots, g_N$.

Так как G — $SAGBI$-базис, то всякое несущественное произведение $p = g_{i_1} \dots g_{i_r}$, т. е. $\overline{g_{i_1} \dots g_{i_r}} < \overline{g_{i_1}} \dots \overline{g_{i_r}}$ в $\langle X\rangle$, как элемент подалгебры B, обладает H-представлением. Пусть φ — его H-представление, тогда $p - \varphi = 0$ является полиномиальным соотношением между порождающими $g_1, \dots, g_N$.

Определение 15. Полиномиальное соотношение $p - \varphi = 0$ между порождающими $g_1, \dots, g_N$ назовем *p-соотношением* между элементами $g_1, \dots, g_N$.

Так как G — $SAGBI$-базис, то всякий s-элемент $s = g_{i_1} \dots g_{i_r} - g_{j_1} \dots g_{j_t}$, как элемент подалгебры B, обладает H-представлением. Пусть δ — его H-представление, тогда $s - \delta = 0$ является полиномиальным соотношением между порождающими $g_1, \dots, g_N$.

Определение 16. Полиномиальное соотношение $s - \delta = 0$ между порождающими $g_1, \dots, g_N$ назовем *s-соотношением* между элементами $g_1, \dots, g_N$.

Теорема 3. *Всякое полиномиальное соотношение между порождающими $g_1, \dots, g_N$ выражается в виде линейной комбинации p- и s-соотношений.*

Доказательство. Пусть $F(g_1,\dots,g_N)=0$ — произвольное соотношение между порождающими $g_1,\dots,g_N$. Представим его в виде

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

где $F_k=\sum\limits_{(i)\in I_k}\alpha_{(i)}g_{i_1}\dots g_{i_r}$, $\overline{g_{i_1}\dots g_{i_r}}=w_k\ \ \forall(i)\in I_k$. Таким образом, имеем $w_1>w_2>\dots>w_L$ в $\langle X\rangle$. Моном w_1 назовем параметром этого соотношения.

Имеем

$$F(g_1,\dots,g_N)=\alpha_{(i_1)}g_{i_{11}}\dots g_{i_{1,r(1)}}+\alpha_{(i_2)}g_{i_{21}}\dots g_{i_{2,r(2)}}+\dots+\alpha_{(i_q)}g_{i_{q1}}\dots g_{i_{q,r(q)}}+\sum_{(i)\in I\setminus I_1}\alpha_{(i)}g_{i_1}\dots g_{i_r},$$
$$(i_1),\dots,(i_q)\in I_1,\quad |I_1|=q.$$

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

Предположим, что существуют нетривиальные полиномиальные соотношения, не лежащие в $\mathrm{Span}\{p-\varphi,\ s-\delta\}$ — линейной оболочке p-, s-соотношений. Выберем среди них соотношение с минимальным параметром w_1, а среди последних — соотношение с минимальным значением $q=|I_1|$. Рассмотрим возможные случаи.

1. Среди произведений

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

нет существенных. Из исходного соотношения вычтем соотношение $\alpha_{(i_1)}(p_1(G)-\varphi)=0$, где $p_1(G)-\varphi=0$ — p-соотношение, соответствующее несущественному произведению $p=p_1(G)$. Пусть

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

где $\overline{g_{j_{11}}\dots g_{j_{1,t(1)}}}=\overline{g_{j_{11}}}\dots\overline{g_{j_{1,t(1)}}}>\overline{g_{j_1}\dots g_{j_t}}=\overline{g_{j_1}}\dots\overline{g_{j_t}}\ \ \forall(j)\in J$. Тогда в результате получим соотношение

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

которое не лежит в $\mathrm{Span}\{s-\delta,\ p-\varphi\}$, параметр его равен w_1, число произведений, соответствующих w_1, равно q, но среди этих произведений имеется ровно одно существенное (см. случай 2).

2. Среди произведений $p_1(G),\dots,p_q(G)$ имеется ровно одно существенное произведение. Так как $q\geq 2$, то среди них имеется хотя бы одно несущественное произведение. Будем считать, что $p_1(G)$ — существенное произведение, тогда $p_2(G)$ не является существенным произведением. Вычтем из исходного соотношения соотношение $\alpha_{(i_2)}(p_2(G)-\varphi)=0$, где $p_2(G)-\varphi=0$ — p-соотношение, соответствующее несущественному произведению $p=p_2(G)$. Пусть φ имеет вид (3). Тогда в результате получим

а) соотношение

$$(\alpha_{(i_1)}+\alpha_{(i_2)}\beta_{(j_1)})g_{i_{11}}\dots g_{i_{1,r(1)}}+\alpha_{(i_3)}g_{i_{31}}\dots g_{i_{3,r(3)}}+\dots+$$
$$+\alpha_{(i_q)}g_{i_{q_1}}\dots g_{i_{q,r(q)}}+\sum_{(i)\in I\setminus I_1}\alpha_{(i)}g_{i_1}\dots g_{i_r}+\sum_{(j)\in J}\alpha_{(i_1)}\beta_{(j)}g_{j_1}\dots g_{j_t}=0,$$

если $g_{i_{11}}\dots g_{i_{1,r(1)}} = g_{j_{11}}\dots g_{j_{1,t(1)}}$ лексикографически в переменных $g_1,\dots,g_N$; полученное соотношение не лежит в $\mathrm{Span}\{p-\varphi,\ s-\delta\}$, имеет параметр, равный w_1, но число Q произведений, соответствующих параметру w_1, меньше q, а именно,

$$Q = \begin{cases} q-1, & \text{если } \ \alpha_{(i_1)} + \alpha_{(i_2)}\beta_{(j_1)} \neq 0; \\ q-2, & \text{иначе,} \end{cases}$$

что противоречит выбору исходного соотношения;

б) соотношение

$$\alpha_{(i_1)}g_{i_{11}}\dots g_{1,r(1)} + \alpha_{(i_2)}\beta_{(j_1)}g_{j_{11}}\dots g_{j_{1,t(1)}} + \alpha_{(i_3)}g_{i_{31}}\dots g_{i_{3,r(3)}} + \dots + \\ + \alpha_{(i_q)}g_{i_{q,1}}\dots g_{i_{q,r(q)}} + \sum_{(i)\in I\setminus I_1}\alpha_{(i)}g_{i_1}\dots g_{i_r} + \sum_{(j)\in J}\alpha_{(i_1)}\beta_{(j)}g_{j_1}\dots g_{j_t} = 0,$$

если $g_{i_{11}}\dots g_{i_{1,r(1)}} \neq g_{j_{11}}\dots g_{j_{1,t(1)}}$ лексикографически в переменных $g_1,\dots,g_N$; оно не лежит в $\mathrm{Span}\{p-\varphi,\ s-\delta\}$, его параметр равен w_1, число произведений, соответствующих w_1, равно q, но среди этих произведений ровно два существенных произведения (см. случай 3).

3. Среди произведений $p_1(G),\dots,p_q(G)$ имеется хотя бы два существенных произведения. Можем считать, что это $p_1(G)$, $p_2(G)$. Вычтем из исходного соотношения соотношение вида

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

где δ — H-представление s-элемента $s = p_1(G) - p_2(G)$. Тогда получим соотношение

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

которое не лежит в $\mathrm{Span}\{p-\varphi,\ s-\delta\}$, его параметр равен w_1, число Q произведений, соответствующих параметру w_1, меньше q, а именно,

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

что противоречит выбору исходного соотношения. □

Алгебраическая зависимость множества $G = \{g_1,\dots,g_N\}$, когда порождающие $g_1,\dots,g_N$ не являются свободными, означает существование полиномиального соотношения между порождающими $g_1,\dots,g_N$, что равносильно существованию некоторого несущественного произведения или s-элемента относительно G. Для данного конечного множества G можно алгоритмически проверить существование несущественного произведения.

Пусть d_μ — наибольшая из степеней мономов $\overline{f_1},\dots,\overline{f_M}$ в переменных X. Если имеет место равенство $\overline{g_{i_1}}\dots\overline{g_{i_r}} = u\overline{f_{j_1}}\dots\overline{f_{j_l}}v$ в $\langle X\rangle$ для некоторых $r \le d_\mu$, $g_{i_1},\dots,g_{i_r} \in G$, $u,v \in \langle X\rangle \bigcup 1$, $f_{j_1},\dots,f_{j_l} \in \phi$, то произведение $g_{i_1}\dots g_{i_r}$ не является существенным, следовательно, существует p-соотношение и множество G алгебраически зависимо. Если $\overline{g_{i_1}}\dots\overline{g_{i_r}} \neq u\overline{f_{j_1}}\dots\overline{f_{j_l}}v$ в $\langle X\rangle$ $\forall r \le d_\mu$, $\forall g_{i_1},\dots,g_{i_r} \in G$, $\forall u,v \in \langle X\rangle \bigcup 1$, $\forall f_{j_1},\dots,f_{j_l} \in \phi$, то все произведения вида $g_{i_1}\dots g_{i_t}$ для любого натурального t являются существенными и p-соотношений не существует.

Если существует p-соотношение, то делаем вывод о том, что множество $G = \{g_1,\dots,g_N\}$ алгебраически зависимо или подалгебра, им порожденная, не является свободной с данными порождающими.

Если p-соотношений не существует, приступаем к проверке существования s-элемента. В этом случае существование s-элемента $s = p_1(G) - p_2(G) = g_{i_1}\dots g_{i_r} - g_{j_1}\dots g_{j_t}$, где $p_1(\overline{G}) = \overline{g_{i_1}}\dots\overline{g_{i_r}} = \overline{g_{j_1}}\dots\overline{g_{j_t}} = p_2(\overline{G})$, означает алгебраическую зависимость мономиального множества

$\overline{G} = \{\overline{g_1}, \dots, \overline{g_N}\}$ в свободной ассоциативной алгебре $\mathcal{K}\langle X\rangle$. Алгоритмическая распознаваемость этого свойства изучалась в теории кодирования.

На интуитивном уровне код можно определить как такое множество слов, что любое произведение этих слов может быть "декодировано" только одним способом.

Определение 17 ([3]). *Языком C в алфавите X* называется множество слов, образованных из букв алфавита X.

Например, множество $\overline{G}$ есть конечный язык в алфавите X.

Определение 18 ([3]). Непустой язык C в алфавите X называется *кодом*, если для любых слов $c_{i_1}, \dots, c_{i_r}$, $c_{j_1}, \dots, c_{j_t}$ из C таких, что

$$c_{i_1} \dots c_{i_r} = c_{j_1} \dots c_{j_t}$$

лексикографически в алфавите X, имеет место $c_{i_1} = c_{j_1}$.

Если C является кодом, то, очевидно, $r = t$ и $c_{i_k} = c_{j_k}$ при $k = 1, \dots, r$.

Алгебраическая независимость множества $\overline{G} = \{\overline{g_1}, \dots, \overline{g_N}\}$ означает, что $\overline{G}$ есть код в алфавите X.

Теорема 4 ([3]). *Пусть C — непустой язык в алфавите X. Определим индуктивно языки $C_0, C_1, C_2, \dots$ над X, полагая $C_0 = C$,*

$$C_{i+1} = \{w \in \langle X\rangle \mid \exists x \in C,\ \exists y \in C_i \quad yw = x \quad \text{или} \quad xw = y\}.$$

Язык C является кодом тогда и только тогда, когда $C_i \bigcap C = \emptyset$ для каждого $i \geq 1$.

В случае конечного языка C длина каждого слова в каждом C_i не превосходит длину самого длинного слова в C. Следовательно, существует лишь конечное число различных языков C_i. Если на каком-то шаге получим $C_{i-1} = C_i$, то $C_i = C_{i+1}$. Действительно, пусть $w \in C_i$, тогда $\exists y \in C_{i-1}$, $\exists x \in C$ такие, что либо $yw = x$, но $y \in C_i$, следовательно, $w \in C_{i+1}$; либо $xw = y$, но $y \in C_i$, следовательно, $w \in C_{i+1}$. Обратно, пусть $w \in C_{i+1}$, тогда $(\exists y \in C_i)(\exists x \in C)$ такие, что либо $yw = x$, но $y \in C_{i-1}$, следовательно, $w \in C_i$; либо $xw = y$, но $y \in C_{i-1}$, следовательно, $w \in C_i$.

Действительно, теорема 4 обеспечивает эффективный метод, определяющий, является ли множество C кодом.

Таким образом, имеет место

Теорема 5. *Пусть подалгебра B с. к. о. алгебры $A = \mathcal{K}\langle X\rangle/I$ задана своим конечным $SAGBI$-базисом $G = \{g_1, \dots, g_N\}$. Тогда алгоритмически распознаваемо свойство "B — свободная подалгебра со свободными порождающими $g_1, \dots, g_N$".*

3. Распознавание конечномерности подалгебр

Пусть B, как и в § 2, — подалгебра с. к. о. алгебры A, заданная своим конечным $SAGBI$-базисом $G = \{g_1, \dots, g_N\}$. Рассмотрим вопрос об алгоритмической распознаваемости конечномерности подалгебры B.

$\mathcal{K}$-линейным базисом подалгебры B является множество $\mathcal{B} = \{p(G)\}$ всевозможных существенных произведений таких, что $p_1(\overline{G}) \neq p_2(\overline{G})$ в $\langle X\rangle$ при различных $p_1(G), p_2(G) \in \mathcal{B}$ в $\langle G\rangle$. Множество $\mathcal{B}$ линейно независимо. В самом деле, пусть $\sum\limits_{i=1}^{k} \lambda_i p_i(G) = 0$, $p_i(G) \in \mathcal{B}\ \ \forall i = 1, \dots, k$, $p_1(\overline{G}) < \dots < p_k(\overline{G})$ в $\langle X\rangle$. Тогда $\overline{\sum\limits_{i=1}^{k} \lambda_i p_i(G)} = p_k(\overline{G}) \not\equiv 0 \pmod{I}$. Поэтому $\lambda_k = 0$ и $\sum\limits_{i=1}^{k-1} \lambda_i p_i(G) = 0$. Аналогично $\lambda_{k-1} = \dots = \lambda_1 = 0$.

Всякий элемент $b \in B$ выражается в виде линейной комбинации элементов из $\mathcal{B}$. Действительно, b можно представить в виде

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

$\lambda_i \in \mathcal{K}$, $p_i(G)$ — существенное произведение для любого $i = 1, \dots, k$, $p_1(\overline{G}) \le \dots \le p_k(\overline{G})$ в $\langle X \rangle$.

Пусть k_0 наибольшее из $\{1, 2, \dots, k\}$ такое, что $p_{k_0}(G) \notin \mathcal{B}$. Тогда имеется существенное произведение $p(G) \in \mathcal{B}$: $p_{k_0}(\overline{G}) = p(\overline{G})$ в $\langle X \rangle$ и s-элемент $s = p_{k_0}(G) - p(G) = \sum\limits_{(i)} \gamma_{(i)} g_{i_1} \dots g_{i_r}$, $g_{i_1} \dots g_{i_r}$ — существенные произведения, $\overline{g_{i_1}} \dots \overline{g_{i_r}} < p_{k_0}(\overline{G})$. Подставим в (4) выражение

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

получим равенство вида (4), в котором значение, аналогичное $p_{k_0}(\overline{G})$, меньше либо равно $p_{k_0}(\overline{G})$, но число различных слагаемых со старшим членом $p_{k_0}(\overline{G})$, не принадлежащих базису $\mathcal{B}$, уменьшилось. Применив аналогичные рассуждения в силу d. c. c., получим выражение элемента $b \in B$ в виде линейной комбинации элементов из $\mathcal{B}$.

Множество всевозможных существенных произведений $p(G) = g_{i_1} \dots g_{i_r}$, где $g_{i_1}, \dots, g_{i_r} \in G$ обозначим следующим образом: $\mathcal{S} = \{p_{1,0}(G), p_{1,1}(G), \dots, p_{1,t(1)}(G), p_{2,0}(G), p_{2,1}(G), \dots, p_{2,t(2)}(G), \dots, p_{R,0}(G), p_{R,1}(G), \dots, p_{R,t(R)}(G), \dots\}$. Пусть $\mathcal{B} = \{p_{i,0}(G)\}$ — $\mathcal{K}$-линейный базис подалгебры B; $p_{1,0}(\overline{G}) < \dots < p_{R,0}(\overline{G}) < \dots$ в $\langle X \rangle$; $\mathcal{S}(i) = \{p_{i,j}(G)\}_{j=0}^{t(i)}$ — множество всевозможных различных существенных произведений таких, что $p_{i,j}(\overline{G}) = p_{i,j'}(\overline{G})$ $\forall j, j' = 0, 1, \dots, t(i)$. Для фиксированного i мономы $p_{i,j}(G)$, $j = 0, 1, \dots, t(i)$, попарно различны в $\langle G \rangle$, но их старшие члены совпадают в алфавите X. Для некоторых i возможно $t(i) = 0$, но для любого i верно $t(i) < \infty$.

Символом d_μ, как и в § 2, обозначим максимальную степень мономов из множества μ в переменных X. Построим вспомогательную мономиальную алгебру $D = \mathcal{K}\langle y_1, \dots, y_N \rangle / (\eta)$, где η — конечное мономиальное множество от переменных y_i. Считаем, что моном $v = y_{j_1} \dots y_{j_l} \in \eta$, $l \le d_\mu$, в том и только том случае, когда $g_{j_1} \dots g_{j_l}$ не является существенным произведением. Тогда $\mathcal{K}$-линейным базисом алгебры D являются мономы вида $y_{j_1} \dots y_{j_l}$ такие, что $g_{j_1} \dots g_{j_l}$ — существенное произведение.

В случае, когда B – свободная алгебра, выполнено равенство $\dim B = \dim D$; в этом случае $t(i) = 0$ для любого натурального i. Если B не является свободной подалгеброй, то $\dim B \ne \dim D$ или $t(i) > 0$ для некоторого i. Так как $t(i) < \infty$ для любого i, то верна

Теорема 6. *Подалгебра B конечномерна тогда и только тогда, когда D — конечномерная мономиальная алгебра.*

Конечномерность алгебры D алгоритмически проверяется [8]. Таким образом, имеет место

Теорема 7. *Существует алгоритм распознавания конечномерности алгебры B.*

Литература

1. Умирбаев У.У. *Некоторые алгоритмические вопросы ассоциативных алгебр*// Алгебра и логика. – 1993. – Т. 32. – № 4. – С. 450–470.
2. Sardinas A., Patterson G. *A nesserary and sufficient condition for the unique decomposition of coded messages* // IRE Intern. conf. record. – 1958. – V. 8. – P. 104–108.
3. Саломаа А. *Жемчужины теории формальных языков.* – М.: Мир, 1986. – 159 с.
4. Robbiano L., Sweedler M. *Subalgebra bases* // Comm. algebra. Proc. of the workshop held at the Federal Univ. of Bahia, Salvador, 1988. – Lect. notes Math. – 1990. – V. 1430. – P. 61–87.
5. Kapur D., Madlener K. *A completion procedure for computing a canonical basis for a K-subalgebra* // Computers and Mathematics, Cambridge, MA. – Springer, New York–Berlin: 1989. – P. 1–11.

6. Иыуду Н. К. *Стандартный базис и проблема вхождения в подалгебры свободной ассоциативной алгебры* // Международн. алг. семин., посв. 70-летию каф. высш. алг. – Москва, февраль 1999: Тез. докл. – Москва, 1999. – С. 29–31.
7. Latyshev V. N. *An improved version of standard bases* // Proc. of the 12th intern. conf. FPSAC'00, Moscow, June 26–30, 2000. – P. 496–506.
8. Gateva-Ivanova T., Latyshev V. N. *On the recognizable properties of assosiative algebras* // Special vol. of J. S. C.: On comp. aspects comm. algebras. – London: Acad. Press. – 1988. – P. 237–254.

Ульяновский государственный университет

Поступили
первый вариант 01.02.2001
окончательный вариант 16.04.2002