Math-Net.Ru

Общероссийский математический портал

М. Плукас, О некоторых свойствах алгебр с простым умножением, содержащих ассоциативные подалгебры, *Дискрет. матем.*, 1997, том 9, выпуск 2, 79–90

DOI: <https://doi.org/10.4213/dm475>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.90.164.192

26 апреля 2023 г., 10:57:24

О некоторых свойствах алгебр с простым умножением, содержащих ассоциативные подалгебры

© 1997 г. М. Плукас

Установлены некоторые свойства алгебр с простым умножением, содержащих ассоциативную и в некотором смысле невырожденную подалгебру. Получены нижние оценки размерности алгебр с простым умножением.

1. Введение

В [1] был введен класс алгебр с простым умножением. Этот класс связан с оптимальными по сложности билинейными алгоритмами умножения в некоторых известных алгебрах. Дадим несколько определений.

Линейная алгебра над полем P представляет собой линейное пространство над полем P , в котором введена операция умножения векторов xu . Операция умножения векторов дистрибутивна относительно сложения векторов и перестановочна с операцией умножения вектора на число из поля.

Далее поле будем считать фиксированным и говорить просто об алгебре.

Пусть в n -мерной алгебре A существуют базис $e_1, \dots, e_n$ и подстановка π на множестве $\{1, \dots, n\}$ такие, что

$$\begin{aligned} e_i e_{\pi(i)} &\neq 0, & i &= 1, \dots, n, \\ e_i e_j &= 0, & j &\neq \pi(i). \end{aligned}$$

Тогда алгебру A будем называть алгеброй с простым умножением (n, π) (в базисе $e_1, \dots, e_n$). В частности, если π — тождественная подстановка e , то будем говорить, что алгебра A является алгеброй с простым умножением (n, e) .

Если алгебра B изоморфна некоторой подалгебре алгебры A , то будем говорить, что алгебра B вкладывается в алгебру A .

Нетрудно видеть, что, если некоторая алгебра B вкладывается в алгебру A размерности n с простым умножением, то существует билинейный алгоритм с мультипликативной сложностью n для умножения векторов алгебры B . Следовательно, билинейная сложность внутренней алгебры не превышает размерности внешней алгебры. С другой стороны, ряд известных алгебр (комплексные числа как двумерная алгебра над вещественным полем, алгебра кватернионов, алгебра 2×2 матриц)

вкладываются в алгебры с простым умножением, размерность которых равна билинейной сложности вкладываемых алгебр, то есть, билинейные алгоритмы, получаемые из вложения в алгебру с простым умножением, в этих случаях оказываются оптимальными. Таким образом, класс билинейных алгоритмов, получаемых из вложения в алгебры с простым умножением, представляет интерес с точки зрения исследований билинейной сложности линейных алгебр. Задача нахождения билинейного алгоритма из этого класса с малой мультипликативной сложностью для умножения векторов какой-либо алгебры является задачей нахождения алгебры с простым умножением малой размерности, содержащей интересующую нас алгебру (см. [1, 2]).

В данной работе устанавливаются некоторые свойства алгебры с простым умножением, содержащей ассоциативную и в некотором смысле невырожденную алгебру, и получаются нижние оценки размерности алгебр с простым умножением.

2. Формулировка и доказательство результатов

Нам потребуется еще несколько определений.

Будем говорить, что алгебра A распадается на прямую сумму подалгебр $A_1, \dots, A_s$ и писать $A = A_1 \oplus \dots \oplus A_s$, если A как линейное пространство является прямой суммой $A_1, \dots, A_s$ как линейных пространств и

$$\forall i, j (i \neq j): \forall a \in A_i, \forall b \in A_j: ab = ba = 0.$$

Через $L(S)$ будем обозначать линейную оболочку множества векторов S .

Квадратом алгебры A будем называть $A^2 = L(\{ab \mid a, b \in A\})$.

Будем говорить, что алгебра B удовлетворяет условию $\mathcal{A}$, если

- умножение в B ассоциативно;
- алгебра B не сжимается, т.е. $B^2 = B$;
- алгебра B не имеет аннуляторов, т.е.

$$\forall a \in B (a \neq 0): \exists b_1, b_2 \in B: b_1 a \neq 0, a b_2 \neq 0.$$

Предложение 1. Пусть d -мерная алгебра B вкладывается в n -мерную алгебру A с простым умножением (n, π) (в базисе $e_1, \dots, e_n$).

Тогда алгебра B вкладывается в n -мерную алгебру $\bar{A}$ с простым умножением (n, π) , при этом квадрат $\bar{A}$ содержится в изоморфном образе алгебры B .

Доказательство. Пусть алгебра B изоморфна подалгебре B_A алгебры A . Пусть $\mathcal{F}: B \rightarrow B_A$ — линейный оператор, задающий изоморфизм, а $\mathcal{G}: A \rightarrow B$ — линейный оператор такой, что $\mathcal{F}(\mathcal{G}(a)) = a$ для всех $a \in B_A$.

Пусть для произвольных $a, b \in B$

$$\mathcal{F}(a) = \sum_{i=1}^n \alpha_i e_i, \quad \mathcal{F}(b) = \sum_{i=1}^n \beta_i e_i.$$

Тогда

$$\begin{aligned}\mathcal{F}(a)\mathcal{F}(b) &= \mathcal{F}(\mathcal{G}(\mathcal{F}(a)\mathcal{F}(b))) \\ &= \mathcal{F}\left(\mathcal{G}\left(\sum_{i=1}^n \alpha_i \beta_i (e_i e_{\pi(i)})\right)\right) = \sum_{i=1}^n \alpha_i \beta_i \mathcal{F}(\mathcal{G}(e_i e_{\pi(i)})).\end{aligned}$$

Значит, $\mathcal{F}(a)\mathcal{F}(b)$ не изменится и, следовательно, изоморфизм $B \cong B_A$, задаваемый оператором $\mathcal{F}$, сохранится, если в алгебре A переопределить умножение (то есть перейти к алгебре $\bar{A}$), положив $e_i e_{\pi(i)}$ равным $\mathcal{F}(\mathcal{G}(e_i e_{\pi(i)}))$, $i = 1, \dots, n$.

Теперь $(e_i e_{\pi(i)}) \in B_A$, $i = 1, \dots, n$. Следовательно, $\bar{A}^2 \subseteq B_A$. Предложение 1 доказано.

Лемма 1. Пусть $S = \{v_i\}_{i \in I}$ — совокупность (возможно с повторениями) векторов m -мерного линейного пространства и

$$\begin{aligned}K &= \{i \in I \mid \exists j \in I: v_i \notin L(\{v_k\}_{k \in I \setminus \{i,j\}})\}, \\ K_1 &= \{i \in I \mid v_i \notin L(\{v_k\}_{k \in I \setminus \{i\}})\}.\end{aligned}$$

Тогда $|K| \leq 2m - |K_1|$.

Доказательство. Ясно, что $K_1 \subseteq K$. Положим

$$K_2 = K \setminus K_1 = \{i \in K \mid v_i \in L(\{v_k\}_{k \in I \setminus \{i\}})\}.$$

На множестве K_2 рассмотрим бинарное отношение $\mathcal{R}$, определяемое соотношением

$$i\mathcal{R}j \iff i = j \text{ или } v_i \notin L(\{v_k\}_{k \in I \setminus \{i,j\}}).$$

Ясно, что отношение $\mathcal{R}$ является рефлексивным.

Отношение $\mathcal{R}$ является симметричным. Действительно, пусть $i\mathcal{R}j$ и не справедливо $j\mathcal{R}i$. Тогда $i \neq j$ и $v_i \notin L(\{v_k\}_{k \in I \setminus \{i,j\}})$. Из несправедливости $j\mathcal{R}i$ следует, что

$$v_j = \sum_{z \neq i,j} \alpha_z v_z.$$

Но

$$v_i = \sum_{z \neq i} \beta_z v_z$$

и, следовательно,

$$v_i = \sum_{z \neq i,j} \gamma_z v_z.$$

Получили противоречие.

Отношение $\mathcal{R}$ является транзитивным. Действительно, пусть $i\mathcal{R}j$, $j\mathcal{R}l$ и не справедливо $i\mathcal{R}l$. Тогда

$$i \neq j, \quad j \neq l, \quad i \neq l, \quad v_i \notin L(\{v_k\}_{k \in I \setminus \{i,j\}}), \quad v_j \notin L(\{v_k\}_{k \in I \setminus \{j,l\}}).$$

Из того, что не выполняется соотношение $i\mathcal{R}l$, следует, что

$$v_i = \sum_{z \neq i, l} \alpha_z v_z = \alpha_j v_j + \sum_{z \neq i, l, j} \alpha_z v_z,$$

откуда, учитывая, что $\alpha_j \neq 0$, находим, что

$$v_j = \sum_{z \neq j, l} \beta_z v_z.$$

Получили противоречие.

Итак, отношение $\mathcal{R}$ — это отношение эквивалентности на множестве K_2 и оно разбивает K_2 на классы эквивалентности.

Для любого $i \in K_2$ существует $j \in I$ такое, что $v_i \notin L(\{v_k\}_{k \in I \setminus \{i, j\}})$ и $j \neq i$, так как $v_i \in L(\{v_k\}_{k \in I \setminus \{i\}})$.

Из соотношений

$$v_i \notin L(\{v_k\}_{k \in I \setminus \{i, j\}}), \quad v_i \in L(\{v_k\}_{k \in I \setminus \{i\}})$$

следует, что

$$v_j \notin L(\{v_k\}_{k \in I \setminus \{i, j\}}),$$

откуда $j \in K$ и

$$v_i = \alpha_j v_j + \sum_{z \neq i, j} \alpha_z v_z.$$

Учитывая теперь, что $\alpha_j \neq 0$, находим, что

$$v_j = \sum_{z \neq j} \beta_z v_z,$$

откуда, в силу того, что $j \in K$, получаем, что $j \in K_2$.

Таким образом, для любого $i \in K_2$ существует $j \in K_2$ такое, что $j \neq i$ и $i\mathcal{R}j$. Значит, классы эквивалентности имеют мощность, не меньшую двух. Число классов эквивалентности мощности s обозначим через k_s .

Как следует из определения отношения $\mathcal{R}$, для любого $i \in K_2$, если

$$v_i = \sum_{z \neq i} \alpha_z v_z,$$

то $\alpha_z \neq 0$ для всех $z \in \mathcal{E} \setminus \{i\}$, где $\mathcal{E}$ — класс эквивалентности, содержащий i . Значит, любое минимальное подмножество V векторов из S такое, что через векторы V линейно выражается любой вектор из S , должно содержать не менее $|\mathcal{E}| - 1$ векторов из $\{v_i\}_{i \in \mathcal{E}}$ для каждого класса эквивалентности $\mathcal{E}$, а также все векторы $\{v_i\}_{i \in K_1}$ (так как $v_i \notin L(\{v_k\}_{k \in I \setminus \{i\}})$ для любого $i \in K_1$). Таким образом,

$$\sum_{s \geq 2} k_s(s-1) + |K_1| \leq |V| \leq m.$$

Отсюда

$$\begin{aligned}\sum_{s \geq 2} k_s &\leq m - |K_1|, \\ |K| &= \sum_{s \geq 2} s k_s + |K_1| \\ &= \sum_{s \geq 2} k_s (s - 1) + |K_1| + \sum_{s \geq 2} k_s \leq 2m - |K_1|.\end{aligned}$$

Лемма 1 доказана.

Предложение 2. Пусть B — d -мерная алгебра, удовлетворяющая условию $\mathcal{A}$, и пусть B вкладывается в n -мерную алгебру A с простым умножением (n, π) (в базисе $e_1, \dots, e_n$). Пусть $p = n - d$.

Тогда существует $d' \leq 8p$ такое, что общая длина циклов длины, большей единицы, подстановки π не превосходит $d' + p \leq 9p$, и алгебра B распадается на прямую сумму $d - d'$ одномерных и одной d' -мерной подалгебр; последняя подалгебра вкладывается в n' -мерную, $n' = d' + p$, алгебру с простым умножением (n', π') , где цикловая структура подстановки π' получается из цикловой структуры подстановки π удалением $d - d'$ циклов длины единица.

Доказательство. Обозначим

$$a_i = e_i e_{\pi(i)}, \quad i = 1, \dots, n.$$

Алгебру B и ей изоморфную подалгебру алгебры A можем не различать и далее считаем, что B — подалгебра A .

В алгебре B можно выбрать базис $\{f_i\}_{i \in I}$ такой, что

$$f_i = e_i + \sum_{j \in E} b_{ij} e_j, \quad i \in I,$$

где

$$\begin{aligned}I &\subseteq \{1, \dots, n\}, & |I| &= d, \\ E &= \{1, \dots, n\} \setminus I, & |E| &= p.\end{aligned}$$

Пусть

$$g \in A, \quad g = \sum_{r=1}^n \alpha_r e_r.$$

Будем обозначать

$$\varphi(g) = \sum_{r \in E} \alpha_r e_r, \quad c_r(g) = \alpha_r, \quad r = 1, \dots, n.$$

Пусть $f \in B$ и

$$f = \sum_{i \in I} \beta_i f_i.$$

Тогда будем писать $f_i \in f$, если $\beta_i \neq 0$, и $f_i \notin f$, если $\beta_i = 0$. Положим

$$\begin{aligned} I'_1 &= \{i \in I \mid \pi^{-1}(i) \in E\}, \\ I''_1 &= \{i \in I \mid \pi(i) \in E\}, \\ I_1 &= I'_1 \cup I''_1. \end{aligned}$$

Ясно, что $|I_1| \leq 2p$, так как $|E| = p$. Пусть $I_2 = I \setminus I_1$. Отметим, что $\pi^{-1}(i), \pi(i) \in I$ для любого $i \in I_2$. Пусть также

$$\begin{aligned} I_3 &= \{i \in I_2 \mid \exists j \in I_2: \varphi(f_i) \notin L(\{\varphi(f_k) \mid k \in I_2 \setminus \{i, j\}\})\}, \\ I_{30} &= \{i \in I_2 \mid \varphi(f_i) \notin L(\{\varphi(f_k) \mid k \in I_2 \setminus \{i\}\})\}, \quad I_{30} \subseteq I_3. \end{aligned}$$

По Лемме 1

$$|I_3| \leq 2|E| - |I_{30}| = 2p - |I_{30}|.$$

Положим $I_4 = I_2 \setminus I_3$. Фиксируем $i \in I_4$ и возьмем произвольное $j \in I \setminus \{\pi^{-1}(i)\}$. Тогда для $i \in I_4$ существует α_r такое, что

$$\varphi(f_i) = \sum_{\substack{r \in I_2 \\ r \neq i, \pi(j)}} \alpha_r \varphi(f_r).$$

Рассмотрим вектор $g^{ij} \in B$ такой, что

$$g^{ij} = f_i - \sum_{\substack{r \in I_2 \\ r \neq i, \pi(j)}} \alpha_r f_r.$$

Для этого вектора из равенства $\varphi(g^{ij}) = 0$ следует, что $c_k(g^{ij}) = 0$ для всех $k \in E$, $c_{\pi(j)}(g^{ij}) = 0$, так как, если $\pi(j) \notin E$, то $f_{\pi(j)} \notin g^{ij}$. Из того, что $f_k \notin g^{ij}$ для всех $k \in I_1$, следует, что $c_k(g^{ij}) = 0$ для всех $k \in I_1$, и наконец, $c_i(g^{ij}) = 1$.

Следовательно,

$$f_j g^{ij} = c_{\pi(j)}(g^{ij}) a_j + \sum_{r \in E} c_r(f_j) c_{\pi(r)}(g^{ij}) a_r = 0,$$

поскольку $c_{\pi(j)}(g^{ij}) = 0$ и $c_{\pi(r)}(g^{ij}) = 0$ для всех $r \in E$, так как $\pi(E) \subseteq E \cup I'_1$, и

$$g^{ij} f_{\pi(i)} = c_i(g^{ij}) a_i + \sum_{r \in \pi^{-1}(E)} c_r(g^{ij}) c_{\pi(r)}(f_{\pi(i)}) a_r = a_i,$$

поскольку $c_i(g^{ij}) = 1$ и $c_r(g^{ij}) = 0$ для всех $r \in \pi^{-1}(E)$, так как $\pi^{-1}(E) \subseteq E \cup I''_1$.

Отсюда, в частности, следует, что $a_i \in B$.

Далее, в силу ассоциативности B

$$f_j a_i = f_j(g^{ij} f_{\pi(i)}) = (f_j g^{ij}) f_{\pi(i)} = 0.$$

Итак, для всех $i \in I_4$ и $j \in I$, $j \neq \pi^{-1}(i)$

$$f_j a_i = 0. \quad (1)$$

Так как $a_i \neq 0$ и B не имеет аннуляторов,

$$f_{\pi^{-1}(i)}a_i \neq 0. \quad (2)$$

Покажем, что для всех $k, l \in I$, $l \neq \pi^{-1}(i)$

$$f_{\pi^{-1}(i)} \notin (f_k f_l). \quad (3)$$

Действительно, пусть

$$f_k f_l = \alpha f_{\pi^{-1}(i)} + \sum_{\substack{r \in I \\ r \neq \pi^{-1}(i)}} \alpha_r f_r.$$

Тогда в силу (1)

$$0 = f_k(f_l a_i) = (f_k f_l)a_i = \alpha(f_{\pi^{-1}(i)}a_i)$$

откуда в силу (2) следует, что $\alpha = 0$.

Аналогично получаем, что для любого $i \in I_4$

$$a_{\pi^{-1}(i)}f_j = 0, \quad j \in I, \quad j \neq \pi(i), \quad (4)$$

$$a_{\pi^{-1}(i)}f_{\pi(i)} \neq 0, \quad (5)$$

$$f_{\pi(i)} \notin (f_k f_l), \quad k, l \in I, \quad k \neq \pi(i). \quad (6)$$

Рассмотрим множества индексов

$$I_5 = \{i \in I_2 \mid \pi^{-1}(i), \pi(i) \in I_1 \cup I_3\},$$

$$I_6 = I_2 \setminus (I_5 \cup I_{30}) = \{i \in I_2 \setminus I_{30} \mid \pi^{-1}(i), \pi(i) \in I_4\}.$$

Ясно, что $|I_5| \leq |I_1| + 2|I_3| \leq 6p - 2|I_{30}|$.

Отметим, что для любого $i \in I_6$ из того, что $i \in I_2 \setminus I_{30}$, следует, что существует такой набор коэффициентов $\{\alpha_r\}$, что

$$\varphi(f_i) = \sum_{\substack{r \in I_2 \\ r \neq i}} \alpha_r \varphi(f_r),$$

и из того, что $\pi(i) \in I_4$, следует, что существует такой набор коэффициентов $\{\beta_r\}$, что

$$\varphi(f_{\pi(i)}) = \sum_{\substack{r \in I_2 \\ r \neq i, \pi(i)}} \beta_r \varphi(f_r).$$

Следовательно, существует такой набор коэффициентов $\{\gamma_r\}$, что

$$\varphi(f_i) = \sum_{\substack{r \in I_2 \\ r \neq i, \pi(i)}} \gamma_r \varphi(f_r).$$

Для любого $j \in I_6$ из (3),(6) (в качестве i берем $\pi(j)$ и $\pi^{-1}(j)$, соответственно) следует, что $f_j \notin (f_k f_l)$ для всех $k, l \in I$ таких, что $k \neq j$ или $l \neq j$. Алгебра B не сжимается, значит, $f_j \in (f_j f_j)$ для любого $j \in I_6$.

Покажем, что $\pi(i) = i$ для любого $i \in I_6$ (отсюда, в частности, будет следовать, что $I_6 \subseteq I_4$). Пусть это не так, то есть существует $j \in I_6$ такое, что $\pi(j) \neq j$. Тогда существует набор коэффициентов $\{\alpha_r\}$ такой, что

$$\varphi(f_j) = \sum_{\substack{r \in I_2 \\ r \neq j, \pi(j)}} \alpha_r \varphi(f_r),$$

и в силу того, что $\pi(j) \neq j$ и $j \notin I_1$

$$f_j \in (f_j f_j) = f_j \varphi(f_j) = \sum_{\substack{r \in I_2 \\ r \neq j, \pi(j)}} \alpha_r (f_r \varphi(f_r)) = \sum_{\substack{r \in I_2 \\ r \neq j, \pi(j)}} \alpha_r (f_j f_r).$$

Получаем противоречие, так как

$$f_j \notin \sum_{\substack{r \in I_2 \\ r \neq j, \pi(j)}} \alpha_r (f_j f_r).$$

Итак,

$$I = I' \cup I'', \quad I' \cap I'' = \emptyset,$$

где $I' = I \setminus I_6 = I_1 \cup I_5 \cup I_{30}$, $|I'| \leq 8p$, $I'' = I_6$, $I'' \subseteq I_4$ и $\pi(i) = i$ для всех $i \in I$.

Фиксируем $i \in I''$. Как уже было показано,

$$f_i \in f_i f_i, \quad (7)$$

$$f_i \notin f_k f_l \quad (8)$$

для всех $k, l \in I$ таких, что $k \neq i$ или $l \neq i$.

Далее, из (1), (4), (2), (5) следует, что

$$f_j a_i = 0, \quad a_i f_j = 0, \quad j \in I, \quad j \neq i, \quad (9)$$

$$f_i a_i \neq 0, \quad a_i f_i \neq 0, \quad (10)$$

при этом $a_i \in B$.

Покажем, что $f_i \in a_i$. Действительно, в силу того, что $i \notin I_1$,

$$f_i f_i = a_i + f_i \varphi(f_i) = a_i + \sum_{\substack{r \in I_2 \\ r \neq i, \pi(i)}} \alpha_r (f_i \varphi(f_r)) = a_i + \sum_{\substack{r \in I_2 \\ r \neq i, \pi(i)}} \alpha_r (f_i f_r),$$

и в силу (7) и (8) справедливо включение $f_i \in a_i$.

Пусть

$$a_i = \sum_{r \in I} \beta_r f_r,$$

где $\beta_i \neq 0$. Тогда

$$a_i a_i = \beta_i \beta_i (f_i f_i) + \sum_{\substack{k, l \in I \\ (k, l) \neq (i, i)}} \beta_k \beta_l (f_k f_l)$$

и в силу (7) и (8) отсюда следует, что $f_i \in a_i a_i$. Далее,

$$a_i a_i = \gamma f_i + \sum_{\substack{r \in I \\ r \neq i}} \gamma_r f_r = \delta a_i + \sum_{\substack{r \in I \\ r \neq i}} \delta_r f_r,$$

где $\delta \neq 0$, и в силу (9)

$$(a_i a_i) a_i = \delta(a_i a_i) + \sum_{\substack{r \in I \\ r \neq i}} \delta_r (f_r a_i) = \delta(a_i a_i).$$

Положим $g_i = a_i a_i$. В этих обозначениях

$$f_i \in g_i, \quad (11)$$

$$g_i g_i = (a_i a_i)(a_i a_i) = ((a_i a_i) a_i) a_i = \delta^2(a_i a_i) = \delta^2 g_i, \quad (12)$$

$$f_j g_i = 0, \quad g_i f_j = 0, \quad j \in I, \quad j \neq i. \quad (13)$$

Покажем, что

$$f_j \notin g_i, \quad j \in I'', \quad j \neq i. \quad (14)$$

Действительно, если

$$g_i = \sum_{r \in I} \alpha_r f_r,$$

где $\alpha_j \neq 0$, то из равенства

$$g_i f_j = \alpha_j (f_j f_j) + \sum_{\substack{r \in I \\ r \neq j}} \alpha_r (f_r f_j)$$

в силу (7) и (8) следует, что $f_j \in g_i f_j$ и $g_i f_j \neq 0$, что противоречит (13).

Из (13) и (14) следует, что

$$g_i g_j = 0, \quad i, j \in I'', \quad i \neq j. \quad (15)$$

Далее, из (11) и (14) получаем, что векторы $\{g_i\}_{i \in I''} \cup \{f_i\}_{i \in I'}$ линейно независимы.

Итак, учитывая (12), (13), (15) и (8), получаем, что в алгебре B существует базис $\{h_i\}_{i \in I}$:

$$h_i = \begin{cases} (1/\delta^2)g_i, & \text{если } i \in I'', \\ f_i, & \text{если } i \in I', \end{cases}$$

для которого

$$\begin{aligned} h_i h_i &= h_i, & i &\in I'', \\ h_i h_j &= 0, \quad h_j h_i = 0, & i &\in I'', \quad j \in I, \quad j \neq i, \\ h_i h_j &\in L(\{h_k\}_{k \in I'}), & i, j &\in I'. \end{aligned} \quad (16)$$

Следовательно, алгебра B распадается на прямую сумму d' -мерной, $d' = |I'| \leq 8p$, подалгебры $C = L(\{h_i\}_{i \in I'})$ и $d - d'$ одномерных подалгебр $L(\{h_i\})$, $i \in I''$.

Как следует из определения I' и I'' , общая длина циклов длины, большей единицы, в подстановке π не превышает $|I'| + |E| = d' + p \leq 9p$.

Рассмотрим n' -мерную, $n' = d' + p$, алгебру D со следующей таблицей умножения в базисе $\{v_i\}_{i \in K}$:

$$\begin{aligned} v_i v_{\pi(i)} &= \sum_{j \in K} a_{ij} v_j, \quad i \in K, \\ v_i v_j &= 0, \quad i, j \in K, \quad j \neq \pi(i), \end{aligned}$$

где

$$K = \{1, \dots, n\} \setminus I'' = I' \cup E, \quad |K| = n',$$

а a_{ij} такие числа, что

$$e_i e_{\pi(i)} = a_i = \sum_{j=1}^n a_{ij} e_j, \quad i = 1, \dots, n.$$

Тогда, в силу (16), алгебра C вкладывается в алгебру D при помощи отображения

$$h_i = f_i = e_i + \sum_{j \in E} b_{ij} e_j \rightarrow v_i + \sum_{j \in E} b_{ij} v_j, \quad i \in I'.$$

Осталось заметить, что алгебра D имеет простое умножение (n', π') , где π' — подстановка, соответствующая π на множестве K .

Предложение 2 доказано.

Непосредственным следствием предложений 2 и 1 является следующее утверждение.

Следствие 1. Пусть выполнены условия предложения 2.

Тогда алгебра B вкладывается в n -мерную алгебру $\bar{A}$ с простым умножением (n, σ) (в базисе $e_1, \dots, e_n$), где цикловая структура σ совпадает с цикловой структурой π , квадрат $\bar{A}$ содержится в изоморфном образе B , а таблица умножения алгебры $\bar{A}$ имеет вид

$$\begin{aligned} \sigma(i) &= i, \quad i = n' + 1, \dots, n, \quad n' \leq 9p, \\ e_i e_{\sigma(i)} &\in L(\{e_k\}_{k=1, \dots, n'}), \quad i = 1, \dots, n', \\ e_i e_i &= e_i, \quad i = n' + 1, \dots, n. \end{aligned}$$

Следствие 2. Пусть выполнены условия предложения 2 и по крайней мере одно из условий:

- подстановка π не имеет циклов длины единица,
- алгебра B не представляется в виде прямой суммы подалгебр, одна из которых одномерная.

Тогда $n \geq (9/8)d$.

Доказательство. Если выполняется первое условие, то из предложения 2 следует, что $n \leq 9p$; если выполняется второе условие, то $d \leq 8p$, где $p = n - d$. В любом случае получаем, что $n \geq (9/8)d$. Следствие 2 доказано.

Предложение 3. Пусть B — d -мерная алгебра, удовлетворяющая условию $\mathcal{A}$, и пусть B вкладывается в n -мерную алгебру A с простым умножением (n, e) (в базисе $e_1, \dots, e_n$). Пусть $p = n - d$.

Тогда алгебра B распадается на прямую сумму $d - d'$ одномерных и одной d' -мерной подалгебр, где $d' \leq 2p$; последняя подалгебра вкладывается в n' -мерную, $n' = d' + p$, алгебру с простым умножением (n', e) .

Доказательство. Доказательство проводится аналогично доказательству предложения 2, только теперь $I_1 = \emptyset$, $I_5 = I_3$ и, следовательно, $I' = I_3$, $|I'| \leq 2p$, $d' = |I'| \leq 2p$.

Следствие 3. Пусть выполнены условия предложения 3.

Тогда алгебра B вкладывается в n -мерную алгебру $\bar{A}$ с простым умножением (n, e) (в базисе $e_1, \dots, e_n$), где квадрат $\bar{A}$ содержится в изоморфном образе B , а таблица умножения алгебры $\bar{A}$ имеет вид

$$\begin{aligned} e_i e_i &\in L(\{e_k\}_{k=1, \dots, n'}), \quad i = 1, \dots, n', \quad n' \leq 3p, \\ e_i e_i &= e_i, \quad i = n' + 1, \dots, n. \end{aligned}$$

Следствие 4. Пусть выполнены условия предложения 3 и алгебра B не представляется в виде прямой суммы подалгебр, одна из которых одномерная.

Тогда $n \geq (3/2)d$.

Предложение 4. Оценка $d' \leq 2p$ предложения 3 достигается для любого p .

Доказательство. Для любого $t = 1, 2, \dots$ рассмотрим $2t$ -мерную алгебру

$$B_t = U_1 \oplus \dots \oplus U_t,$$

где U_j — алгебра комплексных чисел над полем вещественных чисел.

Рассмотрим $3t$ -мерную алгебру V_j с простым умножением в базисе e_1, e_2, e_3 :

$$\begin{aligned} e_1 e_1 &= e_1 - e_2, \\ e_2 e_2 &= -e_1 - e_2 - 2e_3, \\ e_3 e_3 &= e_2 + e_3. \end{aligned}$$

Тогда U_j вкладывается в V_j при помощи отображения

$$a + bi \rightarrow ae_1 + be_2 + (a + b)e_3,$$

где $1, i$ — стандартный базис U_j . Значит, алгебра B_t вкладывается в $3t$ -мерную алгебру $A_t = V_1 \oplus \dots \oplus V_t$, которая имеет простое умножение $(3t, e)$.

Алгебра B_t не распадается на прямую сумму подалгебр, одна из которых одномерна, так как в алгебре B_t не существует базиса $q_1, q_2, \dots, q_{2t}$, для которого $q_1 q_k = 0$ для всех $k = 2, 3, \dots, 2t$. Действительно, пусть такой базис существует. Пусть (v_j, w_j) — базис алгебры U_j , $j = 1, \dots, t$. Не ограничивая общности, можем считать, что

$$q_1 = \sum_{j=1}^t (\alpha_j v_j + \beta_j w_j),$$

где $\alpha_1 \neq 0$. Существует $k \geq 2$ такое, что

$$q_k = \sum_{j=1}^t (\gamma_j v_j + \delta_j w_j),$$

где $\gamma_1 \neq 0$ или $\delta_1 \neq 0$. Тогда $q_1 q_k = b' + b''$, где

$$\begin{aligned} b' &\in U_2 \oplus \dots \oplus U_t, \\ b'' &\in U_1, \quad b'' = (\alpha_1 v_1 + \beta_1 w_1)(\gamma_1 v_1 + \delta_1 w_1) \neq 0, \end{aligned}$$

так как

$$U_1 \ni (\alpha_1 v_1 + \beta_1 w_1) \neq 0, \quad U_1 \ni (\gamma_1 v_1 + \delta_1 w_1) \neq 0.$$

Значит, $q_1 q_k \neq 0$, и мы получаем противоречие.

Из подобных же соображений следует, что алгебра B_t не имеет аннуляторов. Также легко видеть, что B_t не сжимается, а умножение векторов в алгебре B_t ассоциативно.

Таким образом, алгебра B_t удовлетворяет условиям предложения 3 и для нее в обозначениях предложения 3

$$d = 2t, \quad n = 3t, \quad p = n - d = t, \quad d' = d = 2p.$$

Предложение 4 доказано.

Отметим, что в силу следствия 4 алгебра, являющаяся прямой суммой t алгебр комплексных чисел, не может быть вложена в алгебру размерности, меньшей $3t$ с простым умножением вида (n, e) .

В заключение я хотел бы выразить благодарность В. Б. Алексееву за постановку задачи и руководство.

Список литературы

1. Алексеев В. Б. О некоторых алгебрах, связанных с быстрыми алгоритмами. *Дискретная математика* (1996) 8, №1, 52–64.
2. Алексеев В. Б. Минимальные расширения с простым умножением для алгебры матриц второго порядка. *Дискретная математика* (1997) 9, №1, 71–82.

Статья поступила 12.06.1994.