Записки научных
семинаров ПОМИ
Том 419, 2013 г.

А. Э. Гутерман, О. В. Маркова, С. Д. Сочнев

АЛГЕБРА ПОЛУМАГИЧЕСКИХ МАТРИЦ И ЕЕ ДЛИНА

§1. Введение

Пусть даны конечномерная ассоциативная алгебра $\mathcal{A}$ с единицей над произвольным полем $\mathbb{F}$ и $\mathcal{S} = \{a_1, \dots, a_k\}$ — конечная система порождающих этой алгебры. Приведем определение длины системы порождающих и длины алгебры.

Обозначение 1.1. Произведения элементов из $\mathcal{S}$ будем называть словами. *Длина* слова $a_{i_1} \dots a_{i_t}$, где $a_{i_j} \in \mathcal{S}$, равна t. Будем считать 1 (пустое слово) словом от элементов $\mathcal{S}$ *длины* 0.

Обозначение 1.2. Пусть $\mathcal{S}^i$ обозначает множество всех слов в алфавите $\mathcal{S}$ длины не большей i, $i \geqslant 0$.

Обозначение 1.3. Положим $\mathcal{L}_i(\mathcal{S}) = \langle \mathcal{S}^i \rangle$, где $\langle S \rangle$ обозначает линейную оболочку (множество всех конечных линейных комбинаций с коэффициентами из $\mathbb{F}$) множества S. Заметим, что $\mathcal{L}_0(\mathcal{S}) = \langle 1 \rangle = \mathbb{F}$. Пусть также $\mathcal{L}(\mathcal{S}) = \bigcup\limits_{i=0}^{\infty} \mathcal{L}_i(\mathcal{S})$.

Замечание 1.4. Множество $\mathcal{S}$ является системой порождающих для $\mathcal{A}$ тогда и только тогда, когда $\mathcal{A} = \mathcal{L}(\mathcal{S})$.

Определение 1.5. Длиной системы порождающих $\mathcal{S}$ *для конечномерной алгебры* $\mathcal{A}$ *называется число* $l(\mathcal{S}) = \min\{k \in \mathbb{Z}_+ : \mathcal{L}_k(\mathcal{S}) = \mathcal{A}\}$.

Определение 1.6. Длиной алгебры $\mathcal{A}$ *называется число*

$$l(\mathcal{A}) = \max\{l(\mathcal{S}) : \mathcal{L}(\mathcal{S}) = \mathcal{A}\}.$$

Обозначение 1.7. Обозначим через $M_n(\mathbb{F})$ алгебру квадратных $n \times n$ матриц над полем $\mathbb{F}$, через $T_n(\mathbb{F})$ – ее подалгебру верхнетреугольных матриц.

Ключевые слова: полумагические матрицы, функция длины, конечномерные алгебры, системы порождающих.

Работа выполнена при частичной финансовой поддержке грантов МД-2502.2012.1, РФФИ 13-01-00234а и РФФИ 12-01-00140а.

Через E_{ij} мы будем обозначать (i,j)-ую матричную единицу, т.е. матрицу, у которой на месте (i,j) стоит 1, а на всех остальных местах – 0. Через E будем обозначать единичную матрицу.

Обозначение 1.8. Пусть S_n обозначает группу перестановок n-элементного множества.

Определение 1.9. *Матрица $P_\sigma = (x_{ij}) \in M_n(\mathbb{F})$ называется* перестановочной матрицей, *если $x_{ij} = 1$ в том и только том случае, когда $j = \sigma(i)$, а все остальные элементы P_σ равняются нулю. В этом случае говорят, что матрица P_σ* соответствует *перестановке σ. Пусть S_n – группа перестановок на n элементах. Множество всех перестановочных матриц обозначается $\mathcal{P}_n = \{P_\sigma \in M_n | \sigma \in S_n\}$.*

Задача вычисления длины алгебры матриц $M_n(\mathbb{F})$ как функции порядка матриц была поставлена в [10], но так и не решена. Известны лишь верхние оценки А. Паза и К. Паппачены:

Теорема 1.10 ([10, теорема 1, замечание 2])**.** *Пусть $\mathbb{F}$ – произвольное поле. Тогда*

$$l(M_n(\mathbb{F})) \leqslant \lceil (n^2+2)/3 \rceil.$$

Теорема 1.11 ([9, следствие 3.2])**.** *Пусть $\mathbb{F}$ — произвольное поле. Тогда*

$$l(M_n(\mathbb{F})) < n\sqrt{2n^2/(n-1)+1/4} + n/2 - 2.$$

Как видно, оценки нелинейны. Однако, существует гипотеза о линейности верхней оценки.

Определение 1.12. *Слово $v \in \mathcal{S}^j$ длины j называется* сократимым над $\mathcal{S}$, *если найдется такой номер $i < j$, что $v \in \mathcal{L}_i(\mathcal{S})$, т.е. v представляется в виде линейной комбинации слов меньшей длины.*
Назовем слово $v \in \mathcal{S}^j$ несократимым над $\mathcal{S}$, *если оно не является сократимым.*

Обозначение 1.13. Пусть $a \in \mathcal{A}$ и пусть $\deg a$ обозначает степень минимального многочлена элемента a над полем $\mathbb{F}$. Из конечномерности алгебры $\mathcal{A}$ следует, что для любого $a \in \mathcal{A}$ справедлива оценка $\deg a \leqslant \dim \mathcal{A}$. Тогда для любого непустого подмножества $\mathcal{B} \subseteq \mathcal{A}$ положим $m(\mathcal{B}) = \max\{\deg b : b \in \mathcal{B}\}$.

О. В. Марковой в [6] доказано, что для произвольного поля $\mathbb{F}$ имеет место равенство $l(T_n(\mathbb{F})) = n-1$. В той же работе доказана следующая теорема об оценке длины прямой суммы двух конечномерных алгебр.

Теорема 1.14 ([6, теорема 2]). *Пусть $\mathcal{A}$ и $\mathcal{B}$ – конечномерные алгебры над полем $\mathbb{F}$ с длинами $l(\mathcal{A})$ и $l(\mathcal{B})$ соответственно. Тогда выполнены следующие неравенства*:

$$max\{l(\mathcal{A}), l(\mathcal{B})\} \leqslant l(\mathcal{A} \oplus \mathcal{B}) \leqslant l(\mathcal{A}) + l(\mathcal{B}) + 1.$$

С помощью последней теоремы и оценки для верхнетреугольных матриц получается оценка для блочно-треугольных матриц:

Следствие 1.15 ([6, следствие 3]). *Пусть $\mathcal{A}$ – подалгебра блочно-диагональных или блочно-треугольных матриц, у которых на диагонали стоят k блоков с длинами $l_1, \dots, l_k$ соответственно. Тогда выполнены следующие неравенства*:

$$\max\{l_1, \dots, l_k\} \leqslant l(\mathcal{A}) \leqslant \sum_{j=1}^{k} l_j + k - 1.$$

Также в [4] получена линейная верхняя оценка для коммутативных подалгебр матриц над произвольным полем, равная $n - 1$.

В данной работе авторами проводится исследование функции длины алгебр полумагических матриц. В §2 показано, что полумагические матрицы образуют алгебру, и посчитана ее размерность. §3 посвящен выводу верхней и нижней оценок длины алгебры полумагических матриц. В §4 определена длина систем порождающих, соответствующих множествам транспозиций на n элементах. В последнем параграфе определяется длина алгебры полумагических матриц при малых n.

§2. Полумагические матрицы

Определение 2.1. *Матрица $X \in M_n(\mathbb{F})$ называется* полумагической, *если сумма ее элементов в каждой строке равняется сумме элементов в каждом столбце, равняется некоторому числу $M = M(X)$. Число $M(X)$ называется "магическим числом" матрицы X.*

Обозначим через $SMag(n)$ множество полумагических матриц размера $n \times n$ над произвольным полем $\mathbb{F}$.

Лемма 2.2. *Для любого поля $\mathbb{F}$ множество $SMag(n)$ является алгеброй.*

Доказательство. Достаточно доказать замкнутость множества полумагических матриц относительно сложения и умножения.

Пусть даны две матрицы $X = (x_{ij})$ и $Y = (y_{ij})$. Пусть $X + Y = Z = (z_{ij})$. Покажем, что матрица Z также является полумагической. Действительно, для любого фиксированного j

$$\sum_{i=1}^{n} z_{ij} = \sum_{i=1}^{n}(x_{ij} + y_{ij}) = \sum_{i=1}^{n} x_{ij} + \sum_{i=1}^{n} y_{ij} = M(X) + M(Y).$$

Следовательно, $M(Z) = M(X) + M(Y)$.

Пусть теперь $Z = X \cdot Y$. Покажем, что Z является полумагической и $M(Z) = M(X) \cdot M(Y)$. Во-первых,

$$z_{ij} = \sum_{k=1}^{n} x_{ik} y_{kj}.$$

Сумма же элементов произвольного столбца равна

$$\sum_{i=1}^{n} z_{ij} = \sum_{i=1}^{n} \sum_{k=1}^{n} x_{ik} y_{kj} = \sum_{k=1}^{n} \sum_{i=1}^{n} x_{ik} y_{kj} = \sum_{k=1}^{n} y_{kj} \cdot \sum_{i=1}^{n} x_{ik}$$
$$= \sum_{k=1}^{n} y_{kj} \cdot M(X) = M(X) \cdot M(Y).$$

Таким образом, $SMag(n)$ действительно является алгеброй. $\square$

Отметим, что термин “полумагические матрицы” имеет следующее происхождение, восходящее к понятию “магический квадрат”.

Определение 2.3. *Матрица называется* магической, *если суммы ее элементов по всем строкам, столбцам, а также главной и побочной диагоналям одинаковы.*

Известно, см., например [1, 2], что множество магических матриц образует линейное пространство, и определена его размерность:

Теорема 2.4 ([1, с. 33, 35, теорема 1])**.** *Размерность пространства магических матриц над произвольным полем при $n = 1$ и $n = 2$ равняется* 1.

При $n \geqslant 3$ размерность пространства магических матриц равняется $n^2 - 2n$, за исключением следующего случая: при $n = 4$ и $\operatorname{char} \mathbb{F} = 2$ размерность равняется 9, т.е. $n^2 - 2n + 1$.

Заметим, что при $n = 2$ множество магических матриц также образует алгебру, так как в этом случае все магические матрицы имеют вид $\left(\begin{smallmatrix} x & x \\ x & x \end{smallmatrix}\right)$, а это множество замкнуто относительно сложения и умножения.

Однако справедлив следующий результат:

Теорема 2.5. *При $n \geqslant 3$ множество магических матриц порядка n над полем характеристики 0 не образует алгебру.*

Доказательство. I. Случай $n = 3$ разобран, например, в [11, пример после теоремы 1].

II. Пусть $n \geqslant 4$.

1. В случае четного n рассмотрим матрицу X, соответствующую перестановке $(2, 3, \ldots, n)$. Она является полумагической с магическим числом $M(X) = 1$. На главной и побочной диагоналях находится ровно по одной единице, так что X является магической. Однако $X^{n-1} = E$ есть единичная матрица, которая магической не является (строчные и столбцовые суммы равны 1, сумма элементов на побочной диагонали равна 0). Значит, при четном n магические матрицы не образуют алгебру, поскольку нарушена замкнутость по умножению.

2. В случае нечетного n рассмотрим матрицу X, соответствующую перестановке $(n, n-2, n-4, \ldots, 3, n-1, n-3, \ldots, 2)$. Матрица X является магической, однако матрица $X^{n-1} = E$ таковой не является $((M(E) = 1 \neq \mathrm{tr}\,(E) = n)$. Значит, и при нечетных n магические матрицы также не образуют алгебру. $\square$

Таким образом, магические матрицы в общем случае не образуют алгебру, а полумагические образуют. В настоящей работе мы имеем дело с алгеброй полумагических матриц $SMag(n)$.

Найдём размерность алгебры $SMag(n)$ как векторного пространства.

Лемма 2.6. *Пусть $\mathbb{F}$ – произвольное поле. Тогда* $\dim(SMag(n)) \leqslant n^2 - 2n + 2$.

Доказательство. Пусть $X = (x_{ij}) \in M_n(\mathbb{F})$. Покажем, что для любого набора значений элементов x_{ij}, $1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant n-1$, и $x_{1,n} \in \mathbb{F}$ возможно выбрать оставшиеся элементы $x_{i,n}$, и $x_{n,j}$ так, что $X \in SMag(n)$.

Рассмотрим матрицу

$$X = \begin{pmatrix} x_{1,1} & \dots & x_{1,n-1} & x_{1,n} \\ \dots & \dots & \dots & * \\ x_{n-1,1} & \dots & x_{n-1,n-1} & * \\ * & \dots & * & * \end{pmatrix}.$$

Здесь символом $*$ обозначены неизвестные элементы матрицы X.

Обозначим $M = M(X) = \sum\limits_{i=1}^{n} x_{1,i}$.

Для элементов последнего столбца, за исключением элемента $x_{n,n}$, положим $x_{j,n} = M - \sum\limits_{i=1}^{n-1} x_{j,i}$, $j = 2, \dots, n-1$; таким образом, условие магичности выполнено для первых $n-1$ строк.

Аналогично определим элементы нижней строки по формуле $x_{n,i} = M - \sum\limits_{i=1}^{n-1} x_{j,i}$, $i = 1, \dots, n-1$; таким образом, условие магичности выполнено для первых $n-1$ столбцов.

Найдем элемент $x_{n,n}$. Заметим, что

$$\sum_{i=1}^{n-1} x_{i,n} = (n-1) \cdot M - \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} x_{i,j} = \sum_{j=1}^{n-1} x_{n,j};$$

здесь первое равенство есть сумма строчных сумм, а второе – сумма столбцовых сумм.

В силу равенства (2) значение $x_{n,n} = M - \sum\limits_{i=1}^{n-1} x_{i,n} = M - \sum\limits_{j=1}^{n-1} x_{n,j}$ определено корректно и влечет выполнение условия $X \in SMag(n)$.

Таким образом, каждая полумагическая матрица определяется набором из $n^2 - 2n + 2$ параметров $x_{ij}, 1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant n-1$, и $x_{1,n}$. Следовательно, $\dim(SMag(n)) \leqslant n^2 - 2n + 2$. □

Следствие 2.7. *Пусть* $\mathbb{F}$ *– произвольное поле. Тогда* $\dim(SMag(n)) = n^2 - 2n + 2$.

Доказательство. В качестве базиса алгебры как линейного пространства можно взять множество всевозможных матриц вида $E_{ij} - E_{in} - E_{ni} + E_{nn}$, $1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant n-1$, и матрицу $J = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} E_{ij}$. Они линейно независимы и в силу доказанного в предыдущем утверждении имеем $\dim(SMag(n)) = n^2 - 2n + 2$. □

§3. Оценка длины алгебры полумагических матриц

Вначале нам потребуется несколько технических утверждений.

Лемма 3.1. *Полумагическая трехдиагональная матрица является симметричной.*

Доказательство. Суммы элементов первой строки и первого столбца матрицы $X = (x_{i,j})$ равны между собой. Следовательно, $x_{1,2} = x_{2,1}$. Далее, по индукции для всех $i, i = 2, \dots, n-1$ имеем $x_{i-1,i} + x_{i,i} + x_{i+1,i} = x_{i,i-1} + x_{i,i} + x_{i,i+1}$, где $x_{i-1,i} = x_{i,i-1}$ по предположению индукции. Отсюда, $x_{i+1,i} = x_{i,i+1}$. □

Заметим, что все перестановочные матрицы, см. определение 1.9, являются полумагическими по определению (содержат ровно одну единицу в каждой строке и каждом столбце).

Лемма 3.2. *Над произвольным полем множество перестановочных матриц $\mathcal{P}_n$ порождает алгебру $SMag(n)$.*

Доказательство. Возьмём произвольную полумагическую матрицу $X \in SMag(n)$ и представим её в виде линейной комбинации матриц из $\mathcal{P}_n$. Через $\langle T \rangle$ обозначается линейная оболочка множества T.

Докажем по индукции, что для каждого k, $0 \leqslant k \leqslant n$, существуют такие $M_1, \dots, M_k \in \langle \mathcal{P}_n \rangle$, $X_k \in SMag(n)$, что $X = \sum\limits_{i=1}^{k} M_i + X_k$, где $X_k = \begin{pmatrix} D_k & 0 \\ 0 & Y_{n-k} \end{pmatrix}$ и для каждого i, $1 \leqslant i \leqslant k$,

$$M_i = \begin{pmatrix} D'_{i-1} & 0 \\ 0 & N_{n-i+1} \end{pmatrix}$$

– блочно-диагональные матрицы, причем $D_k \in M_k(\mathbb{F})$, $D'_{i-1} \in M_{i-1}(\mathbb{F})$ – диагональные матрицы, $Y_{n-k} \in SMag(n-k)$, а N_{n-i+1} является линейной комбинацией матриц из $\mathcal{P}_{n-i+1}$.

База индукции: $k = 0$. Положим в этом случае $X_0 = X$.

Шаг индукции. Предположим, что требуемые матрицы $M_1, \dots, M_k$, X_k построены. Для $j = k+3, \dots, n$ рассмотрим перестановочные матрицы P_{σ_j}, отвечающие перестановкам $\sigma_j = (k+2, k+1, j)$. Пусть $L = \sum\limits_{j=k+3}^{n} x_{k+1,j} P_{\sigma_j}$. Также рассмотрим перестановочные матрицы P_{σ^j}, отвечающие перестановкам $\sigma^j = (k+1, k+2, j)$. Пусть $\hat{L} =$

$\sum\limits_{j=k+3}^{n} x_{j,k+1} P_{\sigma^j}$. Тогда для матрицы $Y = (y_{ij}) = X_k - L - \hat{L}$ имеем $y_{k+1,j} = y_{j,k+1} = 0$ при всех $j = k+3, \ldots, n$.

Матрица $Y = X - \sum\limits_{i=1}^{k} M_i - L - \hat{L}$ полумагическая, так как все матрицы в правой части полумагические. Следовательно, $y_{k+1,k+1} + y_{k+1,k+2} = y_{k+1,k+1} + y_{k+2,k+1}$, откуда $y_{k+1,k+2} = y_{k+2,k+1}$.

Тогда матрица $Y - y_{k+1,k+2} P_{(k+1,k+2)}$ содержит нулевые коэффициенты на позициях $(k+1, k+2)$ и $(k+2, k+1)$. Здесь матрица $P_{(k+1,k+2)}$ – перестановочная матрица, отвечающая транспозиции $(k+1, k+2)$.

Следовательно, выбирая $M_{k+1} = L + \hat{L} + y_{k+1,k+2} P_{(k+1,k+2)}$, $X_{k+1} = X_k - M_{k+1}$, получаем шаг индукции.

При $k = n-1$ имеем: $X = \sum\limits_{i=1}^{n} M_i + X_n$, где $M_i \in \mathcal{P}_n$, X_n – диагональная матрица. Так как X_n – полумагическая матрица, ее строчные и столбцовые суммы совпадают. Следовательно, она скалярна и, значит, кратна матрице E.

Таким образом, X представлена в виде линейной комбинации перестановочных матриц. $\square$

Определение 3.3. *Для подмножеств*

$$G_1 = \{\tau_1 = (1,2), \tau_2 = (2,3), \ldots, \tau_{n-1} = (n-1, n)\}$$

и

$$G_2 = \{\sigma_n = (1, 2, \ldots, n), \tau_1\}$$

в S_n *определим* $\mathcal{G}_1 = \{X_{\tau_1}, X_{\tau_2}, \ldots, X_{\tau_{n-1}}\}$ *и* $\mathcal{G}_2 = \{X_{\tau_1}, X_{\sigma_n}\}$ *– множества перестановочных матриц, соответствующих рассматриваемым перестановкам.*

Лемма 3.4. *Множества* $\mathcal{G}_1$ *и* $\mathcal{G}_2$ *являются порождающими для алгебры* $SMag(n)$.

Доказательство. Утверждение леммы следует непосредственно из того, что каждое из множеств G_1 и G_2 порождает группу S_n, и из леммы 3.2. $\square$

Утверждение 3.5. *Пусть* $n \in \mathbb{N}$, $n \geqslant 2$. *Тогда верны следующие утверждения.*

1. *Если*

$$X_{\tau_{i_p}} \cdots X_{\tau_{i_1}} e_1 = e_n,$$

где $X_{\tau_{i_s}} \in \mathcal{G}_1 \subset \mathcal{P}_n$, $s = 1, \ldots, p$, e_j *– столбец высоты* n *с* 1 *на позиции* j *и нулями на остальных, то* $p \geqslant n-1$.

2. *Если в тех же обозначениях* $X_{\tau_{j_q}} \cdots X_{\tau_{j_1}} e_n = e_1$, *то* $q \geqslant n-1$.

Доказательство. I. Индукция по n.

База индукции. При $n = 2$ очевидно, что преобразование не является тождественным.

Шаг индукции. Пусть $n > 2$. Докажем утверждение для слова наименьшей возможной длины p, удовлетворяющего условию предложения. Имеем $p \geqslant 2$. Множество чисел $\{i_1, \ldots, i_p\}$ содержит $n-1$, так как иначе $X_{\tau_{i_p}} \cdots X_{\tau_{i_1}} e_1 = e_r, r < n$, т.е. не удовлетворяет условию. В силу выбора $p = \min\{t \in \{1, \ldots, p\} : i_t = n-1$ и $X_{\tau_{i_t}} \cdots X_{\tau_{i_1}} e_1 = e_n\}$. Также из условия минимальности p следует, что множество $i_1, \ldots, i_{p-1}$ не содержит $n-1$, иначе если $i_s = n-1$, то соответствующая этому индексу матрица $X_{\tau_{i_s}}$ действует как тождественное преобразование, и можно уменьшить длину слова. Значит, $i_{p-1} = n-2$, и к слову $X_{\tau_{i_{p-1}}} \cdots X_{\tau_{i_1}}$ применимо предположение индукции, т.е. $p-1 \geqslant n-2$, откуда $p \geqslant n-1$.

II. Следует из I, поскольку $X_{\tau_i} = X_{\tau_i}^{-1}$. □

Отметим, что длина алгебры — сложный для вычисления инвариант, явное вычисление которого реализовано лишь для небольшого количества примеров. В этой связи большое значение приобретает задача вычисления длин различных порождающих множеств. Этой задаче также было уделено значительное внимание, см., например, [7,9]. Рассмотрим аналогичную задачу для алгебры полумагических матриц.

Лемма 3.6. *При* $n \geqslant 2$ *над любым полем справедливо равенство* $l(\mathcal{G}_1) = n-1$.

Доказательство. I. Докажем, что $l(\mathcal{G}_1) \geqslant n-1$. Пространство $\mathcal{L}(\mathcal{G}_1)$ содержит матрицу

$$E' = E_{1,n} + E_{2,n-1} + \cdots + E_{n-1,2} + E_{n,1}$$

(поскольку $E' \in \mathcal{P}_n$), откуда следует, что $E' \in \mathcal{L}_r(\mathcal{G}_1)$ для некоторого $r \in \mathbb{N}$. Перепишем данное условие в виде $E' = c_1 V_1 + \ldots + c_t V_t$, где $c_i \in \mathbb{F} \setminus \{0\}$, $V_i \in \mathcal{G}_1^r$ – несократимое слово, $i = 1, \ldots, t$. Покажем, что $r \geqslant n-1$.

Поскольку $(E')_{1,n} = 1 \neq 0$, то для некоторого индекса $j \in \{1, \ldots, t\}$ также выполнено равенство $(V_j)_{1,n} = 1$. Рассмотрим слово V_j, оно имеет вид $X_{\tau_{i_1}} \cdots X_{\tau_{i_p}}$, где p – длина данного слова.

По условию, n-ый столбец матрицы $X_{\tau_{i_1}} \cdots X_{\tau_{i_p}}$ равен e_1 (в обозначениях предложения 3.5), и равен n-ому столбцу матрицы $X_{\tau_{i_1}} \cdots X_{\tau_{i_p}} E$, который можно записать в виде $X_{\tau_{i_1}} \cdots X_{\tau_{i_p}} e_n$. Тогда неравенство $p \geqslant n-1$ следует из предложения 3.5.

II. Теперь докажем, что $l(\mathcal{G}_1) \leqslant n-1$. Для этого покажем, что любую полумагическую матрицу $X = \{x_{i,j}\} \in SMag(n)$ можно представить в виде многочлена от порождающей системы $\mathcal{G}_1$ степени, не превосходящей $n-1$.

Определим подмножество слов от элементов $\mathcal{G}_1$, по которому мы разложим матрицу X.

1. Рассмотрим множество матриц

$$\{R_{ij}, 1 \leqslant i \leqslant n-1, i+1 \leqslant j \leqslant n\},$$

где $R_{ij} = X_{\tau_i} \cdot X_{\tau_{i+1}} \cdots X_{\tau_{j-1}} \in \mathcal{G}_1^{j-i-2}$. В такой матрице в i-ой строке единица находится на j-ой позиции, а в остальных строках – на главной диагонали или на диагонали, смежной с ней. Значит, в матрице

$$Y = X - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} x_{i,j} R_{ij}$$

все элементы, лежащие выше диагонали, смежной с главной, нулевые.

2. Аналогично определяем множество матриц

$$L_{ij} = \{X_{\tau_j} \cdot X_{\tau_{j-1}} \cdots X_{\tau_{i+1}}, 1 \leqslant i \leqslant n-1, i+1 \leqslant j \leqslant n\}.$$

В такой матрице в $(j+1)$-ой строке единица находится на i-ой позиции, а в остальных строках – на главной диагонали или на смежной с ней диагонали. Следовательно, матрица

$$Z = Y - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} x_{i,j} L_{ij}$$

трёхдиагональна.

3. Обозначим $Z = (z_{ij})$. По лемме 3.1 матрица Z симметрична. Возьмем матрицу

$$W = Z - \sum_{i=1}^{n-1} z_{i,i+1} X_{\tau_i}.$$

В силу симметричности матрицы Z, матрица W диагональна. Произвольная полумагическая диагональная матрица является скалярной.

4. Комбинируя разложения из 1–3, для исходной матрицы X получаем

$$X = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} x_{i,j}R_{ij} + \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} x_{i,j}L_{ij} + \sum_{i=1}^{n-1} z_{i,i+1}X_{\tau_i} + \alpha E;$$

следовательно,

$$X \in \mathcal{L}_{n-1}(\mathcal{G}_1).$$

Объединяя I и II, получаем, что $l(\mathcal{G}_1) = n-1$. □

Исследуем длину порождающей системы $\mathcal{G}_2 = \{X_{(1,2,\ldots,n)}, X_{(1,2)}\}$.

Сначала рассмотрим пространство слов от $\mathcal{G}_2$ длины $2n-5$.

Лемма 3.7. *Пусть $\mathbb{F}$ – произвольное поле, $n \in \mathbb{N}$, $n \geqslant 4$. Рассмотрим подпространство $\mathcal{U} \subset SMag(n)$, задаваемое следующим образом:*

$$\mathcal{U} = \left\{X = (x_{i,j}) \in SMag(n) | x_{3,n-1} = x_{4,n}\right\}$$

– пространство решений однородного линейного уравнения $x_{3,n-1} - x_{4,n} = 0$. Тогда $\mathcal{L}_{2n-5}(\mathcal{G}_2) \subseteq \mathcal{U}$.

Доказательство. Будем доказывать включение $\mathcal{L}_m(\mathcal{G}_2) \subseteq \mathcal{U}$ при $0 \leqslant m \leqslant 2n-5$ индукцией по m.

База индукции: $m = 0, 1$. Очевидно, что $E, X_{\tau_1}, X_{\sigma_n} \in \mathcal{U}$, поэтому $\mathcal{L}_1(\mathcal{G}_2) = \langle E, X_{\tau_1}, X_{\sigma_n}\rangle \subseteq \mathcal{U}$.

Шаг индукции. Пусть $1 < m \leqslant 2n-5$. Предположим, что $\mathcal{L}_{m-1}(\mathcal{G}_2) \subseteq \mathcal{U}$. В силу линейности пространств $\mathcal{U}$ и $\mathcal{L}_m(\mathcal{G}_2)$, для доказательства включения $\mathcal{L}_m(\mathcal{G}_2) \subseteq \mathcal{U}$ достаточно проверить, что все несократимые слова из $\mathcal{G}_2^m$ длины m содержатся в $\mathcal{U}$.

I. Сначала проверим условие для однобуквенных слов. Будем обозначать (i,j)-ый элемент матрицы W через W_{ij}. Используем следующие соотношения:

$$X_{\tau_1}^2 = E = X_{\sigma_n}^n,$$
$$(X_{\tau_1})_{3,n-1} = (X_{\tau_1})_{4,n} = 0,$$
$$(X_{\sigma_n}^{n-4})_{3,n-1} = (X_{\sigma_n}^{n-4})_{4,n} = 1,$$
$$(X_{\sigma_n}^m)_{3,n-1} = (X_{\sigma_n}^m)_{4,n} = 0 \text{ при } 0 \leqslant m \leqslant n-1,\ m \neq n-4.$$

Следовательно, $X_{\sigma_n}^m \in \mathcal{U}$ при всех $2 \leqslant m \leqslant n-1$; при больших длинах слова сократимы.

II. Теперь будем рассматривать слова, содержащие оба элемента из $\mathcal{G}_2$. Из соотношений, приведенных в пункте I, следует, что несократимые двухбуквенные слова будут иметь вид

$$X_{\tau_1}^t X_{\sigma_n}^{k_1} X_{\tau_1} X_{\sigma_n}^{k_2} \cdots X_{\tau_1} X_{\sigma_n}^{k_r} X_{\tau_1}^s,$$

где $r \geqslant 1$, $t, s = 0, 1$, $1 \leqslant k_i \leqslant n-1$, $i = 1, \ldots, r$.

Заметим, что достаточно рассматривать слова, начинающиеся и заканчивающиеся на X_{σ_n}, т.е. считать, что $s = t = 0$. Действительно, $(AX_{\tau_1})_{i,j} = A_{i,j} = (X_{\tau_1}A)_{i,j}$ для всех $3 \leqslant i, j \leqslant n$ и произвольной матрицы $A \in M_n(\mathbb{F})$. Тогда $X_{\tau_1}U \in \mathcal{U}$ и $UX_{\tau_1} \in \mathcal{U}$ для всех матриц $U \in \mathcal{U}$. При этом $\mathcal{L}_{m-1}(\mathcal{G}_2) \subseteq \mathcal{U}$ по предположению индукции, откуда $X_{\tau_1}\mathcal{L}_{m-1}(\mathcal{G}_2) \subseteq \mathcal{U}$ и $\mathcal{L}_{m-1}(\mathcal{G}_2)X_{\tau_1} \subseteq \mathcal{U}$.

Матрица $P_\pi = X_{\sigma_n}^{k_1} X_{\tau_1} X_{\sigma_n}^{k_2} \cdots X_{\tau_1} X_{\sigma_n}^{k_r}$ является перестановочной и соответствует перестановке $\pi = \sigma_n^{k_r}\tau_1\sigma_n^{k_{r-1}} \cdots \tau_1\sigma_n^{k_1}$.

Дальнейшее доказательство проведем отдельно для различных значений числа k_1.

1. Пусть $k_1 < n-3$. Тогда $\sigma_n^{k_1}(i) = k_1 + i$ при $i = 3, 4$, следовательно, $\tau_1\sigma_n^{k_1}(i) = k_1 + i$ при $i = 3, 4$. Рассмотрим подстановку $\pi_1 = \sigma_n^{k_r}\tau_1\sigma_n^{k_{r-1}} \cdots \sigma_n^{k_2}\sigma_n^{k_1}$. Соответствующая ей матрица P_{π_1} – слово от элементов $\mathcal{G}_2$ длины $m-1$. По построению имеют место равенства $(P_\pi - P_{\pi_1})_{3,j} = (P_\pi - P_{\pi_1})_{4,j} = 0$ для всех $j = 1, \ldots, n$. Таким образом, $P_\pi - P_{\pi_1} \in \mathcal{U}$. Включение $P_{\pi_1} \in \mathcal{U}$ выполнено по предположению индукции. Следовательно, $P_\pi = (P_\pi - P_{\pi_1}) + P_{\pi_1} \in \mathcal{U}$.

2. Пусть $k_1 = n-3+q$, $q = 0, 1, 2$. Докажем, что $(P_\pi)_{3,n-1} = (P_\pi)_{4,n} = 0$. Непосредственная проверка показывает, что в третьей строке матрицы P_π единственный ненулевой элемент расположен в столбце с номером $\pi(3)$, а в четвертой строке матрицы P_π – в столбце $\pi(4)$. Поэтому для наших целей достаточно доказать, что $\pi(3) < n-1$ и $\pi(4) < n$.

i. Вычислим образы 3 и 4 при применении σ_n^{n-3+q}:

$$\sigma_n^{n-3}(3) = n, \quad \sigma_n^{n-2}(3) = 1, \quad \sigma_n^{n-1}(3) = 2,$$
$$\sigma_n^{n-3+q}(4) = q+1 \text{ для всех } q = 0, 1, 2.$$

ii. Применим к значениям, найденным в (i), подстановку τ_1:

$$\begin{aligned}
&\text{при } q = 0 \text{ имеем:} \quad && \tau_1\sigma_n^{n-3}(3) = n, \quad \tau_1\sigma_n^{n-3}(4) = 2,\\
&\text{при } q = 1 \text{ имеем:} \quad && \tau_1\sigma_n^{n-2}(3) = 2, \quad \tau_1\sigma_n^{n-2}(4) = 1,\\
&\text{при } q = 2 \text{ имеем:} \quad && \tau_1\sigma_n^{n-1}(3) = 1, \quad \tau_1\sigma_n^{n-1}(4) = 3.
\end{aligned}$$

iii. Из ограничения на длину слова следует, что

$$n-3+q+1+k_2+1+k_3+1+\dots+k_r = n-4+q+r+k_2+k_3+\dots+k_r \leqslant 2n-5,$$

$$r + k_2 + k_3 + \ldots + k_r \leqslant n - 1 - q, \tag{3.1}$$

в частности, $k_2 \leqslant n - 3 - q$, откуда после применения σ^{k_2} к полученному в (ii) находим, что

при $q = 0$ $\quad \sigma_n^{k_2}\tau_1\sigma_n^{n-3}(3) = k_2,\ \sigma_n^{k_2}\tau_1\sigma_n^{n-3}(4) = k_2 + 2(\operatorname{mod} n) = k_2 + 2,$

при $q = 1$ $\quad \sigma_n^{k_2}\tau_1\sigma_n^{n-2}(3) = k_2 + 2,\ \sigma_n^{k_2}\tau_1\sigma_n^{n-2}(4) = k_2 + 1,$

при $q = 2$ $\quad \sigma_n^{k_2}\tau_1\sigma_n^{n-1}(3) = k_2 + 1,\ \sigma_n^{k_2}\tau_1\sigma_n^{n-1}(4) = k_2 + 3.$

Из этих равенств сразу следует, что $P_\pi \in \mathcal{U}$ при $r = 2$.

iv. Пусть $r \geqslant 3$.

a) При $k_2 + i \geqslant 3$, $i = 0, 1, 2, 3$, имеем

$$\sigma_n^{k_r} \cdots \sigma_n^{k_3}\tau_1(k_2 + i) = k_r + \cdots + k_3 + k_2 + i.$$

Используя неравенство (3.1), получим, что

$$K = k_r + \cdots + k_3 + k_2 + i \leqslant k_r + \cdots + k_3 + k_2 + r \leqslant n - 1 - q. \tag{3.2}$$

Тогда $K < n - 1$, если $q \geqslant 1$.

В случае $q = 0$ из пункта (iii) следует, что $i = 0 < r$ или $i = 2 < r$; следовательно, первое неравенство в формуле (3.2) является строгим, откуда опять $K < n - 1$.

b) При $k_2 = 1$

$$\sigma_n^{k_r} \cdots \sigma_n^{k_3}\tau_1(k_2) = k_r + \cdots + k_3 + k_2 + 1 < k_r + \cdots + k_3 + k_2 + r,$$
$$\sigma_n^{k_r} \cdots \sigma_n^{k_3}\tau_1(k_2 + 1) = \sigma_n^{k_r} \cdots \sigma_n^{k_3}(1) \leqslant k_r + \ldots + k_3 + k_2.$$

c) При $k_2 = 2$

$$\sigma_n^{k_r} \cdots \sigma_n^{k_3}\tau_1(k_2) = \sigma_n^{k_r} \cdots \sigma_n^{k_3}(1) \leqslant k_r + \ldots + k_3 + k_2 - 1.$$

Соответственно, из (iv) следует, что при всех значениях k_2 образы элементов 3 и 4 меньше $n-1$ и n соответственно, следовательно, имеют места равенства $(P_\pi)_{3,n-1} = (P_\pi)_{4,n} = 0$.

Таким образом, нами во всех случая доказано, что $P_\pi \in \mathcal{U}$. Следовательно, $\mathcal{L}_{2n-5}(\mathcal{G}_2) \subseteq \mathcal{U}$. □

Лемма 3.8. *При $n \geqslant 4$ над любым полем справедливо неравенство $l(\mathcal{G}_2) \geqslant 2n - 4$.*

Доказательство. Для доказательства оценки $l(\mathcal{G}_2) \geqslant 2n-4$ достаточно показать, что множество $\mathcal{G}_2^{2n-4}$ содержит хотя бы одно несократимое слово длины $2n-4$.

Установим, что несократимым является, например, слово $X_{\sigma_n}^{n-3} X_{\tau_1} X_{\sigma_n}^{n-2}$. Выпишем соответствующую матрицу в явном виде.

При $n = 4$ имеем:

$$X_{\sigma_4} X_{\tau_1} X_{\sigma_4}^2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

при $n > 4$ имеем

$$X_{\sigma_n}^m = \sum_{i=1}^{n-m} E_{i,i+m} + \sum_{j=1}^{m} E_{j+n-m,j}$$

для $m = 1, \ldots, n-1$; в частности,

$$X_{\sigma_n}^{n-3} = E_{1,n-2} + E_{2,n-1} + E_{3,n} + \sum_{j=1}^{n-3} E_{j+3,j},$$

$$X_{\sigma_n}^{n-2} = E_{1,n-1} + E_{2,n} + \sum_{j=1}^{n-2} E_{j+2,j},$$

$$X_{\sigma_n}^{n-3} X_{\tau_1} = E_{1,n-2} + E_{2,n-1} + E_{3,n} + E_{4,2} + E_{5,1} + \sum_{j=3}^{n-3} E_{j+3,j},$$

$$X_{\sigma_n}^{n-3} X_{\tau_1} X_{\sigma_n}^{n-2} = (X_{\sigma_n}^{n-3} X_{\tau_1})(X_{\sigma_n}^{n-2})$$

$$= E_{1,n-4} + E_{2,n-3} + E_{3,n-2} + E_{4,n} + E_{5,n-1} + \sum_{j=3}^{n-3} E_{j+3,j+n-2 (\mathrm{mod}\, n)}.$$

Заметим, что при всех $n \geqslant 4$ выполнено неравенство

$$(X_{\sigma_n}^{n-3} X_{\tau_1} X_{\sigma_n}^{n-2})_{3,n-1} = 0 \neq 1 = (X_{\sigma_n}^{n-3} X_{\tau_1} X_{\sigma_n}^{n-2})_{4,n}.$$

Таким образом, $X_{\sigma_n}^{n-3}X_{\tau_1}X_{\sigma_n}^{n-2}\notin\mathcal{U}$, где пространство $\mathcal{U}$ определено в лемме 3.7, в то время как $\mathcal{L}_{2n-5}(\mathcal{G}_2)\subseteq\mathcal{U}$. Следовательно,

$$X_{\sigma_n}^{n-3}X_{\tau_1}X_{\sigma_n}^{n-2}\notin\mathcal{L}_{2n-5}(\mathcal{G}_2),$$

т.е. несократимо.

В результате получаем, что $l(\mathcal{G}_2)\geqslant 2n-4$. □

Лемма 3.9. *При $n\geqslant 4$ над любым полем справедливо неравенство $l(\mathcal{G}_2)\leqslant 2n-4$.*

Доказательство. Покажем, что каждую матрицу $X\in SMag(n)$ можно представить в виде суммы слов от элементов $\mathcal{G}_2$ длин, не превосходящих $2n-4$.

I. Сначала определим подмножество слов от элементов $\mathcal{G}_2$, по которому мы разложим матрицу X.

Пронумеруем диагонали матрицы X. Главную диагональ – номером 1, соседнюю справа от неё – номером 2 и так далее, до номера n.

Возьмем произвольную клетку матрицы с координатами (i,j), она находится на диагонали под номером $1+j-i(\operatorname{mod} n)$.

Обозначим:

$$\begin{aligned}&\alpha=n-i+1(\operatorname{mod} n), \quad \beta=j-2(\operatorname{mod} n),\\ &\gamma=n-i+2(\operatorname{mod} n), \quad \delta=j-1(\operatorname{mod} n).\end{aligned}$$

Рассмотрим слова двух видов:

$$U_{i,j}=X_{\sigma_n}^{\alpha}\cdot X_{\tau_1}\cdot X_{\sigma_n}^{\beta}$$

и

$$D_{i,j}=X_{\sigma_n}^{\gamma}\cdot X_{\tau_1}\cdot X_{\sigma_n}^{\delta}.$$

Заметим, что в матрице $U_{i,j}$ единицы находятся в клетке (i,j), а также в некоторых клетках двух диагоналей, предшествующих диагонали, содержащей клетку (i,j). А в матрице $D_{i,j}$ одна единица находится в клетке (i,j), а остальные – в некоторых клетках двух диагоналей, следующих за диагональю, содержащей (i,j).

Верхним индексом клетки (i,j) данной матрицы назовем длину слова $U_{i,j}$; *нижним индексом* клетки (i,j) данной матрицы назовем длину слова $D_{i,j}$. Составим матрицу размера $n\times n$, элементами которой являются следующие выражения вида $\frac{p}{q}$, у которых над чертой записан верхний индекс соответствующей клетки, а под чертой – нижний:

$$\begin{pmatrix}
\frac{n}{2} & \frac{1}{3} & \frac{2}{4} & \dots & \dots & \dots & \frac{n-1}{n+1} \\
\frac{2n-1}{1} & \frac{n}{2} & \frac{n+1}{3} & \dots & \frac{2n-4}{n-2} & \frac{2n-3}{n-1} & \frac{2n-2}{n} \\
\frac{2n-2}{n} & \frac{n-1}{n+1} & \frac{n}{n+2} & \dots & \frac{n-5}{2n-3} & \frac{2n-4}{2n-2} & \frac{2n-3}{2n-1} \\
\frac{2n-3}{n-1} & \frac{n-2}{n} & \dots & \dots & \dots & \frac{2n-5}{2n-3} & \frac{2n-4}{2n-2} \\
\frac{2n-4}{n-2} & \frac{n-3}{n-1} & \dots & \dots & \dots & \frac{2n-6}{2n-4} & \frac{2n-5}{2n-3} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\frac{n+1}{3} & \frac{2}{4} & \frac{3}{5} & \dots & \dots & \frac{n-1}{n+1} & \frac{n}{n+2}
\end{pmatrix}.$$

Нас интересуют индексы, которые больше либо равны $2n-3$; их всего 12 штук во всей матрице, в последующих строках индексы лишь уменьшаются. Назовем такие индексы “плохими”. Также заметим, что “плохие” индексы содержатся лишь в $n-4$, $n-3$, $n-2$, $n-1$ и n-й диагоналях.

II. Покажем, как данную матрицу представить в виде линейной комбинации слов первого и второго типа длин, не больших $2n-4$. Последовательно по диагоналям будем менять разложение матрицы X, чтобы избавиться от “плохих” индексов.

(1) Начнем с $(n-2)$-ой диагонали. На ней расположен ровно один элемент с “плохим” нижним индексом, так что можно вычесть из матрицы X слово $X_{\sigma_n}^{n-3}$ и занулить соответствующий элемент матрицы: пусть $X^{(0)} = X - x_{3,n}X_{\sigma_n}^{n-3}$.

У $X^{(0)}$ на $(n-2)$-ой диагонали ненулевыми остаются лишь элементы с “хорошим” нижним индексом. Поскольку слова типа $D_{i,j}$ для элементов этой диагонали содержат ровно по одной 1 на $(n-2)$-ой диагонали, а остальные – на $(n-1)$-ой и n-ой, то вычитая из X^0 слова этого типа, соответствующие ненулевым элементам $(n-2)$-ой диагонали, мы занулим $(n-2)$-ую диагональ. Рассмотрим матрицу

$$X^{(1)} = X^{(0)} - \sum_{\substack{i,j:1\leqslant i,j\leqslant n \\ j-i+1\equiv n-2 (\operatorname{mod} n)}} x_{i,j}D_{i,j};$$

у неё $(n-2)$-ая диагональ нулевая.

Отметим, что если для матрицы $X^{(1)}$ мы найдем разложение, в которое входят только такие слова из $\mathcal{L}_{2n-4}(\mathcal{G}_2)$, у которых все элементы на $(n-2)$-ой диагонали равны 0, то, прибавив к нему $X - X^{(1)} \in \mathcal{L}_{2n-4}(\mathcal{G}_2)$, получим требуемое разложение для X.

(2) Теперь будем обнулять элементы, расположенные на $(n-1)$-ой диагонали матрицы $X^{(1)}$. Для этого рассмотрим матрицу

$$X^{(2)} = X^{(1)} - \sum_{\substack{i,j:1\leqslant i,j\leqslant n\\ j-i+1\equiv n-2 (\mathrm{mod}\, n)}} x_{i,j} D_{i,j}.$$

Слова типа $D_{i,j}$ для этой диагонали не содержат элементов на $(n-2)$-ой диагонали, так что у матрицы $X^{(2)}$ уже две диагонали содержат лишь нули: $(n-2)$-ая и $(n-1)$-ая.

(3) Аналогично обнуляем n-ую диагональ, не затрагивая предыдущие:

$$X^{(3)} = X^{(2)} - \sum_{\substack{i,j:1\leqslant i,j\leqslant n\\ j-i+1\equiv n-2 (\mathrm{mod}\, n)}} x_{i,j} D_{i,j}.$$

(4) Далее по очереди обнуляем диагонали с номерами $n-3$, потом $n-4$ и т.д., до третьей диагонали словами типа $U_{i,j}$. Поскольку в этих диагоналях все верхние индексы “хорошие”, то используемые слова будут иметь длину, не превышающую $2n-4$:

$$X^{(4)} = X^{(3)} - \sum_{\substack{i,j:1\leqslant i,j\leqslant n\\ j-i+1\equiv n-2 (\mathrm{mod}\, n)}} x_{i,j} U_{i,j},$$

$$\dots$$

$$X^{(n-2)} = X^{(n-3)} - \sum_{\substack{i,j:1\leqslant i,j\leqslant n\\ j-i+1\equiv n-2 (\mathrm{mod}\, n)}} x_{i,j} U_{i,j}.$$

Так как слова типа $U_{i,j}$ содержат единицы только в диагонали самого элемента, а также в диагоналях с меньшими номерами, то в итоге получим матрицу, содержащую ненулевые элементы лишь в первой и второй диагоналях.

(5) Из полумагичности матрицы следует, что на главной диагонали все элементы равны. Так же, как и на второй диагонали. Полученная матрица раскладывается в линейную комбинацию

двух слагаемых: единичной матрицы и перестановочной матрицы X_{σ_n}.

Таким образом, мы разложили исходную матрицу в линейную комбинацию слов длины не больше, чем $2n-4$. □

Объединяя леммы 3.8–3.9, получаем следующий результат.

Теорема 3.10. *При $n \geqslant 4$ над любым полем справедливо равенство $l(\mathcal{G}_2) = 2n-4$.*

Теорема 3.11. *Пусть $\mathbb{F}$ – произвольное поле.*

1. *При $n=2$ справедливо $l(SMag(2)) = 1$.*
2. *При $n=3,4$ справедливо $l(SMag(n)) = 2n-4$.*
3. *При $n \geqslant 5$ справедливы неравенства*

$$2n-4 \leqslant l(SMag(n)) \leqslant n\sqrt{2(n-1)+\frac{2}{(n-1)}+\frac{1}{4}}+\frac{n}{2}-2.$$

Доказательство. 1, 2. Случай $n \leqslant 4$ рассмотрен отдельно в §5.

3. Верхняя оценка следует из теоремы, доказанной К. Паппаченой в [9, теорема 3.1], которая утверждает, что для произвольной алгебры $\mathcal{A}$ размерности d и с максимальной степенью минимального многочлена e элементов алгебры выполняется неравенство: $l(\mathcal{A}) \leqslant e\sqrt{2d/(e-1)+1/4}+e/2-2$. В случае алгебры полумагических матриц имеем $d = n^2-2n+2$, $e=n$, откуда получаем оценку

$$l(SMag(n)) \leqslant n\sqrt{2(n-1)+\frac{2}{(n-1)}+\frac{1}{4}}+\frac{n}{2}-2.$$

Нижняя оценка следует из теоремы 3.10. □

§4. Нахождение длины порождающих множеств, состоящих из транспозиций

Через $X_{(i,j)} \in \mathcal{P}_n$ обозначим матрицу, соответствующую транспозиции $(i,j) \in S_n$.

Определение 4.1. *Множеству транспозиций T, состоящему из элементов вида (i,j), сопоставим граф G, состоящий из n вершин, пронумерованных от 1 до n. Вершины i и j графа G соединены ребром тогда и только тогда, когда транспозиция $(i,j) \in T$.*

Через $\mathcal{T}$ обозначим подмножество $\mathcal{P}_n$, состоящее из всех матриц $X_{(i,j)}$ таких, что $(i,j) \in T$.

Утверждение 4.2 ([3, леммы 3.10.1, 3.10.2])**.** 1. *Множество T является порождающим для группы перестановок S_n тогда и только тогда, когда граф G связен.*

2. *Порождающее множество минимально (т.е. при исключении любого элемента перестает быть порождающим), если соответствующий ему граф – дерево.*

Определение 4.3 ([5])**.** Диаметром *$l(G)$ графа G называется максимальное из расстояний между парами его вершин.* Расстояние *между вершинами определяется как наименьшее число ребер, которые необходимо пройти, чтобы добраться из одной вершины в другую.*

Теорема 4.4. *При $n \in \mathbb{N}$ над произвольным полем длина множества $\mathcal{T} \subset \mathcal{P}_n$, построенного по минимальной порождающей системе транспозиций $T \subset S_n$, равна диаметру соответствующего системе T графа G.*

Доказательство. Во-первых, индукцией по n, то есть по числу вершин графа, докажем, что $l(G)$ не превосходит диаметра графа. Затем приведем пример матрицы, которую невозможно разложить в линейную комбинацию слов длины, меньшей диаметра графа.

База индукции. При $n = 1$ граф G состоит из одной вершины, $l(G) = 0$. Алгебра, порожденная пустым множеством T, изоморфна основному полю и имеет длину 0.

Шаг индукции. Пусть $n \geqslant 2$ и для всех $1 \leqslant p < n$ утверждение теоремы выполнено. Пусть дано минимальное порождающее множество транспозиций $T \subset S_n$, $\mathcal{T} \subset \mathcal{P}_n$. Покажем, что произвольную матрицу $X = \{x_{i,j}\} \in SMag(n)$ можно представить в виде суммы слов от элементов $\mathcal{T}$ длин, не превосходящих $l(G)$. Согласно предложению 4.2 граф G является деревом, поэтому в нем существует хотя бы одна висячая вершина, т.е. такая вершина, которая соединена ребром только с одной вершиной графа. Без ограничения общности вершины можно перенумеровать так, что данная висячая вершина будет иметь номер 1, вершина, с которой она соединена ребром – номер 2.

I. Покажем, как подобрать линейную комбинацию слов от элементов $\mathcal{T}$ такую, что она занулит 1-ый столбец и 1-ую строку матрицы X, кроме элемента, стоящего на их пересечении, причем слова имеют длину, не превосходящую диаметр графа.

Для каждого номера $l \in 1, \dots, n$ существует путь $a_{1,l} a_{2,l} \dots a_{s_l,l}$ такой, что $a_1 = a_{1,l} = 1, a_{s_l} = a_{s_l,l} = l, s_l \leqslant l(G)$.

1. Для начала обнулим все элементы 1-ой строки. Рассмотрим слово

$$Y_{1,l} = X_{(a_1,a_2)} X_{(a_2,a_3)} \cdots X_{(a_{s_l-1},a_{s_l})},$$

$l \in 1, \dots, n$. В нем в 1-ой строке, l-ом столбце стоит единица, остальные элементы 1-ой строки нулевые, и длина слова меньше либо равна диаметру графа. Тогда в матрице $X_0 = X - \sum\limits_{j=1}^{n} x_{1,j} Y_{1,j}$ все элементы 1-ой строки нулевые.

2. Затем обнулим 1-ый столбец. Рассмотрим слово

$$Z_{l,1} = X_{(a_{s_l},a_{s_l-1})} X_{(a_{s_l-1},a_{s_l-2})} \dots X_{(a_2,a_1)},$$

$l \in 1, \dots, n$. Заметим, что в таком слове в 1-ом столбце, l-ой строке находится единица, а в k-ой строке единица всё время находится на месте $a_{2,l}$. Поскольку вершина $a_1 = a_{1,l} = 1$ висячая, то для всех $l \in 1, \dots, n$ индексы $a_{2,l} = 2$. Таким образом, мы составим линейную комбинацию $x'_{l,1} Z_{l,1}$, после вычитания которой из матрицы X_0 мы получим такую матрицу X_1, что в 1-ой строке элементы всех столбцов, кроме 1-го, равны нулю; в 1-ом столбце осталось, возможно, лишь 2 ненулевых элемента. В силу полумагичности матрицы указанный выше второй элемент обязан быть нулевым.

II. Число 1 встречалось в единственной транспозиции $(1, 2) \in T$. Рассмотрим множество транспозиций $T_1 = T \setminus \{(1, 2)\}$, все транспозиции из T_1 являются подстановками на множестве $\{2, \dots, \dots, n\}$ мощности $n - 1$. Граф G', соответствующий T_1, получен из графа G удалением вершины 1 и ребра 1–2. Диаметр G' не превосходит диаметра G. T_1 является минимальным порождающим множеством в S_{n-1} (считаем S_{n-1} группой подстановок на множестве $2, \dots, n$). Подматрицы $X_1[2, \dots, n|2, \dots, n]$ и $X_{(i,j)}[2, \dots, n|2, \dots, n]$ матрицы X_1 и всех матриц $X_{(i,j)} \in \mathcal{T}_1$ соответственно, полученные вычеркиванием 1-ой строки и 1-го столбца, являются полумагическими матрицами порядка $n - 1$ (в силу указанного в п. 2 выше). По предположению индукции существует матрица V, являющаяся линейной комбинацией слов длин не больших $l(G')$ от элементов $X_{(i,j)}[2, \dots, n|2, \dots, n], (i, j) \in T_1$, такая, что $X_1[2, \dots, n|2, \dots, n] = V$. Возьмем матрицу $W = (w_{ij}) \in \mathcal{L}_{l(G')}(\mathcal{T}_1)$, являющуюся прообразом V. Тогда по построению для всех

$1 \leqslant j \leqslant n$ имеем $w_{1,j} = w_{j,1} = 0$. Матрица $X_1 - W = \alpha E_{1,1}$ является полумагической, поэтому $\alpha = 0$. Следовательно, $X_1 = W$, откуда $X = W + \sum\limits_{j=1}^{n}(x_{1,j}Y_{1,j} + x'_{j,1}Z_{j,1}) \in \mathcal{L}_{l(G)}(\mathcal{T})$.

Нижняя оценка доказывается аналогично первому пункту леммы 3.6. Рассмотрим вершины i и j, расстояние между которыми равно диаметру графа. Рассмотрим произвольную полумагическую матрицу E' такую, что её (i,j)-ый элемент равен единице. Разложим E' в линейную комбинацию слов $\mathcal{T}$: $E' = c_1V_1 + \dots + c_tV_t$, где $c_i \in \mathbb{F}\backslash\{0\}$, $V_i \in \mathcal{T}^r$ – несократимое слово, $i = 1, \dots, t$. Среди слов, в комбинацию которых мы разложили E', есть слово с единицей на (i,j)-ой позиции. Пусть оно имеет вид $V = X_{(p_1,q_1)} \cdots X_{(p_s,q_s)}$. Покажем, что его длина не меньше расстояния от вершины i до вершины j. Докажем это по индукции.

База индукции. Пусть расстояние от i до j равно 1, т.е. $i \neq j$. Значит, искомое слово имеет длину хотя бы 1.

Шаг индукции. Пусть расстояние от i до j равно d, а для меньших расстояний утверждение верно. Рассмотрим максимальное $k \in \mathbb{N}$ такое, что $p_k = j$ или $q_k = j$. Пусть $p_k = j$. Тогда в матрице $V' = X_{(p_1,q_1)} \cdots X_{(p_k,q_k)}$ на позиции (i,j) стоит единица, а вершины $j = p_k$ и q_k являются смежными. Значит, расстояние от вершины i до вершины q_k больше либо равно $d-1$. А поскольку в матрице $V'' = X_{(p_1,q_1)} \cdots X_{(p_{k-1},q_{k-1})}$ единица стоит на позиции (i,k), то по предположению индукции длина слова V'' больше либо равна $d-1$. Так как $V' = V''X_{(p_k,q_k)}$, то длина V' больше либо равна d. Следовательно, длина V тоже больше либо равна d. Шаг индукции доказан. □

§5. Вычисление длин алгебр полумагических матриц малых порядков

Приведем точные вычисления длин алгебр полумагических матриц порядков 2–4 над произвольным полем.

Лемма 5.1. *Пусть $\mathbb{F}$ – произвольное поле, тогда $l(SMag(2)) = 1$.*

Доказательство. 1. Имеем $\dim(SMag(2)) = 2$. Воспользуемся тривиальной верхней оценкой длины и получим

$$l(SMag(2)) \leqslant \dim(SMag(2)) - 1 = 1.$$

2. С другой стороны, алгебра $SMag(2)$ не изоморфна основному полю $\mathbb{F}$, поэтому $l(SMag(2)) \geqslant 1$. □

Лемма 5.2. *Пусть $\mathbb{F}$ – произвольное поле, тогда $l(SMag(3)) = 2$.*

Доказательство. 1. Чтобы доказать верхнюю оценку $l(SMag(3)) \leqslant 2$, воспользуемся [7, лемма 5.62], которая утверждает, что для произвольной алгебры $\mathcal{A}$ с единицей над любым полем, удовлетворяющей условиям $\dim \mathcal{A} = 5$ и $m(\mathcal{A}) = 3$, выполнена оценка $l(\mathcal{A}) \leqslant 2$.

Действительно, алгебра $SMag(3)$ содержит единицу (единичную матрицу), как было показано выше, $\dim SMag(3) = 5$ и $m(SMag(3)) = 3$, значит, $l(SMag(3)) \leqslant 2$.

2. Нижняя оценка $l(SMag(3)) \geqslant 2$ выполнена в силу леммы 3.6. □

Насколько же точна нижняя оценка $l(SMag(n)) \geqslant 2n-4$? Покажем, что в случае, когда характеристика поля не делит порядок матриц, к нижней оценке $2n-4$ можно прийти из других соображений.

Теорема 5.3. *Пусть $n \in \mathbb{N}$.*

1. *Пусть $n \geqslant 2$. Если $\mathbb{F}$ — поле характеристики 0 или взаимно простой с n, то*

$$2n-4 \leqslant l(M_{n-1}(\mathbb{F})) \leqslant l(SMag(n)) \leqslant l(M_{n-1}(\mathbb{F})) + 1.$$

2. *Пусть $n \geqslant 3$. Если характеристика поля $\mathbb{F}$ делит n, то*

$$l(M_{n-2}(\mathbb{F})) \leqslant l(SMag(n)) \leqslant l(M_{n-2}(\mathbb{F})) + 2.$$

Доказательство. Оценка $l(M_n(\mathbb{F})) \geqslant 2n-2$ достигается, например, на системе порождающих, состоящей из матриц X_{σ_n} и $E_{1,2}$.

1. В [8, теорема 2] показано, что в том случае, когда характеристика поля $\mathbb{F}$ не делит n, алгебра $SMag(n)$ является полупростой и изоморфна алгебре $M_{n-1}(\mathbb{F}) \oplus \mathbb{F}$. Применяем оценки из теоремы 1.14 о длине прямой суммы алгебр:

$$l(M_{n-1}(\mathbb{F})) = \max\{l(M_{n-1}(\mathbb{F})), l(\mathbb{F})\} \leqslant l(SMag(n))$$
$$l(SMag(n)) \leqslant l(M_{n-1}(\mathbb{F})) + l(\mathbb{F}) + 1 = l(M_{n-1}(\mathbb{F})) + 1.$$

2. В [8, Теорема 3] показано, что в случае, когда характеристика поля $\mathbb{F}$ делит n, алгебра $SMag(n)$ сопряжена с блочно-треугольной матричной подалгеброй, на диагонали у которой стоят три блока, являющиеся полными матричными алгебрами размеров 1×1, $(n-2)\times(n-2)$ и 1×1 соответственно. Применяем оценки из следствия 1.15:

$$l(M_{n-2}(\mathbb{F})) \leqslant \max\{l(M_{n-2}(\mathbb{F})), l(\mathbb{F})\} \leqslant l(SMag(n))$$
$$l(SMag(n)) \leqslant l(M_{n-2}(\mathbb{F})) + l(\mathbb{F}) + l(\mathbb{F}) + 2 = l(M_{n-2}(\mathbb{F})) + 2.$$

□

Перейдем к рассмотрению случая $n = 4$.

Теорема 5.4. *Пусть* $\mathbb{F}$ *– произвольное поле. Тогда* $l(M_3(\mathbb{F}) \oplus \mathbb{F}) = 4$.

Доказательство. I. Имеем $l(M_3(\mathbb{F})) = 4$ (см., например, [7, лемма 5.55]), поэтому неравенство $l(M_3(\mathbb{F}) \oplus \mathbb{F}) \geqslant 4$ следует из теоремы 1.14.

II. Докажем верхнюю оценку $l(M_3(\mathbb{F}) \oplus \mathbb{F}) \leqslant 4$. Для этого рассмотрим произвольную систему порождающих $\mathcal{S}$ для алгебры $M_3(\mathbb{F}) \oplus \mathbb{F}$ и покажем, что $l(\mathcal{S}) \leqslant 4$.

1. Пусть существует элемент $A = (A_0, a) \in \mathcal{L}_1(\mathcal{S})$, такой, что $\chi_{A_0}(a) = b \neq 0$, где $\chi_{A_0}(t)$ обозначает характеристический многочлен матрицы A_0. В этом случае, $(O_3, 1) = b^{-1}\chi_{A_0}(A) \in \mathcal{L}_3(\mathcal{S})$. При этом из равенства $l(M_3(\mathbb{F})) = 4$ следует, что $(E_{i,j}, a_{i,j}) \in \mathcal{L}_4(\mathcal{S})$ для всех $i, j = 1, 2, 3$. Значит, $\mathcal{L}_4(\mathcal{S}) = M_3(\mathbb{F}) \oplus \mathbb{F}$ и $l(\mathcal{S}) \leqslant 4$.

2. Далее будем предполагать, что для любого элемента $A = (A_0, a) \in \mathcal{L}_1(\mathcal{S})$ выполнено $\chi_{A_0}(a) = 0$. Это, в частности, означает, что

$$m(\mathcal{L}_1(\mathcal{S})) \leqslant 3.$$

Заметим, что $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 3$.

i. Пусть $\dim \mathcal{L}_1(\mathcal{S}) \geqslant 4$. Предположим, что существует несократимое слово длины 5, и приведем это утверждение к противоречию. Как и в пунктах I–II доказательства [7, лемма 5.55], получаем, что любое из равенств $\dim \mathcal{L}_i(\mathcal{S}) - \dim \mathcal{L}_{i-1}(\mathcal{S}) = 1$, $i = 2, 3, 4$, противоречит несократимости слова длины 5. Значит, $\dim \mathcal{L}_i(\mathcal{S}) - \dim \mathcal{L}_{i-1}(\mathcal{S}) \geqslant 2$ для всех $i = 2, 3, 4$. Тогда $\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_1(\mathcal{S}) + 3 \cdot 2 = 10 = \dim(M_3(\mathbb{F}) \oplus \mathbb{F})$, что также противоречит несократимости слова длины 5. Следовательно, $l(\mathcal{S}) \leqslant 4$.

ii. Пусть $\dim \mathcal{L}_1(\mathcal{S}) = 3$. В этом случае без ограничения общности можно считать, что $|\mathcal{S}| = 2$. Воспользуемся [10, Лемма 1], согласно которой при выполнении любого из неравенств

$$\dim \mathcal{L}_2(\mathcal{S}) - \dim \mathcal{L}_1(\mathcal{S}) \leqslant 2,$$
$$\dim \mathcal{L}_3(\mathcal{S}) - \dim \mathcal{L}_2(\mathcal{S}) \leqslant 2,$$
$$\dim \mathcal{L}_4(\mathcal{S}) - \dim \mathcal{L}_3(\mathcal{S}) \leqslant 1$$

выполнено неравенство $l(\mathcal{S}) \leqslant 4$.

Если ни одно из трёх приведенных неравенств не выполнено, то

$$\dim \mathcal{L}_4(\mathcal{S}) \geqslant \dim \mathcal{L}_3(\mathcal{S}) + 2 \geqslant \dim \mathcal{L}_2(\mathcal{S}) + 5$$
$$> \dim \mathcal{L}_1(\mathcal{S}) + 7 = 10 = \dim(M_3(\mathbb{F}) \oplus \mathbb{F}),$$

что невозможно. □

Следствие 5.5. *Пусть $\mathbb{F}$ – произвольное поле. Тогда*

$$l(SMag(4)) = 4.$$

Доказательство. Результат следует из теорем 3.10, 5.3 и 5.4. □

§6. Гипотезы

Замечание 6.1. Как было показано выше, справедливы следующие оценки для длины алгебры полумагических матриц:

$$l(M_{n-1}(\mathbb{F})) \leqslant l(SMag(n)) \leqslant l(M_{n-1}(\mathbb{F})) + 1,$$

если характеристика поля равна 0 или взаимно проста с n, и

$$l(M_{n-2}(\mathbb{F})) \leqslant l(SMag(n)) \leqslant l(M_{n-2}(\mathbb{F})) + 2,$$

если характеристика поля делит n.

Таким образом, гипотеза о линейности длины алгебры квадратных матриц эквивалентна гипотезе о линейности длины алгебры полумагических матриц.

Гипотеза 6.2. *Пусть $\mathbb{F}$ – произвольное поле, $n \in \mathbb{N}$, $n \geqslant 3$. Тогда $l(SMag(n)) = 2n - 4$.*

Как было показано в работе, эта гипотеза верна при $n = 3, 4$.

Гипотеза 6.3. *Пусть $\mathbb{F}$ – произвольное поле, $n \in \mathbb{N}$, $n \geqslant 2$. Тогда $l(M_n(\mathbb{F}) \oplus \mathbb{F}) = l(M_n(\mathbb{F}))$.*

Данная гипотеза верна для $n = 2, 3$ согласно [7, лемма 3.17] и теореме 5.4.

Благодарность. Идея этой статьи родилась, когда первый автор предложил задачу No. 3 (2008 г.) на ежегодной алгебраической олимпиаде, которая проходит на мехмате МГУ имени М. В. Ломоносова. Авторы выражают благодарность организаторам и участникам этой олимпиады, а также всем сотрудникам кафедры Высшей Алгебры, за интерес и внимание к задаче, который послужил основным стимулом дальнейших исследований.

Литература

1. И. В. Аржанцев, В. В. Батырев, Е. И. Бунина, Е. С. Голод, А. Э. Гутерман, М. В. Зайцев, А. И. Зобнин, А. А. Клячко, В. Т. Марков, А. А. Нечаев, Ю. А. Ольшанский, Е. А. Поршнев, Ю. Г. Прохоров. Студенческие олимпиады по алгебре на мехмате МГУ, МЦНМО, М., 2012.
2. A. Van Den Essen, *Magic squares and linear algebra.* — Amer. Math. Monthly **97**, No. 1 (1990), 60–62.
3. Ch. Godsil, G. Royle, *Algebraic Graph Theory.* Springer-Verlag, New York, 2004.
4. A. E. Guterman, O. V. Markova, *Commutative matrix subalgebras and length function.* — Linear Algebra Appl. **430** (2009), 1790–1805.
5. Ф. Харари, *Теория графов.* Мир, М., 1973.
6. О. В. Маркова, *О длине алгебры верхнетреугольных матриц.* — Усп. матем. наук **60**, No. 3 (2005), 177–178.
7. О. В. Маркова, *Функция длины и матричные алгебры.* — Фундам прикл. матем. **17**, вып. 6 (2012), 65–173.
8. I. Murase, *Semimagic squares and non-semisimple algebras.* — Amer. Math. Monthly **64**, No. 3 (1957), 168–173.
9. C. J. Pappacena, *An upper bound for the length of a finite-dimensional algebra.* — J. Algebra **197** (1997), 535–545.
10. A. Paz, *An application of the Cayley-Hamilton theorem to matrix polynomials in several variables.* — Linear Multilinear Algebra **15** (1984), 161–170.
11. L. M. Weiner, *The algebra of semimagic squares.* — Amer. Math. Monthly **62**, No. 4 (1955), 237–239.

Guterman A. E., Markova O. V., Sochnev S. D. Algebra of semimagic matrices and its length.

A matrix is called semimagic if all its row and column sums are equal. The length of the algebra of semimagic matrices with respect to different generating systems is investigated.

Московский государственный университет
имени М. В. Ломоносова
Москва, Россия
E-mail: `guterman@list.ru`

Поступило 11 ноября 2013 г.