

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/9/1

УДК 519.142

О ГРУППАХ АВТОМОРФИЗМОВ МАТРИЦ

В. Н. Егоров

*Московский государственный университет им. М. В. Ломоносова,
Институт проблем информационной безопасности, г. Москва, Россия*

E-mail: Egorov49@inbox.ru

В работе рассматриваются группы левых (правых) автоморфизмов матриц, а также группы автоморфизмов. Вид элементов матрицы не играет роли, поэтому рассматриваются квадратные матрицы над кольцом целых чисел. Вводится понятие квазиавтоморфизма матрицы и соответственно понятие группы квазиавтоморфизмов. Дано описание дважды транзитивных групп левых (правых) автоморфизмов в терминах блок-схем. Структурная теория циклических блок-схем использована для вычисления групп левых (правых) автоморфизмов и групп квазиавтоморфизмов циркулянтов. Прикладное значение этой задачи связано с описанием групп автоморфизмов графов и проблемой изоморфизма графов, а также с вопросами групповой эквивалентности дискретных функций.

Ключевые слова: группы автоморфизмов матриц, группы квазиавтоморфизмов матриц, циркулянты, блок-схемы.

Введение

При изучении свойств симметрии различных комбинаторных объектов — матриц, графов, блок-схем, дискретных функций и т. д. — естественным образом возникает понятие автоморфизма данного объекта и соответственно группы автоморфизмов. Вместе с тем оказывается, что для всех этих объектов существует удобное обобщение, а именно — группы автоморфизмов матриц.

При этом вводится понятие левых (правых) автоморфизмов. Кроме того, в работе [1] было введено понятие квазиавтоморфизма матрицы и соответственно группы квазиавтоморфизмов. Оно играет важную роль, например, при описании импримитивных групп автоморфизмов графов, в частности циркулянтов.

В данной работе рассматриваются группы левых (правых) автоморфизмов, а также группы автоморфизмов и группы квазиавтоморфизмов матриц. Учитывая, что при этом вид элементов матриц не играет роли, рассматриваются квадратные матрицы над кольцом целых чисел.

В п. 1 приводятся основные определения и обозначения. В п. 2 дано описание матриц, обладающих 2-транзитивными группами левых (правых) автоморфизмов, с помощью матриц инцидентий симметричных блок-схем. Получено описание циркулянтов размера $n \times n$ при простом $n \leq 97$ с 2-транзитивной группой левых (правых) автоморфизмов.

В п. 3 изучаются группы квазиавтоморфизмов матриц. Известно [2], что группа автоморфизмов матрицы A является 2-транзитивной тогда и только тогда, когда она

совпадает с симметрической группой S_n . В то же время известны примеры таких матриц A , что группа левых (правых) автоморфизмов является 2-транзитивной, но не совпадает с S_n . В теореме 5 доказано, что если n четно или свободно от квадратов и при этом группа квазиавтоморфизмов циркулянта 2-транзитивна, то она совпадает с S_n , а циркулянт имеет простой вид.

1. Основные определения и обозначения

Обозначим: $\mathbb{N}$ — множество натуральных чисел; $\mathbb{Z}$ — множество целых чисел; (n, m) — наибольший общий делитель чисел n и m ; $M_n(\mathbb{Z})$ — множество целочисленных матриц размера $n \times n$; $(0)_n$, I_n , J_n — соответственно нулевая, единичная матрица и матрица из единиц; $|A|$ — определитель матрицы A ; A^t — транспонированная матрица; S_n — симметрическая группа подстановок множества вычетов по модулю n ; $g(i)$ и $g(M)$ — соответственно образы элемента $i \in \mathbb{Z}/n\mathbb{Z}$ и подмножества $M \subseteq \mathbb{Z}/n\mathbb{Z}$ под действием подстановки $g \in S_n$; $\hat{g}$ — подстановочная матрица, соответствующая подстановке $g \in S_n$; $\text{Aff}(n)$ — аффинная группа подстановок, т.е. множество таких подстановок g , что $g(i) \equiv (\delta i + \nu) \pmod{n}$, где $i, \delta, \nu \in \mathbb{Z}/n\mathbb{Z}$, причем $(\delta, n) = 1$; G_i — стабилизатор точки i в группе $G \subseteq S_n$.

Определение 1. Пусть $A \in M_n(\mathbb{Z})$, $x, y \in S_n$ и выполняется матричное равенство

$$\hat{x}A = A\hat{y}. \quad (1)$$

Тогда подстановки x и y называются соответственно *левым* и *правым автоморфизмами* матрицы A . Множество $LG(A)$ всех левых автоморфизмов, очевидно, образует группу. Аналогично определяется группа $RG(A)$ всех правых автоморфизмов матрицы A . Если выполняется равенство

$$\hat{x}A = A\hat{x}, \quad (2)$$

то подстановка называется *автоморфизмом* матрицы A . Группу автоморфизмов матрицы A будем обозначать $G(A)$. Матрицы A и B называются эквивалентными, если существуют такие $x, y \in S_n$, что $\hat{x}A = B\hat{y}$.

Все перечисленные группы неоднократно рассматривались ранее (см., например, [1–7]). Заметим, что для произвольной матрицы $A \in M_n(\mathbb{Z})$ всегда существует матрица $A' \in M_n(\mathbb{Z})$ с неотрицательными элементами, такая, что все перечисленные группы идентичны для матриц A и A' . В силу сделанного замечания далее будем рассматривать матрицы с неотрицательными элементами. Отметим некоторые простые, но важные соотношения, непосредственно вытекающие из (1) и (2):

$$G(A) \subseteq LG(A) \cap RG(A); \quad (3.1)$$

$$LG(A) \subseteq G(AA^t); \quad RG(A) \subseteq G(A^tA); \quad (3.2)$$

$$RG(A) = LG(A^t). \quad (3.3)$$

Включения (3.1) и (3.3) очевидны. Для доказательства (3.2) заметим, что если $\hat{x}A = A\hat{y}$, то $\hat{x}^{-1}A\hat{y} = A$. Транспонируя, получим $A^t = \hat{y}^{-1}A^t\hat{x}$, следовательно, $\hat{x}^{-1}AA^t\hat{x} = AA^t$ или $\hat{x}AA^t = AA^t\hat{x}$.

Хорошо известно [2], что если $A \in M_n(\mathbb{Z})$ и $G(A)$ является 2-транзитивной группой, то

$$A = a_1 I_n + a_2 J_n, \quad a_1, a_2 \in \mathbb{Z},$$

и поэтому $G(A) = S_n$. Задача же описания матриц, обладающих 2-транзитивными группами левых (правых) автоморфизмов, представляется гораздо более сложной и в настоящее время далека от завершения. Интересные и глубокие результаты в этом направлении получены Фейтом [4, 5], который рассматривал блок-схемы с 2-транзитивными группами автоморфизмов.

Приведем формулировку теоремы, принадлежащей Бернсайд [8, с. 29], которая потребуется в дальнейшем.

Теорема 1. Пусть p — простое, а $G \subset S_p$ — транзитивная группа подстановок. Тогда G либо 2-транзитивна, либо изоморфна некоторой собственной подгруппе $\text{Aff}(p)$.

2. 2-транзитивные группы автоморфизмов

Покажем, что любая матрица $A \in M_n(\mathbb{Z})$, обладающая 2-транзитивной группой левых автоморфизмов, может быть представлена через матрицу инцидентий некоторой симметричной блок-схемы, за исключением вырожденного случая, когда все строки матрицы равны между собой. Предварительно докажем вспомогательное утверждение.

Лемма 1. Пусть A, B — ненулевые $(0,1)$ -матрицы из $M_n(\mathbb{Z})$, такие, что

$$A^t A = a_1 I_n + a_2 J_n, \quad a_1 \neq 0; \quad (4)$$

$$B A^t = b_1 I_n + b_2 J_n, \quad (5)$$

тогда $A^t A = A A^t$ и $B \in \{A, J_n - A, J_n\}$.

Доказательство. Умножая обе части равенства (5) справа на A , получим

$$B A^t A = b_1 A + b_2 J_n A.$$

Отсюда, учитывая (4), имеем

$$a_1 B + a_2 B J_n = b_1 A + b_2 J_n A. \quad (6)$$

Покажем, что $J_n A = \mu_1 J_n$, а $B J_n = \mu_2 J_n$. Действительно, из (4) вытекает, что число единиц в i -й строке матрицы A^t постоянно и равно $a_1 + a_2$, следовательно, то же самое верно и для столбцов матрицы A , поэтому $J_n A = \mu_1 J_n$, где $\mu_1 = a_1 + a_2$. Далее, умножая обе части равенства (5) справа на J_n , получим

$$B A^t J_n = b_1 J_n + b_2 J_n^2 = (b_1 + n b_2) J_n.$$

Но $A^t J_n = (J_n A)^t = \mu_1 J_n$, поэтому

$$(a_1 + a_2) B J_n = (b_1 + n b_2) J_n,$$

т. е. $B J_n = \mu_2 J_n$, где $\mu_2 = (b_1 + n b_2) / (a_1 + a_2)$.

Теперь равенство (6) можно переписать в виде

$$b_1 A - a_1 B = \mu_3 J_n. \quad (7)$$

Пусть $b_1 = 0$, тогда $a_1 B = -\mu_3 J_n$, а $a_1 \neq 0$, следовательно, $B = (-\mu_3 / a_1) J_n = J_n$, поскольку B — ненулевая $(0,1)$ -матрица.

Пусть $b_1 \neq 0$. Рассмотрим матрицы $A \vee B$, $A \& B$ (дизъюнкция и конъюнкция берутся поэлементно). Из (7) непосредственно следует, что если $\mu_3 = 0$, то $A = B$. Рассмотрим поэтому случай $\mu_3 \neq 0$. Из (7) получаем $A \vee B = J_n$. Если $A \& B = (0)_n$, то, очевидно, $B = J_n - A$. Если же $A \& B \neq (0)_n$ и $A \neq B$, то из (7) можно заключить, что должно выполняться одно из равенств $b_1 = \mu_3$ или $-a_1 = \mu_3$, причем $b_1 - a_1 = \mu_3$. Однако это при $a_1 \neq 0$, $b_1 \neq 0$ невозможно. ■

Теорема 2. Пусть $A \in M_n(\mathbb{Z})$ и $LG(A)$ — 2-транзитивная группа подстановок. Тогда либо

$$A = a_1 V_n + a_2 J_n, \quad a_1 \neq 0,$$

где V_n — матрица инцидентий симметричной блок-схемы и $LG(A) = LG(V_n)$, либо все строки матрицы A равны и $LG(A) = S_n$.

Доказательство. Пусть матрица A содержит равные строки, тогда в силу 2-транзитивности $LG(A)$ пара равных строк w_1 и w_2 может быть с помощью подстановок из $RG(A)$ преобразована в любую пару строк матрицы A . Отсюда непосредственно следует, что все строки матрицы A попарно равны и поэтому $LG(A) = S_n$.

Пусть все строки матрицы A попарно различны. Не теряя общности, можно считать, что все элементы матрицы A являются ненулевыми, в противном случае вместо A можно рассмотреть матрицу $\tilde{A} = A + cJ_n, c \neq 0$, поскольку очевидно, что $LG(A) = LG(\tilde{A})$.

Обозначим через ν число различных элементов матрицы A . Тогда матрицу A можно представить в виде

$$A = a_1 A_1 + a_2 A_2 + \dots + a_\nu A_\nu, \quad (8)$$

где A_i — (0,1) матрица, $a_i \neq a_j \neq 0$, $A_i A_j = (0)_n$ при $i \neq j$, $i, j = 1, \dots, \nu$. Заметим сразу, что из (8) следует $LG(A) \subseteq G(A_i A_j^t)$, $i, j = 1, \dots, \nu$. Отсюда, в частности, получаем $A_i J_n = r_i J_n$, поскольку в силу транзитивности группы $LG(A)$, а следовательно и группы $LG(A_i)$, количество единиц в строках матрицы A_i постоянно. Кроме того, $LG(A) \subseteq G(A_i A_j^t)$, $i, j = 1, \dots, \nu$. Доказательство этого факта аналогично доказательству включения (3.2). Таким образом, группы $G(A_i A_j^t)$ являются 2-транзитивными, и поэтому для некоторых $r_i, k_{ij}, \lambda_{ij}$ имеют место равенства

$$A_i A_j^t = (k_{ij} - \lambda_{ij}) I_n + \lambda_{ij} J_n, \quad (9)$$

$$A_i J_n = r_i J_n.$$

При $i = j$ из (9) получаем

$$A_i A_i^t = (r_i - s_i) I_n + s_i J_n,$$

где $s_i = \lambda_{ii}$. Поскольку матрица A не содержит равных строк, существует такое $1 \leq i \leq \nu$, что $r_i - s_i \neq 0$, откуда следует, что

$$|A_i A_i^t| = (r_i + s_i(n-1))(r_i - s_i)^{n-1} \neq 0.$$

Но тогда и $|A_i| \neq 0$, поэтому [9, стр. 146]

$$A_i A_i^t = A_i^t A_i.$$

На основании последнего равенства, пользуясь (9), можно заключить, что при сделанных предположениях в (8) найдутся матрицы A_i и A_j , удовлетворяющие условиям леммы 1, такие, что $A_i A_j = (0)_n$. Но тогда в силу леммы 1 $A_j = J_n - A_i$, т. е. $A_i \vee A_j = J_n$ и матрицу A можно представить в виде $A = a_1 V_n + a_2 J_n$, где V_n — (0,1)-матрица, $a_1 \neq 0$. Кроме того, как уже было отмечено выше, матрица A должна удовлетворять соотношениям

$$AA^t = a'_1 I_n + a'_2 J_n, \quad AJ_n = (a'_1 + a'_2) J_n.$$

Отсюда нетрудно показать, что матрица V_n должна удовлетворять соотношениям

$$V_n V_n^t = (k - \lambda)I_n + \lambda J_n, \quad V_n J_n = k J_n.$$

В этом случае [9, теорема 10.2.3] V_n есть матрица инцидентий симметричной блок-схемы с параметрами n, k, λ , удовлетворяющими соотношению

$$k(k - 1) = \lambda(n - 1). \quad (10)$$

Равенство $LG(A) = LG(V_n)$ выполняется в силу того, что $J_n \hat{x} = \hat{y} J_n$ для любых $x, y \in S_n$. ■

Полученное условие является необходимым условием 2-транзитивности группы левых автоморфизмов. Что же касается достаточного условия, то эта задача представляется гораздо более сложной, поскольку в настоящее время полностью не решен вопрос даже о существовании нетривиальных симметричных блок-схем, т. е. блок-схем, для которых $k - \lambda \notin \{0, 1\}$. Наиболее важная теорема существования нетривиальных симметричных блок-схем принадлежит Бруку, Райзеру и Човла. Приведем её формулировку.

Теорема 3 [9, теорема 10.3.1]. Для существования нетривиальной симметричной (n, k, λ) -блок-схемы необходимы условия:

- если n чётно, то $k - \lambda = x^2$, $x \in \mathbb{N}$;
- если n нечётно, то существуют целые x, y, z , не все равные 0, удовлетворяющие уравнению

$$x = (k - \lambda)y + (-1)^{\frac{n-1}{2}} \lambda z^2.$$

Сейчас сформулируем и докажем теорему, анонсированную в [1], которая является дополнением к теореме 3.

Теорема 4. При $n = 2p, 2p^2, 4p, p^m + 1$, где p — простое число, существуют только тривиальные блок-схемы.

Доказательство. Пусть параметры n, k, λ удовлетворяют (10). Не теряя общности, можно положить $k \leq [n/2]$, поскольку всегда можно перейти к блок-схеме — дополнению. Кроме того, будем считать $\lambda \neq 0$, иначе из (10) следует $k - \lambda \in \{0, 1\}$. Разберем случаи.

a) $n = p^m + 1$.

Из (10) следует, что $k(k - 1) = \lambda p$. Поскольку $(k, k - 1) = 1$, то либо $p^m | (k - 1)$, либо $p^m | k$, и $k \leq p^m$ при $\lambda \neq 0$, т. е. $k \geq n - 1$, а это противоречит предположению, что $k \leq [n/2]$.

С помощью (10) нетрудно показать, что при $n = 2, 8$ существуют только тривиальные симметричные блок-схемы, поэтому будем предполагать, что p — нечётное простое число.

b) $n = 2p$.

Перепишем (10) в виде

$$k^2 - (k - \lambda) = \lambda n. \quad (11)$$

По теореме 2 имеем $k - \lambda = x^2$, где $x \in \mathbb{N}$. Из (11) получим $k^2 - x^2 = (k - x)(k + x) = 2\lambda p$. Если $x \neq 0$, то отсюда получаем $k - x < p$ и $k + x < 2p$. Но тогда $k + x = p$, поскольку p — простое, а $(k - x)(k + x)$ делится на p . Отсюда $k - x = 2\lambda$. Однако из равенств $k - x = 2\lambda$, $k + x = p$ следует $2k = 2\lambda + p$, что невозможно, поскольку p — нечётное.

c) $n = 2p^2$.

В этом случае имеем равенства $k - \lambda = x^2$ и $(k - x)(k + x) = 2\lambda p^2$. Как и выше, $k - x < p^2$, $k + x < 2p^2$. Предположим, что $k + x$ делится на p^2 , тогда $k + x = p^2$. Отсюда $k - x = 2\lambda$, $k + x = p^2$, т. е. $2k = 2\lambda + p^2$, что невозможно, поскольку p^2 — нечётное. Остаётся рассмотреть случай $k - x = \mu_1 p$, $k + x = \mu_2 p$. При этом k и x делятся на p , следовательно, λ также делится на p . Однако $2\lambda = \mu_1 \mu_2$, а $(\mu_1 \mu_2, p) = 1$. Противоречие.

d) $n = 4p$.

Аналогично «b» и «c» $k - \lambda = x^2$, $(k - x)(k + x) = 4\lambda p$, $k - x < 2p$. Пусть $k - x$ делится на p , тогда $k - x = p$, $k + x = 4\lambda$. В этом случае $2k = 4\lambda + p$, что невозможно, поскольку p — нечётное. Пусть $k + x$ делится на p . Предположим, что $k + x = sp$, где s — нечётное. Тогда $k - x = r$ — чётное число, следовательно, $2k = r + sp$, что невозможно, так как $r + sp$ — нечётное число. Остаётся рассмотреть случай $k + x = 2p$. При этом $k - x = 2\lambda$, т. е. $k - \lambda = \lambda + x = x^2$. Отсюда $\lambda = x^2 - x$ и $k - x(x - 1) = x^2$ или $k + x = 2x^2$. Последнее равенство, однако, противоречит тому, что $k + x = 2p$, где p — простое. ■

Из теорем 2, 3 и 4 получаем

Следствие 1. Пусть $A \in M_n(\mathbb{Z})$, $n = 2p, 2p^2, 4p, p^m + 1$ или противоречит условиям теоремы 3 и пусть $LG(A)$ — 2-транзитивная группа подстановок. Тогда $A = a_1 \hat{g} + a_2 J_n$, $g \in S_n$ и $LG(A) = S_n$.

Доказательство. Действительно, по теореме 2 $A = a'_1 V_n + a'_2 J_n$, где V_n — матрица симметричной блок-схемы. По теоремам 3 и 4, в свою очередь, $V_n = v_1 \hat{g} + v_2 J_n$, где $\hat{g}$ — подстановочная матрица. Тогда $A = a'_1 v_1 \hat{g} + (a'_2 + v_2) J_n$ и $LG(A) = LG(\hat{g}) = S_n$. ■

Приведём важный результат, принадлежащий Фейту, относительно *циклических блок-схем*. Это симметричные блок-схемы, матрицы инцидентий которых являются *циркулянтами*, т. е. имеют вид

$$\begin{bmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_0 \end{bmatrix}. \quad (12)$$

В дальнейшем множество циркулянтов размерности $n \times n$ с элементами из $\mathbb{Z}$ будем обозначать $CM_n(\mathbb{Z})$.

В нашей терминологии изоморфизм блок-схем означает эквивалентность матриц инцидентий, а группа автоморфизмов блок-схемы есть группа левых автоморфизмов матрицы инцидентий.

Обозначим чрез $D_m(q)$ блок-схему Зингера [9, с. 179] с параметрами

$$n = (q^{m+1} - 1)/(q - 1), \quad k = (q^m - 1)/(q - 1), \quad \lambda = (q^{m-1} - 1)/(q - 1),$$

где $q = p^r$, p — простое, а через $H(11)$ — циклическую блок-схему с параметрами $(11, 5, 2)$, матрица инцидентий которой имеет вид (12) при

$$n = 11, \quad c_0 = c_1 = c_2 = c_4 = c_7 = 1, \quad c_3 = c_5 = c_6 = c_8 = c_9 = c_{10} = 0.$$

Теорема 5 [5]. Пусть D — циклическая (n, k, λ) блок-схема с 2-транзитивной группой автоморфизмов, $k \leq 50$ и D не изоморфна $H(11)$ или $D_m(q)$ при любых m и q . Тогда (n, k, λ) есть либо $(109, 28, 7)$, либо $(133, 22, 8)$.

Сейчас на основании теоремы 5 получим описание циркулянтов из $CM_n(\mathbb{Z})$ с 2-транзитивной группой левых автоморфизмов при простом $n \leq 97$.

Таблица значений параметра n блок-схемы $D_m(q)$ при различных m и q имеет вид

	2	3	4	5	7	8	9	11
2	7	13	21	31	57	73	91	*
3	15	40	85	*	*	*	*	*
4	31	*	*	*	*	*	*	*
5	63	*	*	*	*	*	*	*
6	*	*	*	*	*	*	*	*

Значком * отмечены значения параметра n , превосходящие 97. Анализируя данную таблицу, видим, что при простом $n < 97$ либо $m = 2$, либо $m = 4$, $q = 2$. При $m = 2$ имеем $\lambda = (q - 1)/(q - 1) = 1$, а при $m = 4$ — $q = 2$ и $(n, k, \lambda) = (31, 15, 7)$, поэтому на основании теорем 2 и 5 имеет место

Следствие 2. Пусть $C \in CM_n(\mathbb{Z})$, n — простое, $n \leq 97$ и $LG(C)$ — 2-транзитивная группа подстановок. Тогда

$$C = c_1 V_n + c_2 J_n,$$

где V_n — матрица инцидентий симметричной блок-схемы с параметрами

$$(n, k, 1), \quad (11, 5, 2), \quad (31, 15, 7).$$

3. Группы квазиавтоморфизмов матриц

В [1] введена некоторая специальная подгруппа группы $LG(A)$ матрицы A , которая называется группой квазиавтоморфизмов матрицы и обозначается $Q(A)$. Группы квазиавтоморфизмов имеют ряд интересных свойств, причём в некоторых случаях строение групп $G(A)$ и $LG(A)$ матрицы A существенно зависит от строения группы квазиавтоморфизмов некоторой ее подматрицы.

Определение 2. Группой квазиавтоморфизмов матрицы $A \in M_n(\mathbb{Z})$ называется подгруппа группы $LG(A)$ вида

$$Q(A) = \{x \in LG(A) \mid \exists y \in LG(A) : \hat{x}^{-1} A \hat{y} = A\}.$$

Нетрудно видеть, что указанное множество является группой. Кроме того, очевидно, что

$$G(A) \subseteq Q(A) \subseteq LG(A).$$

Ниже будет показано, что эти включения могут быть строгими.

Лемма 2. Пусть $A \in M_n(\mathbb{Z})$, тогда $Q(A) \subseteq LG(A^2)$.

Доказательство. Пусть $x \in Q(A)$. Тогда $\hat{x}^{-1} A \hat{y} = A$, $\hat{y}^{-1} A \hat{z} = A$, где $x, y \in LG(A)$, $z \in RG(A)$. Перемножая эти равенства, получаем $\hat{x}^{-1} A^2 \hat{z} = A^2$, т.е. $x \in LG(A^2)$. ■

В п. 2 были рассмотрены условия, при которых группы $G(A)$ и $LG(A)$ являются 2-транзитивными. При этом оказывается, что обязательно $G(A) = S_n$, а относительно группы левых автоморфизмов известны примеры матриц A , таких, что $LG(A)$ 2-транзитивна, но не совпадает с S_n . Таковыми являются, например, матрицы инцидентий зингеровских блок-схем. В связи с этим представляет интерес вопрос о том,

какие 2-транзитивные группы подстановок могут встречаться среди групп $Q(A)$ и какой вид имеют соответствующие матрицы. Рассмотрим этот вопрос для циркулянтов.

Отметим некоторые простые, но важные свойства циркулянтов, которые потребуются в дальнейшем:

- 1) $\langle t_n \rangle \subseteq G(C)$;
- 2) $C^t \in CM_n(\mathbb{Z})$;
- 3) $CM_n(\mathbb{Z})$ является коммутативным кольцом;
- 4) если C — периодический циркулянт периода d , т. е. последовательность $c_0, c_1, \dots, c_{n-1}$ является периодической периода d , то C^t обладает тем же свойством;
- 5) если найдётся такая подстановка $x \in S_n, x \neq e_n$, что $\hat{x}C = C$ или $C\hat{x} = C$, то C — периодический циркулянт;
- 6) если C является матрицей инцидентий симметричной блок-схемы и $\Delta(C) = \{i | c_i = 1\}$, то $\Delta(C)$ — разностное множество.

Для доказательства п. 1–4 представим C в виде многочлена от матрицы $\hat{t}_n$ с коэффициентами из $\mathbb{Z}$, т. е.

$$C = f(\hat{t}_n), \quad (13)$$

где $f(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$. Тогда, очевидно, $t_n \in G(C)$, а

$$C^t = g(\hat{t}_n), \quad (14)$$

где $g(x) = c_0 + c_{n-1}x + \dots + c_1x^{n-1}$, что доказывает свойства 1 и 2. Свойство 3 также легко следует из (13).

Пусть $c_0, c_1, \dots, c_{n-1}$ — периодическая последовательность периода d , тогда, как нетрудно видеть, последовательность $c_0, c_{n-1}, \dots, c_1$ также обладает этим свойством. Из равенства (14) теперь следует свойство 4.

Для доказательства свойства 5 достаточно заметить, что равенство $\hat{x}C = C$ выполняется при $x \neq e_n$ в том и только в том случае, если в C имеются равные строки, что равносильно периодичности C . Аналогично при $C\hat{x} = C$ в C есть равные столбцы, т. е. в C^t есть равные строки, поэтому можно воспользоваться свойством 4.

Свойство 6 непосредственно следует из определений циркулянта, блок-схемы и разностного множества.

Теорема 6. Пусть $C \in CM_n(\mathbb{Z})$, а n чётно или свободно от квадратов, и пусть $Q(C)$ — 2-транзитивная группа подстановок. Тогда $C = c_1\hat{t}_n^s + c_2J_n$, $0 \leq s \leq n-1$, и $Q(C) = S_n$.

Предварительно докажем вспомогательное утверждение.

Лемма 3. Пусть $C \in CM_n(\mathbb{Z})$ и является $(0,1)$ -матрицей, $|\Delta(C)| = k$ и первая строка матрицы C^2 имеет вид $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$. Тогда

- а) при $n = 2m + 1$ среди элементов $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ ровно k нечётных;
- б) если, кроме того, матрица C есть матрица инцидентий симметричной блок-схемы с параметрами (n, k, λ) , то при $n = 2m$ все элементы $\alpha_0, \alpha_3, \dots, \alpha_{n-1}$ — чётные, а среди элементов $\alpha_0, \alpha_2, \dots, \alpha_{n-2}$ ровно $k - \lambda$ нечётных.

Доказательство. а) По условию леммы

$$C = \hat{t}_n^{s_1} + \hat{t}_n^{s_2} + \dots + \hat{t}_n^{s_k},$$

где $\{s_1, s_2, \dots, s_k\} = \Delta(C)$. Нетрудно видеть, что

$$C^2 = \hat{t}_n^{2s_1} + \hat{t}_n^{2s_2} + \dots + \hat{t}_n^{2s_k} + Q, \quad Q = 2 \cdot \sum_{i \neq j} \hat{t}_n^{s_i + s_j}, \quad 1 \leq i, j \leq k.$$

Матрица Q , очевидно, содержит только чётные элементы, поэтому рассмотрим матрицу

$$C' = \hat{t}_n^{2s_1} + \hat{t}_n^{2s_2} + \dots + \hat{t}_n^{2s_k}. \quad (15)$$

Если $n = 2m + 1$, то $(2, n) = 1$ и из сравнения $2s_i \equiv 2s_j \pmod{n}$ получаем $s_i \equiv s_j \pmod{n}$. Отсюда следует, что C' является $(0, 1)$ -матрицей из $CM_n(\mathbb{Z})$ и $|\Delta(C')| = k$, т. е. утверждение «а» доказано.

б) Пусть $n = 2m$ и C есть матрица инцидентий симметричной блок-схемы, а первая строка матрицы C' имеет вид $\alpha'_0, \alpha'_3, \dots, \alpha'_{n-1}$. Из (15) следует, что все элементы $\alpha'_1, \alpha'_3, \dots, \alpha'_{n-1}$ равны 0, поскольку $2s_i$ есть чётное число по модулю n , следовательно, все элементы $\alpha_1, \alpha_3, \dots, \alpha_{n-1}$ чётны. На основании свойства 6 $\Delta(C)$ является разностным множеством с параметрами (n, k, λ) . Пусть $s_i, s_j \in \Delta(C)$ и $s_i - s_j \equiv m \pmod{n}$, тогда, очевидно, $s_j - s_i \equiv -m \pmod{n} \equiv m \pmod{n}$. Из последнего соотношения следует, что λ чётно и что существует ровно $\lambda/2$ пар $\{s_\xi, s_\eta\}$, таких, что $\xi < \eta$ и $s_\xi - s_\eta \equiv m \pmod{n}$. Но тогда $2s_\xi \equiv 2s_\eta \pmod{n}$ и поэтому $\lambda/2$ элементов среди $\alpha'_0, \alpha'_2, \dots, \alpha'_{n-2}$ равны 2, $k - \lambda$ элементов равны 1, а остальные — нули. ■

Перейдём к доказательству теоремы 6.

Доказательство. По условию $Q(C)$ — 2-транзитивная группа подстановок, следовательно, $LG(C)$ также 2-транзитивна, поскольку $Q(C) \subseteq LG(C)$. Отсюда на основании теоремы 2 получаем $C = c_1\tilde{C} + c_2J_n$, где $\tilde{C}$ — матрица инцидентий симметричной блок-схемы. Поскольку $C, J_n \in CM_n(\mathbb{Z})$, то $\tilde{C}$ также лежит в $CM_n(\mathbb{Z})$ (свойство 3). Кроме того, нетрудно видеть, что $Q(C) = Q(\tilde{C})$, и если теорема верна для матрицы $\tilde{C}$, то она верна и для матрицы C и наоборот. Поэтому далее будем считать, что C — матрица инцидентий симметричной блок-схемы с параметрами (n, k, λ) .

Рассмотрим матрицу C^2 . По лемме 2 $Q(C) \subseteq LG(C^2)$, поэтому $LG(C^2)$ — 2-транзитивная группа подстановок. На основании теоремы 2 получаем $C^2 = c_1C' + c_2J_n$, где C' — матрица инцидентий симметричной блок-схемы, причём по свойству 3 $C' \in CM_n(\mathbb{Z})$.

Пусть первые строки матриц C^2 и C' имеют соответственно вид $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ и $\alpha'_0, \alpha'_1, \dots, \alpha'_{n-1}$. Рассмотрим отдельно два случая:

а) $n = 2m$.

Применяя к матрице C лемму 3, видим, что элементы $\alpha_1, \alpha_3, \dots, \alpha_{n-1}$ все чётные, а среди элементов $\alpha_0, \alpha_2, \dots, \alpha_{n-2}$ ровно $k - \lambda$ нечётных. Выбирая подходящие c_1 и c_2 , можно добиться того, что $\alpha'_i = 1$ в том и только в том случае, когда α_i — нечётный элемент. Таким образом, $\Delta(C') = \{s_1, s_2, \dots, s_{k-\lambda}\}$, где все s_i являются чётными вычетами по модулю n . При $k - \lambda > 1$ это множество, как нетрудно видеть, не может быть разностным, поскольку его элементы порождают только чётные разности, однако оно обязано им быть, так как $C' \in CM_n(\mathbb{Z})$ (свойство 6). Отсюда $k - \lambda \in \{0, 1\}$, т. е. C является матрицей инцидентий тривиальной циклической блок-схемы, и поэтому существуют такие c_1 и c_2 , что $C = c_1\hat{t}_n^s + c_2J_n$, $0 \leq s \leq n - 1$.

б) Пусть n свободно от квадратов и нечётно. Применяя к матрице C' лемму 3, получаем, что среди элементов $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ ровно k нечётных. Как и выше, можно считать, что $\alpha'_i = 1$ в том и только в том случае, если α_i — нечётный элемент. Отсюда следует, что $\Delta(C')$ есть разностное множество с параметрами (n, k, λ) . Вернёмся к равенству $C^2 = c_1C' + c_2J_n$. Поскольку все элементы матрицы C^2 неотрицательны, то $c_2 > 0$. Сравнивая модули собственных значений матриц C^2 и $c_1C' + c_2J_n$ [9, с. 145], получаем

$$k^2 = c_1k + c_2n; \quad (16.1)$$

$$k - \lambda = |c_1| \sqrt{k - \lambda}. \quad (16.2)$$

Пусть $c_1 \geq 0$. Если $c_1 = 0$, то из (16.2) следует $k - \lambda = 0$, т. е. параметры k и λ — тривиальные. Если же $c_1 > 0$, то

$$c_1 = \sqrt{k - \lambda}. \quad (17)$$

Вместе с (16.1) это даёт $k^2 = k\sqrt{k - \lambda} + c_2 n$, или

$$k(k - \sqrt{k - \lambda}) = c_2 n. \quad (18)$$

Можно считать, что $k \neq 0, k - \sqrt{k - \lambda} \neq 0$, поскольку в противном случае параметры k и λ тривиальные. Пусть $d = (k, n)$. Положим $k = dx, n = dy$. В этом случае из (10) следует, что λ делится на d . Заметим, что d свободно от квадратов, поскольку n свободно от квадратов, а $k - \lambda$ на основании (16) является полным квадратом, следовательно, $k - \lambda$ делится на d^2 . Отсюда $\sqrt{k - \lambda}$ делится на d и поэтому $k - \sqrt{k - \lambda}$ делится на d . Положим $k - \sqrt{k - \lambda} = dz$. Из (3.6) теперь имеем

$$dxdz = c_2 dy, \quad (19)$$

причём $(y, d) = 1$, поскольку n свободно от квадратов. Но тогда c_2 делится на d . Положим $c_2 = dv$. Подставляя это выражение в (19), получаем $dxdz = dvdy$, или $xz = vy$. Но $(x, y) = 1$, следовательно, v делится на x . Отсюда c_2 делится на k , т. е. $c_2 \geq k$.

Перепишем (11) в виде

$$(k - \sqrt{k - \lambda})(k + \sqrt{k - \lambda}) = \lambda n. \quad (20)$$

Сравнивая (17) и (19), видим, что $\lambda \geq c_2 \geq k$. Но, с другой стороны, из определения блок-схемы $\lambda \leq k$. Поэтому $\lambda = k$, т. е. параметры k и λ тривиальные.

Пусть $c_1 < 0$. Рассуждая аналогичным образом, получим $c_1 = -\sqrt{k - \lambda}$, $k(k + \sqrt{k - \lambda}) = c_2 n$. Применяя те же рассуждения, что и выше, получим, что c_2 делится на k . Но $k + \sqrt{k - \lambda} \leq 2k$, поэтому либо $c_2 = k$, либо $k = n$. Если $k = n$, то $\lambda = k$, т. е. параметры k и λ тривиальные, поэтому рассмотрим случай $c_2 = k$. При этом $k + \sqrt{k - \lambda} = n$, и из (20) следует $k - \sqrt{k - \lambda} = \lambda$. Но, очевидно, $k - (k - \lambda) = \lambda$, поэтому $k - \lambda = \sqrt{k - \lambda}$, а это возможно, только если $k - \lambda \in \{0, 1\}$. Таким образом, при всех случаях параметры k и λ являются тривиальными. Поэтому существуют такие c_1 и c_2 , что

$$C = c_1 \hat{t}_n^s + c_2 J_n, \quad 0 \leq s \leq n - 1,$$

и теорема доказана. ■

При простом n справедливы более общие утверждения.

Теорема 7. Пусть n — простое число, $C \in CM_n(\mathbb{Z})$ и $\text{Aff}(n) \subseteq LG(C)$. Тогда $C = c_1 \hat{t}_n^s + c_2 J_n$.

Доказательство. Пусть i — примитивный элемент поля $\mathbb{Z}/n\mathbb{Z}$, а $g \in \text{Aff}(n)$ — подстановка, соответствующая элементу i , т. е. $g(x) \equiv ix \pmod{n}$. Группа $\text{Aff}(n)$ при простом n 2-транзитивна, поэтому по теореме 2 можно считать, что C — матрица инцидентий симметричной блок-схемы, следовательно, $|C| \neq 0$ [9, с. 144]. По условию $g \in LG(C)$, т. е. $\hat{g}^{-1}C\hat{g}' = C$, причём цикловые структуры подстановок g и g' совпадают [11, с. 22]. Подстановка g в силу примитивности элемента i имеет цикловую структуру $[1^{(1)}, (n-1)^{(1)}]$. Такую же структуру имеет и подстановка g' . Из равенства $\hat{g}^{-1}C\hat{g}' = C$ получаем, что матрица C содержит столбец вида $(01\dots 1)^t$ или $(10\dots 0)^t$. ■

Теорема 8. Пусть n — простое число, $C \in CM_n(\mathbb{Z})$, $C \neq c_1 \hat{t}_n^s + c_2 J_n$. Тогда

$$Q(C) = LG(C) \cap \text{Aff}(n),$$

и либо $Q(C) = G(C)$, либо $G(C) = \langle t_n \rangle$.

Доказательство. Пусть $H = LG(C) \cap \text{Aff}(n)$, $x \in H$ и $\hat{x}^{-1}C\hat{y} = C$. Рассмотрим подстановки $z_1 = x^{-1}t_n x$ и $z_2 = y^{-1}t_n y$. Нетрудно видеть, что $\hat{z}_1^{-1}C\hat{z}_2 = C$. Но $z_1 = t_n^k$, поскольку $x \in \text{Aff}(n)$, а $\text{Aff}(n)$ является нормализатором группы $\langle t_n \rangle$. На основании свойства 5 получаем, что $y^{-1}t_n y = t_n^k$ (в противном случае матрица C имеет равные столбцы, т. е. $C = cJ_n$, так как n простое). Но тогда нетрудно показать, что $y = xt_n^m$, т. е. $y \in H$, поскольку $\langle t_n \rangle \subset H$. Отсюда по определению группы $Q(C)$ получаем $H \subset Q(C)$. С другой стороны, по теореме 6 $Q(C)$ при данных предположениях не является 2-транзитивной, поэтому по теореме 1 $Q(C) \subset \text{Aff}(n)$. Отсюда $Q(C) = H$.

Как отмечено выше, $\text{Aff}_0(n) = \langle g \rangle$, следовательно, $Q_0(C) = \langle g^k \rangle$, $G_0(C) = \langle g^{km} \rangle$ для некоторых натуральных k и m , поскольку

$$G_0(C) \subseteq Q_0(C) \subset \text{Aff}_0(n).$$

Если $m = 1$, то $g^{km} = g$, т. е. $G(C) = Q(C) = \langle t_n, g^k \rangle$. Пусть $\langle g^{km} \rangle \subset \langle g \rangle$. Имеем равенство

$$\hat{g}^{-k}C\hat{g}^k = C. \quad (21)$$

При этом, как мы уже показали выше, $g' = g^k t_n^l$. Из (21) получаем $\hat{g}^{-km}C\hat{g}^{km} = C$. Но $g^{km} \in G(C)$, поэтому $\hat{g}^{-km}C\hat{g}^{km} = C$. Сравнивая последние два равенства, по свойству 5 получаем $g'^m = g^{km}$, или $(g^k t_n^l)^m = g^{km}$. Но тогда подстановки $g^k t_n^l$ и g^{km} перестановочны, следовательно, их коммутатор $[g^k t_n^l, g^{km}]$ равен e_n . Отсюда по свойству сложных коммутаторов

$$[g^k t_n^l, g^{km}] = [g^k, g^{km}][g^k, g^{km}, t_n^l][t_n^l, g^{km}] = [t_n^l, g^{km}] = e_n.$$

Последнее равенство верно, только если $l \equiv 0 \pmod{n}$ либо $g^{km} = e_n$. В первом случае $g' = g^k$, т. е. $G_0(C) = \langle g^k \rangle$, что противоречит нашему предположению. Во втором случае $G_0(C) = \langle e_n \rangle$, т. е. $G(C) = \langle t_n \rangle$. ■

Пример 1. Пусть C — матрица инциденций зингеровской блок-схемы с параметрами $(7, 3, 1)$, т. е.

$$C = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

В этом случае $LG(C)$ 2-транзитивна, $Q(C) = \langle t_7, g^2 \rangle$, где $g(x) \equiv 3x \pmod{7}$, $G(C) = \langle t_7 \rangle$. Таким образом, $G(C) \subset Q(C) \subset LG(C)$.

ЛИТЕРАТУРА

1. Егоров В. Н., Марков А. И. О гипотезе Адама для графов с циркулянтными матрицами смежности вершин // ДАН СССР. 1979. Т. 249. № 3. С. 529–532.
2. Давыдов Э. Г. О симметрии графов // Вопросы кибернетики. М., 1973. С. 26–49.

3. *Chao C.* On groups and graphs // TMA. 1965. V. 118. No. 6. P. 488–497.
4. *Feit W.* Automorphisms of symmetric balanced incomplete block designs // Math. Z. 1970. No. 118. P. 40–49.
5. *Feit W.* On symmetric balanced incomplete block designs with doubly transitive automorphism groups // J. Combin. Theory. 1973. V. 14. No. 2. P. 221–247.
6. *Huang Q., Meng J.* On the isomorphism and automorphism groups of circulants // Graphs Combin. 1996. V. 12. P. 179–187.
7. *Тараканов В. Е.* Группы автоморфизмов циркулянтов и присоединенные матрицы графов // Математические заметки. 1999. Т. 65. Вып. 3. С. 402–411.
8. *Wielandt H.* Finite permutation groups. New York; London: Academic Press, 1964.
9. *Холл М.* Комбинаторика. М.: Мир, 1970.
10. *Adam A.* Research problem 2–10 // J. Combin. Theory. 1967. V. 2. P. 393.
11. *Dembowski P.* Finite geometries. Berlin and New York: Springer Verlag, 1968.