Math-Net.Ru

Общероссийский математический портал

В. Е. Тараканов, Группы автоморфизмов циркулянтов и присоединенные матрицы графов, *Матем. заметки*, 1999, том 65, выпуск 3, 402–411

DOI: <https://doi.org/10.4213/mzm1064>

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: 54.197.217.227

26 апреля 2023 г., 14:33:13

УДК 519.17

ГРУППЫ АВТОМОРФИЗМОВ ЦИРКУЛЯНТОВ И ПРИСОЕДИНЕННЫЕ МАТРИЦЫ ГРАФОВ

В. Е. Тараканов

С графом (или орграфом) Γ связываются две матрицы $N(A)$ и $N^{(-1)}(A)$ скалярных произведений вектор-строк (соответственно вектор-столбцов) его матрицы смежности, называемые присоединенными матрицами. Развивается подход к изучению групп автоморфизмов $\text{Aut } C_n$ циркулянтов C_n на n вершинах с помощью присоединенных матриц. Устанавливается необходимый признак изоморфизма двух циркулянтов в терминах матрицы $N(A)$ (теорема 1). С его помощью выделяются некоторые классы циркулянтов C_n с $\text{Aut } C_n$, изоморфной циклической группе и группе диэдра (теорема 2). В качестве приложения дается классификация циркулянтов C_n степени $m = 4$ и в случае простого n описание в явном виде их групп автоморфизмов (теорема 3).

Библиография: 11 названий.

Циклической матрицей (или *циркулянт*ом) называется квадратная матрица A такая, что каждая ее строка получается из предыдущей (а также первая из последней) циклическим сдвигом на одно место вправо. Ориентированный граф Γ без петель и параллельных одинаково направленных дуг, обладающий в качестве матрицы смежности циклической $(0, 1)$ -матрицей $A = A(\Gamma)$, также называется циркулянт $ом$. Множеством вершин циркулянта Γ , имеющего n вершин, будем считать множество $Z_n = \{0, 1, \dots, n-1\}$, а столбцы матрицы $A(\Gamma) = (a_{ij})$ будем нумеровать числами из Z_n . Имеем, очевидно, $a_{ii} = 0$, $i = 0, 1, \dots, n-1$. Через $r_A(i)$ (через $c_A(j)$) обозначаем i -ю вектор-строку (j -й вектор-столбец) в A , $i, j = 0, 1, \dots, n-1$. Пусть $S = \{j \in Z_n \mid a_{0j} = 1\} = \{s_1, \dots, s_m\}$. Ясно, что (i, j) – дуга в Γ тогда и только тогда, когда $j - i \equiv s \pmod{n}$ для некоторого $s \in S$. Множество S называем *порождающим множеством циркулянта* Γ . Циркулянт на n вершинах с порождающим множеством S обозначается через $C_n(S)$, а его группа автоморфизмов – $G = \text{Aut } C_n(S)$.

Вопрос об описании групп автоморфизмов циркулянтов был поставлен в начале 70-х годов [1]. С тех пор появилось немало работ, связанных с этой проблемой (см., например, [2]–[5]). Нетрудно заметить, что соответствие

$$\theta: i \mapsto i + 1 \pmod{n}, \quad i \in Z_n, \quad (1)$$

порождает автоморфизм любого циркулянта на n вершинах. Тем самым, $\text{Aut } C_n(S)$ содержит циклическую подгруппу $\langle \theta \rangle$ порядка n , порожденную соответствием (1). Обозначим через G_0 подгруппу в G , состоящую из всех автоморфизмов τ с $\tau(0) = 0$. Можно

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, грант № 96-91-00531, и программы “Ведущие научные школы”, грант № 96-15-96092.

показать (см. [6]), что $\text{Aut } C_n(S) \cong \langle \theta \rangle G_0$. Тем самым, изучение $\text{Aut } C_n(S)$ во многом сводится к изучению подгруппы G_0 .

Множество Z_n рассматриваем как кольцо (естественным образом изоморфное Z/nZ). Хорошо известно, что $\text{Aut } Z_n \cong Z_n^*$, где Z_n^* – мультипликативная группа, состоящая из всех обратимых по модулю n элементов Z_n . Пусть $\text{Aut}_S Z_n$ – это множество $\{\tau \in \text{Aut } Z_n \mid \tau(S) = S\}$, где S – порождающее множество циркулянта $C_n(S)$. Ясно, что $\text{Aut}_S Z_n \subseteq G_0$. Во многих случаях $G_0 = \text{Aut}_S Z_n$. Существовало предположение, впоследствии опровергнутое, что вообще $G_0 \cong \text{Aut}_S Z_n$ (гипотеза Адама [7]). Были выделены некоторые классы циркулянтов, для которых эта гипотеза справедлива (см. [4]). В [5] было дано описание групп автоморфизмов циркулянтов степени 3.

В настоящей работе предлагается новый подход к изучению автоморфизмов и изоморфизмов циркулянтов. Этот подход связан с критерием изоморфизма гиперграфов [8]. В применении к графам для изучения вопроса об их изоморфизме при этом подходе привлекается матрица скалярных произведений вектор-столбцов (а также соответствующая матрица для вектор-строк) матрицы смежности графа; такая матрица называется *присоединенной матрицей графа*. Для циркулянтов эта матрица имеет наиболее простой вид: она – циклическая матрица и, следовательно, вполне определяется своей начальной строкой.

Если порождающее множество $S = \{s_1, \dots, s_m\}$ циркулянта $\Gamma = C_n(S)$ имеет свойство $\text{НОД}(s_1, \dots, s_m, n) = d > 1$, то Γ не может быть сильно связным, но состоит из d компонент. В этом случае его группа автоморфизмов есть сплетение d одинаковых групп $\text{Aut } C_n(T)$, где $T = \{s_1/d, s_2/d, \dots, s_m/d\}$ (см. [9]). В связи с этим мы рассматриваем лишь сильно связные циркулянты.

Предлагаемый нами подход развивается в п. 1, где устанавливается необходимый признак изоморфизма циркулянтов в терминах присоединенных матриц (теорема 1). Ряд общих свойств автоморфизмов циркулянтов рассматривается в п. 2, где, в частности, выделяются некоторые классы циркулянтов с группами автоморфизмов, изоморфными циклической группе и группе диэдра (теорема 2). В качестве приложения полученных результатов проводится классификация циркулянтов $C_n(S)$ степени $m = 4$ и при простом n описываются в явном виде их группы автоморфизмов (теорема 3).

1. Присоединенные матрицы и признаки изоморфизма циркулянтов. Две матрицы A и B с m строками и n столбцами называются *перестановочно эквивалентными*, если существуют подстановочные матрицы P порядка m и Q порядка n такие, что $P^{-1}AQ = B$. Это условие, очевидно, эквивалентно тому, что B получается из A перестановкой строк π (которой соответствует матрица P) и перестановкой столбцов ρ (которой соответствует матрица Q). Если при этом $P = Q$, то A и B называются *перестановочно изоморфными*; если также $A = B$, то имеем перестановочный автоморфизм матрицы A , определяемый матрицей P (или, что то же самое, подстановкой π на номерах строк и столбцов, которой соответствует P). Пусть $A_1 = A_1(\Gamma_1)$ и $A_2 = A_2(\Gamma_2)$ – матрицы смежности орграфов (или графов) Γ_1 и Γ_2 . Ясно, что изоморфизм Γ_1 и Γ_2 равносильно перестановочному изоморфизму A_1 и A_2 ; аналогично, автоморфизм орграфа Γ равносильно перестановочному автоморфизму его матрицы смежности $A(\Gamma)$.

Пусть $A = (a_{ij}) - (0, 1)$ -матрица порядка n . В связи с A рассмотрим две матрицы: $N(A)$ с элементами

$$\nu_{ij} = (r_A(i), r_A(j)) = \sum_{k=0}^{n-1} a_{ik} a_{jk} \quad (2)$$

– матрицу скалярных произведений строк – и $N^{(-1)}(A)$ с элементами

$$\nu_{ij}^{(-1)} = (c_A(i), c_A(j)) = \sum_{k=0}^{n-1} a_{ki} a_{kj} \quad (3)$$

– матрицу скалярных произведений столбцов. Это две неотрицательные целочисленные симметрические матрицы порядка n . В работе [8] был получен критерий изоморфизма гиперграфов в терминах их матриц инцидентности, а также ряд его следствий. Приведем одно из них.

Предложение А. Пусть $(0, 1)$ -матрицы A_1 и A_2 с t строками и n столбцами перестановочно эквивалентны: $P^{-1}A_1Q = A_2$ для некоторой пары (P, Q) подстановочных матриц P порядка t и n соответственно. Тогда матрицы $N_i = N^{(-1)}(A_i)$, $i = 1, 2$, перестановочно изоморфны: $N_2 = Q^{-1}N_1Q$.

Отсюда непосредственно вытекает следующее утверждение.

Предложение 1. Пусть Γ_1 и Γ_2 – два ориентированных графа на n вершинах, $A_1 = A_1(\Gamma_1)$, $A_2 = A_2(\Gamma_2)$ – их матрицы смежности, $N_1 = N_1^{(-1)}(A_1)$, $N_2 = N_2^{(-1)}(A_2)$ – присоединенные матрицы. Тогда перестановочный изоморфизм N_1 и N_2 является необходимым условием изоморфизма Γ_1 и Γ_2 ; при этом если $R^{-1}A_1R = A_2$ для некоторой подстановочной матрицы R порядка n , то $R^{-1}N_1R = N_2$.

В последующем, говоря о графах и их матрицах смежности, подразумеваем как орграфы (без петель и кратных дуг), так и просто графы (в последнем случае матрица смежности симметрическая). Пусть Γ – граф на n вершинах с матрицей смежности $A = A(\Gamma)$. Матрицы $N(A)$ и $N^{(-1)}(A)$, определенные выше в (2) и (3), называются *присоединенными матрицами графа* Γ . Ясно, что если Γ – неориентированный граф, то $N(A) = N^{(-1)}(A)$. Пусть v – вершина графа Γ с n вершинами. Обозначим через $\Gamma(v)$ множество концов всех дуг, исходящих из v (“окрестность +” вершины v), через $\Gamma^{-1}(v)$ множество начальных вершин всех дуг с концами в v (“окрестность –” вершины v). Тогда для любой пары i, j , $i \neq j$, вершин Γ имеем

$$\nu_{ij} = |\Gamma(i) \cap \Gamma(j)|, \quad \nu_{ij}^{(-1)} = |\Gamma^{(-1)}(i) \cap \Gamma^{(-1)}(j)|,$$

где $|X|$ – число элементов в множестве X . Кроме того,

$$d_i^+ = |\Gamma(i)| = |(r_A(i), r_A(i))|, \quad d_i^- = |\Gamma^{(-1)}(i)| = |(c_A(i), c_A(i))|,$$

где A – матрица смежности Γ , d_i^+ – полустепень исхода, d_i^- – полустепень захода вершины $i \in \Gamma$. Таким образом, присоединенные матрицы содержат информацию о мощностях пересечения окрестностей любой пары различных вершин графа, а также о полустепенях исхода и захода каждой его вершины.

Найдем некоторые свойства присоединенных матриц циркулянтов $C_n(S)$, которые будут полезны при изучении их групп автоморфизмов. Положим $\nu_i = \nu_{0i}$, $\nu_i^{(-1)} = \nu_{0i}^{(-1)}$, $i = 0, 1, \dots, n-1$.

ТЕОРЕМА 1. Пусть $\Gamma = C_n(S)$ – циркулянт на n вершинах с порождающим множеством S , матрицей смежности $A = A(\Gamma) = (a_{ij})$ и присоединенными матрицами $N(A), N^{(-1)}(A)$. Тогда справедливы следующие утверждения.

1) $N(A)$ – циклическая матрица порядка n с первой строкой $(\nu_0, \nu_1, \dots, \nu_{n-1})$.

2) $N^{(-1)}(A) = N(A)$.

3) Пусть $\Gamma_1 = C_n(S_1)$, $\Gamma_2 = C_n(S_2)$ – циркулянты с матрицами смежности A_1, A_2 и присоединенными матрицами $N_1 = N(A_1) = (\nu_{ij}^{(1)})$, $N_2 = N(A_2) = (\nu_{ij}^{(2)})$ соответственно и $\varphi: \Gamma_1 \rightarrow \Gamma_2$ – изоморфизм такой, что $\varphi(0) = 0$. Предположим, что для $u, v \in Z_n$ имеем $\varphi(u) = v$. Тогда

а) либо $u \in S_1$, $v \in S_2$, либо $u \in Z_n - S_1$, $v \in Z_n - S_2$;

б) $\nu_u^{(1)} = \nu_v^{(2)}$.

ДОКАЗАТЕЛЬСТВО. 1) Характеристическое свойство циклической матрицы $X = (x_{ij})$ порядка n имеет вид

$$x_{i+r, j+r} = x_{ij} \quad (4)$$

для любых $i, j, r \in Z_n$ (индексы складываем по модулю n). Имеем

$$\nu_{i+r, j+r} = \sum_{k=0}^{n-1} a_{i+r, k} a_{j+r, k}, \quad r, i, j = 0, 1, \dots, n-1.$$

Полагаем $k = l + r$. Тогда

$$\nu_{i+r, j+r} = \sum_{l=0}^{n-1} a_{i+r, l+r} a_{j+r, l+r} = \sum_{l=0}^{n-1} a_{il} a_{jl} = (r_A(i), r_A(j)) = \nu_{ij}.$$

В силу (4) матрица $N(A)$ циклическая порядка n с начальной строкой $(\nu_0, \nu_1, \dots, \nu_{n-1})$.

2) Обозначим через $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ начальную вектор-строку матрицы A . Транспонированная матрица A^T есть, как известно, циклическая матрица с начальной строкой $(\alpha'_0, \alpha'_1, \dots, \alpha'_{n-1})$, где

$$\alpha'_i = \alpha_{n-i}, \quad i = 0, 1, \dots, n-1. \quad (5)$$

Далее, по доказанному выше (п. 1)) матрицы $N(A)$ и $N^{(-1)}(A)$ циклические, и потому полностью определяются начальными строками:

$$\nu_{ij} = \nu_{0, j-i}, \quad \nu_{ij}^{(-1)} = \nu_{0, j-i}^{(-1)}.$$

Для любого $i \in Z_n$ имеем

$$\nu_i = \sum_{j=0}^{n-1} \alpha_j \alpha_{j-i}, \quad (6)$$

$$\nu_i^{(-1)} = \sum_{k=0}^{n-1} \alpha'_k \alpha'_{k-i}. \quad (7)$$

Пусть для некоторого $j \in Z_n$ $\alpha_j \alpha_{j-i} = 1$, т.е. $\alpha_j = \alpha_{j-i} = 1$. Рассмотрим в (7) член с $k = n + i - j$. Так как по (5) $\alpha'_{n+i-j} = \alpha_{j-i}$, $\alpha'_{n-j} = \alpha_j$, получаем, что

$\alpha'_{n+i-j}\alpha'_{n-j} = 1$. И обратно, любому ненулевому вкладу в (7) однозначно соответствует некоторый ненулевой вклад в (6). Тем самым, $\nu_i^{(-1)} = \nu_i$ и потому $N^{(-1)}(A) = N(A)$.

3) Пусть $\varphi: \Gamma_1 \rightarrow \Gamma_2$ – изоморфизм такой, что $\varphi(0) = 0$, и $Q = (q_{ij})$ – соответствующая ему подстановочная матрица порядка n . Тогда $Q^{-1}A_1Q = A_2$ и $q_{00} = 1$. Ясно, что при таком φ строка $r_{A_1}(0)$ переходит в $r_{A_2}(0)$ и, тем самым, $\varphi(S_1) = S_2$ и $\varphi(Z_n - S_1) = Z_n - S_2$.

Далее, из предложения 1 и части 2) доказательства следует, что

$$N_2 = N(A_2) = N^{(-1)}(A_2) = Q^{-1}N^{(-1)}(A_1)Q = Q^{-1}N(A_1)Q = Q^{-1}N_1Q.$$

Таким образом, φ индуцирует перестановочный изоморфизм φ' матрицы N_1 с матрицей N_2 , который как подстановка на Z_n совпадает с φ ; в частности, $\varphi'(0) = 0$. Отсюда сразу следует, что если $\varphi(u) = v$, то $\nu_u^{(1)} = \nu_v^{(2)}$. Теорема доказана.

Назовем $\bar{\nu} = (\nu_0, \nu_1, \dots, \nu_{n-1})$ *присоединенным вектором циркулянта* $C_n(S)$ с матрицей смежности A . По теореме 1 матрица $N(A)$ полностью определяется вектором $\bar{\nu}$. Полученный результат показывает, что знание присоединенного вектора имеет существенное значение при нахождении автоморфизмов циркулянта $C_n(S)$. Действительно, пусть $S = \bigcup_{\alpha} S_{\alpha}$ и $Z_n - S = \bigcup_{\beta} T_{\beta}$ – разбиения S и $Z_n - S$ такие, что $s_1, s_2 \in S_{\alpha}$ и $t_1, t_2 \in T_{\beta}$ тогда и только тогда, когда $\nu_{s_1} = \nu_{s_2}$ и $\nu_{t_1} = \nu_{t_2}$. Ясно, что любой автоморфизм φ графа такой, что $\varphi(0) = 0$, индуцирует подстановку на каждом из подмножеств S_{α} и T_{β} .

Покажем, как по заданному порождающему подмножеству S циркулянта $C_n(S)$ можно непосредственно находить значения координат его присоединенного вектора. Пусть d, l – целые числа, $1 \leq d, l \leq n - 1$. Последовательность $P^{(d)} = (s_{i_1}, s_{i_2}, \dots, s_{i_l})$ элементов из S назовем *максимальной d -прогрессией длины $l - 1$* , если

- 1) $s_{i_r} \in S, r = 1, \dots, l$;
- 2) $s_{i_{r+1}} - s_{i_r} \equiv d \pmod{n}$;
- 3) либо $s_{i_l} = s_1$, либо $s_{i_l} - d, s_{i_l} + d \notin S$;

при $s_{i_l} = s_{i_1}$ максимальная d -прогрессия называется *полной*. Как несложно заметить, в случае НОД(d, n) = 1 максимальная d -прогрессия не может быть полной. Для каждого $d \in Z_n - \{0\}$ имеем разбиение

$$S = P_1^{(d)} \cup P_2^{(d)} \cup \dots \cup P_r^{(d)} \quad (8)$$

на максимальные d -прогрессии; если $|P_j^{(d)}| = l_j$, то $l_1 + \dots + l_r = |S|$.

ПРЕДЛОЖЕНИЕ 2. Пусть S – порождающее множество циркулянта $\Gamma = C_n(S)$, $|S| = m$ и r – число максимальных d -прогрессий в разбиении (8) множества S на максимальные d -прогрессии для некоторого $d \in Z_n - \{0\}$. Тогда $\nu_d = m - r$, где ν_d – координата присоединенного вектора $\bar{\nu}$.

ДОКАЗАТЕЛЬСТВО. Пусть $A = A(\Gamma)$ – циклическая матрица смежности Γ и $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ – ее начальная строка. Тогда

$$\nu_d = (r_A(0), r_A(d)) = \sum_{j=0}^{n-1} \alpha_j \alpha_{j-d}. \quad (9)$$

По свойству максимальности вклад элементов с индексами, принадлежащими какой-либо d -прогрессии $P_j^{(d)}$ из (8), в сумму (9) равен длине $P_j^{(d)}$. Обозначим эту длину через $l_j - 1$, $j = 1, \dots, r$. Значение ν_d равно, очевидно, сумме таких вкладов:

$$\nu_d = \sum_{j=1}^r (l_j - 1) = \left(\sum_{j=1}^r l_j \right) - r = m - r,$$

что и требовалось доказать.

ПРЕДЛОЖЕНИЕ 3. Пусть $C_n(S)$ – циркулянт порядка n с порождающим множеством S . Тогда для координат его присоединенного вектора справедливо

$$\nu_d = \nu_{n-d}, \quad d = 1, \dots, n-1,$$

а также $\nu_0 = m$.

ДОКАЗАТЕЛЬСТВО. Равенство $\nu_0 = m$ очевидно. Пусть $1 \leq d \leq n-1$. Каждая максимальная d -прогрессия есть, очевидно, записанная в обратном порядке максимальная $(n-d)$ -прогрессия. Поэтому если разбиение S в (8) состоит из r подмножеств $P_j^{(d)}$, $j = 1, \dots, r$, то такое же разбиение для $n-d$ состоит также из r подмножеств $P_j^{(n-d)}$, которые совпадают (как неупорядоченные подмножества) с $P_j^{(d)}$. Наше утверждение теперь следует из предложения 2.

Предложение 3 показывает, что присоединенный вектор определяется своими координатами ν_d , $d = 0, 1, \dots, [n/2]$.

2. Общие свойства автоморфизмов циркулянтов и некоторые приложения. Пусть $C_n(S)$ – циркулянт порядка n с порождающим множеством S и $N = (\nu_{ij})$ – его присоединенная матрица. Для $t \in Z_n$ обозначим через N_t подмножество $\{u \in Z_n \mid \nu_u = \nu_t\}$ в Z_n , где $\nu_t = \nu_{0t}$. Согласно предложению 3 $N_t \supseteq \{t, n-t\}$.

ПРЕДЛОЖЕНИЕ 4. Пусть $\Gamma = C_n(S)$ – циркулянт порядка n с порождающим множеством S , φ – автоморфизм Γ , $\varphi(0) = 0$, t – вершина в Γ . Тогда для любого $r \in Z_n$ имеем $\varphi(t+r) - \varphi(r) \equiv x \pmod{n}$ с некоторым $x \in N_t$.

ДОКАЗАТЕЛЬСТВО. Согласно теореме 1 для элементов присоединенной матрицы N справедливо

$$\nu_{ij} = \nu_{\varphi(i), \varphi(j)} \quad (10)$$

и, так как N – циркулянт,

$$\nu_{ij} = \nu_{0, j-i} = \nu_{j-i}. \quad (11)$$

Положим $\varphi(t) = u$, $\varphi(r) = v$, $\varphi(t+r) = w$. Тогда в силу (10) и (11)

$$\nu_t = \nu_{r, t+r} = \nu_{vw} = \nu_{w-v} = \nu_u.$$

Так как φ индуцирует подстановку на множестве N_t , отсюда следует, что и $w-v \in N_t$, т.е.

$$w-v = \varphi(t+r) - \varphi(r) \equiv x \pmod{n},$$

где $x \in N_t$.

ПРЕДЛОЖЕНИЕ 5. Пусть Γ – циркулянт порядка n с матрицей смежности A и присоединенной матрицей N . Пусть для $d \in Z_n$, $d \neq 0, n/2$, имеем $N_d = \{d, -d\}$. Предположим, что φ – автоморфизм Γ , $\varphi \in G_0$. Тогда для любого $t \in Z_n$ имеем либо

$$\text{а) } \varphi(t + kd) \equiv \varphi(t) + kd \pmod{n}, \text{ либо}$$

$$\text{б) } \varphi(t + kd) \equiv \varphi(t) - kd \pmod{n},$$

где $k = 0, 1, \dots, n/\delta - 1$, $\delta = \text{НОД}(d, n)$.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 4 при наших условиях

$$\varphi(d + t) \equiv \varphi(t) \pm d \pmod{n}.$$

а) Пусть сначала $\varphi(d + t) \equiv \varphi(t) + d \pmod{n}$. Применим индукцию по k , предполагая, что $\varphi(ld + t) \equiv \varphi(t) + ld \pmod{n}$ для $l \leq k < n/\delta$. Используя утверждение предложения 4 с элементами $t' = t + kd$ и $r = d$, находим, что

$$\begin{aligned} \varphi(t + (k + 1)d) &= \varphi(d + (kd + t)) \equiv \varphi(kd + t) \pm d \equiv \varphi(t) + kd \pm d \\ &\equiv \varphi(t) + (k + 1)d \text{ или } \varphi(t) + (k - 1)d \pmod{n}. \end{aligned}$$

По предположению индукции $\varphi(t + (k - 1)d) \equiv \varphi(t) + (k - 1)d \pmod{n}$. Но $(k - 1)d \not\equiv (k + 1)d \pmod{n}$; поэтому $\varphi(t + (k + 1)d) \equiv \varphi(t) + (k + 1)d \pmod{n}$, $k = 0, 1, \dots, n/\delta - 1$.

б) Если $\varphi(d + t) \equiv \varphi(t) - d \pmod{n}$, то, рассуждая в точности так же, как в части а), получаем, что $\varphi(t + kd) \equiv \varphi(t) - kd \pmod{n}$, $k = 0, 1, \dots, n/\delta - 1$.

СЛЕДСТВИЕ. Пусть $P = (s_1, \dots, s_l)$ – максимальная d -прогрессия в S для некоторого d , $1 \leq d \leq n - 1$, и $N_d = \{d, -d\}$. Тогда для любого $\tau \in G_0$ последовательность $(\tau(s_1), \dots, \tau(s_l))$ есть либо максимальная d -прогрессия, либо максимальная $(n - d)$ -прогрессия. Таким образом, для любого $d \in Z_n - \{0\}$ с $N_d = \{d, -d\}$ автоморфизм $\tau \in G_0$ индуцирует подстановку на совокупности всех подмножеств в S , каждое из которых состоит из элементов максимальной d -прогрессии одной и той же длины.

Докажем теперь одно вспомогательное утверждение, которое иногда позволяет при рассмотрении группы автоморфизмов заменить данный циркулянт на изоморфный ему циркулянт более удобного вида (у изоморфных циркулянтов группы автоморфизмов изоморфны).

Для $\lambda \in Z_n^*$ пусть Δ_λ – отображение $C_n(S)$ на $C_n(T)$, где $S = \{s_1, \dots, s_m\}$, $T = \lambda S = \{\lambda s_1, \dots, \lambda s_m\}$. Ясно, что тогда $C_n(S) \cong C_n(T)$.

ЛЕММА 1. Для циркулянта $C_n(S)$ пусть $C_n(T)$ – его образ при изоморфизме Δ_λ , где $\lambda \in Z_n^*$, $T = \lambda S$. Пусть $d \in Z_n$, $1 \leq d \leq n - 1$, $\text{НОД}(d, n) = \delta$, $d = \lambda_1 \delta$. Тогда при отображении Δ_λ , где $\lambda \lambda_1 \equiv 1 \pmod{n}$, любая максимальная d -прогрессия в S переходит в максимальную δ -прогрессию в T и выполнено $\nu'_\delta = \nu_d$ для координат присоединенных векторов $\vec{v}'$ и $\vec{v}$ циркулянтов $C_n(T)$ и $C_n(S)$ соответственно.

Утверждение непосредственно следует из определения Δ_λ и предложения 2 из п. 1.

Для любого $d \in Z_n - \{0\}$ с $\text{НОД}(n, d) = \delta$ циркулянт $C_n(T)$ из леммы 1 называется δ -стандартной формой циркулянта $C_n(S)$, где $T = \lambda S$, $\lambda^{-1}d = d$.

Перед формулировкой следующего результата напомним, что группой диэдра называется конечная группа $D_n = \langle \theta, \tau \rangle$ порядка $2n$ с двумя образующими θ и τ и определяющими соотношениями $\theta^n = \tau^2 = \varepsilon$ и $\tau\theta\tau = \theta^{-1}$ (ε – единица группы). Циркулянт $C_n(S)$ назовем симметрическим, если $S = -S$.

ТЕОРЕМА 2. Пусть $\Gamma = C_n(S)$ – циркулянт на n вершинах с порождающим множеством S . Предположим, что для некоторого $d \in Z_n - \{0\}$ с НОД(d, n) = 1 выполнено $N_d = \{d, -d\}$. Тогда

- а) если $C_n(S)$ – несимметрический, то $\text{Aut } \Gamma \cong Z_n$;
- б) если S – симметрический, то $\text{Aut } \Gamma \cong D_n$, где $D_n = \langle \theta, \tau \rangle$, θ – отображение из (1), $\tau: t \mapsto n - t$ для всех $t \in Z_n$.

ДОКАЗАТЕЛЬСТВО. Как мы упоминали выше, $\text{Aut } \Gamma \cong Z_n G_0$. Циркулянт $C_n(S)$ рассматриваем в его 1-стандартной форме $C_n(T)$, где T разбивается на объединение максимальных 1-прогрессий. При отображении Δ_λ , $\lambda \in Z_n^*$, свойство симметричности сохраняется, поэтому безразлично, говорить о симметричности $C_n(S)$ или $C_n(T)$. Пусть φ – автоморфизм из G_0 , т.е. $\varphi(0) = 0$.

а) Если $C_n(S)$ – несимметрический, то из предложения 5 следует, что $\varphi(1) = 1$, $\varphi(t+1) = \varphi(t) + 1 = t + 1$, $t = 1, \dots, n-2$.

Таким образом, $\varphi = \varepsilon$, $G_0 = \{\varepsilon\}$ и $\text{Aut } \Gamma \cong Z_n$.

б) Пусть $C_n(S)$ – симметрический циркулянт. Из предложения 5 следует, что при $\varphi \neq \varepsilon$ должно быть $\varphi(t) = -t$ для любого $t \in Z_n$, т.е. φ должен совпадать с τ . В силу того, что $T = -T$, τ – действительно автоморфизм $C_n(T)$. Свойство $\tau\theta\tau = \theta^{-1}$ проверяется непосредственно. Теорема доказана.

Отметим, что в контексте бинарных матриц и их перестановочной эквивалентности утверждение, аналогичное теореме 2, было доказано в [10] (см. также [11]).

Как применение полученных результатов найдем группы автоморфизмов для всех циркулянтов $C_n(S)$ степени 4 при n простым. Описанию групп автоморфизмов циркулянтов степени 3 посвящена работа [5]. Вначале дадим некоторую классификацию циркулянтов $C_n(S)$ степени 4 при произвольном n , основанную на разбиении (8) порождающего множества S в объединение максимальных d -прогрессий, $d \in Z_n - \{0\}$, и представлении циркулянтов в δ -стандартной форме, $\delta \mid n$, $\delta \geq 1$ (лемма 1).

Всякий циркулянт степени 4 на n вершинах изоморфен циркулянту $C_n(S)$ одного из следующих видов:

- I) $S = P^{(\delta)}$;
- II) $S = P_1^{(\delta)} \cup P_2^{(\delta)}$, где $P_1^{(\delta)}, P_2^{(\delta)}$ – максимальные δ -прогрессии длин 2 и 0 соответственно;
- III) $S = P_1^{(\delta)} \cup P_2^{(\delta)}$, где $P_1^{(\delta)}, P_2^{(\delta)}$ – максимальные δ -прогрессии длины 1;
- IV) в S нет максимальных d -прогрессий длины 2, а также двух максимальных d -прогрессий длины 1 ни для какого $d \in Z_n - \{0\}$.

В I)–III) δ – делитель n , $1 \leq \delta < n$.

Установим один вспомогательный результат.

ЛЕММА 2. Пусть для циркулянта $\Gamma = C_n(S)$ с присоединенной матрицей $N = (\nu_{ij})$ имеем $\nu_i \leq 1$, $i = 0, 1, \dots, n-1$. Тогда $G_0 \cong \text{Aut}_S Z_n$.

Действительно, $\nu_{ij} = |\Gamma(i) \cap \Gamma(j)|$, $i, j = 0, 1, \dots, n-1$ (см. п. 1). Далее, $\nu_{ij} = \nu_{j-i}$, $i, j \in Z_n$ (по теореме 1). Поэтому $|\Gamma(s) \cap \Gamma(t)| = \nu_{st} \leq 1$ для $s, t \in S$; следовательно, $\Gamma(s) \cap \Gamma(t) = \{s + t\}$. Наше утверждение теперь следует из теоремы 1 в [4].

Далее предполагаем число n простым. Для циркулянтов $C_n(S)$ каждого из видов I)–IV) найдем их группы автоморфизмов; при этом предполагаем $C_n(S)$ заданным в 1-стандартной форме. Так как для $C_n(S)$ и $C_n(Z_n - S)$ их группы G_0 и, следовательно, $\text{Aut } C_n(S)$ и $\text{Aut } C_n(Z_n - S)$ изоморфны, мы можем считать, что $n > 7$.

I) $S = P^{(1)}$. Таким образом, $S = \{s, s+1, s+2, s+3\}$ для некоторого $s \in S$. Для координат вектора $\bar{\nu}$ имеем $\nu_1 = 3, \nu_2 = 2, \nu_3 = 1, \nu_i = 0, i \neq \pm 1, \pm 2, \pm 3$. Применяя теорему 2 при $d = 1$, получаем

$$\text{Aut } C_n(S) \cong \begin{cases} Z_n, & \text{если } S \neq -S, \\ D_n, & \text{если } S = -S, \end{cases}$$

где D_n – группа диэдра порядка $2n$.

II) $S = P_1^{(1)} \cup P_2^{(1)}, P^{(1)} = (s, s+1, s+2), P_2 = \{s_1\}, s_1 - (s+2) > 1$ или $s - s_1 > 1$. Ясно, что $S \neq -S$. Если $s_1 - (s+2) > 2$ или если $s - s_1 > 2$, то для координат $\bar{\nu}$ имеем $\nu_1 = 2, \nu_i \leq 1, i \neq \pm 1$. Тогда согласно теореме 2 при $d = 1$ $G_0 = \{\varepsilon\}$ и $\text{Aut } C_n(S) \cong Z_n$.

Предположим, что $s_1 - (s+2) = 2$. Тогда $\nu_1 = \nu_2 = 2, \nu_3 = \nu_4 = 1, \nu_i = 0, i \neq \pm 1, \pm 2, \pm 3, \pm 4$, (предложение 2). Пусть $\varphi \in G_0$. Из предложения 4 следует, что $\varphi(s_1) = \varphi(s+4) \equiv \varphi(s) \pm 3$ или $\varphi(s) \pm 4$. Отсюда следует, что $\varphi(s), \varphi(s_1) \neq s+2$. Далее, $\varphi(s_1) = \varphi(3 + (s+1)) \equiv \varphi(s+1) \pm 3$ или $\varphi(s+1) \equiv \varphi(s+1) \pm 4 \pmod{n}$. Поэтому $\varphi(s+1) \neq s+2$. Следовательно, $\varphi(s+2) = s+2$ для любого $\varphi \in G_0$. Но $Z_n = \langle s+2 \rangle$ и по теореме 2 работы [5] $\varphi(a) = a$ для любого $a \in Z_n$, т.е. $\varphi = \varepsilon, G_0 = \{\varepsilon\}$. Если $s = s_1 + 2$, то в точности так же получаем, что $\varphi(s) = s$ для любого $\varphi \in G_0$.

Таким образом, для всех рассматриваемых здесь циркулянтов имеем $\text{Aut } C_n(S) \cong Z_n$.

Докажем еще одно вспомогательное предложение.

ЛЕММА 3. Пусть n – простое число, $C_n(S)$ – циркулянт степени 4, заданный в 1-стандартной форме. Тогда подгруппа $\text{Aut}_S Z_n$ группы G_0 циклическая порядка 4 в том и только том случае, когда

- а) $n \equiv 1 \pmod{4}$;
- б) $S = \{s, s+1, -s-1, -s\}$ для $s \equiv -\lambda/(\lambda+1) \pmod{n}$, где $\lambda^4 \equiv 1 \pmod{n}$, $\lambda \neq \pm 1$.

ДОКАЗАТЕЛЬСТВО. Пусть сначала $\text{Aut}_S Z_n$ есть циклическая группа $\langle \Delta_\lambda \rangle$ порядка 4. Тогда $\lambda^4 \equiv 1 \pmod{n}$, $\lambda \neq \pm 1$. Заметим, во-первых, что это возможно лишь при $n \equiv 1 \pmod{4}$. Далее, Δ_λ^2 – автоморфизм порядка 2; в силу простоты n должно быть $\lambda^2 \equiv -1 \pmod{n}$. Таким образом, $S = -S, S = \{s, s+1, -s-1, -s\}$. Мы вправе предположить, что $\lambda s \equiv s+1 \pmod{n}$. Тогда $\lambda^2 s \equiv -s \equiv \lambda s + \lambda \pmod{n}$ и $s \equiv -\lambda/(\lambda+1) \pmod{n}$. Тем самым, условия а) и б) леммы 3 выполняются. Обратное утверждение очевидно.

III) $S = P_1^{(1)} \cup P_2^{(1)}, S = \{s_1, s_1+1, s_2, s_2+1\}, s_2 - (s_1+1) = l > 1$. Покажем сначала, что $G_0 \cong \text{Aut}_S Z_n$. Чтобы доказать это, убедимся, что при любом l в S имеется элемент t со свойством $2t \notin \Gamma(s')$ при $s' \neq t$, для всякого $s' \in S, s' \neq t$. Имеем $\Gamma(s) = \{2s, 2s+1, 2s+l+1, 2s+l+2\}$. Нетрудно заметить, что искомым свойством обладает элемент

$$t = \begin{cases} s & \text{при } l \neq \frac{n-3}{2}, \\ s+1 & \text{при } l = \frac{n-3}{2}. \end{cases}$$

Но при наличии в S такого элемента согласно теореме 6 работы [4] $G_0 \cong \text{Aut}_S Z_n$.

Найдем теперь $\text{Aut}_S Z_n$. В силу простоты n $\text{Aut}_S Z_n$ – циклическая группа Z_r порядка $r = 1, 2, 4$ с образующим элементом Δ_λ , где порядок λ в Z_n^* равен r . Далее, очевидно, что

$$\Delta_\lambda \theta \Delta_\lambda^{-1} = \theta^\lambda. \quad (12)$$

Итак, учитывая лемму 3, в рассматриваемом случае

$$\text{Aut } C_n(S) \cong \begin{cases} Z_n, & \text{если } S \neq -S, \\ D_n = \langle \theta, \Delta_{-1} \rangle, & \text{если } S = -S \text{ и условия леммы 3 не выполнены,} \\ \langle \theta, \Delta_\lambda \rangle, & \lambda^4 = 1 \pmod{n}, \lambda \neq \pm 1 \\ & \text{и условия леммы 3 выполнены,} \end{cases}$$

образующие элементы θ и Δ_λ переставляются согласно (12).

IV) Циркулянты вида IV) можно, учитывая предложение 2, характеризовать условием $\nu_i \leq 1, i \in Z_n - \{0\}$, на координаты присоединенного вектора $\vec{v}$. По лемме 2 получаем, что для таких циркулянтов $C_n(S)$ справедливо $\text{Aut}_S Z_n \cong G_0$. Ясно также, что $S \neq -S$. Отсюда и из леммы 3 вытекает, что $G_0 = \{\varepsilon\}$ и $\text{Aut } C_n(S) \cong Z_n$.

Тем самым мы пришли к следующему результату.

ТЕОРЕМА 3. Пусть n – простое число, $C_n(S)$ – циркулянт порядка n и степени $m = 4$ с порождающим множеством S . Если S несимметрический, то $\text{Aut } C_n(S) \cong Z_n$. Если S – симметрический циркулянт, то $\text{Aut } C_n(S) \cong D_n$, как только его 1-стандартная форма не есть $C_n(T)$ с $T = \{t, t+1, -t-1, -t\}$, $1 \leq t \leq n-2$, $n \equiv 1 \pmod{4}$ и $t \equiv -\lambda/(\lambda+1) \pmod{n}$, $\lambda \neq \pm 1$; в последнем случае $G = \langle \theta, \Delta_\lambda \rangle$ – группа порядка $4n$, где $\theta^n = \Delta_\lambda^4 = \varepsilon$, $\Delta_\lambda^{-1} \theta \Delta_\lambda = \theta^{\lambda^{-1}}$.

При n составном описание групп автоморфизмов циркулянтов степени 4 более громоздко. Отметим также, что при произвольном n нами получено описание в явном виде групп автоморфизмов циркулянтов $C_n(S)$ степени $m = 3$, основанное на разделении этих циркулянтов на два класса, аналогичном приведенному выше для $m = 4$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Elspas B., Turner J. Graphs with circulant adjacency matrices // J. Combin. Theory. 1970. V. 9. P. 297–307.
- [2] Alspach B., Parsons T. Isomorphisms of circulant graphs and digraphs // Discrete Math. 1979. V. 25. P. 97–108.
- [3] Boesch F., Tindell R. Circulants and their connectivities // J. Graph Theory. 1984. V. 8. P. 487–499.
- [4] Huang Q., Meng J. On the isomorphisms and automorphism groups of circulants // Graphs Combin. 1996. V. 12. P. 179–187.
- [5] Huang Q., Yuan J. The automorphism groups of circulants of degree 3 // Ars Combin. 1996. V. 44. P. 263–271.
- [6] Biggs N. Z. Algebraic Graph Theory. Cambridge: Cambridge Univ. Press, 1974.
- [7] Adam A. Research problem 2–10 // J. Combin. Theory. 1967. V. 2. P. 393.
- [8] Тараканов В. Е. К задаче классификации $(0, 1)$ -матриц // Вопросы кибернетики. Комбинаторный анализ и теория графов. М.: АН СССР, 1980. С. 67–80.
- [9] Cameron P. J. Automorphism groups. Sel. Topics Graph Theory. V. 11. London: Acad. Press, 1983.
- [10] Тараканов В. Е. Комбинаторные задачи на бинарных матрицах // Комбинаторный анализ / ред. К. А. Рыбников. Т. 5. М.: МГУ, 1980. С. 4–15.
- [11] Тараканов В. Е. Циклические бинарные матрицы и их группы перестановочных автоморфизмов // Матем. заметки. 1994. Т. 55. № 4. С. 83–95.