Math-Net.Ru
Общероссийский математический портал

М. М. Глухов, О 2-транзитивных произведениях регулярных групп подстановок,
Тр. по дискр. матем., 2000, том 3, 37–52

https://www.mathnet.ru/tdm36

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

Параметры загрузки:
IP: 18.97.9.169
21 января 2026 г., 20:06:52

Труды по дискретной математике
Том 3, с. 37–52
М.: ФИЗМАТЛИТ, 2000

О 2-ТРАНЗИТИВНЫХ ПРОИЗВЕДЕНИЯХ РЕГУЛЯРНЫХ ГРУПП ПОДСТАНОВОК

М. М. ГЛУХОВ

В работе находятся необходимые условия 2-транзитивности произведения двух регулярных групп подстановок и выделяется класс регулярных систем образующих симметрической группы подстановок степени 2^n с относительно небольшим показателем 2-транзитивности.

§ 1. ВВЕДЕНИЕ

Напомним, что регулярной группой подстановок конечного множества Ω называют любую транзитивную подгруппу G порядка $|\Omega|$ симметрической группы $S(\Omega)$. Регулярные группы из $S(\Omega)$ характеризуются также следующим свойством точной транзитивности: в каждой из них для любых $a, b \in \Omega$ существует единственная подстановка, отображающая a в b. В связи с этим элементы регулярной группы G из $S(\Omega)$ можно занумеровать элементами из Ω так, что $eg_c = c$ при фиксированном e и любом c из Ω. При этом множество Ω с операцией $\cdot$, определенной равенством

$$x \cdot y = xg_y, \tag{1}$$

становится группой с единицей e, а G — правым регулярным представлением группы $(\Omega; \cdot)$. В итоге действие подстановки на букву сводится к реализации групповой операции на Ω. Этим фактом во многом и объясняется широкое использование регулярных групп при конструировании различных автоматов и, в частности, в криптографии для получения требуемых систем подстановок. В случаях, когда сами регулярные группы не удовлетворяют целям приложения, используются различные комбинации регулярных групп (произведение, объединение, разветвление и т.д.). В данной работе рассматривается вопрос о получении 2-транзитивных множеств подстановок как произведений регулярных групп.

© М. М. Глухов, 2000

§ 2. ПРОИЗВЕДЕНИЯ ДВУХ РЕГУЛЯРНЫХ ГРУПП

Пусть регулярные группы G, H из $S(\Omega)$ являются правыми регулярными представлениями соответственно групп $(\Omega;\cdot)$, $(\Omega;\circ)$. Не теряя общности, будем считать, что группы $(\Omega;\cdot)$, $(\Omega;\circ)$ имеют общую единицу e, а элементы в G и H занумерованы по указанному во введении правилу. Тогда, наряду с (1), будем иметь равенство

$$x \circ y = xh_y, \qquad h_y \in H.$$

Рассмотрим вопрос об условии 2-транзитивности системы подстановок

$$F = G \cdot H = \{g \cdot h : q \in G,\ h \in H\}.$$

Заметим, что подстановки в системе F не обязательно все различны, поскольку возможно равенство

$$g_a h_b = g_c h_d \quad \text{при} \quad a \neq c, \quad b \neq d.$$

Близость системы F к 2-транзитивному множеству подстановок можно характеризовать числом $\nu(F)$ ненулевых элементов в матрице $P_F^{(2)}$ частот переходов пар различных букв из Ω под действием подстановок системы F. Элемент p_{cd}^{ab} матрицы $P_F^{(2)}$ равен числу подстановок системы F, отображающих буквы a, b соответственно в буквы c, d (при этом каждая подстановка считается столько раз, сколько она встречается в системе F).

Утверждение 1. *Элемент p_{cd}^{ab} матрицы $P_F^{(2)}$ равен числу решений уравнения*

$$\alpha \cdot x = \beta \circ y, \tag{2}$$

где $\alpha = ab^{-1}$, $\beta = c \circ d^{\circ 1}$. (Здесь и ниже $d^{\circ 1}$ есть элемент, обратный к d в группе $(\Omega;\circ)$.)

Доказательство. Непосредственно из определения матрицы $P_F^{(2)}$ видно, что p_{cd}^{ab} есть число решений системы уравнений

$$(a \cdot x) \circ y = c, \qquad (b \cdot x) \circ y = d \tag{3}$$

относительно неизвестных x, y со значениями из Ω. Исключая из нее неизвестное y, получим уравнение с одним неизвестным:

$$a \cdot x = \left(c \circ d^{\circ 1}\right) \circ (b \cdot x). \tag{4}$$

При этом по найденному из (4) значению x соотношения (3) однозначно определяют соответствующее значение y. Значит, система (3) имеет столько же решений, сколько и уравнение (4). Взаимно однозначная замена $bx = z$ приводит уравнение (4) к виду

$$\left(ab^{-1}\right) \cdot z = \left(c \circ d^{\circ 1}\right) \circ z,$$

из которого следует, что число p_{cd}^{ab} зависит лишь от чисел $\alpha = ab^{-1}$, $\beta = c \circ d^{\circ 1}$ и совпадает с числом решений уравнения (2).

В связи с утверждением 1 естественно ввести в рассмотрение матрицу $Q_F = (q_{\alpha\beta})$, в которой $\alpha, \beta \in \Omega \backslash \{e\}$, а $q_{\alpha\beta}$ — число решений уравнения (2). Так как для α существует ровно $|\Omega|$ пар (a, b) с условием $ab^{-1} = \alpha$, то число μ_F ненулевых элементов в Q_F равно $\nu_F/|\Omega|^2$, и, значит, параметр μ_F (так же, как ν_F) характеризует близость множества F к 2-транзитивному множеству. В частности, F является 2-транзитивным тогда и только тогда, когда $\mu_F = (|\Omega| - 1)^2$, т.е. когда в Q_F нет нулевых элементов. Последний факт будем записывать в виде $Q_F > 0$.

Так как $p_{cd}^{ab} = p_{uv}^{st} = q_{\alpha\beta}$ при условии

$$ab^{-1} = st^{-1} = \alpha, \qquad c \circ d^{\circ 1} = u \circ v^{\circ 1} = \beta,$$

то матрица $P_F^{(2)}$ при определенной нумерации ее строк и столбцов разлагается в тензорное произведение

$$P_F^{(2)} = R \otimes Q_F,$$

где R — матрица размером $|\Omega| \times |\Omega|$, все элементы которой равны 1.

Утверждение 2. *Пусть $|\Omega| = n$ и k_1, k_2 — число инволюций, т.е. элементов порядка 2, соответственно в группах G, H. Тогда для системы $F = G \cdot H$*

$$\mu(F) \leq (n-1)^2 - \frac{k_1 k_2 - \min(k_1, k_2)}{2}. \tag{5}$$

Доказательство. Обозначим через $I(G)$ множество всех инволюций в G. Заметим, что при $\alpha \in I(G)$, $\beta \in I(H)$ уравнение (2) или совсем не имеет решений или имеет по крайней мере 2 решения. Действительно, непосредственная проверка показывает, что если x_1 — решение уравнения (2), то $\alpha \cdot x_1$ и $\beta \circ x_1$ также удовлетворяют уравнению (2), причем $\alpha \cdot x_1 \neq x_1$. Пусть для фиксированного $\alpha \in I(G)$ уравнение (2) разрешимо при s различных $\beta \in I(H)$. Тогда по сделанному выше замечанию имеем:

$$\sum_{\beta \in I(H)} q_{\alpha,\beta} \geq 2s.$$

Из уравнения (2) при фиксированных α, x элемент β находится однозначно. Значит, общее число решений уравнений вида (2) при фиксированном α и всевозможных $\beta \in \Omega \backslash e \stackrel{\text{def}}{=} \Omega^*$ равно n, т.е.

$$\sum_{\beta \in \Omega^*} q_{\alpha,\beta} = n,$$

и потому

$$\sum_{\beta \in \Omega^* \backslash I(H)} q_{\alpha,\beta} \leq n - 2s. \tag{6}$$

Отсюда, учитывая, что $|\Omega^*\backslash I(H)| = n-1-k_2$, получаем: число N_α ненулевых элементов в строке с номером $\alpha \in I(G)$ удовлетворяет неравенству

$$N_\alpha \leq s + \min(n-1-k_2,\, n-2s).$$

Рассматривая отдельно случаи, когда

$$n-1-k_2 \leq n-2s \qquad \text{и} \qquad n-1-k_2 > n-2s,$$

мы в обоих случаях получим неравенство

$$N_\alpha \leq n - \frac{k_2+1}{2}. \tag{7}$$

Суммируя неравенства (7) по всем $\alpha \in I(G)$, получим оценку для числа N' ненулевых элементов в строках с номерами $\alpha \in I(G)$ матрицы Q_F:

$$N' \leq k_1\left(n - \frac{k_2+1}{2}\right).$$

Число N'' ненулевых элементов из остальных строк матрицы Q_F не превосходит общего числа $(n-1)(n-1-k_1)$ их элементов. Отсюда находим

$$\mu(G) = n' + n'' \leq (n-1)^2 - \frac{k_1(k_2-1)}{2}.$$

Аналогично, проводя те же рассуждения для столбцов матрицы Q_F, получим

$$\mu(G) \leq (n-1)^2 - \frac{k_2(k_1-1)}{2}.$$

Из этих оценок, учитывая, что

$$\max\left(\frac{k_1(k_2-1)}{2}, \frac{k_2(k_1-1)}{2}\right) = \frac{k_1k_2 - \min(k_1,k_2)}{2},$$

получим (5). Утверждение доказано.

Заметим, что неравенство (4) является тривиальным для групп G, H нечетного порядка и превращается в равенство для некоторых групп четного порядка.

Следствие 1. *Если число $n = |\Omega|$ четно и хотя бы одна из групп G, H содержит две инволюции, то система подстановок $G \cdot H$ не является 2-транзитивной.*

Действительно, если $G \cdot H$ является 2-транзитивной, то $\mu(F) = (n-1)^2$, а тогда из (5) следует, что $k_1k_2 - \min(k_1,k_2) = 0$. Однако последнее неравенство возможно лишь при $k_1k_2 = 0$ или $k_1k_2 = 1$. В первом случае $k_1 = 0$ или $k_2 = 0$, что возможно лишь при нечетном n, во втором случае $k_1 = k_2 = 1$. Во всех случаях приходим к противоречию с условием следствия.

Утверждение 3. *Если $|\Omega| = n > 2$ и хотя бы одна из групп G, H не совпадает со своим коммутантом, то система $G \cdot H$ не является 2-транзитивной.*

Доказательство. Пусть $G \cdot H$ является 2-транзитивной. Тогда уравнение (2) разрешимо при любых $\alpha, \beta \in \Omega^*$. Так как при фиксированном β каждый элемент из Ω есть решение уравнения (2) при подходящем единственном значении α, то из количественных соображений получаем: при любом фиксированном β уравнение (2) имеет ровно два решения при каком-то одном значении $\alpha = \alpha(\beta)$ и ровно по одному решению при всех остальных значениях α из Ω^*. Следовательно, если x пробегает все множество Ω, то при фиксированном β элемент $\alpha = (\beta \circ x) \cdot x^{-1}$ будет пробегать все элементы из Ω^*, причем только один из них (а именно, $\alpha(\beta)$) повторится дважды. В силу симметрии аналогичное условие будет выполняться и для элементов $\beta = (\alpha \cdot x) \circ x^{\overset{\circ}{-}1}$ при фиксированном α. Отсюда, в частности, следует, что $\alpha(\beta_1) \neq \alpha(\beta_2)$ при $\beta_1 \neq \beta_2$. Значит, при любом фиксированном размещении

$$(a_1, a_2, \ldots, a_{n-1})$$

всех элементов из Ω^* и любом фиксированном $\beta \in \Omega^*$ элементы из Ω можно записать в виде ряда

$$u_1, u_2, \ldots, u_n$$

так, чтобы выполнялись равенства

$$\begin{gathered} a_1 = (\beta \circ u_1) \cdot u_1^{-1}, \ldots, a_{n-1} = (\beta \circ u_{n-1}) \cdot u_{n-1}^{-1}, \\ \alpha(\beta) = (\beta \circ u_n) \cdot u_n^{-1}. \end{gathered} \tag{8}$$

Так как $(\Omega; \cdot)$, $(\Omega; \circ)$ — группы, то каждый из наборов

$$(\beta \circ u_1,\ \beta \circ u_2, \ldots, \beta \circ u_n), \qquad \left(u_1^{-1}, u_2^{-1}, \ldots, u_n^{-1}\right)$$

содержит по одному разу все элементы из Ω. Тогда, перемножив равенства (8) в группе $(\Omega; \cdot)$, получим

$$a_1 \cdot a_2 \cdots a_{n-1} \cdot \alpha(\beta) = b_1 \cdot c_1 \cdot b_2 \cdot c_2 \cdots b_n \cdot c_n, \tag{9}$$

где $b_1, b_2, \ldots, b_n$ и $c_1, c_2, \ldots, c_n$ — некоторые перестановки элементов группы $(\Omega; \cdot)$. Теперь, пользуясь тождеством

$$x \cdot y = y \cdot x \cdot [x, y],$$

где $[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов x, y в группе $(\Omega; \cdot)$, мы сможем в правой части равенства (9) переставить элементы так, что будет выполняться равенство

$$a_1 \cdot a_2 \cdots a_{n-1} \cdot \alpha(\beta) = (a_1 \cdot a_2 \cdots a_{n-1})^2 \cdot k(\beta),$$

где $k(\beta)$ — подходящий элемент из коммутанта $(\Omega'; \cdot)$ группы $(\Omega; \cdot)$. По доказанному выше элемент $\alpha(\beta)$ принимает все значения из Ω^* при изменении β. Значит, то же самое можно сказать и об элементе $k(\beta)$. Отсюда следует, что $|(\Omega'; \cdot)| \geq n - 1$, и значит, при $n > 2$ выполняется равенство $(\Omega'; \cdot) = (\Omega; \cdot)$, а в силу симметрии и равенство $(\Omega; \circ) = (\Omega'; \circ)$. Теперь, учитывая изоморфизмы

$$G \cong (\Omega; \cdot), \qquad G \cong (\Omega; \circ),$$

получаем: каждая из групп G, H совпадает со своим коммутантом, что противоречит условию. Заметим, что при $n = 2$ система $G \cdot H$ всегда 2-транзитивна. Утверждение доказано.

Утверждение 4. *Если система $G \cdot H$ является 2-транзитивной, то число $n = |\Omega|$ четно, и силовские 2-подгруппы групп G, H — обобщенные группы кватернионов.*

Доказательство. Четность числа n следует из утверждения 3, если учесть, что любая группа нечетного порядка разрешима (в силу известной теоремы Файта–Томпсона), а коммутант разрешимой подгруппы не может совпадать с самой группой (в силу определения разрешимой группы, см. [3], стр. 158). По следствию утверждения 2 силовские 2-подгруппы групп G, H содержат лишь по одной инволюции. Тогда по теореме 12.5.2 из [3] они могут быть либо циклическими, либо обобщенными группами кватернионов. Допустим, что, например, группа G имеет циклическую силовскую 2-подгруппу P. Тогда

$$|G| = n = 2^k n_1, \quad \text{где} \quad (n_1, 2) = 1, \quad |P| = 2^k.$$

Пусть P порождается подстановкой $g \in G$. Так как G — регулярная группа подстановок, то в разложении g на независимые циклы все циклы имеют одну и ту же длину. Причем длина эта равна 2^k, поскольку g имеет порядок 2^k. Итак, разложение подстановки g на независимые циклы содержит n_1 циклов длины 2^k. Значит, подстановка g — нечетная. Но все четные подстановки из G образуют подгруппу K индекса 2, являющуюся нормальным делителем группы G. Так как фактор-группа G/K абелева, то K содержит коммутант G' группы G. Следовательно, $G' \neq G$ и по утверждению 4 система $G \cdot H$ не 2-транзитивна. Получили противоречие с условием утверждения.

Объединяя утверждения 2–4 и учитывая, что все группы порядков $p^k q^l$ при простых p, q разрешимы, а минимальный порядок обобщенной группы кватернионов равен 8, получим следующее утверждение.

Теорема 1. *Если G, H — регулярные группы подстановок конечного множества порядка n, то для 2-транзитивности системы $G \cdot H$ необходимы следующие условия:*

1) *n кратно числу $2^3 \cdot p \cdot q$, где p, q — различные нечетные простые числа;*

2) *силовские 2-подгруппы групп G, H являются обобщенными группами кватернионов;*

3) *каждая из групп G, H совпадает со своим коммутантом.*

Из групп, удовлетворяющих условиям 1)–3), автору известна лишь серия специальных линейных групп $\mathrm{SL}(2, q)$ при простых $q \geq 5$. Группа $\mathrm{SL}(2, q)$ состоит из всех невырожденных матриц размером 2×2 над простым полем $\mathrm{GF}(q)$. Ее порядок равен $q(q-1)(q+1)$. Минимальным из таких чисел является $5(5-1)(5+1) = 120$. Вопрос о существовании регулярных групп G, H, удовлетворяющих условиям 1)–3) и таких, что $G \cdot H$ является 2-транзитивной, остается открытым. На наш взгляд, весьма правдоподобной является гипотеза об отсутствии таких групп.

§ 3. ПОСТРОЕНИЕ 2-ТРАНЗИТИВНЫХ ПРОИЗВЕДЕНИЙ РЕГУЛЯРНЫХ ГРУПП С ИСПОЛЬЗОВАНИЕМ СДВИГОВ ПО МОДУЛЮ 2^n И АФФИННЫХ ПРЕОБРАЗОВАНИЙ НАД ПОЛЕМ GF(2)

Теорема 1 § 2 делает маловероятной возможность получения 2-транзитивного множества подстановок путем перемножения двух регулярных групп. В связи с этим естественно попытаться достичь той же цели с помощью произведений большего числа регулярных групп. В этом направлении интересным является известный результат А. С. Амбросимова о множествах подстановок вида $(Gh)^m$. Им доказано, что при случайном и равновероятном выборе подстановки h из $S(\Omega)$ и при $|\Omega| \to \infty$ вероятность 2-транзитивности множества $(Gh)^3$ стремится к 1 равномерно по всем регулярным подгруппам $G < S(\Omega)$. Заметим, что $(Gh)^m$ с точностью до постоянного множителя h^{m-1}, не влияющего на выполнение условия 2-транзитивности, совпадает с произведением регулярных подгрупп

$$G \cdot \left(hGh^{-1}\right)\left(h^2Gh^{-2}\right) \cdots \left(h^{m-1}Gh^{-(m-1)}\right).$$

Указанная теорема Амбросимова имеет асимптотический характер и не снимает задачи построения конкретных, просто реализуемых, регулярных групп G и подстановок h, при которых множества вида $(Gh)^m$ были бы 2-транзитивными при возможно меньших значениях m.

В данном параграфе мы рассмотрим этот вопрос в одном частном случае, когда

$$\Omega = \{0, 1, \ldots, 2^n - 1\}, \qquad n > 1,$$

$G = \langle t \rangle$ — циклическая группа, порожденная подстановкой

$$t = (0, 1, 2, \ldots, 2^n - 1),$$

а h — аффинное преобразование множества Ω, рассматриваемого как линейное пространство строк длины n над полем GF(2) при отождествлении числа

$$x = 2^{n-1}x_{n-1} + \ldots + 2x_1 + x_0, \qquad x_i \in \{0, 1\},$$

с вектором

$$(x_{n-1}, \ldots, x_1, x_0).$$

Компоненту x_i этого вектора отождествим с элементом поля GF(2) и обозначим через $d_i(x)$. Операцию сложения таких векторов будем обозначать значком $\oplus$, а результат действия подстановки h на вектор x определим равенством

$$xh = x \cdot A \oplus \gamma, \tag{10}$$

где A — невырожденная матрица над GF(2), γ — фиксированный вектор из Ω.

Так как G — группа, то $G \cdot G = G$ и множество подстановок $(Gh)^m$ можно представить в виде

$$(Gh)^m = (GhG)^{m-1} \cdot h.$$

Теперь для системы подстановок $F = GhG$, как и в § 2, введем матрицу $Q_F = (q_{\alpha,\beta})$ размером $(2^n - 1) \times (2^n - 1)$. Ее элемент $q_{\alpha,\beta}$ будет равен числу решений уравнения

$$(a + x)\, h - xh = b. \tag{11}$$

При этом множество $(Gh)^m$ будет 2-транзитивным в том и только в том случае, когда $Q_F^{m-1} > 0$. Наименьшее значение m, при котором множество $(Gh)^m$ оказывается 2-транзитивным, называют показателем 2-транзитивности множества Gh и обозначают через $\delta_2(Gh)$, см. [1]. В нашей ситуации, когда группа G зафиксирована, параметр $\delta_2(Gh)$ определяется подстановкой h, т.е. матрицей A и вектором γ. В связи с этим указанную выше матрицу Q_F будем обозначать через Q_h. При некоторых h искомого числа m может не существовать совсем.

В рассматриваемом случае вопрос о существовании такого числа m решается следующей теоремой.

Теорема 2. *Пусть h — аффинное преобразование* (10). *Тогда эквивалентны следующие условия*:

1) *группа $\langle Gh\rangle$, порожденная множеством Gh, примитивна*;

2) $\langle Gh\rangle = S(\Omega)$;

3) *в правом верхнем углу матрицы A не содержится нулевой подматрицы размера $k \times (n-k)$ ни при каком $k \in \{1, \ldots, n-1\}$.*

Доказательство. Так как G — группа, то $\langle Gh\rangle = \langle G, h\rangle$, и потому $\langle G, h\rangle$ примитивна тогда и только тогда, когда группы G и h не имеют общих нетривиальных областей импримитивности. Группа G является правым регулярным представлением группы $(G; +)$, и ее областями импримитивности являются все смежные классы группы $(G; +)$ по ее подгруппам и только они. Отсюда следует, что группа $\langle Gh\rangle$ импримитивна в том и только том случае, когда линейное преобразование $\phi : x \to xA$ пространства Ω оставляет на месте хотя бы одну ненулевую подгруппу группы $(G; +)$. А так как каждая ненулевая подгруппа группы $(G; +)$ имеет вид

$$\{(x_{n-1}, \ldots, x_k, 0, \ldots, 0) \;:\; x_{n-1}, \ldots, x_k \in \mathrm{GF}(2)\},$$

то очевидно, что условие примитивности группы $\langle Gh\rangle$ эквивалентно условию 3). Теперь для доказательства теоремы остается доказать импликацию 1) $\Rightarrow$ 2).

Итак, пусть группа $\langle Gh\rangle$ примитивна. Тогда, как следует из [2], она совпадает с группой $S(\Omega)$ или подстановочно изоморфна представлению проективной линейной группы $PGL(2, p)$ подстановками множества

$$\mathrm{GF}(p) \cup \{\infty\},$$

где p — простое число и $p+1 = 2^n$. Так как указанное подстановочное представление точно 3-транзитивно, то нам достаточно найти в группе $\langle Gh\rangle$ подстановку, оставляющую неподвижными по крайней мере три точки и отличную от тождественной подстановки. Найдем такую подстановку.

Выберем подстановки

$$F_1 = h^{-1}t^{2^{n-1}}h, \qquad F_2 = h^{-1}t^{2^{n-2}}h.$$

Так как

$$xt^{2^{n-1}} = x + 2^{n-1} = x \oplus 2^{n-1},$$

то

$$xF_1 = \left(xA^{-1} \oplus \gamma A^{-1} \oplus 2^{n-1}\right) A \oplus \gamma = x \oplus 2^{n-1}A = x \oplus \alpha,$$

где α — первая строка матрицы A. Далее рассмотрим три случая.

a) $d_i(\alpha) = 0$, $d_{i-1}(\alpha) = 1$ для некоторого $i \in \{1, \ldots, n-1\}$. Прослеживая действие сомножителей из произведения

$$F = t^{2^{i-1}}F_1t^{-2^{i-1}}F_1,$$

получим

$$xFt^{2^i} = \begin{cases} x, & \text{если} \quad d_i(x) = 1,\ d_{i-1}(x) = 0, \\ x + 2^{i-1} + 2^i, & \text{если} \quad d_i(x) = 0,\ d_{i-1}(x) = 1. \end{cases}$$

Заметим еще, что при $n \geq 3$ подстановка Ft^{2i} оставляет на месте также и векторы вида

$$(x_{n-1}, \ldots, x_{i+1}, 0, 0, x_{i-2}, \ldots, x_0).$$

Следовательно, при $n \geq 3$ искомой подстановкой из группы $\langle Gh \rangle$ может служить Ft^{2^i}.

b) $d_i(\alpha) = 1$, $d_{i-1}(\alpha) = 0$ при некотором $i \in \{1, \ldots, n-2\}$; $n \geq 3$. В этом случае $xF = x$, если $d_{i-1}(x) = 0$, и $xF \neq x$, если $d_{i-1}(x) = 1$. Значит, при $n \geq 3$ подстановка Ft^{2^i} искомая.

c) Вектор α не удовлетворяет условиям случаев a), b). Тогда, как легко видеть, α имеет вид $(\epsilon, 1, \ldots, 1)$, где $\epsilon = 0$ или $\epsilon = 1$. В этом случае рассмотрим подстановку F_2. Введя обозначение,

$$(x_{n-1}, x_{n-2}, \ldots, x_0)\, h^{-1} = (y_{n-1}, y_{n-2}, \ldots, y_0), \tag{12}$$

непосредственными вычислениями получим

$$xF_2 = \begin{cases} x \oplus \beta, & \text{если} \quad y_{n-2} = 0, \\ x \oplus \beta \oplus \alpha, & \text{если} \quad y_{n-2} = 1, \end{cases}$$

где β — вторая строка матрицы A. Отсюда видно, что F_2 — одно из преобразований типа $\mathcal{D}(\alpha_0, \alpha_1, f)$, рассмотренных в [1]. При этом

$$\alpha_0 = \beta, \qquad \alpha_1 = \alpha \oplus \beta,$$

$f(x_{n-1}, \ldots, x_0)$ — булева функция, определяемая равенством (12), и

$$xF_2 = x \oplus \alpha_{f(x)}.$$

Из условия (12) следует, что f — аффинная функция. Так как F_2 — подстановка, то в силу утверждения 1 из [1] выполнено условие

$$f(x \oplus \alpha_0) = f(x \oplus \alpha_1). \tag{13}$$

Если, кроме того, функция f существенно зависит от x_{n-1}, то по теореме 2 из [1] имеем:

$$\langle G, F_2 \rangle = S(\Omega)$$

и тем более $\langle Gh \rangle = S(\Omega)$ при любом $n \geq 4$.

Пусть f не зависит от x_{n-1}, тогда f имеет вид:

$$f(x) = x_{n-k} \oplus \phi(x_{n-k-1}, \ldots, x_0), \qquad k > 1. \tag{14}$$

Так как $\alpha = (\epsilon, 1, \ldots, 1)$, то из (13), (14) следует, что $f(x)$ существенно зависит не только от переменного x_{n-k}. Значит,

$$f(x) = x_{n-k} \oplus x_{n-l} \oplus \psi(x_{n-l-1}, \ldots, x_0), \tag{15}$$

где $k < l \leq n-1$. Обозначим $\Phi = F_2 t^{2^{n-k}} F_2$ и рассмотрим 2 подслучая.

c1) $f(\alpha_0) = f(0)$. Тогда для векторов x, удовлетворяющих условиям

$$f(x) = 0, \qquad d_{n-k}(x) = d_{n-k}(\alpha_0), \tag{16}$$

имеем

$$f(xF_2) = f(x \oplus \alpha_0) = f(x) \oplus f(\alpha_0) \oplus f(0) = 0,$$

$$f\left(xF_2 t^{2^{n-k}}\right) = f(xF_2) \oplus 1 = 1,$$

$$x\Phi = (x \oplus \alpha_0) \oplus 2^{n-k} \oplus \alpha_1 = x \oplus \alpha \oplus 2^{n-k},$$

т.е.

$$x\Phi = \begin{cases} x \oplus \alpha + 2^{n-k}, & \text{если} \quad \delta_{n-k}(\alpha_0) = 1, \\ x \oplus \alpha - 2^{n-k}, & \text{если} \quad \delta_{n-k}(\alpha_0) = 0. \end{cases}$$

Пользуясь условием (15), нетрудно убедиться в том, что подстановка Φ иначе действует на остальных векторах. Значит, при

$$d_{n-k}(\alpha_0) = 1 \qquad (d_{n-k}(\alpha_0) = 0)$$

подстановка $\Phi t^{-2^{n-k}}$ (соответственно, подстановка $\Phi t^{2^{n-k}}$) не является тождественной и оставляет на месте все 2^{n-2} векторов, удовлетворяющих условиям (16). При $n \geq 4$ полученная подстановка является искомой.

c2) $f(\alpha_0) \neq f(0)$. В этом случае для векторов x, удовлетворяющих условиям (16), как и в случае c1), находим

$$f(xF_2) = 1, \qquad f\left(xF_2 + 2^{n-k}\right) = 0, \qquad x\Phi = x \oplus 2^{n-k},$$

т.е.

$$x\Phi = \begin{cases} x + 2^{n-k}, & \text{если} \quad d_{n-k}(\alpha_0) = 0, \\ x - 2^{n-k}, & \text{если} \quad d_{n-k}(\alpha_0) = 1. \end{cases}$$

На остальные векторы Φ действует иначе. Значит, здесь искомой подстановкой при $n \geq 4$ может служить $\Phi t^{-2^{n-k}}$ при $d_{n-k}(\alpha_0) = 0$ и $\Phi t^{2^{n-k}}$ при $d_{n-k}(\alpha_0) = 1$.

В итоге при всех $n \geq 4$, а в некоторых случаях и при $n = 3$, теорема доказана. Для $n = 2$ и в оставшихся случаях для $n = 3$ справедливость теоремы устанавливается непосредственной проверкой.

Следствие 2. *Множество $(Gh)^m$ является 2-транзитивным при некотором m в том и только в том случае, когда матрица A удовлетворяет условию* 3) *теоремы* 1.

Для доказательства достаточно заметить, что в Gh содержатся как четные, так и нечетные подстановки. Отсюда по следствию 2 теоремы 1 из [1] получаем, что ширина группы $S(\Omega)$ в системе образующих Gh равна 1, т.е. $(Gh)^m = S(\Omega)$ при подходящем натуральном m.

Следующая теорема выделяет класс аффинных преобразований h с относительно небольшим показателем 2-транзитивности $\delta_2(Gh)$.

Заметим, что, как следует из теоремы 1, в рассматриваемом случае $\delta_2(Gh) \geq 3$ при любой подстановке $h \in S(\Omega)$. В теореме 4 работы [1] выделен класс подстановок h, при которых $\delta_2(Gh) = 4$. При этом в нем имеются и аффинные преобразования. С другой стороны, известна (указанная И. Г. Шапошниковым) аффинная подстановка h, при которой $\delta_2(Gh) = 2^{n-2} + 2$. Таким образом, для известных аффинных подстановок h пространства Ω параметр $\delta_2(Gh)$ колеблется от 4 до $2^{n-2} + 2$.

Теорема 3. *Пусть h есть аффинное преобразование* (10) *пространства Ω и матрица A при некотором $k \in \{0, \ldots, n-1\}$ удовлетворяет условиям:*

1^0. $2^k A = (\epsilon, 1, \ldots, 1)$, $\epsilon \in \mathrm{GF}(2)$;

2^0. $2^k A^{-1} = (\delta, 1, \ldots, 1)$, $\delta \in \mathrm{GF}(2)$;

а в случае $k \neq n-1$ также условиям:

3^0. $\delta_k\left(2^k A\right) = 1$;

4^0. $\delta_k\left(2^k A^{-1}\right) = 1$.

Тогда $\delta_2(Gh) \leq 5$ при $k = 0$ и $\delta_2(Gh) \leq 2(n-k) + 3$ при $k > 0$.

Доказательство. Как было уже отмечено, показатель 2-транзитивности множества Gh на единицу больше, чем экспонента матрицы $Q_h = (q_{a,b})$, элемент $q_{a,b}$ которой равен числу решений уравнения (11) при любых

$$a, b \in \Omega^* = \{1, 2, \ldots, 2^n - 1\}.$$

В связи с этим докажем предварительно несколько вспомогательных утверждений об элементах матриц Q_h.

Лемма 1. *Если матрица A удовлетворяет условиям 1^0, 2^0, то элементы $q_{a,2^k}$ и $q_{2^k,a}$ матрицы Q_h отличны от нуля при любом нечетном $a \in \Omega$.*

Доказательство леммы 1. Из определения элемента $q_{a,b}$ матрицы Q_h видно, что в строке с номером a ненулевые элементы находятся в столбцах с номерами из множества

$$\Delta(a) = \{\Delta_x(a) : x \in \Omega\},$$

где

$$\Delta_x(a) = (x + a)\, h - xh.$$

Для нахождения множества $\Delta(2^k)$ разобьем Ω на два подмножества

$$\Omega^{(r)} = \{x \in \Omega : d_k(x) = r\}, \qquad r = 0, 1.$$

Для $x \in \Omega^{(0)}$ выполняется равенство

$$x + 2^k = x \oplus 2^k, \tag{17}$$

и потому

$$\Delta_x\left(2^k\right) = \left(x \oplus 2^k\right) A \oplus \gamma - xA \oplus \gamma = xA \oplus \gamma \oplus 2^k A - xA \oplus \gamma.$$

Отсюда и из условия 1^0 согласно теореме 1 из [1] имеем: если x пробегает все множество Ω, то

$$xA \oplus \gamma \oplus 2^k A - xA \oplus \gamma$$

пробегает множество всех нечетных чисел из Ω, причем каждое из них дважды — один раз при

$$xA \oplus \gamma = y,$$

другой при

$$xA \oplus \gamma = y + 2^{n-1},$$

т.е. один раз при некотором

$$x_1 = (y \oplus \gamma)\, A^{-1},$$

другой при

$$x_2 = \left(\left(y + 2^{n-1}\right) \oplus \gamma\right) A^{-1}.$$

Покажем, что x_1, x_2 не могут одновременно принадлежать множеству $\Omega^{(0)}$. Допустим, что $x_1, x_2 \in \Omega^{(0)}$, т.е.

$$d_k\left((y\oplus\gamma)A^{-1}\right)=d_k\left(\left(\left(y+2^{n-1}\right)\oplus\gamma\right)A^{-1}\right)=0. \qquad (18)$$

Из (18), (17) и условия 2^0 вытекает невозможное равенство

$$d_k\left((y\oplus\gamma)A^{-1}\right)=d_k\left((y\oplus\gamma)A^{-1}\right)\oplus 1.$$

Значит, при различных значениях x из $\Omega^{(0)}$ разность $\Delta_x\left(2^k\right)$ принимает различные и, очевидно, нечетные значения. Отсюда и следует, что $q_{2^k,a}\neq 0$ при любом нечетном значении a.

Соотношение $q_{a,2^k}\neq 0$ доказывается аналогично. Из (11) находим множество номеров строк с ненулевыми элементами в столбце с номером b:

$$\Delta'(a)=\{\Delta'_x(b):x\in\Omega\},\qquad \text{где}\qquad \Delta'_x(b)=(xh+b)\,h^{-1}-x.$$

Для нахождения элемента $\Delta'_x\left(2^k\right)$ разобьем множество Ω на два подмножества

$$\Sigma^{(r)}=\{x\in\Omega:d_k(x\oplus\gamma)=r\},\qquad r=0,1.$$

Для векторов $x\in\Sigma^{(0)}$ имеем

$$\Delta'_x\left(2^k\right)=x\oplus\gamma A^{-1}\oplus 2^kA^{-1}\oplus\gamma A^{-1}-x=x\oplus 2^kA^{-1}-x.$$

Отсюда и из условия 2^0 мы снова по теореме 1 из [1] получаем: если x пробегает Ω, то $x\oplus 2^kA^{-1}-x$ пробегает по два раза все нечетные числа из Ω, причем один раз при некотором x_1, другой — при $x_2=x_1+2^{n-1}$. Однако, если $x_1\in\Sigma^{(0)}$, то

$$d_k(x_2A\oplus\gamma)=d_k\left(x_1A\oplus 2^{n-1}A\oplus\gamma\right)=d_k(x_1A\oplus\gamma)\oplus 1=1,$$

и, значит, $x_2\notin\Sigma^{(0)}$. Отсюда следует, что величина $\Delta'_x\left(2^k\right)$ при различных значениях x из Ω принимает различные и, очевидно, нечетные значения. Это и означает, что $q_{a,2^k}\neq 0$ при всех нечетных значениях a. Лемма доказана.

Лемма 2. *Пусть матрица A удовлетворяет условиям 1^0–2^0. Если либо $k=0$, либо $k=n-1$ и a — любой элемент из Ω^*, либо $0<k<n-1$ и a не кратно 2^{k+1}, то найдутся такие нечетные $b_1,b_2\in\Omega^*$, что*

$$q_{a,b_1}\neq 0,\qquad q_{b_2,a}\neq 0.$$

Доказательство леммы 2. Пусть при некотором $a\in\Omega^*$ равенство $q_{a,b}=0$ выполняется при всех нечетных b. Это означает, что число

$$\Delta_x(a)=(x+a)\,A\oplus\gamma-xA\oplus\gamma$$

является четным при любом $x\in\Omega$. Обозначим через Ω_0, Ω_1 соответственно множества всех четных и всех нечетных чисел из Ω. Тогда указанный выше факт можно записать в виде равенств

$$\Omega_r A^{-1} + a = \Omega_r A^{-1}, \qquad r = 0, 1.$$

Поэтому равенства

$$\Omega_r A^{-1} + c = \Omega_r A^{-1}, \qquad r = 0, 1, \tag{19}$$

выполняются для всех c из подгруппы $\langle a \rangle$ группы $(\Omega; +)$. Если $a = 2^s a_1$, где $s \geq 0$, a_1 — нечетно, то $\langle a \rangle = \langle 2^s \rangle$, и из (19) следует, что $\Omega_r A^{-1}$ есть объединение смежных классов группы $(\Omega; +)$ по подгруппе $\langle 2^s \rangle$. Отсюда, учитывая, что Ω_0 — подгруппа группы $(\Omega; +)$, получаем включение

$$\langle 2^s \rangle \subset \Omega_0 A^{-1}, \tag{20}$$

а значит, и соотношение $2^{n-1} \in \Omega_0 A^{-1}$, которое при $k = 0$ противоречит условию 3^0, а при $k = n - 1$ противоречит условию 1^0.

Пусть теперь $0 < k < n - 1$ и a не кратно 2^{k+1}, т.е. $3 \leq k$. Тогда $2^k \in \langle 2^s \rangle$ и в силу (20) имеем $2^k \in \Omega_0 A^{-1}$, что противоречит условию 1^0. Таким образом, существование нечетного b_1 при котором $q_{a,b_1} \neq 0$, доказано во всех случаях. Существование требуемого нечетного b_2 доказывается аналогичным образом. Здесь вместо $\Delta_x(a)$ надо будет рассмотреть $\Delta'_x(a)$ и тогда вместо соотношений (19) получатся соотношения

$$\Omega_r A + c = \Omega_r A, \qquad r = 0, 1,$$

которые во всех случаях приводят к противоречию с условием 2^0 или 4^0.

Лемма 3. *Пусть матрица A удовлетворяет условиям 1^0–4^0 теоремы 3, $k \leq n - 2$ и для некоторого $r \in \{k + 1, \ldots, n - 1\}$ число a из Ω^* не кратно 2^{r+1}. Тогда существуют такие не кратные 2^r элементы $b_1, b_2 \in \Omega$, что*

$$q_{a,b_1} \neq 0, \qquad q_{b_2,a} \neq 0.$$

Доказательство леммы 3. Допустив, что $q_{a,b} = 0$ при всех b, не кратных 2^r, как и выше, получим соотношения

$$H_m A^{-1} + a = H_m A^{-1} \tag{21}$$

для любого смежного класса H_m группы $(\Omega; +)$ по подгруппе $H_0 = \langle 2^r \rangle$. Значит, $H_m A^{-1}$ есть объединение смежных классов группы $(\Omega; +)$ по подгруппе $\langle a \rangle$. Если $a = 2^s a_1$, a_1 нечетно, то

$$\langle a \rangle = \langle 2^s \rangle \quad \text{и} \quad |H_m A^{-1}| \geq |\langle 2^s \rangle|,$$

т.е. $s \geq r$. С другой стороны, по условию леммы a не кратно 2^{r+1}, и потому $s \leq r$. Значит, $s = r$, и тогда из (21) получаем

$$H_0 A^{-1} = \langle a \rangle = \langle 2^r \rangle.$$

Из этого равенства следует включение $2^{n-1}A^{-1} \in \langle 2^r \rangle$, противоречащее условию 4^0 (поскольку $r > k$). Аналогичным образом мы получим противоречие с условием 3^0, если допустим, что $q_{b,a} = 0$ при всех b, не кратных 2^r. Лемма доказана.

Лемма 4. *Если матрица A удовлетворяет условиям 1^0–4^0, то при любом $m \in \{2, \ldots, n-k+1\}$ в матрице $Q_h^m = (q_{a,b}^{(m)})$ элементы $q_{2^k,b}^{(m)}$, $q_{b,2^k}^{(m)}$ отличны от нуля при любом b, не кратном 2^{k+m-1}.*

Доказательство этой леммы проведем индукцией по m. Пусть $m = 2$ и b не кратно 2^{k+1}. Рассмотрим элемент

$$q_{2^k,b}^{(2)} = \sum_{c=1}^{2^n-1} q_{2^k,c} q_{c,b}.$$

По лемме 1 имеем $q_{2^k,c} \neq 0$ при любом нечетном c, а по лемме 2 найдется нечетное c, при котором $q_{c,b} \neq 0$. Отсюда и следует, что $q_{2^k,b}^{(2)} \neq 0$. Из лемм 1, 2 следует также, что $q_{b,2^k}^{(2)} \neq 0$, и для $m=2$ утверждение леммы 4 доказано. Допустим, что оно верно для $m=s$ при некотором $s \in \{2, \ldots, n-k\}$, и докажем его для $m = s+1$.

Пусть b не кратно 2^{k+s}. Рассмотрим элемент

$$q_{2^k,b}^{(s+1)} = \sum_{c=1}^{2^n-1} q_{2^k,c}^{(s)} q_{c,b}.$$

По предположению индукции $q_{2^k,c}^{(s)} \neq 0$ при всех c, не кратных 2^{k+s-1}. С другой стороны, по лемме 3 для $k \neq n-1$ и b, не кратного 2^{k+s}, найдется такое c, не кратное 2^{k+s-1}, что $q_{c,b} \neq 0$. При $k = n-1$ такое c найдется согласно лемме 2. Значит, во всех случаях получим $q_{2^k,b}^{(s+1)} \neq 0$. Симметричным образом доказывается, что $q_{b,2^k}^{(s+1)} \neq 0$. Лемма доказана.

Теперь из лемм 1–4 нетрудно получить утверждение теоремы 2. Действительно, по лемме 4 имеем: при $k+m-1 = n$, т.е. при $m = n-k+1$, элементы $q_{2^k,b}^{(m)}$, $q_{b,2^k}^{(m)}$ отличны от нуля при любом $b \in \Omega^*$. Тогда, очевидно,

$$(Q_h^m)^2 > 0, \quad \text{т.е.} \quad Q_h^{2(n-k+1)} > 0,$$

и, значит,

$$\delta_2(Gh) \leq 2(n-k) + 3.$$

При $k = 0$ можно получить более точную оценку. Из лемм 1, 2 следует, что при $k = 0$ выполняются неравенства

$$q_{2^k,b}^{(2)} \neq 0, \qquad q_{b,2^k}^{(2)} \neq 0$$

при любом $b \in \Omega^*$. Значит, $Q_h^4 > 0$, т.е. $\delta_2(Gh) \leq 5$. Теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. *Глухов М. М.* О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 43–66.

2. *Погорелов Б. А.* Примитивные группы подстановок, содержащие 2^m-цикл. — Алгебра и логика, 1980, т. 19, №2, с. 236–247.

3. *Холл М.* Теория групп. — М.: ИЛ, 1962.