УДК 512.542.7

Чётные подстановки, не представимые в виде произведения двух подстановок заданного порядка

В. Г. Бардаков

В работе описываются подстановки из знакопеременной группы A_n, которые для заданного натурального $k \geq 4$ не представимы в виде произведения двух подстановок, каждая из которых в разложении на независимые циклы содержит только циклы длины k и 1. Строится множество натуральных чисел Q_k такое, что для всякого n из Q_k в группе A_n найдутся подстановки, не представимые в указанном виде.

Даются ответы на два вопроса Бреннера и Эванса о представимости четных подстановок в виде произведения двух подстановок заданного порядка k.

Библиография: 5 названий.

Введение. Для произвольной группы G, содержащей элементы конечного порядка k, можно поставить вопрос об описании элементов из G представимых в виде произведения элементов порядка k. В частности, если l — некоторое натуральное число, то возникает вопрос об описании элементов из G представимых в виде произведения $\leq l$ элементов порядка k. Этот вопрос был сформулирован Бреннером–Эвансом [1] для группы подстановок S_n при $l = 2$. В частности, они просили указать для каждого натурального k такую константу $N(k)$ (если она существует), что при всех $n \geq N(k)$ всякая подстановка из знакопеременной группы A_n представима в виде произведения двух подстановок каждая из которых в разложении на независимые циклы содержит только циклы длины k и 1. Там же они сформулировали гипотезу: при любых целых $k \geq 4$ и $m \geq 1$ всякий элемент группы A_{km} представим в виде произведения двух подстановок, каждая из которых в разложении на независимые циклы состоит из m циклов длины k. Полное доказательство этой гипотезы можно найти в работе [2].

Далее, естественно изучать представления подстановок из A_n, где n не делится на k.

В предлагаемой работе для всякого натурального $k \geq 4$ строится множество натуральных чисел Q_k такое, что при всех $n \in Q_k$ в группе A_n найдутся подстановки, не представимые в виде произведения двух подстановок каждая из которых в разложении на независимые циклы содержит только циклы длины k и 1. В частности, мы покажем, что при $k = 4$ множество Q_4 бесконечно, а потому — константы $N(4)$ не существует.

Бреннер и Эванс [1] сформулировали следующие гипотезы:

Гипотеза 1. *Пусть k — простое натуральное число, сравнимое с 1 по модулю 4. Тогда никакая подстановка, имеющая циклический тип $4^1 2^{(3k-5)/2}$ не может быть представлена в группе A_{3k-1} в виде произведения двух подстановок порядка k.*

Гипотеза 2. *Пусть k — простое натуральное число, $k \geq 7$. Тогда никакая подстановка, имеющая циклический тип $3^1 2^{2k-2}$ не может быть представлена в группе A_{4k-1} в виде произведения двух подстановок порядка k.*

Ранее справедливость первой гипотезы была установлена только при $k = 5$ в работе [1]. Там же было отмечено, что при $k = 7$ справедливость второй гипотезы была проверена Листом, который использовал таблицу характеров и компьютерные вычисления.

Из теоремы, доказанной в настоящей работе, в качестве следствия будет установлена справедливость первой гипотезы для всех указанных значений k. Кроме того, будет доказано, что вторая гипотеза неверна уже при $k = 11$, но тем не менее, если k — простое и сравнимо с 1 по модулю 3, то вторая гипотеза справедлива.

Автор благодарит участников семинара "Эварист Галуа", прослушавших доказательства и внёсших ряд полезных предложений.

§ 1. Предварительные замечания

Напомним вначале необходимые определения. Символом S_n будем обозначать группу подстановок n–элементного множества $M = \{1, 2, \ldots, n\}$. Если P — некоторая подстановка из S_n, то под действием группы гр(P) множество M разбивается на непересекающиеся орбиты $M_1, \ldots, M_l$. Действие подстановки P на множестве M индуцирует её действие на каждой орбите M_i. Будем называть ограничение $P_i = P|_{M_i}$ *циклом* подстановки P.

Представив P в виде произведения независимых циклов $P = P_1 \ldots P_l$, определим упорядоченную последовательность чисел $\tau(P) = (\tau_1, \ldots \tau_l)$, где τ_i — длина цикла P_i, которую назовём *циклическим типом* (или просто *типом*) подстановки P. Понятно, что циклический тип определяется неоднозначно, а зависит от порядка следования циклов P_i в разложении $P = P_1 \ldots P_l$. Среди всех типов подстановки P будем выделять такой тип, что его компоненты расположены в невозрастающем порядке. Для сокращения записи, тип $\tau(P) = (\underbrace{\tau_1, \ldots, \tau_1}_{\alpha_1}, \underbrace{\tau_2, \ldots, \tau_2}_{\alpha_2}, \ldots, \underbrace{\tau_s, \ldots, \tau_s}_{\alpha_s})$ будем записывать в виде $\tau(P) = \tau_1^{\alpha_1} \tau_2^{\alpha_2} \ldots \tau_s^{\alpha_s}$.

Подстановку, имеющую циклический тип $k^\alpha 1^\beta$ при некоторых натуральных α и β будем называть *k–подстановкой*. Множество всех k–подстановок группы S_n обозначим символом $S_n^{(k)}$. Если подстановка P из S_n представима в виде произведения $P = A \cdot B$, где A и B — k–подстановки, то P будем называть *k–представимой подстановкой*, а представление $P = A \cdot B$ — *k–представлением*.

Пусть задано некоторое представление $P = A \cdot B$ подстановки P в виде произведения подстановок A и B из S_n. Назовём это представление *расщепляемым*,

если множество M, на котором действуют подстановки A и B, можно так разбить на два непустых непересекающихся подмножества M', M'', что A и B действуют на них инвариантно. Если такого разбиения не существует, то назовём это представление *нерасщепляемым*.

Если $P = A \cdot B$ — расщепляемое представление, то положим $A' = A|_{M'}$, $A'' = A|_{M''}$ и аналогично, $B' = B|_{M'}$, $B'' = B|_{M''}$. Тогда наше представление можно записать в виде:

$$P = A \cdot B = A'A'' \cdot B'B'' = A'B' \cdot A''B''.$$

Если при этом представление $P = A \cdot B$ являлось k–представлением и каждое из представлений $P' = A' \cdot B'$ и $P'' = A'' \cdot B''$ также является k–представлением, то исходное представление назовём *расщепляемым k–представлением*.

В работе Голдстейна и Тёрнера [4] каждому представлению $P = A \cdot B$ подстановки P из S_n сопоставлялась компактная ориентированная поверхность $S_{A,B}$. Напомним эту конструкцию. Пусть $A = A_1A_2 \dots A_q$ и $B = B_1B_2 \dots B_r$ — разложения подстановок A и B в произведение независимых циклов. Каждому циклу A_i, $i = 1, \dots, q$, сопоставим диск D_{A_i}, граница которого разбита на столько рёбер, сколько символов содержит цикл A_i. Эти рёбра ориентированы по часовой стрелке и помечены символами из цикла A_i так, что при обходе по часовой стрелке границы диска D_{A_i}, получим цикл A_i. Аналогично, сопоставим каждому циклу B_j, $j = 1, \dots, r$, диск D_{B_j} так, что обходя границу этого диска по часовой стрелке, получим цикл B_j, но рёбра ориентируем против часовой стрелке. Тогда $S_{A,B}$ — ориентированная поверхность, полученная отождествлением для каждого символа $i \in M$ двух рёбер (в соответствии с ориентацией) помеченных символом i. Очевидно, если $P = A \cdot B$ — нерасщепляемое представление, то поверхность $S_{A,B}$ оказывается связной. В противном случае, она распадается на несколько непересекающихся поверхностей.

Легко заметить, что $S_{A,B}$ будет иметь столько вершин, сколько независимых циклов имеет подстановка $P = A \cdot B$. Кроме того, $S_{A,B}$ содержит n рёбер и $|A| + |B| = q + r$ граней, где $|X|$ — число независимых циклов подстановки X. Следовательно, если поверхность $S_{A,B}$ является связной, то для неё справедлива формула Эйлера–Пуанкаре

$$|A \cdot B| - n + (|A| + |B|) = 2 - 2g,$$

где g — род ориентированной поверхности $S_{A,B}$. Ввиду того, что $g \geq 0$, из этого равенства легко получить следующую оценку

$$|A \cdot B| \leq n + 2 - (|A| + |B|). \tag{1}$$

Эту оценку мы и будем использовать при описании подстановок не являющихся k–представимыми. Для k–подстановок A и B из $S_n^{(k)}$ легко найти максимальное значение правой части неравенства (1). Если, при этом, в группе A_n найдётся подстановка, число независимых циклов которой больше найденного максимума, то такая подстановка не имеет нерасщепляемых k–представлений в группе S_n. Доказательство отсутствия расщепляемых k–представлений проводится с использова-

нием индуктивных рассуждений. В этом и состоит идея доказательства основной теоремы, сформулированной в § 2.

Бертрам [5] изучал подстановки, представимые в виде произведения двух циклов длины k, $k \geq 4$, и доказал, что если k и n — натуральные числа, причём, $k \geq 4$ и $k \leq n \leq [4k/3] + 1$, где квадратные скобки означают взятие целой части, то всякая чётная подстановка из A_n является k–представимой. Если же $n > [4k/3] + 1$, то в группе A_n найдётся подстановка P для которой не существует никакого k–представления $P = A \cdot B$ при условии, что A и B содержат не более одного цикла длины k. При доказательстве этого факта, для каждого натурального $n \geq 4$, был указан класс сопряжённых элементов группы A_n такой, что всякая подстановка из этого класса имеет в разложении на независимые циклы наибольшее число неединичных циклов, по сравнению с подстановками из других классов группы A_n.

Приведём этот список:

при $n \equiv 0 \pmod 4$ такой класс определяется типом $2^{n/2}$,
при $n \equiv 1 \pmod 4$ — типом $5^1 2^{(n-5)/2}$,
при $n \equiv 2 \pmod 4$ — типом $4^1 2^{(n-4)/2}$,
при $n \equiv 3 \pmod 4$ — типом $3^1 2^{(n-3)/2}$,

В соответствии с этим описанием, введём функцию $\nu : \mathbb{N} \longrightarrow \mathbb{N}$, которая каждому натуральному $x \geq 4$ сопоставляет число неединичных циклов построенного выше класса в группе A_x. Тогда $\nu(x)$ определяется следующим образом

$$\nu(x) = \begin{cases} 2x_1, & \text{при } x = 4x_1, \\ 2x_1 - 1, & \text{при } x = 4x_1 + 1, \\ 2x_1, & \text{при } x = 4x_1 + 2, \\ 2x_1 + 1, & \text{при } x = 4x_1 + 3. \end{cases}$$

Ввиду того, что при сопряжении подстановки её циклический тип не меняется (см. [3, с.35]), для доказательства k–представимости подстановки $P \in A_n$, достаточно доказать k–представимость любой подстановки лежащей в том же классе сопряжённых (в S_n) элементов, что и P.

§ 2. Описание подстановок, не являющихся k–представимыми

Пусть p и q — натуральные числа. Символом $[p, q]$ будем обозначать множество таких натуральных чисел x , что $p \leq x \leq q$ при $p \leq q$ и полагаем $[p, q] = \emptyset$ при $p > q$. Для каждого натурального $k \geq 4$ определим множество

$$Q_k = \begin{cases} 4l + 3,\ l = 1, 2, \ldots, & \text{при } k = 4, \\ [2(k - k_1) + 2, 2k - 1] \bigcup [3k - k_1 + 2, 3k - 1], & \text{при } k = 3k_1, \\ [2(k - k_1) + 1, 2k - 1] \bigcup [3k - k_1, 3k - 1] \bigcup [4k - 1, 4k - 1], & \text{при } k = 3k_1 + 1, \\ [2(k - k_1), 2k - 1] \bigcup [3k - k_1, 3k - 1], & \text{при } k = 3k_1 + 2. \end{cases}$$

В этих обозначениях справедлива

Теорема. *Пусть $k \geq 4$ и $n \in Q_k$. Тогда в группе A_n найдётся подстановка, которая не является k–представимой.*

Доказательство. Для всякого натурального $k \geq 4$ определим функцию $\mu_k : \mathbb{N} \longrightarrow \mathbb{N}$ натурального аргумента $x \geq k$ по правилу

$$\mu_k(x) = \max_{A,B \in S_x^{(k)}} (x + 2 - |A| - |B|). \tag{2}$$

Ввиду оценки (1) из § 1, $\mu_k(x)$ равно максимальному числу независимых циклов подстановки $A \cdot B$ по всем k–подстановкам A и B из группы S_x. Очевидно, что максимум в правой части равенства (2) достигается на таких подстановках A и B, которые содержат наибольшее число k–циклов при данном x. Ясно, что такие подстановки содержат $[x/k]$ циклов длины k и $x - k[x/k]$ циклов длины 1. Следовательно,

$$\mu_k(x) = 2(1 + [x/k](k-1)) - x.$$

Аналогично, при $k = 4$, определим функцию

$$\mu_4^+(x) = \max_{A,B \in S_x^{(4)},\ A \cdot B \notin A_x} (x + 2 - |A| - |B|).$$

Ясно, что максимум в правой части этого равенства достигается на таких подстановках A и B, одна из которых имеет максимальное число 4–циклов в группе S_n, а другая — на один 4–цикл меньше, остальные же циклы, входящие в разложения A и B, являются 1–циклами.

Отметим некоторые свойства функции $\mu_k(x)$. Рассмотрим множество $T_i = [ik, (i+1)k-1]$, $i = 1, 2, \ldots$. На этом множестве функция $\mu_k(x)$ монотонно убывает. Если x_0 и x_0+1 принадлежат T_i, то значение $\mu_k(x_0)$ на единицу больше значения $\mu_k(x_0+1)$. Сравнивая поведение функции $\mu_k(x)$ с поведением функции $\nu(x)$, определённой в § 1, заметим, что если для некоторого $x_0 \in T_i$ справедливо неравенство

$$\nu(x_0) > \mu_k(x_0),$$

то и для всякого $x \in [x_0, (i+1)k - 1]$ справедливо неравенство

$$\nu(x) > \mu_k(x).$$

Последнее неравенство, ввиду оценки (1), означает, что в группе A_x подстановка, имеющая максимальное число неединичных циклов не имеет нерасщепляемого k–представления. Аналогичными свойствами обладает и функция $\mu_4^+(x)$.

Приступим непосредственно к доказательству теоремы.

Пусть вначале $k = 4$. Если $n \in Q_4$, т. е. $n = 4l+3$ для некоторого натурального l, то $\nu(n) = 2l + 1$. В то же время, легко проверить, что

$$\mu_4(n) = 2l - 1.$$

Следовательно, если $n \in Q_4$, то никакая подстановка $P \in A_n$, имеющая циклический тип $\tau(P) = 3^1 2^{2l}$ не имеет нерасщепляемого 4–представления в группе S_n.

Покажем теперь, что эта подстановка не может иметь и расщепляемого 4–представления. Для $l = 1$ это очевидно. Рассмотрим некоторое значение $l > 1$ и предположим, что при $n = 4l + 3$ подстановка $P \in A_n$, имеющая циклический тип $\tau(P) = 3^1 2^{2l}$ обладает расщепляемым 4–представлением $P = A \cdot B$, т. е. $P = P' \cdot P''$, $A = A' \cdot A''$, $B = B' \cdot B''$ —такие разложения в произведения независимых циклов, для которых $P' = A' \cdot B'$ и $P'' = A'' \cdot B''$. Найдём циклические типы подстановок P' и P''. Очевидно, что $\tau(P') = 3^1 2^\alpha$, $\tau(P'') = 2^\beta$, где $\alpha + \beta = 2l$. Если предположить, что α чётно, то тогда P' — чётная подстановка и $P' = A' \cdot B'$ — 4–представление, что невозможно по индуктивному предположению. Предположим, что α — нечётно. Не уменьшая общности, можно считать, что либо представление $P' = A' \cdot B'$, либо представление $P'' = A'' \cdot B''$ не является расщепляемым. Допустим, что таким представлением является первое представление. Найдём значение функции μ_4^+ в точке $n_1 = 2\alpha + 3$. Так как α нечётно, то $\alpha = 2\alpha_1 - 1$ для некоторого натурального α_1. Тогда $n_1 = 4\alpha_1 + 1$ и

$$\mu_4^+(n_1) = 2\alpha_1 - 2,$$

т. е. в группе S_{n_1}, нечётная подстановка, обладающая 4–представлением, не может содержать $> 2\alpha_1 - 2$ независимых циклов, а у нас P' имеет $2\alpha_1$ независимых циклов. Следовательно, P' не имеет нерасщепляемого 4–представления. Предположим поэтому, что нерасщепляемым является 4–представление $P'' = A'' \cdot B''$. Так как β нечётно, то $\beta = 2\beta_1 + 1$ для некоторого натурального β_1. Найдём значение функции μ_4^+ в точке $n_2 = 2\beta = 4\beta_1 + 2$. Ввиду того, что

$$\mu_4^+(n_2) = 2\beta_1 - 3,$$

а P'' имеет $2\beta_1 + 1$ независимых циклов, заключаем, вопреки предположению, что и P'' не имеет нерасщепляемого 4–представления. Следовательно, если $n \in Q_4$, то в группе A_n найдутся подстановки, которые не являются 4–представимыми.

Пусть теперь $k > 4$. Легко проверить, что левая граница первого интервала множества Q_k равна $[4k/3] + 2$. Тогда, по теореме Бертрама [4], если n принадлежит первому интервалу, то в группе A_n найдутся подстановки, которые не являются k–представимыми. Более того, так как при этих значениях n подстановка $P \in A_n$ обладает расщепляемым k–представлением лишь в том случае, если она содержит 1–циклы, то, используя свойства функций $\nu(x)$ и $\mu_k(x)$, легко показать, что подстановки, содержащие наибольшее число неединичных циклов, не являются k–представимыми.

Предположим, что n принадлежит второму интервалу множества Q_k. Обозначим левую границу этого интервала через α, а правую — через β. Покажем, что при всех значениях $k \geq 5$ справедливо неравенство

$$\nu(\alpha) > \mu_k(\alpha). \tag{3}$$

Тогда из рассуждений, проведённых в начале доказательства теоремы, последует, что при всех $n \in [\alpha, \beta]$ в группе A_n найдутся подстановки, которые не имеют нерасщепляемых k–представлений.

Если $k = 3k_1$, т. е. делится нацело на 3, то $\alpha = 2(4k_1 + 1)$ и $\mu_k(\alpha) = 4k_1 - 4$, а $\nu(\alpha) = 4k_1$. Следовательно, неравенство (3) справедливо.

Если $k = 3k_1 + 1$, то $\alpha = 8k_1 + 3$ и $\mu_k(\alpha) = 4k_1 - 1$, а $\nu(\alpha) = 4k_1 + 1$. Опять неравенство (3) справедливо.

Если же $k = 3k_1 + 2$, то $\alpha = 4(2k_1 + 1) + 2$ и $\mu_k(\alpha) = 4k_1$, а $\nu(\alpha) = 4k_1 + 2$. Следовательно, неравенство (3) справедливо при всех значениях k.

Пусть теперь n принадлежит третьему интервалу, т. е. $n = 4k - 1$, $k = 3k_1 + 1$. Опять найдём значение $\nu(n)$ и $\mu_k(n)$. Легко проверить, что $\nu(n) = 6k_1 + 1$, а $\mu_k(n) = 6k_1 - 1$, т. е. опять $\nu(n) > \mu_k(n)$.

Таким образом, мы установили, что при всех $n \in Q_k$ в группе A_n найдутся подстановки, которые не имеют нерасщепляемых k–представлений.

Покажем теперь, что при этих же значениях n подстановки, имеющие в своём разложении наибольшее число неединичных циклов в группе A_n, не обладают и расщепляемыми k–представлениями.

Пусть вначале n принадлежит второму интервалу множества Q_k (для первого интервала требуемое утверждение установлено ранее). Предположим, что подстановка $P \in A_n$ типа $\tau(P) = c^1 2^{(n-c)/2}$, где $c = 2, 3, 4, 5$, — в зависимости от значения n, имеет расщепляемое k–представление $P' \cdot P'' = (A' \cdot B') \cdot (A'' \cdot B'')$, т. е. $P = P' \cdot P''$, $P' = A' \cdot B'$, $P'' = A'' \cdot B''$ и множество символов, на которых определены подстановки со штрихами, не пересекается с множеством символов, на которых определены подстановки с двумя штрихами. Так как $A' \cdot A''$ и $B' \cdot B''$ содержат не более двух неединичных циклов, то обе подстановки P' и P'' являются чётными. Не уменьшая общности, будем считать, что $\tau(P') = c^1 2^{(n-c)/2-2l}$, $\tau(P'') = 2^{2l}$, где l — некоторое положительное целое. Положим $n_2 = 4l$, а $n_1 = n - n_2$. Из циклового строения подстановок P' и P'' видно, что они имеют наибольшее число неединичных циклов в группах A_{n_1} и A_{n_2}, соответственно. Покажем, что обе они не могут быть одновременно k–представимыми. В зависимости от значения k рассмотрим три случая.

Пусть $k = 3k_1$. Так как n лежит во втором интервале множества Q_k, то

$$8k_1 + 2 \le n \le 9k_1 - 1. \tag{4}$$

Значение n_2 не может принадлежать первому интервалу множества Q_k (иначе, представление $P'' = A'' \cdot B''$ не являлось бы k–представлением). Следовательно,

$$n_2 = 4l < 2(k - k_1) + 2 = 4k_1 + 2,$$

Отсюда, $l \le k_1$. Из этой оценки, для $n_1 = n - 4l$ имеем

$$n - 4k_1 \le n - 4l = n_1.$$

С другой стороны, вычитая из всех частей неравенства (4) значение $4k_1$, получим

$$4k_1 + 2 \le n - 4k_1 \le 5k_1 - 1,$$

т. е. $n_1 \ge 4k_1 + 2 = 2(k - k_1) + 2$, а так как подстановка P — расщепляема, то $n_1 \le 2k - 1$. Следовательно, n_1 лежит в первом интервале множества Q_k, а так

как подстановка P' содержит наибольшее число неединичных циклов в группе A_{n_1}, то, вопреки предположению, P' не имеет k–представления в группе S_{n_1}.

Пусть теперь $k = 3k_1 + 1$. Так как n лежит во втором интервале множества Q_k, то

$$8k_1 + 3 \leq n \leq 9k_1 + 2. \tag{5}$$

Так же как и выше, заключаем, что n_2 не лежит в первом интервале множества Q_k. Следовательно,

$$n_2 = 4l < 2(k - k_1) + 1 = 4k_1 + 3.$$

Так как l и k — целые, то отсюда

$$l \leq k_1.$$

Для $n_1 = n - 4l$ опять получим оценку

$$n - 4k_1 \leq n - 4l = n_1.$$

С другой стороны, из (5),

$$4k_1 + 3 \leq n - 4k_1 \leq 5k_1 + 2,$$

т. е. $n_1 \geq 4k_1 + 3$. Опять значение n_1 попадает в первый интервал множества Q_k, а потому — подстановка P' не имеет k–представления в группе S_{n_1}.

Пусть, наконец, $k = 3k_1 + 2$. Ввиду того, что n лежит во втором интервале множества Q_k,

$$8k_1 + 6 \leq n \leq 9k_1 + 5. \tag{6}$$

Так как n_2 не лежит в первом интервале множества Q_k, то

$$n_2 = 4l < 4k_1 + 4.$$

Ввиду того, что l и k — целые,

$$l \leq k_1.$$

Из этого неравенства получим оценку:

$$n - 4k_1 \leq n - 4l = n_1.$$

Вычитая $4k_1$ из всех частей неравенства (6) и, учитывая предыдущее неравенство, находим,

$$4k_1 + 6 \leq n_1.$$

А так как подстановка P расщепляема, то $n_1 \leq 2k - 1$. Следовательно, n_1 опять попадает в первый интервал и, из тех же соображений, что и выше, заключаем, что P' не имеет k–представления.

Таким образом, нами доказано, что если n лежит во втором интервале множества Q_k, то никакая подстановка $P \in A_n$, имеющая в своём разложении на независимые циклы наибольшее число неединичных циклов, не является k–представимой.

Предположим теперь, что n принадлежит третьему интервалу множества Q_k, т. е. $n = 4k-1$ и $k = 3k_1+1$. Рассмотрим подстановку $P \in A_n$, имеющую наибольшее число неединичных циклов, т. е. $\tau(P) = 3^1 2^{2(k-1)}$. Предположим, что P обладает расщепляемым k–представлением, т. е. $P = P' \cdot P''$, где $P' \in A_{n_1}$, $P'' \in A_{n_2}$ и $n = n_1 + n_2$. Не уменьшая общности, будем считать, что $n_1 < n_2$. Так как P — расщепляема, то P' имеет k–представление $P' = A' \cdot B'$. Очевидно, что ни A', ни B' не могут содержать более одного k–цикла. С другой стороны, ни одна из них не может быть тождественной подстановкой, так как $k \geq 5$, а P' не содержит циклов длины > 4. Следовательно, A' и B' содержат по одному циклу длины k и их произведение — подстановка P' является чётной.

Предположим, вначале, что P' содержит цикл длины 3. Тогда $\tau(P') = 3^1 2^{2l}$ для некоторого натурального l. Ввиду того, что $P' = A' \cdot B'$ — k–представление и P' содержит наибольшее число неединичных циклов в группе A_{n_1}, заключаем, что n_1 не лежит в первом интервале множества Q_k, а так как $n_1 < 2k-1$, то

$$n_1 = 4l + 3 < 4k_1 + 3.$$

Так как n_1 нечётно, то из этого неравенства,

$$n_1 = 4l + 3 \leq 4k_1 + 1,$$

а так как l — целое, то отсюда получаем, что

$$l \leq k_1 - 1.$$

Из этих оценок легко получить оценку на n_2:

$$n_2 = n - n_1 = n - (4l+3) \geq n - (4(k_1-1)+3) = 8k_1 + 4 = 3k - k_1 + 1.$$

Следовательно, n_2 лежит во втором интервале множества Q_k. Но P'' имеет наибольшее число неединичных циклов в группе A_{n_2}, а потому, по доказанному ранее, $P'' = A'' \cdot B''$ не может быть k–представлением.

Предположим, что P' не содержит цикла длины 3, т. е. $\tau(P') = 2^{2l}$. Так как $n_1 = 4l$ не принадлежит первому интервалу множества Q_k, то

$$n_1 = 4l < 4k_1 + 3.$$

Отсюда, $l \leq k_1$. Оценим значение n_2:

$$n_2 = n - n_1 = 4k - 1 - 4l \geq 8k_1 + 3 = 3k - k_1.$$

Следовательно, n_2 попадает во второй интервал множества Q_k, а потому, вопреки предположению, P не имеет расщепляемого k–представления. Теорема доказана.

Если k — простое, то очевидно, что подстановка является k–представимой тогда и только тогда, когда она представима в виде произведения двух элементов порядка k.

Пусть k — простое сравнимое с 1 по модулю 4, т. е. $k = 4k_1 + 1$ и $n = 3k - 1 = 12k_1 + 2 \equiv 2 \pmod 4$. Тогда в группе A_n подстановка P, имеющая наибольшее число неединичных циклов, имеет циклический тип $\tau(P) = 4^1 2^{(3k-5)/2}$. Очевидно, что $n \in Q_k$, а тогда из теоремы вытекает

Следствие 1. *Для всякого простого $k \equiv 1 \pmod 4$, никакая подстановка $P \in A_{3k-1}$, имеющая циклический тип $\tau(P) = 4^1 2^{(3k-5)/2}$, не представима в виде произведения двух элементов порядка k в группе A_{3k-1}.*

Это следствие доказывает первую гипотезу Бреннера–Эванса.

Покажем, что вторая гипотеза неверна уже при $k = 11$. Действительно, пусть $P \in A_{43}$ и имеет циклический тип $\tau(P) = 3^1 2^{20}$. Покажем, что P имеет расщепляемое 11–представление. Действительно, представим P в виде $P = P' \cdot P''$, где P' и P'' определены на непересекающихся множествах символов, $\tau(P') = 3^1 2^6$, $\tau(P'') = 2^{14}$. Ввиду упоминавшихся результатов Бертрама, в группе A_{15} найдутся подстановки A' и B' такие, что $\tau(A') = \tau(B') = 11^1 1^4$ и $P' = A' \cdot B'$. Определим в группе A_{28} подстановки

$$A''=(1,2,3,4,5,6,7,8,9,0,a)(b,c,d,e,f,g,k,l,m,n,p)(x)(y)(z)(w)(t)(q),$$

$$B''=(x,2,a,y,0,8,c,z,b,n,3)(d,7,w,6,4,m,k,t,g,q,f)(1)(5)(9)(e)(l)(p).$$

Легко проверить, что их произведение $A'' \cdot B''$ имеет циклический тип 2^{14}. Положим $A = A' \cdot A''$, $B = B' \cdot B''$. Очевидно, что эти подстановки имеют порядок 11 и их произведение $A \cdot B$ имеет циклический тип $3^1 2^{20}$. Сопрягая соответствующим образом найденное представление, получим требуемое представление подстановки P. Таким образом, для произвольного простого k вторая гипотеза Бреннера–Эванса не верна. Но если потребовать, чтобы k было сравнимо с 1 по модулю 3, то из теоремы легко выводится

Следствие 2. *Пусть k — простое, $k \equiv 1 \pmod 3$. Тогда никакая подстановка, имеющая циклический тип $3^1 2^{2k-2}$ не представима в виде произведения двух подстановок порядка k в группе A_{4k-1}.*

Автору не известно, все ли значения n для которых существуют подстановки из A_n, не являющиеся k–представимыми, содержатся в множестве Q_k. В связи с этим, возникает естественный

Вопрос. *Существуют ли натуральные числа k и n, $4 \le k \le n$, такие, что n не содержится в множестве Q_k, но тем не менее, в группе A_n существуют подстановки, не являющиеся k–представимыми?*

Если бы ответ на этот вопрос оказался отрицательным, то это давало бы ответ на вопрос Бреннера–Эванса, упоминавшийся во введении, а в качестве константы $N(k)$ можно было бы взять $N(k) = 4k$ для всех $k \ge 5$.

Автор предполагает, что справедлива

Гипотеза. *Пусть k и n — натуральные числа, $k \ge 5$, $n \ge 4k$. Тогда всякая подстановка из группы A_n является k–представимой.*

ЛИТЕРАТУРА

1. Brenner J. L., Evans R. J. Even permutations as a product of two elements of order five // J. Comb. Theory. Ser. A. 1987. V. 45. №2. P. 196–206.

2. Бардаков В. Г. Разложение чётных подстановок на два множителя заданного циклового строения // Дискрет. матем. 1993. Т. 5. №1. С. 70–90.

3. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. 3–е изд. М.: Наука, 1982.

4. Goldstein R. Z., Turner E. C. Counting orbits of a product of permutations // Discrete Math. 1990. V. 80. №3. P. 267–272.

5. Bertram E. Even permutations as a product of two conjugate cycles // J. Comb. Theory. Ser. A. 1972. V. 12. №2. P. 368–380.