Лекция 8. Перестановки. Симметрическая группа перестановок. Теорема Кэли. Орбита и стабилизатор элемента. Лемма Бернсайда.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте https://mk.cs.msu.ru

Перестановки

Пусть $N = \{1, 2, \ldots, n\}$, где $n \geqslant 1$.

Перестановкой (n элементов) π называется взаимно однозначное отображение

$$\pi : N \to N.$$

Множество всех перестановок n элементов обозначим S_n.

Как задавать перестановки

1) Таблица:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

в каждом столбце элемент в первой строке перестановкой переводится в элемент во второй строке.

Как задавать перестановки

2) Строка:

$$\pi = [2, 1, 4, 3],$$

в строке на i-м месте стоит элемент $\pi(i)$.

Как задавать перестановки

3) Произведение циклов:

$$\pi = (1, 2)(3, 4),$$

каждая скобка является отдельным циклом, в каждой скобке следующий элемент получен из предыдущего применением перестановки, первый элемент получен из последнего применением перестановки.

Тип перестановки

Длиной цикла перестановки называется число элементов в нем.

Типом перестановки $\pi \in S_n$ называется набор

$$\lambda(\pi) = (\lambda_1(\pi), \ldots, \lambda_n(\pi)),$$

где $\lambda_i(\pi)$ — число циклов длины i в перестановке π.

Тип перестановки

Отметим, что для любой перестановки $\pi \in S_n$ верно

$$\sum_{i=1}^{n} i \cdot \lambda_i(\pi) = n,$$

т. к. каждый элемент принадлежит ровно одному циклу.

Тип перестановки

Пример. Для перестановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

ее тип:

$$\lambda(\pi) = (0, 2, 0, 0),$$

т. е. в ней два цикла, каждый из которых содержит по два элемента.

Композиция

Введем операцию **композиции** $\circ$ на множестве перестановок.

Композицией (или **произведением**) перестановок π и ρ называется такая перестановка $\pi \circ \rho$, что для любого элемента $x \in N$ верно

$$(\pi \circ \rho)(x) = \pi(\rho(x)).$$

Композиция

Предложение 1. При $n \geqslant 3$ операция композиции перестановок n элементов не является коммутативной.

Доказательство. Рассмотрим перестановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \text{ и } \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}.$$

Тогда

$$(\pi \circ \rho)(1) = 1,$$

а

$$(\rho \circ \pi)(1) = 3.$$

$\square$

Группа перестановок

Предложение 2. *Множество перестановок* n *элементов* S_n *с операцией композиции* $\circ$ *является группой.*

Группа перестановок

Доказательство. Проверим свойства группы.

1) Ассоциативность операции $\circ$.
Пусть $\pi, \rho, \tau \in S_n$. Тогда для любого элемента $x \in N$

$$((\pi \circ \rho) \circ \tau)(x) = (\pi \circ \rho)(\tau(x)) = \pi(\rho(\tau(x)))$$

и

$$(\pi \circ (\rho \circ \tau))(x) = \pi((\rho \circ \tau)(x)) = \pi(\rho(\tau(x))).$$

Группа перестановок

2) Существование нейтрального элемента e.
Нейтральным элементом является перестановка

$$\pi_e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

оставляющая каждый элемент на месте.

Группа перестановок

3) Для каждого элемента π существование симметричного элемента π'.
Для перестановки

$$\pi = \begin{pmatrix} 1 & \dots & i & \dots & n \\ \pi(1) & \dots & \pi(i) & \dots & \pi(n) \end{pmatrix}$$

обратным (симметричным) элементом является перестановка

$$\pi^{-1} = \begin{pmatrix} \pi(1) & \dots & \pi(i) & \dots & \pi(n) \\ 1 & \dots & i & \dots & n \end{pmatrix}.$$

Следовательно, $(S_n, \circ)$ — группа.

Кроме того, при $n \geqslant 3$ эта группа не коммутативна.

$\square$

Группа перестановок

Группа всех перестановок n элементов с операцией композиции $\circ$ называется **симметрической группой перестановок** и обозначается S_n.

Предложение 3. *Порядок симметрической группы перестановок S_n равен $n!$, т. е.*

$$|S_n| = n!$$

Группа S_3

Рассмотрим симметрическую группу перестановок S_3.

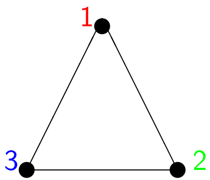
$\pi_1 = e = [123] = (1)(2)(3)$ — нейтральный элемент (единица группы);
$\pi_2 = [132] = (1)(23)$ — элемент 1 остается на месте, элементы 2 и 3 меняются местами;
$\pi_3 = [321] = (13)(2)$ — элемент 2 остается на месте, элементы 1 и 3 меняются местами;
$\pi_4 = [213] = (12)(3)$ — элемент 3 остается на месте, элементы 1 и 2 меняются местами;
$\pi_5 = [231] = (123)$ — элементы 1, 2 и 3 сдвигаются по циклу по часовой стрелке;
$\pi_6 = [321] = (132)$ — элементы 1, 2 и 3 сдвигаются по циклу против часовой стрелки.

Порядок группы $|S_3| = 3! = 6$.

Группа вращений треугольника в плоскости

Найдем группу H перестановок вершин правильного треугольника при его вращениях в плоскости, переводящих его в себя.

Рассмотрим правильный треугольник и будем поворачивать его по часовой стрелке:



поворот на угол 0: $\pi_1 = e = (1)(2)(3)$;
поворот на угол $\frac{2\pi}{3}$: $\pi_2 = (123)$;
поворот на угол $\frac{4\pi}{3}$: $\pi_3 = (132)$.

Группа вращений треугольника в плоскости

Получаем группу вращений вершин правильного треугольника в плоскости $H = (\{\pi_1, \pi_2, \pi_3\}; \circ)$, $|H| = 3$.

Она является подгруппой группы перестановок S_3.

Теорема Кэли

Теорема 1 (Кэли). *Каждая конечная группа изоморфна некоторой подходящей подгруппе симметрической группы перестановок* S_n.

Теорема Кэли

Доказательство. Пусть $G = (S; *)$ — заданная конечная группа, $|G| = n$ и $S = \{g_1 = e, g_2, \ldots, g_n\}$.

Для каждого элемента $g_i \in G$ построим соответствующую ему перестановку $\pi_{g_i} \in S_n$ по правилу

$$\pi_{g_i} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_i * g_1 & g_i * g_2 & \cdots & g_i * g_n \end{pmatrix},$$

или

$$\pi_{g_i} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi_{g_i}(1) & \pi_{g_i}(2) & \ldots & \pi_{g_i}(n) \end{pmatrix},$$

где $\pi_{g_i}(j) = k$, если $g_i * g_j = g_k$.

Теорема Кэли

1. Сначала покажем, что такое определение задает перестановки.

От обратного: пусть это не так, т. е. для некоторого $g_i \in G$ найдутся такие элементы $g_j \in G$ и $g_l \in G$, $g_j \neq g_l$, что

$$g_i * g_j = g_i * g_l.$$

Но тогда по правилу сокращения верно $g_j = g_l$ — противоречие.

Обозначим полученное множество перестановок T, $T \subseteq S_n$.

Теорема Кэли

2. Рассмотрим перестановку π_{g_i}, где $g_i \in G$,

$$\pi_{g_i} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_i * g_1 & g_i * g_2 & \cdots & g_i * g_n \end{pmatrix}.$$

Пусть $g_i' \in G$ — симметричный к g_i элемент. Тогда

$$\pi_{g_i}^{-1} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_i' * g_1 & g_i' * g_2 & \cdots & g_i' * g_n \end{pmatrix}.$$

Значит, $\pi_{g_i}^{-1} = \pi_{g_i'}$.

Теорема Кэли

3. Теперь по критерию подгруппы покажем, что множество перестановок T с операцией композиции образует подгруппу симметрической группы перестановок S_n.

Выберем любые элементы $g_i, g_j \in G$ и рассмотрим перестановку $\pi_{g_i} \circ \pi_{g_j}^{-1}$.

Т. к. G — группа, верно $g_j' \in G$.
Тогда для любого элемента $x \in N$ получаем

$$(\pi_{g_i} \circ \pi_{g_j}^{-1})(x) = (\pi_{g_i} \circ \pi_{g_j'})(x) = \pi_{g_i}(\pi_{g_j'}(x)) = \pi_{g_i * g_j'}(x).$$

Т. к. G — группа, верно $g_i * g_j' = g_k \in G$, откуда $\pi_{g_i * g_j'} = \pi_{g_k}$.
Значит, $\pi_{g_i} \circ \pi_{g_j}^{-1} \in T$.

Следовательно, $H = (T; \circ)$ — подгруппа группы S_n.

Теорема Кэли

4. Теперь покажем, что группы $G = (S; *)$ и $H = (T; \circ)$ — изоморфны.
Рассмотрим отображение

$$\varphi : S \to T, \ g \mapsto \pi_g,$$

которое элемент $g \in S$ переводит в элемент $\varphi(g) = \pi_g \in T$.

1) Отображение φ взаимно однозначно.

2) Если $g_i, g_j \in G$, то

$$\varphi(g_i * g_j) = \pi_{g_i * g_j} = \pi_{g_i} \circ \pi_{g_j} = \varphi(g_i) \circ \varphi(g_j).$$

Т. е. отображение φ сохраняет операцию.

Значит, оно является изоморфизмом групп $G = (S; *)$ и $H = (T; \circ)$.

Регулярное представление Кэли

Для конечной группы $G = (S; *)$ построенная в доказательстве изоморфная ей подгруппа $H = (T; \circ)$ называется **левым регулярным представлением Кэли**.

Регулярное представление Кэли

Пример. Найдем левое регулярное представление Кэли для группы из трех элементов из рассмотренного ранее примера.

Пусть $S = \{e, a, b\}$;

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

, или

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Тогда

$$\pi_e = (1)(2)(3); \quad \pi_a = (123); \quad \pi_b = (132).$$

Получаем группу вращений H правильного треугольника в плоскости, являющуюся подгруппой группы S_3.

Цикловой индекс

Пусть $G = (S; \circ)$ — подгруппа симметрической группы перестановок S_n.

Цикловым индексом группы перестановок G называется многочлен n переменных

$$Z_G(t_1, \ldots, t_n) = \frac{1}{|G|} \sum_{\pi \in G} t_1^{\lambda_1(\pi)} \cdot \ldots \cdot t_n^{\lambda_n(\pi)},$$

где $\lambda(\pi) = (\lambda_1(\pi), \ldots, \lambda_n(\pi))$ — тип перестановки π.

Цикловой индекс

Пример. Найдем цикловой индекс группы H вращений правильного треугольника в плоскости.

Для каждой перестановки ищем ее тип:
$\pi_1 = e = (1)(2)(3)$, $\lambda(\pi_1) = (3, 0, 0)$;
$\pi_2 = (123)$, $\lambda(\pi_2) = (0, 0, 1)$;
$\pi_3 = (132)$, $\lambda(\pi_3) = (0, 0, 1)$.

Замечая, что $|H| = 3$, получаем цикловой индекс

$$Z_H(t_1, t_2, t_3) = \frac{1}{3}(t_1^3 + 2t_3).$$

Цикловой индекс

Пример. Найдем цикловой индекс симметрической группы перестановок S_3.

Аналогично находим типы всех ее перестановок:
$\pi_1 = e = (1)(2)(3), \;\; \lambda(\pi_1) = (3, 0, 0);$
$\pi_2 = (1)(23), \, \pi_3 = (13)(2), \, \pi_4 = (12)(3),$
$\lambda(\pi_2) = \lambda(\pi_3) = \lambda(\pi_4) = (1, 1, 0);$
$\pi_5 = (123), \, \pi_6 = (132), \;\; \lambda(\pi_5) = \lambda(\pi_6) = (0, 0, 1).$
Порядок группы $|S_3| = 3! = 6.$

Поэтому ее цикловой индекс

$$Z_{S_3}(t_1, t_2, t_3) = \frac{1}{6}(t_1^3 + 3t_1t_2 + 2t_3).$$

Действие группы перестановок

Пусть G — подгруппа симметрической группы перестановок S_n и $N = \{1, 2, \ldots, n\}$.

Будем говорить, что группа перестановок G **действует** на множестве N.

При этом при действии элемента $\pi \in G$ элемент $a \in N$ переходит в элемент $\pi(a) \in N$.

Эквивалентность по группе перестановок

Пусть G — подгруппа симметрической группы перестановок S_n и $N = \{1, 2, \ldots, n\}$.

Определим отношение R_G на множестве N: если $a, b \in N$, то

$$R_G(a, b) \Leftrightarrow \exists \pi \in G : \pi(a) = b.$$

Эквивалентность по группе перестановок

Предложение 7. *Отношение R_G является отношением эквивалентности на множестве N.*

Эквивалентность по группе перестановок

Доказательство. Свойства отношения эквивалентности.

1) Рефлексивность. Для каждого элемента $a \in N$ выберем $\pi_1 = e \in G$ — тождественную перестановку. Тогда $\pi_1(a) = a$, поэтому $R_G(a, a)$.

2) Симметричность. Пусть для элементов $a, b \in N$ верно $R_G(a, b)$, т. е. найдется такая перестановка $\pi \in G$, что $\pi(a) = b$. Тогда

$$\pi(a) = b,\ \pi^{-1}(\pi(a)) = \pi^{-1}(b), a = \pi^{-1}(b).$$

Т. к. G — группа, $\pi^{-1} \in G$, поэтому $R_G(b, a)$.

Эквивалентность по группе перестановок

3) Транзитивность. Пусть для элементов $a, b, c \in N$ верно $R_G(a, b)$ и $R_G(b, c)$, т. е. найдутся такие перестановки $\pi_1 \in G$ и $\pi_2 \in G$, что $\pi_1(a) = b$ и $\pi_2(b) = c$. Тогда

$$(\pi_2 \circ \pi_1)(a) = \pi_2(\pi_1(a)) = \pi_2(b) = c.$$

Т. к. G — группа, $\pi_2 \circ \pi_1 = \pi \in G$, поэтому $R_G(a, c)$.

$\square$

Эквивалентность по группе перестановок

Пусть G — подгруппа симметрической группы перестановок S_n.

Отношение эквивалентности R_G обозначается $\sim_G$.

Если для элементов $a, b \in N$ верно $a \sim_G b$, то говорят, что элементы a и b **эквивалентны по группе** G (или **в группе** G).

Орбита элемента

Пусть $G = \{\pi_1 = e, \pi_2, \ldots, \pi_m\}$ — подгруппа симметрической группы перестановок S_n.

Для элемента $a \in N$ его **орбитой** (в группе G) называется порожденный им класс эквивалентности по отношению $\sim_G$.

Обозначение:

$$O_a = \{b \in N \mid \exists \pi \in G : \pi(a) = b\},$$

или

$$O_a = \{\pi_1(a) = a, \pi_2(a), \ldots, \pi_m(a)\}.$$

Пример: вращение треугольника в плоскости

Пример. Пусть $N = \{1, 2, 3\}$ и

$$H = \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132)\} -$$

группа вращений правильного треугольника в плоскости. Группа G является подгруппой симметрической группы перестановок S_3.

Найдем орбиту элемента $1 \in N$ в группе H:

$$O_1 = \{\pi_1(1), \pi_2(1), \pi_3(1)\} = \{1, 2, 3\}.$$

Другими словами, перестановками группы H элемент 1 может быть переведен в любой другой элемент множества N.

Т. е. вращениями правильного треугольника в плоскости вершина 1 может перейти в любую другую его вершину.

Стабилизатор элемента

Пусть $G = \{\pi_1 = e, \pi_2, \ldots, \pi_m\}$ — подгруппа симметрической группы перестановок S_n.

Для элемента $a \in N$ его **стабилизатором** (в группе G) называется подмножество перестановок группы G, оставляющих его на месте.

Обозначение:

$$G_a = \{\pi \in G \mid \pi(a) = a\}.$$

Пример: симметрическая группа перестановок S_3

Пример. Пусть $N = \{1, 2, 3\}$. Рассмотрим симметрическую группу перестановок S_3,

$$\begin{aligned} S_3 \quad = \quad & \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132), \\ & \pi_4 = (1)(23), \pi_5 = (13)(2), \pi_6 = (12)(3)\}. \end{aligned}$$

Найдем стабилизатор элемента $1 \in N$ в группе S_3:

$$G_1 = \{\pi_1 = (1)(2)(3), \pi_4(1) = (1)(23)\}.$$

Несложно увидеть, что G_1 — подгруппа группы S_3.

Оказывается, что стабилизатор элемента в группе перестановок всегда является подгруппой этой группы перестановок.

Стабилизатор элемента

Предложение 4. *Для каждого элемента $a \in N$ его стабилизатор G_a является подгруппой группы G.*

Доказательство проведем по критерию подгруппы.

Пусть $\pi, \rho \in G_a$. Рассмотрим перестановку $\pi \circ \rho^{-1}$. Тогда

$$(\pi \circ \rho^{-1})(a) = \pi(\rho^{-1}(a)) = \pi(a) = a.$$

Т. е. $\pi \circ \rho^{-1} \in G_a$.

$\square$

Индекс стабилизатора в группе перестановок

Теорема 2. *Для каждого элемента $a \in N$ индекс его стабилизатора G_a в группе перестановок G равен мощности его орбиты O_a, т. е. $(G : G_a) = |O_a|$.*

Доказательство. Рассмотрим левостороннее разложение группы G по подгруппе G_a, определяющей отношение эквивалентности $\sim_{G_a}$.

Выберем произвольные перестановки $\rho, \tau \in G$.

Индекс стабилизатора в группе перестановок

Итак, пусть $\rho, \tau \in G$.

1) Если они из одного смежного класса, т. е. $\rho \sim_{G_a} \tau$, то найдется такая перестановка $\pi \in G_a$, что $\rho \circ \pi = \tau$. Тогда

$$\tau(a) = (\rho \circ \pi)(a) = \rho(\pi(a)) = \rho(a).$$

Индекс стабилизатора в группе перестановок

Итак, пусть $\rho, \tau \in G$.

2) Пусть они из разных смежных классов. Предположим, что $\rho(a) = \tau(a)$. Тогда перестановка $\rho^{-1} \circ \tau \in G_a$, и по второму определению отношения эквивалентности по подгруппе $\rho \sim_{G_a} \tau$, т. е. они лежат в одном смежном классе — противоречие. Поэтому $\rho(a) \neq \tau(a)$.

Индекс стабилизатора в группе перестановок

Следовательно,

$$\rho(a) = \tau(a) \;\Leftrightarrow\; \rho \sim_{G_a} \tau \;\Leftrightarrow\; \rho, \tau \text{ из одного смежного класса.}$$

Т. е. $(G : G_a) = |O_a|$.

$\square$

Пример: индекс подгруппы G_1 в группе S_3

Пример. Мы нашли стабилизатор элемента $1 \in N$ в группе S_3:

$$G_1 = \{\pi_1 = (1)(2)(3), \pi_4(1) = (1)(23)\}.$$

Найдем разложение симметрической группы перестановок S_3 на смежные классы по подгруппе G_1:

Класс	π	$\pi(1)$
$(1)(2)(3)G_1$	$(1)(2)(3), (1)(23)$	1
$(123)G_1$	$(123), (12)(3)$	2
$(132)G_1$	$(132), (13)(2)$	3

Несложно увидеть, что $(S_3 : G_1) = |O_1|$.

Лемма Бернсайда

Теорема 3 (лемма У. Бернсайда). *Число $N(G)$ орбит элементов из множества $N = \{1, 2, \ldots, n\}$ по подгруппе G группы перестановок S_n равно*

$$N(G) = \frac{1}{|G|} \sum_{\pi \in G} \lambda_1(\pi),$$

где $\lambda_1(\pi)$ — число неподвижных элементов перестановки π.

Лемма Бернсайда

Доказательство. Пусть $G = \{\pi_1 = e, \pi_2, \dots, \pi_m\}$ — подгруппа группы S_n. Построим таблицу $T = (t_{ij})$, в которой

$$\begin{aligned} t_{ij} &= 1, \quad \text{если } \pi_j(i) = i; \\ t_{ij} &= 0, \quad \text{иначе.} \end{aligned}$$

$$T: \begin{array}{c|cccc|c} N \setminus G & \pi_1 = e & \pi_2 & \dots & \pi_m & \\ \hline 1 & 1 & & \dots & & |G_1| \\ 2 & 1 & & \dots & & |G_2| \\ \dots & & & \dots & & \dots \\ n & 1 & & \dots & & |G_n| \\ \hline & \lambda_1(\pi_1) & \lambda_1(\pi_2) & \dots & \lambda_1(\pi_m) & \end{array}$$

В таблице T число единиц в каждой строке равно порядку стабилизатора элемента — номера этой строки; число единиц в каждом столбце равно числу неподвижных элементов перестановки с номером этого столбца.

Лемма Бернсайда

Число единиц в таблице T можно подсчитать

по строкам как $\sum_{i=1}^{n} |G_i|$

и по столбцам как $\sum_{j=1}^{m} \lambda_1(\pi_j)$.

Тогда

$$\sum_{i=1}^{n} |G_i| = \sum_{j=1}^{m} \lambda_1(\pi_j).$$

Лемма Бернсайда

По предыдущей теореме $|G_i| = \frac{|G|}{|O_i|}$. Поэтому

$$\sum_{i=1}^{n} |G_i| = |G| \sum_{i=1}^{n} \frac{1}{|O_i|}.$$

Если для элементов $i, k \in N$ верно $i \sim_G k$, то $O_i = O_k$, откуда $|O_i| = |O_k|$. Пусть

$$O_{a_1}, \dots, O_{a_{N(G)}}$$

все **различные** орбиты по группе G.

Тогда

$$\sum_{i=1}^{n} \frac{1}{|O_i|} = \sum_{l=1}^{N(G)} \frac{1}{|O_{a_l}|} \sum_{i:i\sim_G a_l} 1 = \sum_{l=1}^{N(G)} \frac{1}{|O_{a_l}|} \cdot |O_{a_l}| = N(G).$$

Лемма Бернсайда

Получаем:

$$|G| \cdot N(G) = \sum_{j=1}^{m} \lambda_1(\pi_j).$$

Значит,

$$N(G) = \frac{1}{|G|} \sum_{\pi \in G} \lambda_1(\pi).$$

$\square$

Лемма Бернсайда

Пример. Найдем число орбит элементов множества $N = \{1, 2, 3\}$ по группе H вращений правильного треугольника в плоскости. Сколько их?

Лемма Бернсайда

Напомним, что

$$H = \{\pi_1 = e = (1)(2)(3), \pi_2 = (123), \pi_3 = (132)\}.$$

Тогда

$$\lambda_1(\pi_1) = 3, \lambda_1(\pi_2) = \lambda_1(\pi_3) = 0.$$

Поэтому

$$N(H) = \frac{1}{|H|}\sum_{j=1}^{3}\lambda_1(\pi_j) = \frac{1}{3}(3+0+0) = 1.$$

Значит, все элементы множества N из одной орбиты, т. е. перестановками группы H каждый элемент множества N можно перевести в любой другой элемент этого множества.

Литература к лекции

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Т. 1. С. 12–23.

2. Чашкин А.В. Лекции по дискретной математике. М.: Изд-во механико-математического факультета МГУ, 2007. С. 53–55.