

Лекция 9. Перестановки.

Гайфуллин Сергей Александрович

МГУ

7 октября, 2021

Определение.

Перестановка степени (длины, порядка) n – это упорядоченный в каком-нибудь порядке набор чисел $1, 2, \dots, n$.

Подстановка степени (длины, порядка) n – это биекция из множества $\{1, 2, \dots, n\}$ в множество $\{1, 2, \dots, n\}$.

Будем записывать подстановку σ в 2 строки:

$$\begin{pmatrix} \dots & i & \dots \\ \dots & \sigma(i) & \dots \end{pmatrix}$$

Например, подстановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ соответствует биекции $\{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$, которая переводит $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 1$, $5 \mapsto 3$.

Обозначение.

Множество подстановок длины n обозначается S_n .

Заметим, что одной и той же подстановке соответствуют разные таблицы из 2-х строк. Важно лишь что под чем стоит:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 3 & 1 & 4 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

Однако каждую подстановку можно записать в стандартном виде, то есть так, чтобы верхняя строка была упорядочена по возрастанию.

Лемма.

Количество перестановок длины n равно количеству подстановок длины n .

Доказательство. Установим биекцию: перестановке сопоставим подстановку, у которой в стандартном виде нижняя строка совпадает с данной перестановкой.

Лемма. $|S_n| = n!$.

Доказательство. Так как количество подстановок и перестановок одинаковое, будем считать перестановки длины n . Оформим подсчет в виде последовательного заполнения элементов перестановки слева-направо. Первый элемент можно выбрать n способами. Для второго есть $n - 1$ вариант (нельзя на 2 место ставить то число, которое поставили на первое). Для третьего элемента существует $n - 2$ варианта и т.д. В итоге получаем $n(n - 1)(n - 2) \dots 1 = n!$ вариантов.

Определение.

Пусть $\sigma, \delta \in S_n$. Произведением (композицией) этих подстановок называется подстановка $\sigma\delta = \sigma \circ \delta \in S_n$.

Имеем $\sigma \circ \delta(i) = \sigma(\delta(i))$.

$$\sigma\delta = \begin{pmatrix} \dots & i & \dots \\ \dots & \sigma(\delta(i)) & \dots \end{pmatrix} = \begin{pmatrix} \dots & \delta(i) & \dots \\ \dots & \sigma(\delta(i)) & \dots \end{pmatrix} \begin{pmatrix} \dots & i & \dots \\ \dots & \delta(i) & \dots \end{pmatrix}.$$

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 3 & 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 5 & 4 & 7 & 3 & 2 \end{pmatrix}$$

- Ассоциативность $(\sigma\delta)\xi = \sigma(\delta\xi)$.
Как мы видели, ассоциативность верна для любых отображений.
- Обобщенная ассоциативность (следствие ассоциативности).
- Рассмотрим тождественную подстановку

$$\text{id} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Для любой подстановки $\sigma \in S_n$ имеем $\sigma \text{id} = \text{id} \sigma = \sigma$.

- Для любой подстановки $\sigma \in S_n$ существует единственная обратная подстановка $\sigma^{-1} \in S_n$ такая, что $\sigma \sigma^{-1} = \sigma^{-1} \sigma = \text{id}$. Подстановка σ^{-1} получается из σ , если поменять 1-ю и 2-ю строки местами.
- При $n > 2$ коммутативность отсутствует. $\sigma \delta \neq \delta \sigma$.

Определение.

Подстановка $\sigma \in S_n$ называется циклом, если существуют числа $a_1, \dots, a_k \in \{1, 2, \dots, n\}$ такие что $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1, \sigma(i) = i$ при $i \notin \{a_1, \dots, a_k\}$.

Данный цикл будем обозначать (a_1, a_2, \dots, a_k) . Число k назовем длиной цикла. При этом

$$(a_1, a_2, \dots, a_k) = (a_2, a_3, \dots, a_k, a_1) = \dots = (a_k, a_1, a_2, \dots, a_{k-1})$$

Легко видеть, что $(a) = \text{id}$. Цикл длины 2 называется транспозицией.

Определение.

Два цикла называются независимыми, если для них множества $\{a_1, \dots, a_k\}$ не пересекаются. То есть подвижные элементы одного цикла являются неподвижными для другого.

Каждой подстановке σ можно сопоставить ориентированный граф $\Gamma(\sigma)$ на n вершинах v_1, \dots, v_n . При этом из v_i есть стрелка в v_j , если и только если $\sigma(i) = j$. Если $\sigma(i) = i$, получаем петлю.

Лемма.

Для любой подстановки σ граф $\Gamma(\sigma)$ есть объединение нескольких ориентированных циклов.

Доказательство. Из каждой вершины выходит ровно одна стрелка и в каждую вершину входит ровно одна стрелка. Пойдем по стрелкам из некоторой вершины. Войдя в некоторую вершину мы всегда будем иметь возможность выйти. В силу конечности количества вершин, мы придем в ту вершину, в которой уже были. Рассмотрим первую такую вершину. Это та вершина, из которой мы начинали (в остальные вершины идут стрелки из тех, где мы уже были). Получим ориентированный цикл. Далее встанем на любую, не вошедшую в него вершину, и пойдем по стрелкам. Получим еще один цикл. И т.д.

Теорема.

Любая подстановка $\sigma \in S_n$ есть произведение независимых циклов.

Доказательство. Рассмотрим граф $\Gamma(\sigma)$ и запишем все его циклы. Произведение этих (независимых) циклов и есть перестановка σ . В самом деле, если $\sigma(i) = j$, то i и j являются подвижными элементами ровно одного цикла и неподвижными для всех остальных. При произведении (идем по множителям справа-налево) сперва много раз i переходит в i , затем i переходит в j , а затем много раз j переходит в j .

Так как циклы длины 1 – это тождественные подстановки, их можно исключить из данного произведения.

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & 1 & 5 & 6 & 3 \end{pmatrix} = (1, 2, 4)(3, 7)(5)(6) = (1, 2, 4)(3, 7).$$

Определение.

Порядком подстановки σ называется минимальное натуральное число m такое, что $\sigma^m = \text{id}$. Будем обозначать порядок $\text{ord}(\sigma)$.

Теорема.

Порядок подстановки σ равен наименьшему общему кратному длин ее независимых циклов.

Доказательство Пусть $\sigma = \gamma_1 \dots \gamma_s$ – разложение на независимые циклы. Легко видеть, что, так как циклы независимы, они коммутируют, а потому $\sigma^m = \gamma_1^m \dots \gamma_s^m$. При этом $\gamma_j^m = \text{id}$ тогда и только тогда, когда m делится на длину γ_j . Если возьмем m равное НОК длин всех циклов, получим $\sigma^m = \text{id}$. Если же возьмем m меньше, то существует j такой, что $\gamma_j^m \neq \text{id}$. Тогда есть подвижный для γ_j элемент u такой, что $\gamma_j^m(u) \neq u$. Однако u является неподвижным для всех остальных γ_i , а значит, и для всех γ_i^m . То есть $\sigma^m(u) \neq u$.

Определение.

Пусть α – перестановка длины n . Тогда пара (i, j) называется инверсией для α , если $i > j$ и при этом i стоит левее, чем j .

Определение.

Четность перестановки α – это четность количества инверсий в ней.

Определение.

Четность подстановки σ – это четность ее нижней строки в стандартном виде.

Эквивалентно, четность σ равна четности количества пар (a, b) таких, что $a < b$ и $\sigma(a) > \sigma(b)$.

Теорема.

Пусть $\sigma \in S_n$. Умножение на транспозицию $\tau = (i, j)$ слева меняет числа i и j в нижней строке. Умножение на $\tau = (i, j)$ справа меняет числа i и j в верхней строке, или, что эквивалентно, меняет числа $\sigma(i)$ и $\sigma(j)$ в нижней строке.

Доказательство. Если $a \notin \{i, j\}$, то $\tau(a) = a$. Значит, если $\sigma(x) \notin \{i, j\}$, то $\tau\sigma(x) = \sigma(x)$. Если же $\sigma(x) = i$, то $\tau\sigma(x) = j$, и наоборот, если $\sigma(x) = j$, то $\tau\sigma(x) = i$. Это доказывает первое утверждение.

Если же рассматривать $\sigma\tau$, то при $a \notin \{i, j\}$, получаем $\sigma\tau(a) = a$. Кроме того $\sigma\tau(i) = \sigma(j)$ и $\sigma\tau(j) = \sigma(i)$. Это доказывает второе утверждение.

Лемма.

При умножении слева на транспозицию $\tau = (i, i + 1)$ подстановка σ меняет четность.

Доказательство. Рассмотрим нижнюю строку подстановки σ в стандартном виде. Обозначим ее α . При умножении слева на τ в α поменяются местами i и $i + 1$, получится α' .

Пусть $a, b \notin \{i, i + 1\}$. Тогда пара (a, b) является или не является инверсией для α и α' одновременно.

Пара (i, a) является инверсией для α тогда и только тогда, когда $(i + 1, a)$ является инверсией для α' . И наоборот, пара $(i + 1, a)$ является инверсией для α тогда и только тогда, когда (i, a) является инверсией для α' .

Таким образом, количество инверсий кроме $(i, i + 1)$ в перестановках α и α' одинаково. Однако, пара $(i, i + 1)$ является инверсией ровно для одной из двух перестановок α и α' . Это доказывает, что четности у α и α' разные.

Лемма.

При умножении слева на транспозицию $\tau = (i, j)$ подстановка σ меняет четность.

Доказательство. Представим транспозицию (i, j) в виде произведения нечетного числа транспозиций соседних элементов. Считаем $j > i$.

$$\begin{aligned}(i, j) &= \\ &= (i, i+1)(i+1, i+2) \dots (j-2, j-1)(j-1, j)(j-2, j-1) \dots \\ &\quad \dots (i+1, i+2)(i, i+1).\end{aligned}$$

Так как при умножении слева на каждую транспозицию соседних четность меняется, то она поменяется.

Лемма.

Любую подстановку σ можно представить в виде произведения некоторого количества транспозиций.

Доказательство. Начнем с тождественной подстановки и будем делать последовательно образы элементы нужными. Пусть $\sigma(1) = a$, домножим id на транспозицию $(1, a)$ и получим δ_1 такое, что $\delta_1(1) = a$. Пусть $\sigma(2) = b$, $\delta_1(2) = b'$. Если $b = b'$, то $\delta_2 = \delta_1$. Если $b \neq b'$, то $\delta_2 = (b, b')\delta_1$. Легко видеть, что $\delta_2(1) = a$, $\delta_2(2) = b$. И т.д. $\delta_{n-1} = \sigma$. Так как при умножении на транспозицию четность меняется, получаем.

Теорема.

Четность подстановки σ – это четность количества транспозиций в любом разложении σ на транспозиции.