§1 Перестановки и подстановки

Определение1. Всякое расположение чисел 1, 2, ... , n в некотором определенном порядке называется перестановкой из n чисел. Другими словами, под перестановками чисел принято понимать всевозможные способы, которыми эти числа можно выстроить в ряд.

Можно подсчитать число таких способов. Одно число можно выстроить в ряд одним способом. Два числа - двумя способами: 1, 2 и 2, 1. Числа 1, 2, 3 можно выстроить в ряд следующими способами: 1, 2 , 3; 1, 3, 2; 2, 1, 3; 2, 3, 1; 3, 1, 2; 3 ,2 , 1. Всего их шесть. Действительно, на первом месте могут стоять только числа 1, 2 и 3, а два остальных числа в каждом из трех возможных случаев можно выстроить в ряд двумя способами. Аналогичный принцип позволяет подсчитать число перестановок из четырех чисел: 1, 2, 3 и 4. Любое из чисел 1, 2, 3 и 4 может стоять на первом месте, а число всех перестановок трех остальных элементов есть 6:

1 2 3 4	2 1 3 4	3 1 2 4	4 1 2 3
1 2 4 3	2 1 4 3	3 1 4 2	4 1 3 2
1 3 2 4	2 3 1 4	3 2 1 4	4 2 1 3
1 3 4 2	2 3 4 1	3 2 4 1	4 2 3 1
1 4 2 3	2 4 1 3	3 4 1 2	4 3 1 2
1 4 3 2	2 4 3 1	3 4 2 1	4 3 2 1 .

Число перестановок из четырех элементов равно 4· 6=24, т.е. умножаем число перестановок из трех элементов (6) на 4. Шесть перестановок из трех чисел мы получим, умножив число перестановок из двух чисел (2) на 3. Таким образом, число перестановок из четырех элементов можно представить в виде 24=4· 3· 2· 1. Можно показать, что число перестановок из пяти чисел равно 5· 4· 3· 2· 1=120.

Теорема1. Число различных перестановок из n чисел равно произведению 1· 2· 3· ...· n, обозначаемому $n!$ (читается: "эн факториал").

Доказательство. Действительно, общий вид перестановки из n символов есть $i_1, i_2, \dots, i_n$, где каждое из i_s есть одно из чисел 1, 2, ... , n, причем ни одно из этих чисел не встречается дважды. В качестве i_1 можно взять любое из чисел 1, 2, ... , n; это дает n различных возможностей. Если, однако, i_1 уже выбрано, то в качестве i_2 можно взять лишь одно из оставшихся n-1 чисел, т.е. число различных способов выбора пары символов i_1, i_2 равно произведению $n(n-1)$. Если, уже выбраны i_1 и i_2, то в качестве i_3 можно взять лишь одно из оставшихся n-2 чисел, т.е. число различных способов выбора тройки символов i_1, i_2, i_3 равно произведению $n(n-1)(n-2)$ и т.д. Аналогично, если выбраны числа $i_1, i_2, i_3, \dots, i_{n-2}$, то в качестве i_{n-1} можно взять лишь одно из оставшихся двух чисел, а возможность выбора для i_n остается одна. Таким образом, число различных способов, которыми можно выбрать символы $i_1, i_2, \dots, i_n$ равно произведению $n\cdot (n-1)\cdot (n-2)\cdot (n-3)\cdot \dots \cdot 2\cdot 1 = =1\cdot 2\cdot 3\cdot \dots \cdot (n-2)\cdot (n-1)\cdot n=n!$

Определение 2. Говорят, что в данной перестановке числа i и j составляют инверсию, если $i>j$, но i стоит в этой перестановке раньше j.

Определение 3. Перестановка называется четной, если ее числа составляют четное число инверсий, и нечетной - в противоположном случае. Так, перестановка 4, 5, 1, 3, 6, 2 четная, т.к. число инверсий в ней равно 8.

Перестановка 1, 2, ... , n будет четной при любом n, т.к. число инверсий в ней равно нулю.

Определение 4. Преобразование в перестановке, при котором мы поменяем местами какие-либо два символа (необязательно стоящие рядом), а все остальные символы оставим на месте, называется транспозицией.

Теорема 2. Все $n!$ перестановок из n символов можно расположить в таком порядке, что каждая следующая будет получаться из предыдущей одной транспозицией, причем начинать можно с любой перестановки.

Доказательство. Докажем эту теорему методом математической индукции.

Утверждение справедливо при n=2: если требуется начинать с перестановки 12, то искомое расположение будет 12, 21; если же мы должны начать с перестановки 21, то это будет расположение 21, 12.

Предположим, что наше утверждение уже доказано для n-1, и докажем его для n. Пусть мы должны начать с перестановки $i_1, i_2, \dots, i_n$. Рассмотрим все перестановки из n символов, у которых на первом месте стоит i_1. Таких перестановок $(n\text{-}1)!$ и их можно упорядочить в согласии с требованиями теоремы, притом начиная с перестановки $i_1, i_2, \dots, i_n$, так как это сводится на самом деле к упорядочению всех перестановок из n-1 символов, которое, по индуктивному предположению, можно начать с любой перестановки, в частности с перестановки $i_2, \dots, i_n$. В последней из полученных таким путем перестановок из n символов совершаем транспозицию символа i_1 с любым другим символом, например с i_2, и, начиная с вновь полученной перестановки, упорядочиваем нужным образом все те перестановки, у которых на первом месте стоит i_2. И в этом случае это сводится к упорядочению всех перестановок из n-1 символов $(i_1, i_3, i_4, \dots, i_n)$, которое по индуктивному предположению, можно начать с любой перестановки. В последней из полученных таким путем перестановок из n символов совершаем транспозицию символа i_2 с i_3. Теперь будем упорядочивать все те перестановки, у которых на первом месте стоит i_3 и так далее. Получаем n групп перестановок, в каждой группе по $(n\text{-}1)!$ перестановок:

$$\left.\begin{array}{l} i_1 i_2 \dots . i_n \\ i_1 \dots . . . . . i_{s_1} \\ \dots\dots\dots \\ i_1 \dots . . . . . i_{l_1} \end{array}\right\}$$ $(n\text{-}1)!$ перестановок, где $s_1, \dots, l_1$ принимают одно из значений 2, 3, ..., n-1.

$$\left.\begin{array}{l} i_1 \dots . . . . . i_{s_2} \\ i_1 \dots . . . . . i_{t_2} \\ \dots\dots\dots \\ i_1 \dots . . . . . i_{l_2} \end{array}\right\}$$ $(n\text{-}1)!$ перестановок, где $s_2, t_2, \dots, l_2$ принимают одно из значений 1, 3, ..., n.

…….

$\left.\begin{array}{l} i_1 \ldots\ldots i_{s_n} \\ i_1 \ldots\ldots i_{t_n} \\ \ldots\ldots\ldots \\ i_1 \ldots\ldots i_{l_n} \end{array}\right\}$ (n-1)! перестановок, где s_n, t_n, ... , l_n принимают одно из значений 1, 2,

...,n-1.

Всего n (n-1)!=n! перестановок. Этим путем можно перебрать все n! перестановок из n символов. Теорема доказана.

Из этой теоремы вытекает, что от любой перестановки из n символов можно перейти к любой другой перестановке из тех же символов при помощи нескольких транспозиций.

Теорема 3. Всякая транспозиция меняет четность перестановки.

Доказательство. Для доказательства этой теоремы рассмотрим сначала случай, когда транспонируемые символы i и j стоят рядом, то есть перестановка имеет вид

... , i, j, ... ,

где многоточия заменяют те символы, которые не затрагиваются транспозицией. Транспозиция превращает нашу перестановку в перестановку ..., j, i, ... , причем, понятно, в обеих перестановках каждый из символов i, j составляет одни и те же инверсии с символами, остающимися на месте. Если символы i и j раньше не составляли инверсии, то в новой перестановке появляется одна новая инверсия, то есть число инверсий увеличивается на единицу; если же они раньше составляли инверсию, то теперь она пропадает, то есть число инверсий на единицу уменьшается. В обоих случаях четность перестановки меняется.

Пусть теперь между транспонируемыми символами i и j расположены S символов, S>0, то есть перестановка имеет вид

... i, k_1, k_2, ... , k_s, j,...

Транспозицию символов i, j можно получить в результате последовательного выполнения 2S+1 транспозиций соседних элементов. А именно, это будут транспозиции, переставляющие символы i и k_1, затем i (уже стоящее на месте символа k_1) и k_2 и так далее, пока i не займет место символа k_s. За этими S транспозициями следует транспозиция, перемещающая символы i и j, а затем S транспозиций символа j со всеми k, после чего j занимает место символа i, а символы k возвращаются на свои старые места. Таким образом, мы нечетное число раз меняли четность перестановки, а поэтому перестановки ... , i, k_1, k_2, ... , k_s, j, ... и ..., j, k_1, k_2, ... , k_s, i, ... имеют противоположные четности. Теорема доказана.

Из теорем 2 и 3 вытекает, что при n ?2 число четных перестановок из n символов равно числу нечетных, то есть равно n!/2.

Определим новое понятие, понятие подстановки n-й степени.

Определение 5. Всякое взаимно однозначное отображение A множества первых n натуральных чисел на себя называется подстановкой n-ой степени.

Всякая подстановка A может быть записана при помощи двух перестановок, подписанных одна под другой

$$\begin{pmatrix} i_1 & i_2 & i_3 & \ldots & i_n \\ \alpha_{i_1} & \alpha_{i_2} & \alpha_{i_3} & \ldots & \alpha_{i_n} \end{pmatrix};$$

через α_i обозначается то число, в которое при подстановке A переходит число i, i=1, 2, … , n. Подстановка A обладает многими различными записями. Так при n=5

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

может иметь другие записи, например:

$$A=\begin{pmatrix} 5 & 4 & 3 & 1 & 2 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix},\ A=\begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$ и так далее.

Во всех этих записях мы имеем одно и то же взаимно однозначное отображение множества из первых пяти натуральных чисел на себя. При этом отображении число 1 переходит в 4, число 2 переходит в 3, число 3 - в 2, число 4 - в 3, число 5 - в 1. Эту же перестановку мы можем записать в виде

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

то есть с натуральным расположением чисел в верхней строке.

Также всякая подстановка n-ой степени A может быть записана в виде

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix}.$$

При такой записи различные перестановки отличаются друг от друга только перестановками, стоящими в нижней строке, и поэтому число подстановок n-ой степени равно числу перестановок из n символов, то есть равно n!

Примером подстановки n-ой степени служит тождественная подстановка

$$\mathrm{E}=\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix},$$

в которой на месте остаются все числа.

Рассмотрим произвольную запись

$$A=\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \alpha_{i_1} & \alpha_{i_2} & \dots & \alpha_{i_n} \end{pmatrix}$$

некоторой подстановки n-й степени. Перестановки, составляющие верхнюю и нижнюю строки в этой записи, могут иметь или одинаковые, или противоположные четности. Переход к любой другой записи подстановки A можно осуществить путем последовательного выполнения нескольких транспозиций в верхней строке и соответствующих им транспозиций в нижней строке. Однако, совершая одну транспозицию в верхней строке (перестановке) записи A и одну транспозицию соответствующих элементов в нижней строке (перестановке) мы одновременно меняем четности обеих перестановок и поэтому сохраняем совпадение или противоположность этих четностей.

При всех записях подстановки A четности верхней и нижней строк совпадают, либо же при всех записях они противоположны.

Определение 6. Подстановка A называется четной, если четности верхней и нижней строк совпадают и подстановка A называется нечетной, если четности верхней и нижней строк противоположны. В частности, тождественная подстановка будет четной.

Если подстановка A записана в виде

$$A=\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix}$$

то четность подстановки A будет определяться четностью перестановки ?$_1$, α_2, ... , α_n. Отсюда следует, что число четных подстановок n-й степени равно числу нечетных, то есть равно $n!/2$.

Определению четности подстановки можно дать другие формы.

Определение 7. Подстановка A будет четной, если общее число инверсий в двух строках четно, и нечетной - в противном случае.

Определение 8. Результат последовательного выполнения двух взаимно однозначных отображений множества 1, 2, ... , n на себя снова будет, некоторым взаимно однозначным отображением этого множества на себя, то есть подстановкой n-й степени, называемой произведением первой из заданных подстановок (первое отображение) на вторую. Например: если даны подстановки третьей степени

$$A=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ и } B=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ то } AB=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Действительно, при подстановке A число 1 переходит в 3, но при B число 3 переходит в 1 и так далее. Можно перемножить лишь подстановки одинаковой степени.

Умножение подстановок n–ой степени при n?3 не коммутативно.

Из ассоциативности произведения отображений, вытекает, что умножение подстановок ассоциативно. Очевидно, что $EA=AE=A$.

Определение 9. Обратной для подстановки A называется подстановка той же степени A^{-1} такая, что $AA^{-1}=A^{-1}A=E$.

Так для подстановки

$$A=\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix}$$

обратной служит подстановка

$$A^{-1}=\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Если нам нужно решить уравнения в подстановках: а) $AX=B$; б) $XA=B$; в) $AXB=C$, то мы поступим таким образом: 1) в случае а) умножим обе части уравнения $AX=B$ слева (в виду не коммутативности умножения) на A^{-1}, получим, $A^{-1}(AX)=A^{-1}B$, а так как умножение подстановок ассоциативно, то $(A^{-1}A)X=A^{-1}B$, $EX=A^{-1}B$, $X=A^{-1}B$ – решение уравнения $AX=B$; 2) в случае б) $XA=B$, $(XA)A^{-1}=BA^{-1}$,

$X(AA^{-1})=BA^{-1}$, $X=BA^{-1}$; 3) в случае в) $AXB=C$, $A^{-1}(AXB)=A^{-1}C$, $XB=A^{-1}C$, $(XB)B^{-1}=(A^{-1}C)B^{-1}$, $X(BB^{-1})=A^{-1}CB^{-1}$, $X=A^{-1}CB^{-1}$.

Определение 10. Назовем транспозицией (если речь идет о подстановке), нечетную подстановку вида

$$\begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix},$$

которая получается из тождественной подстановки E при помощи одной транспозиции, производимой в нижней строке. Многоточиями заменены символы, остающиеся на месте. Условимся обозначать эту транспозицию символом (i, j). (В дальнейшем символ (i, j) мы назовем циклом длины два).

Применение транспозиции символов i, j к нижней строке подстановки

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix}.$$

Равносильно умножению подстановки A справа на подстановку

$$\begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix},$$

то есть на (i, j). Мы знаем, что все перестановки из n символов можно получить из одной из них, например, из 1, 2, … , n, последовательным выполнением транспозиций, поэтому всякая подстановка может быть получена из тождественной подстановки путем последовательного выполнения нескольких транспозиций в нижней строке, то есть путем последовательного умножения на подстановки вида (i, j). Можно утверждать, следовательно (опуская множитель E), что всякая подстановка представима в виде произведения транспозиций. Например:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}=(12)(15)(34)=(14)(24)(45)(34)(13).$$

Всякую подстановку можно многими разными способами разложить в произведение транспозиций. Всегда можно добавить два одинаковых множителя вида $(i, j)(i, j)$, которые дают в произведении подстановку E, то есть, взаимно уничтожаются.

Новый способ определения четности подстановки основан на следующей теореме:

Теорема 4. При всех разложениях подстановки в произведение транспозиций четность числа этих транспозиций будет одна и та же, причем она совпадает с четностью самой подстановки.

Доказательство. Эта теорема будет доказана, если мы покажем, что произведение любых k транспозиций есть подстановка, четность которой совпадает с четностью k. Это утверждение доказываем по методу математической индукции. При k=1 это верно, так как транспозиция есть нечетная подстановка. Пусть наше утверждение уже доказано для случая k-1 множителей. Тогда его справедливость для k множителей вытекает из того, что

числа k-1 и k имеют противоположные четности, а умножение подстановки (в данном случае – произведение первых k-1 множителей – мы предположили, что это подстановка, четность которой совпадает с четностью числа k-1) на транспозицию равносильно выполнению этой транспозиции в нижней строке подстановки, то есть, меняет ее четность.

Согласно этой теореме, определить четность подстановки можно разложением подстановки в произведение транспозиций – их число определяет четность подстановки.

Рассмотрим подробнее один из способов разложения подстановки в произведение транспозиций. Он заключается в следующем: сначала разложим подстановку в произведение циклов, а затем каждый цикл разложим в произведение транспозиций. Для этого приведем новые определения и факты.

Определение 11. Циклической подстановкой или циклом называется такая подстановка, что при повторении ее достаточное число раз всякий из действительно перемещаемых ею символов может быть переведен в любой другой из этих символов. Такова, например, подстановка восьмой степени

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 6 & 4 & 5 & 2 & 7 & 3 \end{pmatrix}.$$

Она действительно перемещает символы 2, 3 , 6 и 8, причем переводит символ 2 в 8, символ 8 в 3, символ 3 в 6, а символ 6 снова в 2.

Для циклов употребляется следующая запись: действительно переставляемые символы записываются в круглых скобках друг за другом в том порядке, в каком они друг в друга переходят при повторении подстановки; начинается запись с любого из действительно перемещаемых символов, а последний символ считается переходящим в первый. Так, для указанного выше примера эта запись имеет вид (2836).

Число символов, действительно перемещаемых циклом, называется длиной цикла.

Два цикла n-й степени называются независимыми, если они не имеют общих действительно переставляемых символов. Понятно, что при перемножении независимых циклов порядок расположения множителей не влияет на результат.

Всякая подстановка может быть единственным способом разложена в произведение независимых циклов.

Практически разложение осуществляется следующим образом: начинаем с любого из действительно перемещаемых символов и выписываем за ними те символы, в которые он переходит при повторении подстановки, пока не вернемся к исходному символу. После этого "закрытия" цикла начинаем с одного из оставшихся действительно перемещаемых символов, получаем второй цикл и так далее. Например,

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

Обратно, для всякой подстановки, заданной разложением в независимые циклы, можно найти запись в обычной форме (при условии, что степень этой подстановки известна). Например,

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

если известно, что степень этой подстановки есть 7.

Пусть дана подстановка n-й степени и пусть s есть число независимых циклов в ее разложении плюс число символов, оставляемых ею на месте.

Определение 12. Разность $n–s$ называется декрементом этой подстановки.

Для рассмотренных выше примеров декремент равен соответственно 3 и 4.

Теорема 5. Четность подстановки совпадает с четностью декремента этой подстановки.

Доказательство. Доказательство основывается на том, что всякий цикл длины k можно представить в виде произведения k-1 транспозиций: $(i_1, i_2, \dots, i_k)=(i_1, i_2)(i_1, i_3)\dots(i_1, i_k)$.

Любую подстановку можно разложить в циклы. Каждый цикл разложить в произведение транспозиций. Число этих транспозиций будет совпадать с декрементом подстановки.

Действительно, пусть $A=(i_{11},i_{12},...,i_{1k_1})(i_{21},i_{22},...,i_{2k_2})...(i_{s1},i_{s2},...,i_{sk_s})$ – разложение произвольной подстановки A n-й степени в произведение s независимых циклов ($k_1+k_2+\dots+k_s=n$). Разложим эти циклы в произведение транспозиций $(i_{11},i_{12},...,i_{1k_1}) = =(i_{11},i_{12})(i_{11},i_{13})...(i_{11},i_{1k_1})$ – цикл длины k_1 разложили в произведение k_1-1 транспозиций. $(i_{21},i_{22},...,i_{2k_2})=(i_{21},i_{22})(i_{21},i_{23})...(i_{21},i_{2k_2})$ – цикл длины k_2 разложили в произведение k_2-1 транспозиций. И так далее, последний s-й цикл длины k_s разложим в произведение k_s-1 транспозиций. Таким образом, $A=(i_{11},i_{12})(i_{11},i_{13})\dots(i_{s1},i_{s2})\ \dots\ (i_{s1},i_{sk_s})$. Суммарное число транспозиций в разложении подстановки A будет $(k_1\text{-}1)+(k_2\text{-}1)+\dots+(k_s\text{-}1)=(k_1+k_2+\dots+k_s)-(1+1+\dots+1)=n\text{-}s$.

Было доказано, что произведение n-s транспозиций есть подстановка, четность которой совпадает с четностью числа n-s. А так как n-s – декремент подстановки, то доказано, что четность подстановки совпадает с четностью декремента этой подстановки.