Теория перестановок и подстановок

Опр: 1. Перестановкой чисел $1, 2, \ldots, n$ называется расположение этих чисел в определенном порядке.

Обозначение: $(i_1, i_2, \ldots, i_n)$, где $\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$.

Пример: перестановка чисел от 1 до 5: $(2, 4, 1, 5, 3)$.

Утв. 1. Количество перестановок чисел $\{1, \ldots, n\}$ равно $n! = 1{\cdot}2{\cdot}\ldots{\cdot}n$.

□ Необходимо перебрать все перестановки. Первый элемент перестановки i_1 можно выбрать n способами. Для каждого выбора i_1 число i_2 мы можем выбрать $(n-1)$ способом. Для каждого выбора (i_1, i_2) число i_3 можно выбрать $(n-2)$ способами. И так далее. Таким образом, мы переберём все перестановки и общее количество вариантов перестановки $(i_1, i_2, \ldots, i_n)$ будет равно произведению количества вариантов на каждом шаге:

$$n{\cdot}(n-1){\cdot}(n-2){\cdot}\ldots{\cdot}2{\cdot}1 = n!$$

■

Опр: 2. Подстановкой степени n называется взаимнооднозначное (биективное) отображение:

$$\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$$

Rm: 1. Вместо чисел можно брать любое конечное множество и занумеровать элементы числами.

Пример: $\sigma(1) = 2$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 1$, $\sigma(5) = 3$ - подстановка, поскольку отображение является взаимнооднозначным.

Пример: $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 5$, $\sigma(5) = 3$ - не подстановка, поскольку отображение не является взаимнооднозначным: нарушается инъективность $\sigma(1) = \sigma(5) = 3$ и сюръективность, поскольку в 2 ничего не отображается.

Rm: 2. Для конечного множества инъективность на самом деле равносильна сюръективности. Если отображение не сюръективно, то оно не инъективно и наоборот.

Обозначим множество всех подстановок степени n, как S_n.

Двухрядная запись подстановки

Опр: 3. Двухрядной записью подстановки называется запись вида (таблица размера $2 \times n$):

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

где $(i_1, \ldots, i_n)$ и $(j_1, \ldots, j_n)$ это две перестановки чисел $1, \ldots, n$. Числа, которые стоят в нижней строке получаются из чисел, которые стоят в верхней строке применением отображениея σ:

$$\sigma(i_k) = j_k,\ \forall k = \overline{1, n}$$

Rm: 3. Заметим, что подстановку можно записать многими способами, потому что мы можем переставлять столбцы этой таблицы местами. Фактически таких способов записи у нас будет $n!$ - столько, сколько всего перестановок.

Опр: 4. Стандартной двухрядной записью подстановки назызвается запись вида:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

где $k_i = \sigma(i)$, $\forall i = \overline{1,n}$.

Пример: рассмотрим пример подстановки выше и запишем её в стандартном двухрядном виде:

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

Можно записать и в другом виде (нестандартном):

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

Утв. 2. Существует взаимнооднозначное соответствие между перестановками и подстановками, которое устроено следующим образом:

$$(k_1, k_2, \dots, k_n) \leftrightarrow \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

□ Очевидно: $\psi\big((k_1, \dots k_n)\big) = \sigma$, где σ - стандартная двухрядная запись. Пусть A_n - множество перестановок чисел $\{1, \dots, n\}$.

$$\forall a = \{a_1, \dots, a_n\},\ \psi(a) = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \in S_n$$

1) **инъективность**:

$$\forall a, b \in A_n,\ a \neq b \Rightarrow \psi(a) = \begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix} \neq \begin{pmatrix} 1 & \dots & n \\ b_1 & \dots & b_n \end{pmatrix} = \psi(b)$$

2) **сюръективность**:

$$\forall \sigma \in S_n,\ \exists\, a \in A_n \colon \psi(a) = \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \Rightarrow a = (i_1, i_2, \dots, i_n)$$

Разным перестановкам будут отвечать разные подстановки, и каждой подстановке будет отвечать какая-то перестановка. ■

Следствие 1. $|S_n| = n!$.

□ Следует сразу из взаимной однозначности между перестановками и подстановками. ■

Умножение подстановок

Опр: 5. Умножением подстановок степени n определим композицию отображений:

$$\forall \sigma, \pi \in S_n,\ \sigma{\cdot}\pi \in S_n,\ \sigma{\cdot}\pi\colon \{1,\dots,n\} \to \{1,\dots,n\}$$

$$\sigma{\cdot}\pi(k) = \sigma(\pi(k)),\ \forall k = \overline{1,n}$$

В двухрядной записи удобно вычислять умножение подстановок, особенно если эти две записи согласованны между собой, рассмотрим пример:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},\ \pi = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \Rightarrow \sigma{\cdot}\pi = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

Это так, поскольку композиция перестановок будет давать следующий результат:

$$\pi(k_1) = i_1,\ \sigma(i_1) = j_1 \Rightarrow \sigma(\pi(k_1)) = j_1 \Rightarrow \sigma{\cdot}\pi(k_m) = j_m,\ \forall m = \overline{1,n}$$

Свойства умножения подстановок

Опр: 6. Тождественная подстановка это подстановка вида:

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

1) **Ассоциативность умножения перестановок**:

$$(\sigma{\cdot}\pi){\cdot}\varphi = \sigma{\cdot}(\pi{\cdot}\varphi),\ \forall \sigma, \pi, \varphi \in S_n$$

□ В обоих случаях будет верно:

$$\forall k \in \{1,2,\dots,n\},\ k \mapsto \varphi(k) \mapsto \pi(\varphi(k)) \mapsto \sigma(\pi(\varphi(k)))$$

$$\forall k \in \{1,2,\dots,n\},\ (\sigma{\cdot}\pi){\cdot}\varphi(k) = \sigma{\cdot}\pi(\varphi(k)) = \sigma(\pi(\varphi(k)))$$
$$\forall k \in \{1,2,\dots,n\},\ \sigma{\cdot}(\pi{\cdot}\varphi)(k) = \sigma{\cdot}(\pi(\varphi(k))) = \sigma(\pi(\varphi(k)))$$

■

2) **Умножение на тождественную подстановку**:

$$\forall \sigma \in S_n,\ \varepsilon{\cdot}\sigma = \sigma{\cdot}\varepsilon = \sigma$$

□ Очевидно, поскольку:

$$\sigma{\cdot}\varepsilon(k) = \sigma(\varepsilon(k)) = \sigma(k) = \varepsilon(\sigma(k)) = \varepsilon{\cdot}\sigma(k),\ \forall k = \{1,\dots,n\}$$

■

3) **Существование обратной подстановки**:

$$\forall \sigma \in S_n,\ \exists\, \sigma^{-1} \in S_n\colon \sigma{\cdot}\sigma^{-1} = \sigma^{-1}{\cdot}\sigma = \varepsilon$$

□ Обратная подстановка существует в силу взаимной однозначности отображения.

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},\ \sigma^{-1} \in S_n$$

$$\forall k = \overline{1,n},\ \sigma{\cdot}\sigma^{-1}(j_k) = \sigma(\sigma^{-1}(j_k)) = \sigma(i_k) = j_k \Rightarrow \sigma{\cdot}\sigma^{-1} = \varepsilon$$

$$\forall k = \overline{1,n},\ \sigma^{-1}{\cdot}\sigma(i_k) = \sigma^{-1}(\sigma(i_k)) = \sigma^{-1}(j_k) = i_k \Rightarrow \sigma{\cdot}\sigma^{-1} = \varepsilon$$

■

4) **Некоммутативность**:

$$\exists\, \sigma, \pi \in S_n \colon \sigma{\cdot}\pi \neq \pi{\cdot}\sigma$$

□ Рассмотрим подстановки степени 3:

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

$$\sigma{\cdot}\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \pi{\cdot}\sigma$$

■

Циклические подстановки

Опр: 7. Подстановка $\sigma \in S_n$ называется циклической или циклом длины $l > 1$, если она действует по следующей схеме:

$$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \xrightarrow{\sigma} \dots \xrightarrow{\sigma} i_{l-1} \xrightarrow{\sigma} i_l \xrightarrow{\sigma} i_1$$

$$i \xrightarrow{\sigma} i,\ \forall i \neq i_1, \dots, i_l$$

Опр: 8. Однорядной записью цикла длины l называется запись вида:

$$\sigma = (i_1, i_2, \dots, i_{l-1}, i_l) = (i_1 i_2 \dots i_l)$$

Опр: 9. Множество чисел: $\{i_1, i_2, \dots, i_l\}$ называются орбитой цикла σ.

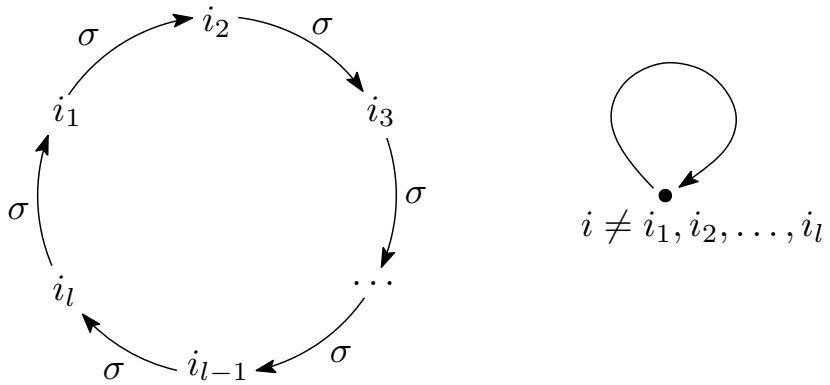

Рис. 1: Орбита цикла $\sigma = (i_1, \dots, i_l)$.

Пример: рассмотрим следующую подстановку:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \Rightarrow 1 \to 4 \to 3 \to 5 \to 1,\ 2 \to 2$$

Следовательно, наша подстановка это цикл длины 4. Запишем её в однорядной записи:

$$\sigma = (1435)$$

Rm: 4. Циклы это простейшие, после тождественной, подстановки.

Опр: 10. Два цикла $\sigma = (i_1 \dots i_l)$ и $\pi = (j_1 \dots j_m)$ называются независимыми, если их орбиты не пересекаются:

$$\{i_1, \dots, i_l\} \cap \{j_1, \dots, j_m\} = \varnothing$$

Утв. 3. Независимые циклы коммутируют: если σ и π - независимы, то:

$$\sigma \cdot \pi = \pi \cdot \sigma$$

□ Пусть $\sigma = (i_1 \dots i_l)$ и $\pi = (j_1 \dots j_m)$ - независимы, тогда:

$$\forall k \in \{i_1, \dots, i_l\},\ \sigma \cdot \pi(k) = \sigma(\pi(k)) = \sigma(k) = \pi(\sigma(k)) = \pi \cdot \sigma(k)$$

$$\forall k \in \{j_1, \dots, j_m\},\ \sigma \cdot \pi(k) = \sigma(\pi(k)) = \pi(k) = \pi(\sigma(k)) = \pi \cdot \sigma(k)$$

$$\forall k \in \{1, \dots, n\} \setminus (\{i_1, \dots, i_l\} \cup \{j_1, \dots j_m\}),\ \sigma \cdot \pi(k) = \sigma(\pi(k)) = k = \pi(\sigma(k)) = \pi \cdot \sigma(k)$$

■

Разложение подстановки в попарно независимые циклы

Перед формулировкой теоремы определим ряд понятий.

Опр: 11. Определим возведение подстановок в степень следующим образом:

$$\sigma^k = \underbrace{\sigma\cdot\ldots\cdot\sigma}_{k},\ k\in\mathbb{N},\quad \sigma^k = \underbrace{\sigma^{-1}\cdot\ldots\cdot\sigma^{-1}}_{|k|>0},\ k\in\mathbb{Z},\ k<0,\quad \sigma^k=\varepsilon,\ k=0$$

Утв. 4. (**свойства возведения подстановки в степень**)

(1) $\sigma^k\cdot\sigma^l=\sigma^{k+l}$, $\forall k,l\in\mathbb{Z}$;

(2) $(\sigma^k)^l=\sigma^{k\cdot l}$, $\forall k,l\in\mathbb{Z}$;

□

(1) Рассмотрим случаи:

$$\forall k,l\in\mathbb{Z}\colon k,l>0\Rightarrow \sigma^k\cdot\sigma^l=\underbrace{\sigma\cdot\ldots\cdot\sigma}_{k}\cdot\underbrace{\sigma\cdot\ldots\cdot\sigma}_{l}=\sigma^{k+l}$$

$$\forall k,l\in\mathbb{Z}\colon k,l<0\Rightarrow \sigma^k\cdot\sigma^l=\underbrace{\sigma^{-1}\cdot\ldots\cdot\sigma^{-1}}_{k}\cdot\underbrace{\sigma^{-1}\cdot\ldots\cdot\sigma^{-1}}_{l}=\sigma^{k+l}$$

$$\forall k,l\in\mathbb{Z}\colon k<0,l>0\Rightarrow \sigma^k\cdot\sigma^l=\underbrace{\sigma^{-1}\cdot\ldots\cdot\sigma^{-1}}_{k}\cdot\underbrace{\sigma\cdot\ldots\cdot\sigma}_{l}=\sigma^{\operatorname{sgn}(k+l)\cdot|k+l|}=\sigma^{k+l}$$

(2) Рассмотрим случаи:

$$l>0\Rightarrow(\sigma^k)^l=\underbrace{\sigma^k\cdot\ldots\cdot\sigma^k}_{l}=\sigma^{k\cdot l}$$

$$l<0\Rightarrow(\sigma^k)^l=\underbrace{\sigma^{-k}\cdot\ldots\cdot\sigma^{-k}}_{|l|}=\sigma^{k\cdot l}$$

$$l=0\Rightarrow(\sigma^k)^0=\varepsilon$$

■

Опр: 12. Орбитой числа $i\in\{1,\ldots,n\}$ под действием σ называется множество:

$$O(i)=\{\sigma^k(i)\mid k\in\mathbb{Z}\}$$

Утв. 5. Орбита любого числа $i\in\{1,\ldots,n\}$ есть следующее множество:

$$O(i)=\{i,\sigma(i),\sigma^2(i),\ldots\sigma^{m-1}(i)\}$$

где m такое наименьшее число, что $\sigma^m(i)=i$.

□ Все точки в одной орбите связаны следующим образом:

$$\ldots \to \sigma^{-2}(i) \to \sigma^{-1}(i) \to i = \sigma^0(i) \to \sigma(i) \to \sigma^2(i) \to \ldots$$

Цепочка бесконечная, но при этом орбита это конечное множество, поскольку $\{1, \ldots, n\}$ - конечное множество чисел. Тогда:

$$\exists\, k \neq l \colon \sigma^k(i) = \sigma^l(i)$$

Без ограничения общности, пусть $k > l$, тогда можем применить к левой и правой части σ^{-l}, тогда:

$$\sigma^{k-l}(i) = \sigma^0(i) = \varepsilon(i) = i,\ k - l > 0$$

Поскольку существует $k - l > 0$ со свойством выше, то мы можем выбрать наименьшую положительную степень с таким свойством. Пусть $m > 0$ - наименьшая степень, такая что: $\sigma^m(i) = i$, тогда:

$$i \xrightarrow{\sigma} \sigma(i) \xrightarrow{\sigma} \sigma^2(i) \xrightarrow{\sigma} \ldots \xrightarrow{\sigma} \sigma^m(i) \xrightarrow{\sigma} i \Rightarrow O(i) = \{i, \sigma(i), \sigma^2(i), \ldots \sigma^{m-1}(i)\}$$

$$O(i) = \{\sigma^k(i) \mid k \in \mathbb{Z}\} = \{i, \sigma(i), \sigma^2(i), \ldots \sigma^{m-1}(i)\}$$

■

Утв. 6. (**свойства орбит чисел**)

(1) Разные орбиты не пересекаются;

(2) Орбиты образуют разбиение $\{1, \ldots, n\}$ на попарно не пересекающиеся подмножества;

□

(1) Пусть $O(i) \cap O(j) \neq \varnothing$, тогда $\exists\, k \in O(i) \cap O(j) \Rightarrow k = \sigma^p(i) = \sigma^q(j)$, следовательно, применив σ^{-p}:

$$i = \sigma^{q-p}(j) \Rightarrow i \in O(j) \Rightarrow \forall l \in \mathbb{Z},\ \sigma^l(i) = \sigma^{l+q-p}(j) \in O(j) \Rightarrow O(i) \subseteq O(j)$$

Аналогично, можно доказать обратное включение: $O(j) \subseteq O(i) \Rightarrow O(i) = O(j)$;

(2) Следует из того, что каждое число лежит в какой-нибудь орбите, например, в своей собственной:

$$\forall i \in \{1, \ldots, n\},\ i \in O(i)$$

■

Теорема 1. Для любой подстановки $\sigma \in S_n$, существует разложение этой подстановки в произведение попарно независимых циклов $\sigma_1, \ldots, \sigma_s$:

$$\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$$

Причем это разложение единственно с точностью до перестановки сомножителей.

□

1) **Построение разложения σ в произведение независимых циклов**: из свойств орбит числа получается, что:

$$\{1, \ldots, n\} = O_1 \cup O_2 \cup \ldots \cup O_s \cup O_{s+1} \cup \ldots \cup O_t$$

где орбиты $1, \ldots, s$ состоят из нескольких чисел и орбиты $(s+1), \ldots, t$ состоят из одного числа. Отсюда, мы получим:

$$\sigma = (i_1^1 \ldots i_{l_1}^1) \cdot (i_1^2 \ldots i_{l_2}^2) \cdot \ldots \cdot (i_1^s \ldots i_{l_s}^s) = \sigma_1 \cdot \ldots \cdot \sigma_s$$

они будут независимы, поскольку каждый цикл действует на своей орбите, а орбиты не пересекаются. Таким образом, мы получили разложение;

2) **Единственность**: пусть $\sigma = \sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_s$, где σ_i - попарно независимые циклы:

$$\sigma_1 = (i_1^1 \ldots i_{l_1}^1), \ldots, \sigma_s = (i_1^s, \ldots, i_{l_s}^s)$$

Тогда σ действует на множество чисел $\{1, \ldots, n\}$ по схеме:

$$\forall i_j^k \in \{1, \ldots, n\},\ \sigma(i_j^k) = \sigma_k(i_j^k)$$

Следовательно, орбиты подстановки σ в $\{1, \ldots, n\}$ - это орбиты циклов $\sigma_1, \ldots, \sigma_s$, потому что каждое из чисел попадает в одну из орбит и на это число будет действовать только соответствующий цикл, остальные циклы будут оставлять это число на месте. Также заметим, что по σ можно однозначно восстановить орбиты независимых циклов $\sigma_1, \ldots, \sigma_s$ в разложении $\sigma \Rightarrow$ можно восстановить и сами циклы σ_i, потому что на своей орбите σ_i действует также как вся подстановка σ.

Таким образом, зная подстановку σ мы можем однозначно восстановить орбиты этих циклов. А зная эти орбиты и подстановку σ мы можем восстановить порядок перестановки элементов в орбите, то есть восстановить сами циклы;

■

Пример:

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

$$1 \to 4 \to 3 \to 5 \to 1, \quad 2 \to 7 \to 8 \to 2, \quad 6 \to 6 \Rightarrow$$

$$\Rightarrow \sigma = (1435) \cdot (278) = \sigma_1 \cdot \sigma_2$$

Получили циклы длины 4, 3 и стационарную точку.