

ЛЕКЦИЯ 10

Алгоритм поиска обратной матрицы. Пусть нам дана матрица A размера $n \times n$. Наша цель – проверить, обратима ли матрица A и, если да, то найти обратную.

1) приписываем справа к матрице A единичную матрицу такого же размера, получаем матрицу $Z = (A|E)$ размера $n \times 2n$.

2) Делаем элементарные преобразования строк матрицы Z так, чтобы левая часть привелась к улучшенному ступенчатому виду.

3) Если улучшенный ступенчатый вид левой части не E , то матрица A не обратима.

4) Если улучшенный ступенчатый вид A равен E , то получаем матрицу $(E|B)$. При этом $A^{-1} = B$.

Обоснование алгоритма

Если улучшенный ступенчатый вид квадратной матрицы A не единичный, то в нем есть нулевые строки. Это значит, что $\text{rk } A < n$, то есть матрица не обратима.

Пусть теперь улучшенный ступенчатый вид A равен E . При элементарных преобразованиях строк матрица умножается слева на матрицу элементарного преобразования. Так как с обоими частями происходит одинаковое преобразование строк, они умножаются на одинаковые матрицы:

$$(A|E) \rightarrow (S_1 A | S_1 E) \rightarrow (S_2 S_1 A | S_2 S_1 E) \rightarrow \dots \rightarrow (S_k \dots S_1 A | S_k \dots S_1 E) = (E|B).$$

Получаем, что $B = S_k \dots S_1$ и $S_k \dots S_1 A = BA = E$, то есть $B = A^{-1}$.

Лемма 1. Матрица, обратная к матрице элементарного преобразования – это матрица обратного элементарного преобразования.

Доказательство. Докажем это для элементарных преобразований строк, для элементарных преобразований столбцов надо поменять порядок произведения матриц. Пусть S – матрица элементарного преобразования φ , а T – матрица элементарного преобразования φ^{-1} . Тогда $S = \varphi(E)$. Значит,

$$E = \varphi^{-1}(\varphi(E)) = \varphi^{-1}(S) = TS.$$

□

Предложение 1. Любая невырожденная матрица может быть разложена в произведение элементарных матриц.

Доказательство. Пусть A – невырожденная квадратная матрица. Тогда ее можно привести элементарными преобразованиями строк к единичному виду. Получаем $S_k \dots S_1 A = E$. Отсюда $A = (S_k \dots S_1)^{-1} = S_1^{-1} \dots S_k^{-1}$ – произведение элементарных матриц. □

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

Подстановка длины (степени, 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 $1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 5, 4 \mapsto 1, 5 \mapsto 3$.

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 2. 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 3. $|S_n| = n!$.

Доказательство. Так как количество подстановок и перестановок одинаковое, будем считать перестановки длины n . Оформи́м 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. $\square$

Определение 2. Пусть $\sigma, \delta \in S_n$. *Произведением* (композицией) этих подстановок называется подстановка $\sigma\delta = \sigma \circ \delta \in S_n$.

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

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

Пример 1.

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

Теорема 1 (Свойства произведения подстановок).

- 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. $\sigma \delta \neq \delta \sigma$.

Пример 2 (Пример отсутствия коммутативности).

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

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

Определение 3. 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 4. 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 4. 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. $\square$

Теорема 2 (Разложение в независимые циклы). *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 j , затем j переходит в i , а затем много раз j переходит в i . $\square$

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

Пример 3.

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

Замечание 1. В записи подстановки в виде произведения независимых циклов не важен порядок циклов (независимые циклы коммутируют) и не важно, с какого элемента начинать цикл (последовательность, что за чем идет важна). Например,

$$(1, 2, 3, 4)(5, 6)(7, 8, 9) = (8, 9, 7)(3, 4, 1, 2)(6, 5).$$

Определение 5. 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 6. *Четность* перестановки α – это четность количества инверсий в ней.

Определение 7. *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 $\sigma(a) > \sigma(b)$. (Такие пары мы называем *инверсиями* в подстановке.)

Теорема 3. 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. $\square$

Лемма 5. При умножении справа на транспозицию $\tau = (i, i+1)$ подстановка σ меняет четность.

Доказательство. Рассмотрим нижнюю строку подстановки σ в стандартном виде. Обозначим ее α . При умножении справа на τ в α поменяются местами элементы u и v на местах i и $i+1$, получится α' , которая соответствует подстановке σ' .

Пусть $a, b \notin \{i, i+1\}$. Тогда пара (a, b) является или не является инверсией для σ и σ' одновременно. В самом деле на местах a и b в α и α' стоят одинаковые числа.

Пара (i, a) является инверсией для σ тогда и только тогда, когда $(i+1, a)$ является инверсией для σ' . И наоборот, пара $(i+1, a)$ является инверсией для σ тогда и только тогда, когда (i, a) является инверсией для σ' . В самом деле, $\sigma(i)$ теперь стоит на месте $i+1$. Но если $a > i$, то $a > i+1$ (напомним, $a \notin \{i, i+1\}$), и если $a < i$, то $a < i+1$.

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

Лемма 6. При умножении справа на транспозицию $\tau = (i, j)$ подстановка σ меняет четность.

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

$$(i, j) = (i, i+1)(i+1, i+2) \dots (j-2, j-1)(j-1, j)(j-2, j-1) \dots (i+1, i+2)(i, i+1).$$

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

Лемма 7. Любую подстановку σ можно представить в виде произведения некоторого количества транспозиций.

Доказательство. Начнем с тождественной подстановки и будем делать последовательно образы элементы нужными. Пусть $\sigma(1) = a$. Если $a \neq 1$, домножим id на транспозицию $(1, a)$ слева 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. $\delta_{n-1} = \sigma$. $\square$

Так как при умножении на транспозицию четность меняется, получаем.

Теорема 4. Четность подстановки σ – это четность количества транспозиций в любом разложении σ на транспозиции.

Доказательство. Пусть $\sigma = \tau_1 \dots \tau_k$, где τ_i – транспозиция. Тогда можно сказать, что $\sigma = \text{id} \tau_1 \dots \tau_k$. Рассмотрим последовательность подстановок

$$\delta_0 = \text{id}, \quad \delta_1 = \text{id} \circ \tau_1, \quad \delta_2 = \text{id} \circ \tau_1 \circ \tau_2, \quad \dots, \quad \delta_k = \text{id} \circ \tau_1 \circ \dots \circ \tau_k = \sigma.$$

При этом $\delta_0 = \text{id}$ – четная подстановка (0 инверсий), а при переходе от δ_i к δ_{i+1} происходит умножение на транспозицию справа, что по лемме 5 меняет четность. Следовательно, четность σ совпадает с четностью числа k . $\square$