Тема 8.

Обратими матрици.
Методи за намиране на обратна матрица

Преди да стигнем до темата на тази лекция, нека започнем с още едно приложение на матричното умножение.

Матрични кодове на Хил

- Разработени през 1929 г. от английския математик Лестър Хил.
- Използват матрично умножение и елементарна теория на числата (модулна алгебра) за кодиране и декодиране на съобщения.
- Съобщение, съставено от символи (букви и др.), първо се превръща в последователност от числа, от която се формира матрица. Тази матрица се умножава с кодираща матрица и получената нова последователност от числа отново се преобразува до съобщение от символи - кодираното съобщение.
- https://www.dcode.fr/hill-cipher

Нека разгледаме един пример - да кодираме думата *математика*. Първо нека на всяка буква съпоставим поредния ѝ номер в азбуката.

М	А	Т	Е	М	А	Т	И	К	А
13	1	19	4	13	1	19	9	11	1

След това формираме матрица X от получените числа, като типът на тази матрица зависи от типа на кодиращата матрица, тъй като двете трябва да могат да бъдат умножени (в избрания от нас ред). Кодиращата матрица трябва да бъде *обратима* (ще изясним това понятие и защо е необходимо да се постави това условие). Засега поставяме условието A да бъде квадратна. Нека кодиращата матрица A и съобщението X формираме така:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \qquad X = \begin{pmatrix} 13 & 1 & 19 & 4 & 13 \\ 1 & 19 & 9 & 11 & 1 \end{pmatrix}.$$

Първият етап на кодирането на съобщението се състои в умножаването на кодиращата матрица A и оригиналното съобщение X в избран от нас ред. Нека кодираното съобщение означим с B. Тогава

$$B = AX = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 13 & 1 & 19 & 4 & 13 \\ 1 & 19 & 9 & 11 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 15 & 39 & 37 & 28 & 15 \\ 43 & 79 & 93 & 62 & 43 \end{pmatrix}.$$

Процесът на кодиране за нас ще спре дотук. В оригиналния код на Хил номерацията на символите в кодиращата азбука започва от 0. След като се намери матрицата B, нейните елементи отново се преобразуват от числа до символи от кодиращата азбука, като стойността на всеки неин елемент се дели на броя на символите k в азбуката и се взима остатъка при това делене $(0, 1, 2, ..., k-1)$.

След като бъде получено съобщението B от получателя, то трябва да може да бъде декодирано еднозначно. Нека си припомним, че

$$AX = B.$$

При процеса на декодиране са известни матриците A и B и се търси матрицата X, т.е. трябва да бъде решено горното *матрично уравнение* за X.

Известно е, че ако a, x и b са числа, то уравнението $ax = b$ има единствено решение, точно когато $a \neq 0$. В такъв случай решението е $x = \frac{b}{a} = a^{-1}b$.
Нека разгледаме аналогична идея за матрици.

Разглеждаме векторното пространство $M_n(\mathbb{R})$ на квадратните матрици от n-ти ред.

Определение 8.1. Квадратна матрица A от n-ти ред се нарича ***обратима*** (*неособена, неизродена*), ако съществува матрицата A^{-1} също от ред n такава, че

$$AA^{-1} = A^{-1}A = E.$$

Матрицата A^{-1} се нарича ***обратна матрица*** на матрицата A. Обратната матрица на всяка матрица е единствена. Изпълнено е

$$\left(A^{-1}\right)^{-1} = A.$$

Обратната матрица на единичната матрица E е единичната матрица, т. е. $E^{-1} = E$.

За произволни квадратни матрици A и B от n-ти ред е изпълнено

$$(AB)^{-1} = B^{-1}A^{-1}, \qquad (A^{-1})^T = (A^T)^{-1}.$$

Множеството от всички обратими матрици в $M_n(\mathbb{R})$ означаваме с $GL_n(\mathbb{R})$.

Второто свойство се доказва по следния начин. Тъй като

$$AA^{-1} = E,$$

то

$$(AA^{-1})^T = E^T = E,$$

откъдето поради $(AB)^T = B^T A^T$ имаме

$$(AA^{-1})^T = (A^{-1})^T A^T = E.$$

Следователно A^T е обратната матрица на $(A^{-1})^T$, т.е. $(A^T)^{-1} = (A^{-1})^T$.

Теорема 8.1. *Една квадратна матрица A е обратима, точно когато* $\det A \neq 0$.

Доказателство.
($\Rightarrow$) Нека A е обратима. Следователно съществува квадратната матрица A^{-1}, такава че $AA^{-1} = E$. Тогава

$$\det(AA^{-1}) = \det(E) \quad \Leftrightarrow \quad \det(A)\det(A^{-1}) = \det(E).$$

Тъй като $\det(E) = 1$, от от последното равенство следва, че

$$\det(A)\det(A^{-1}) = 1.$$

Тогава

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

и $\det(A) \neq 0$, $\det(A^{-1}) \neq 0$.

($\Leftarrow$) Нека A е квадратна матрица от n-ти ред, за която $\det(A) \neq 0$ и да разгледаме следната матрица

$$A^{-1} = \frac{1}{\det A}(A_{ij})^T = \begin{pmatrix} \frac{A_{11}}{\det A} & \frac{A_{21}}{\det A} & \cdots & \frac{A_{n1}}{\det A} \\ \frac{A_{12}}{\det A} & \frac{A_{22}}{\det A} & \cdots & \frac{A_{n2}}{\det A} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{A_{1n}}{\det A} & \frac{A_{2n}}{\det A} & \cdots & \frac{A_{nn}}{\det A} \end{pmatrix}.$$

От правилото на Лаплас за пресмятане на детерминанта и от правило, което от някои е наричано "обратно правило на Лаплас" - *сумата от произведенията на елементите от произволен ред (стълб) на детерминанта и адюнгираните количества на съответните им елементи от* ***друг*** *ред (стълб)* ***е равна на нула***, следва, че $AA^{-1} = A^{-1}A = E$.

$$AA^{-1} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} \frac{A_{11}}{\det A} & \frac{A_{21}}{\det A} & \dots & \frac{A_{n1}}{\det A} \\ \frac{A_{12}}{\det A} & \frac{A_{22}}{\det A} & \dots & \frac{A_{n2}}{\det A} \\ \dots & \dots & \dots & \dots \\ \frac{A_{1n}}{\det A} & \frac{A_{2n}}{\det A} & \dots & \frac{A_{nn}}{\det A} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} = E.$$

Метод на адюнгираните количества за намиране на обратна матрица

Нека $A = (a_{ij})$ е квадратна матрица от n-ти ред, за която $\det A \neq 0$. Образуваме матрицата (A_{ij}) от адюнгираните количества A_{ij} на елементите a_{ij}. Тогава матрицата

$$A^{-1} = \frac{1}{\det A}(A_{ij})^T = \begin{pmatrix} \frac{A_{11}}{\det A} & \frac{A_{21}}{\det A} & \cdots & \frac{A_{n1}}{\det A} \\ \frac{A_{12}}{\det A} & \frac{A_{22}}{\det A} & \cdots & \frac{A_{n2}}{\det A} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{A_{1n}}{\det A} & \frac{A_{2n}}{\det A} & \cdots & \frac{A_{nn}}{\det A} \end{pmatrix}$$

е обратната матрица на A. Този метод е удобен за намиране на обратната матрица на A, ако A е квадратна матрица от втори или трети ред.

Пример 8.1. Намерете обратната матрица на

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Матрицата A е обратима, точно когато $\det A = ad - bc \neq 0$. Тогава

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}.$$

Пресмятаме

$$A_{11} = (-1)^{1+1}.d = d, \qquad A_{21} = (-1)^{1+2}.b = -b,$$
$$A_{12} = (-1)^{2+1}.c = -c, \qquad A_{22} = (-1)^{2+2}.a = a.$$

Следователно

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Пример 8.2. Намерете обратната матрица на

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

Първо пресмятаме детерминантата на A, за да се убедим, че е обратима

$$\det A = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = -2 \neq 0.$$

Следователно съществува A^{-1}. Пресмятаме адюнгираните количества на елементите на A:

$$A_{11} = (-1)^{1+1}.4 = 4, \qquad A_{21} = (-1)^{1+2}.2 = -2,$$
$$A_{12} = (-1)^{2+1}.3 = -3, \qquad A_{22} = (-1)^{2+2}.1 = 1.$$

Тогава за обратната матрица имаме

$$A^{-1} = -\frac{1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}.$$

Следователно кодиращата ни матрица A отговаря на поставеното от нас условие да бъде обратима ($\det A \neq 0$).

В оригиналния код на Хил обратимостта на матрицата е при деление с остатък на броя на символите k в кодиращата азбука, затова условието, което се поставя, е $\det A$ и броят на символите k в кодиращата азбука да бъдат взаимнопрости числа (НОД $= 1$).

Нека се върнем към декодирането на съобщението X, т.е. към матричното уравнение, което решаваме $AX = B$. За да намерим неизвестната матрица X, умножаваме двете страни (отляво) на уравнението с обратната матрица A^{-1}

$$AX = B \quad |A^{-1} \text{ отляво} \quad \Rightarrow \quad (A^{-1}A)X = A^{-1}B \quad \Rightarrow$$
$$\Rightarrow \quad EX = A^{-1}B \quad \Rightarrow \quad X = A^{-1}B.$$

Така

$$X = A^{-1}B = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 15 & 39 & 37 & 28 & 15 \\ 43 & 79 & 93 & 62 & 43 \end{pmatrix} =$$

$$= \begin{pmatrix} 13 & 1 & 19 & 4 & 13 \\ 1 & 19 & 9 & 11 & 1 \end{pmatrix}.$$

Отбелязваме, че е важно дали умножаваме двете страни на матрично уравнение с матрица отляво или отдясно, тъй като матричното умножение не е комутативно ($AB \neq BA$).

Матричното уравнение $XA = B$ в случай, че матрицата A е обратима ($\det A \neq 0$) се решава по следния начин

$$XA = B \quad |A^{-1} \text{ отдясно} \quad \Rightarrow \quad X(AA^{-1}) = BA^{-1} \quad \Rightarrow$$
$$\Rightarrow \quad XE = BA^{-1} \quad \Rightarrow \quad X = BA^{-1}.$$

Матричният код на Хил не е особено надежден. Кодът е сравнително лесно пробиваем, ако е известен типът на кодиращата матрица и съответстващи части от оригиналното и кодираното съобщение, които са от същия тип като кодиращата матрица. Нека в нашия случай са известни първите два стълба на матриците X и B, които са означени съответно с

$$\overline{X} = \begin{pmatrix} 13 & 1 \\ 1 & 19 \end{pmatrix}, \qquad \overline{B} = \begin{pmatrix} 15 & 39 \\ 43 & 79 \end{pmatrix}.$$

Тогава тъй като $A\overline{X} = \overline{B}$, то в случай, че матрицата $\overline{X}$ е обратима ($\det \overline{X} \neq 0$), последното матрично уравнение може да се реши еднозначно относно кодиращата матрица A. Намирането на A означава пълно разбиване на кода, защото позволява разкодиране на цялото съобщение.

$$A = \overline{B}\,\overline{X}^{-1} = \frac{1}{246} \begin{pmatrix} 15 & 39 \\ 43 & 79 \end{pmatrix} \begin{pmatrix} 19 & -1 \\ -1 & 13 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Пример 8.3. Намерете обратната матрица на

$$A = \begin{pmatrix} -1 & 1 & 0 \\ 1 & -1 & -3 \\ 1 & 0 & 1 \end{pmatrix}.$$

Имаме $\det A = -3 \neq 0$. Пресмятаме адюнгираните количества на елементите на матрицата.

$$A_{11} = (-1)^{1+1} \begin{vmatrix} -1 & -3 \\ 0 & 1 \end{vmatrix} = -1, \quad A_{12} = (-1)^{1+2} \begin{vmatrix} 1 & -3 \\ 1 & 1 \end{vmatrix} = -4,$$

$$A_{13} = (-1)^{1+3} \begin{vmatrix} 1 & -1 \\ 1 & 0 \end{vmatrix} = 1,$$

$$A_{21} = (-1)^{2+1} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = -1, \quad A_{22} = (-1)^{2+2} \begin{vmatrix} -1 & 0 \\ 1 & 1 \end{vmatrix} = -1,$$

$$A_{23} = (-1)^{2+3} \begin{vmatrix} -1 & 1 \\ 1 & 0 \end{vmatrix} = 1,$$

$$A_{31} = (-1)^{3+1} \begin{vmatrix} 1 & 0 \\ -1 & -3 \end{vmatrix} = -3, \; A_{32} = (-1)^{3+2} \begin{vmatrix} -1 & 0 \\ 1 & -3 \end{vmatrix} = -3,$$

$$A_{33} = (-1)^{3+3} \begin{vmatrix} -1 & 1 \\ 1 & -1 \end{vmatrix} = 0.$$

Тогава обратната матрица на A има вида

$$A^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & 1 \\ \frac{4}{3} & \frac{1}{3} & 1 \\ -\frac{1}{3} & -\frac{1}{3} & 0 \end{pmatrix}.$$

Метод на Гаус-Жордан за намиране на обратна матрица

При този метод започваме с матрицата $(A|E)$, където E е единичната матрица от същия ред както A и чрез елементарни преобразувания **само върху редовете на цялата матрица** $(A|E)$ са стремим на мястото на A да получим E. Тогава на мястото на E ще стои обратната матрица A^{-1} на A.

$$(A|E) \sim ... \sim (E|A^{-1}).$$

Елементарните преобразувания върху редовете включват:

разместване на редове;

умножаване на ред с число, различно от нула;

умножаване на ред с число и прибавянето му към друг ред.

Нека да намерим обратната матрица на A от Пример 9.2 чрез метода на Гаус-Жордан.

Започваме с матрицата $(A|E)$. Първото нещо, което ще направим е да да се уверим, че **елементът в първи ред и първи стълб на** $(A|E)$ **е числото 1**. Ако това не е изпълнено, чрез подходяща комбинация от елементарни преобразувания преобразуваме този елемент в 1.

В нашия пример можем да умножим целия първи ред на $(A|E)$ с (-1). Друг начин е да разместим редовете на $(A|E)$ така, че вторият или третият ред да застанат на мястото на първия.

$$(A|E) = \left(\begin{array}{ccc|ccc} -1 & 1 & 0 & 1 & 0 & 0 \\ 1 & -1 & -3 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \begin{matrix} \text{(-1)} \\ \sim \end{matrix} \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 1 & -1 & -3 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Следващата ни задача е на **анулираме всички елементи под главния диагонал на A, а по главния диагонал да получим само единици**. Работим първо с първия ред на $(A|E)$, за да направим нули всички елементи в първия стълб, намиращи се под главния диагонал. След това преминаваме към втория ред. Осигуряваме си единица във втори ред и втори стълб (главния диагонал) и анулираме всички елементи във втория стълб под тази единица и т. н.

В нашия пример умножаваме целия първи ред на $(A|E)$ с (-1) и го прибавяме последователно към целия втори и трети ред на $(A|E)$.

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 1 & -1 & -3 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \begin{matrix} \\ \text{(-1)} \\ \\ \end{matrix} \sim \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right)$$

Сега забелязваме, че елементът във втори ред и втори стълб не е 1, а 0. Затова разместваме втория и третия ред на $(A|E)$.

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & -3 & 1 & 1 & 0 \end{array}\right).$$

Елементът в трети ред и трети стълб също трябва да бъде единица. Затова умножаваме целия трети ред на $(A|E)$ с $(-\frac{1}{3})$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & -3 & 1 & 1 & 0 \end{array}\right) \begin{pmatrix} -\frac{1}{3} \end{pmatrix} \sim \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & 0 \end{array}\right).$$

Сега всички елементи под главния диагонал на A са нули, а по главния диагонал имаме само единици. За да превърнем A в

E, следва да **анулираме всички елементи над главния диагонал на** A. За тази цел използваме последния ред, в нашия пример това е третият ред. Първо анулираме всички елементи над главния диагонал, които са разположени в последния стълб на A, в нашия пример - единицата във втори ред и трети стълб. Умножаваме третия ред с (-1) и го прибавяме към втория.

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & 0 \end{array}\right) \begin{array}{l} \\ \\ \urcorner \\ \textbf{(-1)} \end{array} \sim \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & \frac{4}{3} & \frac{1}{3} & 1 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & 0 \end{array}\right)$$

Сега преминаваме към следващия стълб на A в посока от дясно на ляво и анулираме всички елементи над главния диагонал в този стълб. В нашия пример това е вторият стълб. Над главния диагонал в него има само един елемент, който не е нула. За да го анулираме, използваме единицата под него, като прибавяме втория ред към първия.

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & \frac{4}{3} & \frac{1}{3} & 1 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & 0 \end{array}\right) \overset{+}{\sim} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & 1 \\ 0 & 1 & 0 & \frac{4}{3} & \frac{1}{3} & 1 \\ 0 & 0 & 1 & -\frac{1}{3} & -\frac{1}{3} & 0 \end{array}\right).$$

Сега в ляво получихме единичната матрица E. Тогава матрицата в дясно от вертикалната черта ($|$) е обратната матрица A^{-1}.

Литература

1. Д. Мекеров, Н. Начев, Ст. Миховски, Е. Павлов, *Линейна алгебра и аналитична геометрия*, Пловдив, 1997.

2. D. C. Lay, S. R. Lay, Judi J. McDonald, *Linear algebra and its applications*, 5th ed. Pearson, 2016.

3. G. Strang, *Linear algebra and its applications*, 4th ed., Nelson Engineering, 2007, ISBN-13: 978-813-150-172-6.

4. H. Anton, C. Rorres, *Elementary Linear Angebra (applications version)*, 11th ed., Wiley, 2014, ISBN 978-1-118-43441-3.

5. S. Axler, *Linear Algebra Done Right*, 3rd ed., Springer, 2015.

6. K. Singh, *Linear Algebra Step by Step*, Oxford University Press, 2014.

7. C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM, 2000.

8. S. J. Leon, *Linear Algebra with Applications*, 9th ed., Pearson, 2015.