Określenia wstępne

1. **Macierzą** nazywamy prostokątną tablicę liczb

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nm} \end{pmatrix}$$

Macierz ta ma n-wierszy i m-kolumn. Mówimy, że ma wymiar
n na m (n x m).
Zapis a_{ij} oznacza, że element znajduje się w i-tym wierszu i j-tej kolumnie.

2. Jeżeli n=m, to macierz nazywamy kwadratową.

3. Macierzą zerową nazywamy macierz dowolnego wymiaru, której wszystkie elementy są równe zero.

4. Macierz o wymiarze n x 1 nazywamy kolumnową. Macierz o wymiarze 1 x m nazywamy wierszową.

$$A=\begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} \qquad A=\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_m \end{pmatrix}$$

5. **Macierzą diagonalną** nazywamy macierz kwadratową, której elementy położone poza główną przekątną są równe zero.

$$A=\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ 0 & a_{22} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

6. **Macierzą jednostkową** nazywamy macierz diagonalną, której elementy położone na głównej przekątnej są równe jeden.

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

7. Macierze A i B są równe (A = B), jeżeli mają ten sam wymiar i $\underset{i,j}{\forall}\ a_{ij}=b_{ij}$

8. **Macierzą przestawioną (transponowaną)** nazywamy macierz, która powstaje z danej macierzy A przez zamianę wierszy na kolumny.

Np. $A=\begin{pmatrix} 1 & 5 & 7 \\ -1 & 0 & 9 \end{pmatrix} \qquad A^T=\begin{pmatrix} 1 & -1 \\ 5 & 0 \\ 7 & 9 \end{pmatrix}$

Działania na macierzach

1. **Sumą macierzy** A i B nazywamy macierz C = A + B taką, że $\underset{i,j}{\forall}\ c_{ij}=a_{ij}+b_{ij}$

Np. $\begin{pmatrix} 1 & 5 \\ 2 & 7 \end{pmatrix}+\begin{pmatrix} 2 & 3 \\ 5 & 4 \end{pmatrix}=\begin{pmatrix} 3 & 8 \\ 7 & 11 \end{pmatrix}$

Uwaga !
- dodawanie macierzy jest wykonalne tylko wtedy, gdy mają ten sam wymiar
- dodawanie macierzy jest przemienne i łączne

$$A + B = B + A$$
$$(A + B) + C = A + (B + C)$$

- odejmowanie macierzy wykonujemy analogicznie jak dodawanie

2. **Iloczynem macierzy A przez liczbę k** nazywamy macierz C = kA taką, że $\underset{i,j}{\forall} c_{ij} = k \cdot a_{ij}$

Np. $2\begin{pmatrix} 1 & 5 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 2 & 10 \\ 4 & 14 \end{pmatrix}$

3. **Iloczynem macierzy** A_{nxp} i B_{pxm} nazywamy macierz C = AB taką, że

$$\underset{i,j}{\forall} c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + ... + a_{ip} \cdot b_{pj}$$

(elementy wiersza pierwszej macierzy mnożymy przez kolumny drugiej)

Np. $\begin{pmatrix} 1 & 5 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 5 & 4 \end{pmatrix} = \begin{pmatrix} 1\cdot 2+5\cdot 5 & 1\cdot 3+5\cdot 4 \\ 2\cdot 2+7\cdot 5 & 2\cdot 3+7\cdot 4 \end{pmatrix} = \begin{pmatrix} 12 & 23 \\ 39 & 34 \end{pmatrix}$

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

Uwaga!
- iloczyn macierzy jest określony tylko wtedy, gdy liczba kolumn pierwszej macierzy jest równa liczbie wierszy drugiej macierzy
- mnożenie macierzy jest łączne $A \cdot (B \cdot C) = (A \cdot B) \cdot C$
- dla macierzy zachodzi prawo rozdzielności mnożenia względem dodawania $A \cdot (B + C) = A \cdot B + A \cdot C$
- mnożenie macierzy NIE JEST PRZEMIENNE $A \cdot B \neq B \cdot A$

Macierzą odwrotną do macierzy A nazywamy macierz A^{-1} taką, że $A \cdot A^{-1} = A^{-1} \cdot A = I$ (iloczyn macierzy jest równy macierzy jednostkowej)

(odwracanie macierzy – wyznaczanie macierzy odwrotnej- nie jest niestety proste !!!)

Zadania

Dane są macierze

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 3 \\ 2 & -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 & 1 \\ 0 & -1 & 2 \\ 1 & -2 & 1 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & -1 \\ -3 & -1 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ -1 & -1 & 3 \end{pmatrix}$$

Wyznacz:

1. $A + B$
2. $2 \cdot C$
3. $-3 \cdot D + 2 \cdot A$
4. $(A + B) - (C + D)$
5. $A \cdot (B + C)$
6. $(A - B) \cdot D$
7. $A^T - D^T$
8. $(A - B)^T \cdot (C^T + D)$
9. $((B^T + C) \cdot D^T)^T$
10. $(A - C)^T \cdot (B^T + D^T)^T$

Układy równań liniowych

Układ

$$\begin{cases} a_{11}\cdot x_1 + a_{12}\cdot x_2 + a_{13}\cdot x_3 + ... + a_{1n}\cdot x_n = b_1 \\ a_{21}\cdot x_1 + a_{22}\cdot x_2 + a_{23}\cdot x_3 + ... + a_{2n}\cdot x_n = b_2 \\ ..... \\ a_{n1}\cdot x_1 + a_{n2}\cdot x_2 + a_{n3}\cdot x_3 + ... + a_{nn}\cdot x_n = b_n \end{cases}$$

nazywamy układem n równań liniowych o n niewiadomych.

Rozwiązaniem układu jest każdy układ liczb $(x_1, x_2, x_3, \ ... \ x_n)$ dla którego każde z równań jest tożsamością.

Układ, który ma 1 rozwiązanie nazywamy ***oznaczonym***.
Układ, który ma więcej niż jedno rozwiązanie nazywamy ***nieoznaczonym***.
Układ, który nie ma rozwiązania nazywamy ***sprzecznym***.

Operacje elementarne

Układ równań otrzymany w wyniku
- dodania (odjęciu) liczby do obu stron równania
- pomnożenia (podzieleniu) równania przez liczbę różna od zera
- zamiany wierszy (kolumn) miejscami
- dodania wierszy (równań) stronami

jest równoważny układowi „wyjściowemu” (ma te same rozwiązania)

Rozwiązując układ równań metodą podstawiania czy przeciwnych współczynników korzystamy z tych właśnie operacji. Na tych operacjach opiera się również tzw. **metoda Gaussa** oraz **metoda równania macierzowego.**

Metoda równania macierzowego

Przypomnijmy metodę rozwiązywania równania liniowego ($a \neq 0$).

$$\begin{aligned} ax - b &= 0 \\ ax &= b \\ x &= \frac{b}{a} \end{aligned} \qquad \textit{Np.} \qquad \begin{aligned} 2x + 2 &= 8 \\ 2x &= 6 \\ x &= \frac{6}{2} \\ x &= 3 \end{aligned}$$

Jeśli przyjmiemy oznaczenia

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & ... & a_{1n} \\ a_{21} & a_{22} & a_{23} & ... & a_{2n} \\ ..... & & & & \\ a_{n1} & a_{n2} & a_{n3} & ... & a_{nn} \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{pmatrix} \qquad B = \begin{pmatrix} b_1 \\ b_2 \\ ... \\ b_n \end{pmatrix},$$

to zapis

(1) $A \cdot X = B$

będzie odpowiadał układowi równań

$$(2) \begin{cases} a_{11}\cdot x_1 + a_{12}\cdot x_2 + a_{13}\cdot x_3 + ... + a_{1n}\cdot x_n = b_1 \\ a_{21}\cdot x_1 + a_{22}\cdot x_2 + a_{23}\cdot x_3 + ... + a_{2n}\cdot x_n = b_2 \\ ..... \\ a_{n1}\cdot x_1 + a_{n2}\cdot x_2 + a_{n3}\cdot x_3 + ... + a_{nn}\cdot x_n = b_n \end{cases}$$

Zatem rozwiązanie równania (1) będzie równoznaczne z rozwiązaniem układu równań (2). Rozwiązania równania (1) dokonamy analogicznie jak rozwiązania „zwykłego” równania liniowego (pamiętając, że A, X i B są macierzami)

$$\begin{aligned} A \cdot X &= B \ \ | A^{-1} \\ A^{-1} \cdot A \cdot X &= A^{-1} \cdot B \\ X &= A^{-1} \cdot B \end{aligned}$$

Przykład

Rozwiąż układ $\begin{cases} x+y+z=0 \\ -3x+2y+4z=7 \\ 2x-3y+3z=1 \end{cases}$

Rozwiązanie

$$A \cdot X = B$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -3 & 2 & 4 \\ 2 & -3 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 7 \\ 1 \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} \frac{9}{20} & -\frac{3}{20} & \frac{1}{20} \\ \frac{17}{40} & \frac{1}{40} & -\frac{7}{40} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{pmatrix}}_{A^{-1}} \cdot \begin{pmatrix} 1 & 1 & 1 \\ -3 & 2 & 4 \\ 2 & -3 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{9}{20} & -\frac{3}{20} & \frac{1}{20} \\ \frac{17}{40} & \frac{1}{40} & -\frac{7}{40} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 7 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

Zatem rozwiązaniem układu jest trójka liczb $\begin{cases} x=-1 \\ y=0 \\ z=1 \end{cases}$

Metoda schodkowa Gaussa

Metoda Gaussa rozwiązywania układu równań liniowych przez sprowadzenie odpowiadającej mu macierzy do postaci schodkowej.

Przykład

Rozwiąż układ równań z poprzedniego przykładu

(Pierwsza kolumna odpowiada współczynnikom x, druga y, trzecia z, a czwarta wyrazom wolnym. Kolejne zapisy powstają przez pomnożenie wiersza przez ustaloną liczbę i dodaniu go do innego wiersza)

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ -3 & 2 & 4 & 7 \\ 2 & -3 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} -3 & 2 & 4 & 7 \\ 1 & 1 & 1 & 0 \\ 2 & -3 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} -6 & 4 & 8 & 14 \\ 6 & 6 & 6 & 0 \\ 6 & -9 & 9 & 3 \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|c} -6 & 4 & 8 & 14 \\ 0 & 10 & 14 & 14 \\ 0 & -5 & 17 & 17 \end{array}\right) \sim \left(\begin{array}{ccc|c} -6 & 4 & 8 & 14 \\ 0 & 10 & 14 & 14 \\ 0 & -10 & 34 & 34 \end{array}\right) \sim \left(\begin{array}{ccc|c} -6 & 4 & 8 & 14 \\ 0 & 10 & 14 & 14 \\ 0 & 0 & 48 & 48 \end{array}\right)$$

Z ostatniego zapisu i ostatniego w nim wiersz wnioskujemy, że

$$48z = 48$$
$$z = 1$$

Z przedostatniego wiersza wynika, że

$$10y + 14z = 14$$
$$10y + 14 \cdot 1 = 14$$
$$10y = 0$$
$$y = 0$$

Z pierwszego wiersza ostatniego zapisu (ale można wziąć dowolny) mamy

$$-6x + 4y + 8z = 14$$
$$-6x + 4 \cdot 0 + 8 \cdot 1 = 14$$
$$-6x = 6$$
$$x = 1$$

Zadania

Rozwiąż

$$\begin{cases} x+y+z=6 \\ 2x-y-z=-3, \\ x-3y+2z=1 \end{cases} \quad \begin{cases} x-y+z=1 \\ 3x+y+2z=5 \\ 4x-2y+3z=4 \end{cases}, \quad \begin{cases} a+b+c+d=10 \\ b+c+d+e=9 \\ c+d+e+a=8 \\ d+e+a+b=7 \\ e+a+b+c=6 \end{cases}$$

Macierze i kryptografia

Dokonajmy prostego przypisania (zaszyfrowania) liter do kolejnych liczb naturalnych

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Wtedy tekst: ALA MA KOTA
ma postać: 1 12 1 13 1 11 15 19 1

Złamanie takiego szyfru jest oczywiście bardzo proste. Aby utrudnić (i to znacznie ☺) dokonajmy następujących operacji:

1. Podzielmy cały tekst na segmenty o stałej długości np. 9
2. Każdej literze przypiszmy jej odpowiednik liczbowy jak poprzednio
3. Umieśćmy każdą 9-tkę liczb w macierzy o wymiarze 3x3 (jeśli w „ostatniej" macierzy będą „wolne miejsca", to wypełnimy je zerami)
4. Weźmy macierz 3x3 z dowolnymi (ustalonymi) współczynnikami – to będzie nasz klucz szyfrujący
5. Każdy „segment" naszego tekstu pomnóżmy przez „klucz szyfrujący"
6. Zapiszmy powstałe liczby ponownie w ciągu „jedna za drugą")

Taki szyfr odpowiada zapisowi matematycznemu $K \cdot T = S$, gdzie T – to macierz z tekstem „wyjściowym", K – macierz „klucza szyfrującego", a S – macierz z „zaszyfrowanym tekstem"

Przykład

Zaszyfruj tekst „ALA MA KOTA" stosując segmenty długości 9 i klucz szyfrujący $K = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

Rozwiązanie

Zamieńmy tekst „ALA MA KOTA" na ciąg liczb 1, 12,1, 13, 1, 11, 15, 19, 1 i umieśćmy je w macierzy 3x3: $T = \begin{pmatrix} 1 & 12 & 1 \\ 13 & 1 & 11 \\ 15 & 19 & 1 \end{pmatrix}$, a następnie przystąpmy do szyfrowania kluczem K:

$$K \cdot T = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 12 & 1 \\ 13 & 1 & 11 \\ 15 & 19 & 1 \end{pmatrix} = \begin{pmatrix} -18 & -43 & 20 \\ 43 & 39 & 18 \\ 15 & 19 & 1 \end{pmatrix}$$

Zaszyfrowany tekst ma więc postać: -18, -43, 20, 43, 39, 18, 15, 19, 1
(Czy ktoś teraz by zgadł, że chodzi o tekst „ALA MA KOTA" ☺ ?!?)

A teraz przystąpmy do deszyfracji tekstu (musimy znać oczywiście długość segmentu i klucz szyfrujący). Matematycznie deszyfracja odpowiada zapisowi matematycznemu:

$$K \cdot T = S \quad | \cdot K^{-1}$$

$$\underbrace{K^{-1} \cdot K}_{I} \cdot T = K^{-1} \cdot S$$

$$T = K^{-1} \cdot S$$

Zatem dla deszyfracji tekstu musimy wyznaczyć macierz odwrotną do macierzy szyfrującej (klucza szyfrującego)

Przykład

Odszyfruj zapis -18, -43, 20, 43, 39, 18, 15, 19, 1 wiedząc, że segment ma długość 9, a klucz szyfrujący $K = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

Rozwiązanie

Jeśli klucz szyfrujący jest macierzą $K = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$, to klucz deszyfrujący jest macierzą $D = K^{-1} = \begin{pmatrix} 1 & -2 & 7 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$ (wyznaczona programem komp.)

Deszyfracja:

$$T = K^{-1} \cdot S = \begin{pmatrix} 1 & -2 & 7 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -18 & -43 & 20 \\ 43 & 39 & 18 \\ 15 & 19 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 12 & 1 \\ 13 & 1 & 11 \\ 15 & 19 & 1 \end{pmatrix}$$

czyli mamy 1 12 1 13 1 11 15 19 1 i podstawiając litery w miejsce kolejnych liczb otrzymamy odszyfrowany tekst „ALA MA KOTA”

Przykład

1. Stosując poprzedni klucz szyfrujący i długość segmentu zaszyfruj tekst „BRYLANT JEST KAWAŁKIEM WĘGLA, KTÓRY ZDOŁAŁ ZMIENIĆ W RZECZYWISTOŚĆ SWE NAJPIĘKNIEJSZE MARZENIA”
2. Stosując poprzedni klucz deszyfrujący i długość segmentu odszyfruj
   7, 0, 33, 18, 23, 37, 5, 9, 8, -12, 39, 13, 36, 19, 5, 14, 0, 0

O szyfrach...

Szyfry prawdopodobnie wymyślili starożytni kupcy, by przekazywać sobie wiadomości nie mogące dotrzeć do konkurencji. Pewnym jest natomiast, że szyframi posługiwano się w krajach Mezopotamii i Egipcie. Na początku szyfry były bardzo proste – polegały jedynie na zastępowaniu jednych słów innymi. **N**astępną generacją były szyfry również polegające na zamianie – tym razem nie słów , lecz liter (np. sławny szyfr Cezara) - *Niestety, w dzisiejszych czasach coś takiego już się nie sprawdza – bowiem teksty kodowane w ten sposób poddają się metodom analizy statystycznej. Oznacza to po prostu, że odpowiednio wyszkolony człowiek, mając do dyspozycji odpowiednio dużą ilość zaszyfrowanego materiału jest w stanie odtworzyć szyfr i treść listów opierając się na statystykach (np. na przeciętnej częstości występowania danych liter lub ich układów w danym języku)*. **P**rawdziwy przełom w szpiegostwie (a więc i z metodami przekazywania tajnych informacji) przyniosła era nowożytna w czasach Kongresu Wiedeńskiego. Wtedy też powstały pierwsze matematyczne podstawy teorii szyfrowania i rozszyfrowywania. Dość popularnymi w tamtych czasach były szyfry oparte o rysunki. **K**olejnym kamieniem milowym na drodze kryptologii okazało się skonstruowanie w 1915 roku przez Amerykanina Edwarda Heberna maszyny szyfrującej. Z wyglądu przypominała ona dalekopis – nadawca po prostu pisze na klawiaturze tekst depeszy, która automatycznie jest kodowana przez elektryczne, mechaniczne lub elektroniczne układy urządzenia. Odbiorca, wyposażony w podobne urządzenie, po prostu wstukuje tekst, który otrzymał (np. drogą radiową) i dostaje gotowy, rozszyfrowany list. **N**a tej zasadzie działała najsłynniejsza chyba maszyna szyfrująca świata – niemiecka ENIGMA. W zależności od ustawienia początkowych parametrów mogła ona wytworzyć około czterdziestu kwadrylionów kombinacji liter - *I z nią jednak sobie poradzono, a zrobili to polscy matematycy – również metodami naukowymi.*

Szyfry jednak mają też duże zastosowanie we współczesnym “cywilnym” świecie. Od kiedy Internet stał się ogólnodostępny, nikogo nie dziwią już np. zakupy przez Sieć, do których używa się numeru karty kredytowej. Aby przesłać tą informację od kupującego do “sklepu”, trzeba ją uprzednio zakodować, żeby nikt niepowołany nie jej dostał. Podobnie w przypadku sieci komputerowych. Każdy szanujący się system sieciowy po dostaniu hasła od użytkownika koduje go (swoją własną metodą, bardzo skomplikowaną). Za każdym razem, gdy użytkownik podaje owo hasło, jest ono ponownie szyfrowane i w takiej formie porównywane z oryginałem. Szyfry w komputerze są tak zwanymi “szyframi jednostronnymi” – to znaczy, że nie jest możliwym ich odszyfrowanie. To pozwala wykorzystać je jedynie do działań, gdzie dokonuje się tylko porównywania – a więc np. identyfikacji użytkownika w sieci.