# Linear Algebra and Applications
# 01 October 2013

Lect. Erke ARIBAŞ

References:
-***Elementary Linear Algebra-Applications Version”***,
Howard Anton and Chris Rorres, $9^{th}$ Edition, Wiley, 2010.

# An example application of matrix inverse--Cryptography

Cryptography involves encrypting data so that a third party can not intercept and read the data.

## Encryption Process

1. Convert the text of the message into a stream of numerical values.
2. Place the data into a matrix.
3. Multiply the data by the encoding matrix.
4. Convert the matrix into a stream of numerical values that contains the encrypted message.

Consider the message "Red Rum"

A message is converted into numeric form according to some scheme. The easiest scheme is to let space=0, A=1, B=2, ..., Y=25, and Z=26. For example, the message "Red Rum" would become 18, 5, 4, 0, 18, 21, 13.

This data was placed into matrix form. The size of the matrix depends on the size of the encryption key. Let's say that our encryption matrix (encoding matrix) is a 2x2 matrix. Since I have seven pieces of data, I would place that into a 4x2 matrix and fill the last spot with a space to make the matrix complete. Let's call the original, unencrypted data matrix A.

$$A = \begin{bmatrix} 18 & 5 \\ 4 & 0 \\ 18 & 21 \\ 13 & 0 \end{bmatrix}$$

There is an invertible matrix which is called the encryption matrix or the encoding matrix. We'll call it matrix B. Since this matrix needs to be invertible, it must be square.

This could really be anything, it's up to the person encrypting the matrix. I'll use this matrix.

$$B = \begin{bmatrix} 4 & -2 \\ -1 & 3 \end{bmatrix}$$

The unencrypted data is then multiplied by our encoding matrix. The result of this multiplication is the matrix containing the encrypted data. We'll call it matrix X.

$$X = A\,B = \begin{bmatrix} 67 & -21 \\ 16 & -8 \\ 51 & 27 \\ 52 & -26 \end{bmatrix}$$

The message that you would pass on to the other person is the the stream of numbers 67, -21, 16, -8, 51, 27, 52, -26.

## Decryption Process

1. Place the encrypted stream of numbers that represents an encrypted message into a matrix.
2. Multiply by the decoding matrix. The decoding matrix is the inverse of the encoding matrix.
3. Convert the matrix into a stream of numbers.
4. Conver the numbers into the text of the original message.

$$X = \begin{bmatrix} 67 & -21 \\ 16 & -8 \\ 51 & 27 \\ 52 & -26 \end{bmatrix}$$

The receiver must calculate the inverse of the encryption matrix. This would be the decryption matrix or the decoding matrix.

$$B^{-1} = \begin{bmatrix} 0.3 & 0.2 \\ 0.1 & 0.4 \end{bmatrix}$$

The receiver then multiplies the encrypted data by the inverse of the encryption matrix. The result is the original unencrypted matrix.

$$A = X\,B^{-1} = \begin{bmatrix} 18 & 5 \\ 4 & 0 \\ 18 & 21 \\ 13 & 0 \end{bmatrix}$$

The receiver then takes the matrix and breaks it apart into values 18, 5, 4, 0, 18, 21, 13, 0 and converts each of those into a character according to the numbering scheme. 18=R, 5=E, 4=D, 0=space, 18=R, 21=U, 13=M, 0=space.

Trailing spaces will be discarded and the message is received as intended: "RED RUM"

# Diagonal Matrices

A square matrix in which all the entries off the main diagonal are zero is called a ***diagonal matrix***

$$\begin{bmatrix} 2 & 0 \\ 0 & -5 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 6 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8 \end{bmatrix}$$

A general $n \times n$ diagonal matrix $D$ can be written as

$$D = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_n \end{bmatrix}$$

A diagonal matrix is invertible if and only if all of its diagonal entries are nonzero; in this case the inverse of 1 is

$$D^{-1} = \begin{bmatrix} 1/d_1 & 0 & \cdots & 0 \\ 0 & 1/d_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1/d_n \end{bmatrix}$$

# Inverses and Powers of Diagonal Matrices

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}, \qquad A^5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -243 & 0 \\ 0 & 0 & 32 \end{bmatrix}, \qquad A^{-5} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{243} & 0 \\ 0 & 0 & \frac{1}{32} \end{bmatrix}$$

# Triangular Matrices

A square matrix in which all the entries above the main diagonal are zero is called ***lower triangular***, and a square matrix in which all the entries below the main diagonal are zero is called ***upper triangular***. A matrix that is either upper triangular or lower triangular is called ***triangular***.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{bmatrix}$$

A general 4×4 upper triangular matrix

$$\begin{bmatrix} a_{11} & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

A general 4×4 lower triangular matrix

(a) *The transpose of a lower triangular matrix is upper triangular, and the transpose of an upper triangular matrix is lower triangular.*

(b) *The product of lower triangular matrices is lower triangular, and the product of upper triangular matrices is upper triangular.*

(c) *A triangular matrix is invertible if and only if its diagonal entries are all nonzero.*

(d) *The inverse of an invertible lower triangular matrix is lower triangular, and the inverse of an invertible upper triangular matrix is upper triangular.*

# Symmetric Matrices

The following matrices are symmetric, since each is equal to its own transpose

$$\begin{bmatrix} 7 & -3 \\ -3 & 5 \end{bmatrix}, \quad \begin{bmatrix} 1 & 4 & 5 \\ 4 & -3 & 0 \\ 5 & 0 & 7 \end{bmatrix}, \quad \begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 4 & 5 \\ 4 & -3 & 0 \\ 5 & 0 & 7 \end{bmatrix}$$

*If A and B are symmetric matrices with the same size, and if k is any scalar, then:*

(a) $A^T$ *is symmetric.*

(b) $A+B$ *and* $A-B$ *are symmetric.*

(c) $kA$ *is symmetric.*

*If A is an invertible symmetric matrix, then* $A^{-1}$ *is symmetric.*

# The product of a Matrix and Its transpose is symmetric

$$A = \begin{bmatrix} 1 & -2 & 4 \\ 3 & 0 & -5 \end{bmatrix}$$

$$A^T A = \begin{bmatrix} 1 & 3 \\ -2 & 0 \\ 4 & -5 \end{bmatrix} \begin{bmatrix} 1 & -2 & 4 \\ 3 & 0 & -5 \end{bmatrix} = \begin{bmatrix} 10 & -2 & -11 \\ -2 & 4 & -8 \\ -11 & -8 & 41 \end{bmatrix}$$

$$A A^T = \begin{bmatrix} 1 & -2 & 4 \\ 3 & 0 & -5 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ -2 & 0 \\ 4 & -5 \end{bmatrix} = \begin{bmatrix} 21 & -17 \\ -17 & 34 \end{bmatrix}$$

# Determinants

Determinant is a certain kind of function that associates a real number with a square matrix.

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

is invertible if $ad - bc \neq 0$.

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

# Minors and Cofactors

If $A$ is a square matrix, then the ***minor of entry*** $a_{ij}$ is denoted by $M_{ij}$ and is defined to be the determinant of the submatrix that remains after the $i$th row and $j$th column are deleted from $A$. The number $(-1)^{i+j}M_{ij}$ is denoted by $C_{ij}$ and is called the ***cofactor of entry*** $a_{ij}$.

$$A = \begin{bmatrix} 3 & 1 & -4 \\ 2 & 5 & 6 \\ 1 & 4 & 8 \end{bmatrix}$$

The minor of entry $a_{11}$ is

$$M_{11} = \begin{vmatrix} 3 & 1 & -4 \\ 2 & 5 & 6 \\ 1 & 4 & 8 \end{vmatrix} = \begin{vmatrix} 5 & 6 \\ 4 & 8 \end{vmatrix} = 16$$

The cofactor of $a_{11}$ is

$$C_{11} = (-1)^{1+1} M_{11} = M_{11} = 16$$

Similarly, the minor of entry $a_{32}$ is

$$M_{32} = \begin{vmatrix} 3 & 1 & -4 \\ 2 & 5 & 6 \\ 1 & 4 & 8 \end{vmatrix} = \begin{vmatrix} 3 & -4 \\ 2 & 6 \end{vmatrix} = 26$$

The cofactor of $a_{32}$ is

$$C_{32} = (-1)^{3+2} M_{32} = -M_{32} = -26$$

Note that the cofactor and the minor of an element $a_{ij}$ differ only in sign; that is, $C_{ij} = \pm M_{ij}$. A quick way to determine whether to use + or $-$ is to use the fact that the sign relating $C_{ij}$ and $M_{ij}$ is in the $i$th row and $j$ th column of the "checkerboard" array

$$\begin{bmatrix} + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{bmatrix}$$

For example, $C_{11} = M_{11}, C_{21} = -M_{21}, C_{12} = -M_{12}, C_{22} = M_{22}$, and so on.

# Cofactor Expansions

The definition of a $3 \times 3$ determinant in terms of minors and cofactors is

$$\begin{aligned} \det(A) &= a_{11}M_{11} + a_{12}(-M_{12}) + a_{13}M_{13} \\ &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \end{aligned} \tag{1}$$

Equation 1 shows that the determinant of $A$ can be computed by multiplying the entries in the first row of $A$ by their corresponding cofactors and adding the resulting products. More generally, we define the determinant of an $n \times n$ matrix to be

$$\det(A) = a_{11}C_{11} + a_{12}C_{12} + \cdots + a_{1n}C_{1n}$$

This method of evaluating $\det(A)$ is called ***cofactor expansion*** along the first row of $A$.

Let $A = \begin{bmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{bmatrix}$. Evaluate $\det(A)$ by cofactor expansion along the first row of $A$.

## Solution

From 1,

$$\det(A) = \begin{vmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{vmatrix} = 3\begin{vmatrix} -4 & 3 \\ 4 & -2 \end{vmatrix} - 1\begin{vmatrix} -2 & 3 \\ 5 & -2 \end{vmatrix} + 0\begin{vmatrix} -2 & -4 \\ 5 & 4 \end{vmatrix}$$

$$= 3(-4) - (1)(-11) + 0 = -1$$

If $A$ is a $3 \times 3$ matrix, then its determinant is

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

$$\begin{aligned} \det(A) &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \\ &= a_{11}C_{11} + a_{21}C_{21} + a_{31}C_{31} \\ &= a_{21}C_{21} + a_{22}C_{22} + a_{23}C_{23} \\ &= a_{12}C_{12} + a_{22}C_{22} + a_{32}C_{32} \\ &= a_{31}C_{31} + a_{32}C_{32} + a_{33}C_{33} \\ &= a_{13}C_{13} + a_{23}C_{23} + a_{33}C_{33} \end{aligned}$$

# Cofactor expansion along the first column

$$\text{Let } A = \begin{bmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{bmatrix}$$

$$\det(A) = \begin{vmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{vmatrix} = 3\begin{vmatrix} -4 & 3 \\ 4 & -2 \end{vmatrix} - (-2)\begin{vmatrix} 1 & 0 \\ 4 & -2 \end{vmatrix} + 5\begin{vmatrix} 1 & 0 \\ -4 & 3 \end{vmatrix}$$

$$= 3(-4) - (-2)(-2) + 5(3) = -1$$

# Smart Choice of Row or Column

If $A$ is the $4 \times 4$ matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 3 & 1 & 2 & 2 \\ 1 & 0 & -2 & 1 \\ 2 & 0 & 0 & 1 \end{bmatrix}$$

then to find $\det(A)$ it will be easiest to use cofactor expansion along the second column, since it has the most zeros:

$$\det(A) = 1 \cdot \begin{vmatrix} 1 & 0 & -1 \\ 1 & -2 & 1 \\ 2 & 0 & 1 \end{vmatrix}$$

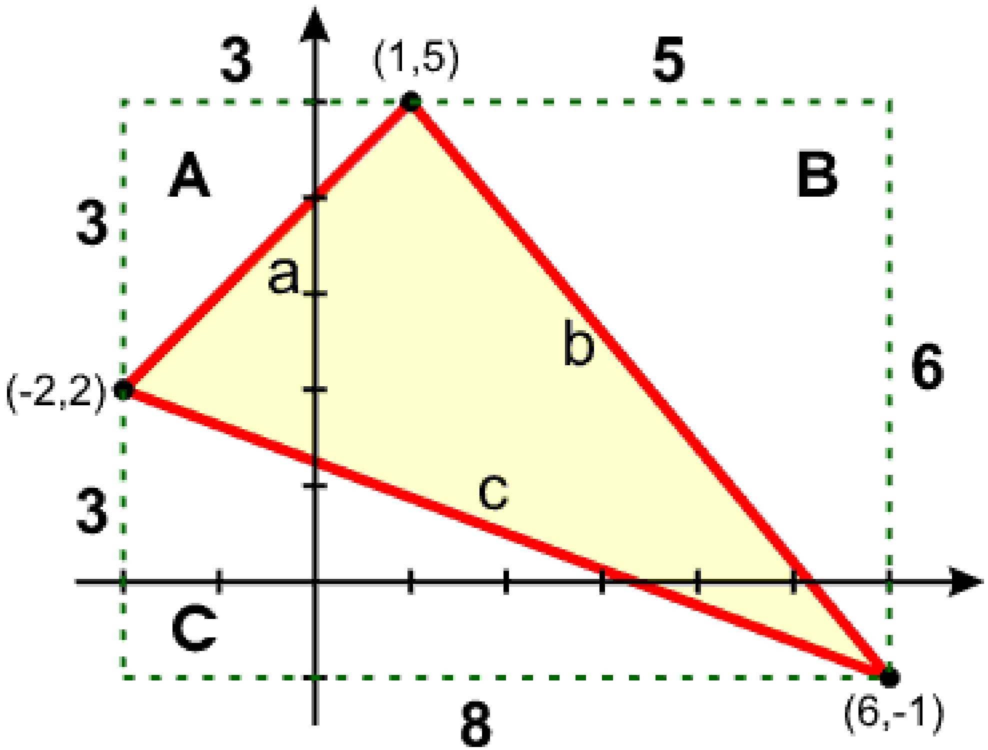
For the $3 \times 3$ determinant, it will be easiest to use cofactor expansion along its second column, since it has the most zeros:

$$\begin{aligned} \det(A) &= 1 \cdot -2 \cdot \begin{vmatrix} 1 & -1 \\ 2 & 1 \end{vmatrix} \\ &= -2(1+2) \\ &= -6 \end{aligned}$$

We would have found the same answer if we had used any other row or column.

# Some usage of Determinants

- Triangle Area Calculation



| | x | y | 1 |
|---|---|---|---|
| **point 1** | -2 | 2 | 1 |
| **point 2** | 1 | 5 | 1 |
| **point 3** | 6 | -1 | 1 |

**Formula for the area of a triangle using determinants**

$$\text{Area} = \pm 1/2 \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$$

Evaluate that determinant. I'll expand on column 1.

$$\begin{vmatrix} -2 & 2 & 1 \\ 1 & 5 & 1 \\ 6 & -1 & 1 \end{vmatrix} = +(-2) \begin{vmatrix} 5 & 1 \\ -1 & 1 \end{vmatrix} - 1 \begin{vmatrix} 2 & 1 \\ -1 & 1 \end{vmatrix} + 6 \begin{vmatrix} 2 & 1 \\ 5 & 1 \end{vmatrix}$$

$= -2 ( 5 + 1 ) - 1 ( 2 + 1 ) + 6 ( 2 - 5 ) = -2 ( 6 ) - 1 ( 3 ) + 6 ( -3 ) = -12 - 3 - 18 = -33.$

$| -33 | = 33$
33 / 2 = 16.5, which was the area.

**Formula for the area of a triangle using determinants**

$$\text{Area} = \pm 1/2 \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$$

# Adjoint of a Matrix

If $A$ is any $n \times n$ matrix and $C_{ij}$ is the cofactor of $a_{ij}$, then the matrix

$$\begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}$$

is called the ***matrix of cofactors from A***. The transpose of this matrix is called the ***adjoint of*** A and is denoted by $\mathrm{adj}(A)$.

Let

$$A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 0 \end{bmatrix}$$

The cofactors of $A$ are

$$\begin{array}{lll} C_{11} = 12 & C_{12} = 6 & C_{13} = -16 \\ C_{21} = 4 & C_{22} = 2 & C_{23} = 16 \\ C_{31} = 12 & C_{32} = -10 & C_{33} = 16 \end{array}$$

so the matrix of cofactors is

$$\begin{bmatrix} 12 & 6 & -16 \\ 4 & 2 & 16 \\ 12 & -10 & 16 \end{bmatrix}$$

and the adjoint of $A$ is

$$\operatorname{adj}(A) = \begin{bmatrix} 12 & 4 & 12 \\ 6 & 2 & -10 \\ -16 & 16 & 16 \end{bmatrix}$$

# Inverse of a Matrix using its adjoint

*If $A$ is an invertible matrix, then*

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

$$A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 0 \end{bmatrix}$$

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A) = \frac{1}{64} \begin{bmatrix} 12 & 4 & 12 \\ 6 & 2 & -10 \\ -16 & 16 & 16 \end{bmatrix} = \begin{bmatrix} \frac{12}{64} & \frac{4}{64} & \frac{12}{64} \\ \frac{6}{64} & \frac{2}{64} & -\frac{10}{64} \\ -\frac{16}{64} & \frac{16}{64} & \frac{16}{64} \end{bmatrix}$$

# Determinant of an Upper Triangular Matrix

$$\begin{vmatrix} 2 & 7 & -3 & 8 & 3 \\ 0 & -3 & 7 & 5 & 1 \\ 0 & 0 & 6 & 7 & 6 \\ 0 & 0 & 0 & 9 & 8 \\ 0 & 0 & 0 & 0 & 4 \end{vmatrix} = (2)(-3)(6)(9)(4) = -1296$$

# Cramer Rule

## Cramer's Rule

*If $A\mathbf{x} = \mathbf{b}$ is a system of $n$ linear equations in $n$ unknowns such that $\det(A) \neq 0$, then the system has a unique solution. This solution is*

$$x_1 = \frac{\det(A_1)}{\det(A)}, \qquad x_2 = \frac{\det(A_2)}{\det(A)}, \dots, \qquad x_n = \frac{\det(A_n)}{\det(A)}$$

where $A_j$ is the matrix obtained by replacing the entries in the $j$th column of $A$ by the entries in the matrix

$$\mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Use Cramer's rule to solve

$$\begin{aligned} x_1 + \quad\quad + 2x_3 &= 6 \\ -3x_1 + 4x_2 + 6x_3 &= 30 \\ -x_1 - 2x_2 + 3x_3 &= 8 \end{aligned}$$

## Solution

$$A = \begin{bmatrix} 1 & 0 & 2 \\ -3 & 4 & 6 \\ -1 & -2 & 3 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 6 & 0 & 2 \\ 30 & 4 & 6 \\ 8 & -2 & 3 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 1 & 6 & 2 \\ -3 & 30 & 6 \\ -1 & 8 & 3 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 0 & 6 \\ -3 & 4 & 30 \\ -1 & -2 & 8 \end{bmatrix}$$

Therefore,

$$x_1 = \frac{\det(A_1)}{\det(A)} = \frac{-40}{44} = \frac{-10}{11}, \quad x_2 = \frac{\det(A_2)}{\det(A)} = \frac{72}{44} = \frac{18}{11},$$

$$x_3 = \frac{\det(A_3)}{\det(A)} = \frac{152}{44} = \frac{38}{11}$$