Cryptography And Cryptanalysis

Ph. D. Course/ 2019-2020

Introduced By

Dr. Faez Hassan Ali

Lecture One-3

Mathematical Basic Concepts

Probability Theory

Definition An **experiment** is a procedure that yields one of a given set of outcomes. The individual possible outcomes are called **simple events**. The set of all possible outcomes is called the **sample space**.

we only considers discrete sample spaces; that is, sample spaces with only finitely many possible outcomes. Let the simple events of a sample space S be labeled $s_1, s_2, \ldots, s_n$.

Definition A **probability distribution** P on S is a sequence of numbers $p_1, p_2, \ldots, p_n$ that are all non-negative and sum to 1. The number p_i is interpreted as the probability of s_i being the outcome of the experiment.

Definition An **event** E is a subset of the sample space S. The probability that event E occurs, denoted P(E), is the sum of the probabilities p_i of all simple events s_i which belong to E. If $s_i \in S$, $P(\{s_i\})$ is simply denoted by $P(s_i)$.

Definition If E is an event, the **complementary event** is the set of simple events not belonging to E, denoted $\bar{E}$.

Fact Let $E \subseteq S$ be an event.

- $0 \leq P(E) \leq 1$. Furthermore, $P(S) = 1$ and $P(\varphi) = 0$. (φ is the empty set).
- $P(\bar{E}) = 1 - P(E)$.

If the outcomes in S are equally likely, then $P(E) = |E|/|S|$.

Definition Two events E_1 and E_2 are called mutually exclusive if $P(E_1 \cap E_2)=0$. That is, the occurrence of one of the two events excludes the possibility that the other occurs.

Fact Let E_1 and E_2 be two events:

- If $E_1 \subseteq E_2$, then $P(E_1) \leq P(E_2)$.
- $P(E_1 \cup E_2)+P(E_1 \cap E_2)=P(E_1)+P(E_2)$. Hence, if E_1 and E_2 are mutually exclusive, then $P(E_1 \cup E_2)=P(E_1) + P(E_2)$.

Linear Equations Systems and Matrices

Linear Equations

Let F be field, let $a_1,a_2,\dots,a_n,b \in F$ and $x_1,x_2,\dots,x_n$ be variables (unknowns), then the combination equation: $a_1x_1+a_2x_2+\dots+a_nx_n=b$

called **Linear Equation**, $a_1,a_2,\dots,a_n$ are **coefficients** and b be the **absolute value**.

A collection of linear equations is:

$$a_{11}x_1+a_{12}x_2+\dots+a_{1n}x_n=b_1$$

$$a_{21}x_1+a_{22}x_2+\dots+a_{2n}x_n=b_2$$

$$\vdots$$

$$a_{m1}x_1+a_{m2}x_2+\dots+a_{mn}x_n=b_m$$

called **m-system of linear equations** with n variables.

If ($b_1=b_2=\dots=b_m=0$), then the system called **Homogeneous Linear Equations**, otherwise its called **Non Homogeneous Linear Equations.**

The values $x_1, x_2, \dots, x_n$ which are satisfied the system of linear equations is called **solution**.

Example : For the following system:

$$2x_1+3x_2+8x_3+x_4= 6$$

$$x_1+x_2+3x_3-x_4= 2$$

$$3x_1-4x_2+8x_3-x_4=5$$

(-1,0,1,0) is a solution and (-3,6,-1,2) is another solution.

Linear Equations Systems and Matrices

Matrices

In example, the coefficients of the linear equations can be written as follows:

$$\begin{bmatrix} 2 & 3 & 8 & 1 \\ 1 & 1 & 3 & -1 \\ 3 & -4 & 8 & -1 \end{bmatrix}$$ This model called a ***Matrix***.

The matrix is rectangular arrangement with orthogonal rows and columns, it can be put in ( ) or [ ].

The general form of the matrix is:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$ The matrix A consists of m rows and n columns so it can be denoted by $(a_{ij})_{mxn}$,

Types of Matrices

- **Square matrix**: the matrix is called square matrix if m=n.
- **Zero matrix**: It's the matrix which all it elements are 0's, and it denoted by O.
- **Identity matrix**: its square matrix which all elements are 0's, accept its 1's on the main diagonal.
- **Transpose Matrix**: change the ever row of the matrix to column, and it denoted by A^t.
- **Triangular matrix**: the square matrix all elements under the main diagonal are 0's called **up-triangular matrix**, while its called **down-triangular matrix** which all elements above the main diagonal are 0's.
- **Diagonal matrix**: it's the matrix which all elements under and above the main diagonal are 0's.

Linear Equations Systems and Matrices

Operations on Matrices

Multiply by Scalar

Multiply the matrix by scalar done when all its elements are multiplied by the same scalar.

Example

If the scalar is 2 then: $2.\begin{bmatrix} 2 & 1 \\ -1 & 3 \\ 0 & -4 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ -2 & 6 \\ 0 & -8 \end{bmatrix}$

Addition of Matrices

We can add only the matrices from the same degree, this operation done when adding the corresponding elements of the two matrices.

$(a_{ij})_{mxn} + (b_{ij})_{mxn} = (a_{ij}+b_{ij})_{mxn}$

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

Matrices Multiplying

We can multiply two matrices if the number of columns of the first matrix equals the number of rows of the second matrix, then the degree of the result matrix is equal to row of the first matrix by the columns of the second matrix, the general form is:

$(a_{ij})_{mxk} \times (b_{ij})_{kxn} = \left(\sum_{t=1}^{k} a_{it} \cdot b_{tj} \right)_{mxn}$

Example

$\begin{bmatrix} 2 & 0 & 5 \\ -1 & 3 & -2 \end{bmatrix}_{2\times 3} * \begin{bmatrix} 0 & -1 \\ 1 & 0 \\ 2 & 3 \end{bmatrix}_{3\times 2} = \begin{bmatrix} 10 & 13 \\ -1 & -4 \end{bmatrix}_{2\times 2}$

Linear Equations Systems and Matrices

Determinants

It's a function with domain is the set of all square matrices with range is the field F. the value of this function is called the determinant of the matrix and its denoted by |A|. The calculation of the matrix determinant done with respect to its degree, which as follows:

1×1 matrix: if A=[a], then |A|=a.

2×2 matrix: if A= $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then |A|=a*d-c*b.

3×3 matrix: if A= $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, then:

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

Inverse of Matrices

The square matrix B will be called the inverse of the square matrix A if: $A \times B = B \times A = I$. And it's denoted by A^{-1}. There are many methods to find the inverse of the matrix like, adjacent matrix method, elementary matrix, Jordan method triangular method…, etc.

Theorem

Let A be square matrix, then A will be invertible matrix if and only if its determinant not equal zero.

Linear Equations Systems and Matrices

Numerical Solutions of the Linear Equations Systems

Let's have the following linear equations system:

$a_{11}x_1+a_{12}x_2+\dots+a_{1n}x_n=b_1$

$a_{21}x_1+a_{22}x_2+\dots+a_{2n}x_n=b_2$

$\vdots$

$a_{m1}x_1+a_{m2}x_2+\dots+a_{mn}x_n=b_m$

This system consists of m equations with n variables. If we use the matrix notation then the above system will be: AX = B s.t.

$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$ is the coefficient matrix,

$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ is the unknown (variables) matrix, and $B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$ is the absolute value matrix.

The augment matrix is the matrix A beside it the column B.

$[A|B] = \left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right]$

The solution of the linear equations systems means find the values of the unknowns $x_1,x_2,\dots,x_n$ which satisfy all equations of the system.

Definitions: The zero solution is the solution of the linear system if all the values of matrix X equal 0, s.t.

$x_1= x_2 = x_3 = \dots = x_n = 0$

Definitions: The square matrix A called singular if and only if $|A|=0$.

Theorem: Let A be square matrix of degree n, then the following relation are equivalent:

- The homogenous system AX = 0 has zero solution only.
- The system AX = B has unique solution for every different column B.
- The matrix A has inverse.

Linear Equations Systems and Matrices

Matrices Solving Methods

Cramer Rule

Theorem: If A is the coefficient matrix of linear equations system consists of n variables, and $|A| \neq 0$, then the solution is: $x_1 = D_1/D$, $x_2 = D_2/D$, … , $x_n = D_n/D$,
where $D=|A|$, and $D_i=|A_i|$, A_i is the matrix A when change the column B with column i, s.t. $1 \leq i \leq n$.

Example

$3x_1 - 2x_2 = 6$
$2x_1 + x_2 = 0.5$
AX = B
$A = \begin{bmatrix} 3 & -2 \\ 2 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 6 \\ 0.5 \end{bmatrix}$, $X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, $|A| = 7$ then $x_1 = \dfrac{\begin{bmatrix} 6 & -2 \\ 0.6 & 1 \end{bmatrix}}{7} = \dfrac{7}{7} = 1$, $x_2 = \dfrac{\begin{bmatrix} 3 & 6 \\ 2 & 0.5 \end{bmatrix}}{7} = \dfrac{-10.5}{7} = -1.5$

Inverse of Matrix Method

Since AX = B, then $X = A^{-1}B$. That if we can find the inverse of matrix A in one of the methods mentioned in previous subsection, then the multiplication of A^{-1} with B give the unknowns columns X.

Example: $\begin{bmatrix} -2 & 2 & -3 \\ 2 & 1 & -6 \\ -1 & -2 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \\ -5 \end{bmatrix}$, then $\begin{bmatrix} -2 & 2 & -3 \\ 2 & 1 & -6 \\ -1 & -2 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} -4/15 & 2/15 & -1/5 \\ 2/15 & -1/15 & -2/5 \\ -1/15 & -2/15 & -2/15 \end{bmatrix}$

$X = \begin{bmatrix} -4/15 & 2/15 & -1/5 \\ 2/15 & -1/15 & -2/5 \\ -1/15 & -2/15 & -2/15 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \\ -5 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}$

$x_1 = 1$, $x_2 = 2$ and $x_3 = -1$.

Linear Equations Systems and Matrices

Applications of Matrices in cryptography

Example : Let the coding system be #'A'=0, #'B'=1,…, #'Z'=25; Encrypt the plaintext Message "MATH"

Using the key Matrix $\mathrm{A} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$;

Solution: #'MATH'=(12,0,19,6); using the system B=AX.

$X_1 = \begin{bmatrix} 12 \\ 0 \end{bmatrix}$ and $X_2 = \begin{bmatrix} 19 \\ 6 \end{bmatrix}$, then the cipher text will be

$B_1 = \begin{bmatrix} 24 \\ 12 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 44 \\ 25 \end{bmatrix}$.

HW: if you have the cipher text $B_1 = \begin{bmatrix} 24 \\ 12 \end{bmatrix}$ and $B_2 = \begin{bmatrix} 44 \\ 25 \end{bmatrix}$.

Find the plaintext message using the key Matrix A?