Hill Cipher

Math 4175

§2.5.1. Hill Cipher

In this section we will learn another polyalphabetic cryptosystem called Hill Cipher invented by Lester S. Hill in 1929.

The idea is again to convert m plaintext characters to m cipher text characters at a time. But instead of using a key word of length m as in Vigenère Cipher, Hill Cipher uses a $m \times m$ matrix with entries from $\mathbb{Z}_{26}$.

In other words, in Hill Cipher, each key $k \in \mathcal{K}$ is a matrix of size $m \times m$ in $\mathbb{Z}_{26}$, for a fixed positive integer m.

For example, let us say we want to encrypt

`secure`

§2.5.1. Hill Cipher

Example: Let us assume that the key is:

$$K = \begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix}.$$

Solution: Here $m = 2$. We first break the plaintext into blocks of two, and encode each one:

s	e
18	4

c	u
2	20

r	e
17	4

§2.5.1. Hill Cipher

Next we multiply each of these blocks on the right by the key matrix and reduce to mod 26.

$$(18 \;\; 4)\begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix} = (18 \cdot 5 + 4 \cdot 1 \quad 18 \cdot 4 + 4 \cdot 9) = (94 \;\; 108) = (16 \;\; 4)$$

Similarly

$$(2 \;\; 20)\begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix} = (30 \;\; 188) = (4 \;\; 6)$$

$$(17 \;\; 4)\begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix} = (89 \;\; 104) = (11 \;\; 0)$$

So we get $(16 \;\; 4 \;\; 4 \;\; 6 \;\; 11 \;\; 0)$ and hence the ciphered text is `QEEGLA`.

§2.5.1. Hill Cipher

More generally, if $\mathbf{x} = (x_1, x_2)$ is the plaintext element and $\mathbf{y} = (y_1, y_2)$ is the corresponding cipher text element, then

$$(x_1 \quad x_2)\begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix} = (5x_1 + 1x_2 \qquad 4x_1 + 9x_2) = (y_1 \quad y_2) \mod 26$$

So we have,

$$\begin{aligned} y_1 &= (5x_1 + 1x_2) \mod 26 \\ y_2 &= (4x_1 + 9x_2) \mod 26 \end{aligned}$$

For this reason, we say that the cipher text is obtained from a plaintext by means of a linear transformation.

§2.5.1. Hill Cipher

In order for Hill Cipher encryption makes sense, we need to make sure that the given key yields unique cipher text string **y** for any given plaintext string **x**.

Recall from previous linear algebra course: This is true only if the key, that is the preselected $m \times m$ matrix, is invertible.

Recall: A matrix K is called invertible if there exists another matrix L such that $KL = LK = I$, where I is the identity matrix. In this case, L is called the inverse of K and is written as K^{-1}.

As mentioned earlier, the encryption in the Hill Cipher is done by multiplying the plaintext by a key matrix K, and hence, the decryption multiplies the cipher text by the inverse of the key matrix K^{-1} in $\mathbb{Z}_{26}$.

§2.5.1. Hill Cipher

Now we are in a position to provide a precise mathematical definition of Hill Cipher:

> Hill Cipher is a cryptosystem with $\mathcal{P} = \mathcal{C} = \left(\mathbb{Z}_{26}\right)^m$ where m is a positive integer. The key space $\mathcal{K}$ is the set of all $m \times m$ invertible matrices over $\mathbb{Z}_{26}$. For a key $K \in \mathcal{K}$, we define
>
> $$e_K(\mathbf{x}) = \mathbf{x}K$$
>
> $$d_K(\mathbf{y}) = \mathbf{y}K^{-1}$$
>
> where all operations are performed in $\mathbb{Z}_{26}$.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

So we need to learn how to find the inverse matrix in $\mathbb{Z}_{26}$.

Method 1: Only for 2×2 matrices

Suppose that

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

Then K is invertible if and only if $\det(K) = ad - cb$ is invertible in $\mathbb{Z}_{26}$.

In that case,

$$K^{-1} = (\det K)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

For example, let $K = \begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix}$

Then $\det(K) = (5)(9) - (1)(4) = 41 \equiv 15 \mod 26$
which is invertible in $\mathbb{Z}_{26}$ with $15^{-1} = 7$.

Hence

$$K^{-1} = 7\begin{pmatrix} 9 & -4 \\ -1 & 5 \end{pmatrix} = \begin{pmatrix} 63 & -28 \\ -7 & 35 \end{pmatrix} = \begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix}$$

Check that above calculation is correct.

§2.5.2. Cryptanalysis of Hill Cipher

Example: Now suppose that we have a ciphertext

$$\texttt{SCETLNVIEDFRBA}$$

which was given using the key

$$K = \begin{pmatrix} 5 & 4 \\ 1 & 9 \end{pmatrix}.$$

How do we decrypt?

Recall that $K^{-1} = \begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix}$.

§2.5.2. Cryptanalysis of Hill Cipher

So multiply block by block on the cipher text by K^{-1} to get the plaintext.

Note that

S	C	E	T	L	N	V	I	E	D	F	R	B	A
18	2	4	19	11	13	21	8	4	3	5	17	1	0

§2.5.2. Cryptanalysis of Hill Cipher

$$(18 \quad 2)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (2 \quad 8)$$

$$(4 \quad 19)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (15 \quad 7)$$

$$(11 \quad 13)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (4 \quad 17)$$

$$(21 \quad 8)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (19 \quad 4)$$

$$(4\ 3)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (23 \quad 19)$$

$$(5 \quad 17)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (14 \quad 13)$$

$$(1 \quad 0)\begin{pmatrix} 11 & 24 \\ 19 & 9 \end{pmatrix} = (11 \quad 24)$$

§2.5.2. Cryptanalysis of Hill Cipher

2	8	15	7	4	17	19	4	23	19	14	13	11	24
c	i	p	h	e	r	t	e	x	t	o	n	l	y

The plaintext is

`ciphertextonly`.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Method 2: Suppose that $K = (k_{ij})$ is an $n \times n$ matrix. Let K_{ij} be the matrix obtained from K by deleting the ith row and the jth column.

The determinant of K, denoted $\det(K)$, is the value k_{11} if $n = 1$.

If $n > 1$, then $\det(K)$ is computed recursively from the formula

$$\det(K) = \sum_{j=1}^{n} (-1)^{i+j} k_{ij} \det(K_{ij}),$$

where i is any fixed integer between 1 and n.

Remember that we apply the arithmetic rules given on $\mathbb{Z}_{26}$. The basic fact we need is that a square matrix is invertible mod 26 if and only if its determinant is invertible in $\mathbb{Z}_{26}$, or other words, $\det(K)$ and 26 are relatively prime, that is, $\gcd(\det(K), 26) = 1$.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

We now give an explicit formula for the inverse of a matrix K.

Define a matrix K^* to have as its (i, j)-entry the value $(-1)^{i+j}\det(K_{ji})$. (Recall that K_{ji} is obtained from K by deleting the jth row and the ith column.) K^* is called the adjoint matrix of K.

We state the following theorem without proof.

Theorem. Suppose K is an $m \times m$ matrix over $\mathbb{Z}_n$ such that $\det K$ is invertible in $\mathbb{Z}_n$. Then

$$K^{-1} = (\det K)^{-1} K^*,$$

where K^* is the adjoint matrix of K.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Remark: The above formula for K^{-1} is not very efficient to compute by pencil and paper, but is useful to write an algorithm to compute the inverse by using a software, particularly for a large m.

Example: Suppose we want to find the inverse of

$$K = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 4 & 9 \end{pmatrix}$$

where all the entries are in $\mathbb{Z}_{26}$.

Now $\det(K) = 3$ and $3^{-1} = 9$.

So,

$$K^{-1} = 9 \begin{pmatrix} 6 & -5 & 1 \\ -3 & 7 & -2 \\ 0 & -2 & 1 \end{pmatrix}.$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Hence,

$$K^{-1} = \begin{pmatrix} 54 & -45 & 9 \\ -27 & 63 & -18 \\ 0 & -18 & 9 \end{pmatrix} = \begin{pmatrix} 2 & 7 & 9 \\ 25 & 11 & 8 \\ 0 & 8 & 9 \end{pmatrix}.$$

Method 3: (Row Reduction Method) For $m > 2$, the preferred method of computing inverse matrices by hand would involve performing elementary row operations on the matrix K.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Row Reduction Method:

We need to find the inverse of

$$K = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 4 & 9 \end{pmatrix}$$

where all the entries are in $\mathbb{Z}_{26}$.

We will start by attaching the identity matrix at the end of the given matrix:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 1 & 0 \\ 2 & 4 & 9 & 0 & 0 & 1 \end{array}\right)$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

There are three row reduction operations or elementary row operations we can do:

1. Operation I: Reorder the rows
2. Operation II: Multiply a row by a non-zero constant number
3. Operation III: Add/subtract a multiple of one row to/from another, and replace one of the two rows with the result.

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Our goal is to do the row operations to change the first matrix to the identity matrix:

First work on the first column. Since already the $(1, 1)$ entry is 1, we proceed to make other entries 0.

Perform the row operation $R_2 - R_1$ (second row minus first row) to replace second row:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 2 & 4 & 9 & 0 & 0 & 1 \end{array}\right)$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Now perform $R_3 - 2R_1$ to replace third row:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 2 & 7 & -2 & 0 & 1 \end{array}\right)$$

Now work on the second column: Perform $R_1 - R_2$ to replace first row and $R_3 - 2R_2$ to replace third row.

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 3 & 0 & -2 & 1 \end{array}\right)$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Now work on third column: Multiply third row by the inverse of 3, which is 9:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 27 & 0 & -18 & 9 \end{array}\right)$$

By reducing to mod 26, we get:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 8 & 9 \end{array}\right)$$

§2.5.1. Inverse Matrix over $\mathbb{Z}_{26}$

Perform $R_1 + R_3$ to replace first row and $R_2 - 2R_3$ to replace second row:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 7 & 9 \\ 0 & 1 & 0 & -1 & -15 & -18 \\ 0 & 0 & 1 & 0 & 8 & 9 \end{array}\right)$$

Now

$$K^{-1} = \begin{pmatrix} 2 & 7 & 9 \\ -1 & -15 & -18 \\ 0 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 2 & 7 & 9 \\ 25 & 11 & 8 \\ 0 & 8 & 9 \end{pmatrix}$$

§2.5.2. Cryptanalysis of Hill Cipher

Decrypt the message:

TMDDOGGMENXDGSJWKL

with the key

$$K = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 4 & 9 \end{pmatrix}$$

T	M	D	D	O	G	G	M	E	N	X	D	G	S	J	W	K	L
19	12	3	3	14	6	6	12	4	13	23	3	6	18	9	22	10	11

§2.5.2. Cryptanalysis of Hill Cipher

$$\begin{pmatrix} 19 & 12 & 3 \\ 3 & 14 & 6 \\ 6 & 12 & 4 \\ 13 & 23 & 3 \\ 6 & 18 & 9 \\ 22 & 10 & 11 \end{pmatrix} \begin{pmatrix} 2 & 7 & 9 \\ 25 & 11 & 8 \\ 0 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 338 & 289 & 294 \\ 356 & 223 & 193 \\ 312 & 206 & 186 \\ 601 & 368 & 328 \\ 462 & 312 & 279 \\ 294 & 352 & 377 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 3 & 8 \\ 18 & 15 & 11 \\ 0 & 24 & 4 \\ 3 & 4 & 16 \\ 20 & 0 & 19 \\ 8 & 14 & 13 \end{pmatrix}$$

§2.5.2. Cryptanalysis of Hill Cipher

0	3	8	18	15	11	0	24	4	3	4	16	20	0	19	8	14	13
a	d	i	s	p	l	a	y	e	d	e	q	u	a	t	i	o	n

So the decrypted message is:

$$\text{a displayed equation}$$

§2.5.2. Cryptanalysis of Hill Cipher

The Hill Cipher can be difficult (but not impossible) to break with a cipher text-only attack, but it succumbs easily to a known plaintext attack.

Let us first assume that the opponent has determine the value of m being used. Suppose he has at least m different plaintext-cipher text pairs, say

$$\mathbf{x}_j = (x_{1j},\ x_{2j}, \cdots, x_{mj})$$

and

$$\mathbf{y}_j = (y_{1j},\ y_{2j}, \cdots, y_{mj})$$

for $1 \le j \le m$, such that $\mathbf{y}_j = e_K(\mathbf{x}_j)$, $1 \le j \le m$.

If we define two $m \times m$ matrices $X = (x_{ij})$ and $Y = (y_{ij})$, then we have the matrix equation

$$Y = XK,$$

where the $m \times m$ matrix K is the unknown key.

§2.5.2. Cryptanalysis of Hill Cipher

Example: Suppose the plaintext `friday` is encrypted using a Hill Cipher with $m = 2$, to give the cipher text `PQCFKU`.

This leads us to

5	17
15	16

8	3
2	5

0	24
10	20

From the first two plaintext-ciphertext pairs, we get the matrix equation

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K$$

§2.5.2. Cryptanalysis of Hill Cipher

Since the matrix $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ has determinant 9 in $\mathbb{Z}_{26}$, it is invertible.

Moreover

$$\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}$$

and so

$$K = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

This can be verified by using the third plaintext-ciphertext pair.

§2.5.2. Cryptanalysis of Hill Cipher

What would the opponent do if he does not know m?

- Assuming that m is not too big, he could simply try $m = 2, 3, \cdots$ until the key is found.

- If a guessed value of m is incorrect, then an $m \times m$ matrix found by using the algorithm described above will not agree with further plaintext-ciphertext pairs. In this way, the value of m can be determined if it is not known ahead of time.