Using Matrices for Cryptography

In the newspaper, usually on the comics page, there will be a puzzle that looks similar to this:

BRJDJ WT X BWUJ AHD PJYXDBODJ JQJV ZRJV GRJDJ'T VH EJDBXWV YSXEJ BH FH. [1]

Cryptograms are very common puzzles, along with crossword puzzles. Each cipher letter represents a plaintext letter. The above puzzle is usually fairly easy to solve because the lengths of the words can easily be seen, along with any punctuation. But, what if the above message were written as follows:

BRJFJ WTXBW UJAHD PJYXD BODJJ QJVZR JVGRJ TVHEJ DBXWV YSXEJ BHFH

This would not be as easy to solve since there is no punctuation nor any indication as to how long the words are. The example above is called a monoalphabetic cipher message. It is so named because there is only one alphabet used to make the cipher message. In this paper, polyalphabetic cipher messages will be used to encrypt and decrypt a message. Polyalphabetic means more than one alphabet will be used. Moreover, matrices will be used to encrypt these messages.

Take a simple message, such as:

THE RAIN IN SPAIN FALLS MAINLY ON THE PLAIN.

The following matrix will be used to encrypt this message:

$$\begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} (mod\ 26)^2$$

The matrix is modulo 26, since there are 26 letters in the alphabet. So, taking each letter to represent a number, where A is 1, B is 2, etc., the matrix and the vector made up of the first two letters, T and H, will be multiplied together.

$$\begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 0 \end{pmatrix} (mod\ 26)$$

The T and the H in the plaintext is encrypted to be D and Z in the ciphertext (since Z, the 26th letter, is congruent to 0 modulo 26). Following in similar fashion, the entire message would be encrypted to read:

DZO WJGW TI JQHGM YDJXP EJGXDX UR VFL JJGTP

Notice that the two times the plaintext "THE" appears, it's a different cipher: DZO the first time and VFL the second time. If this were put in groups of five, it would be even harder to discern:

DZOWJ GWTIJ QHGMY DJXPE JGXDX URVFL JJGTP

In order to decrypt this message, the corresponding inverse matrix would need to be used:

$$\begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix}$$ [3]

Multiplying this matrix by the vector based on the first two letters of the ciphertext will give back the original letters:

[1] Patience Rayn's Decodaquote(R) March 3, 2000
[2] Sinkov, pg. 115
[3] Ibid. pg. 118

$$\begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 8 \end{pmatrix} (mod\ 26)$$

The question is: Will there always be an inverse to any matrix that is chosen modulo 26? The answer is no. There are 14 numbers that do not have inverses modulo 26. Any number that is not relatively prime, that is its greatest common divisor is greater than 1, does not have an inverse modulo 26. The same goes for matrices. In the above example, 18 was in the inverse of the original matrix (gcd(18,26)=2), but that matrix still has an inverse. It needs to be shown that the matrices that are being dealt with have inverses. Consider this linear transformation T_a:

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1f} + a_1 \\ \vdots \quad & \quad \vdots \quad \quad \vdots \quad \quad \vdots \\ y_f &= a_{f1}x_1 + a_{f2}x_2 + \cdots + a_{ff} + a_1 \end{aligned}$$

where f is any positive integer, and x_i, y_i, a_{ij}, a_i are matrices in $\Re^n$ within modulo 26. The rectangular array of $f \times (f+1)$ matrices,

$$P_a = \begin{bmatrix} a_{11} & \cdots & a_{1f} & a_1 \\ \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdots & \cdot & \cdot \\ a_{f1} & \cdots & a_{ff} & a_f \end{bmatrix},$$

will be called the *schedule* of T_a and will be designated as $P_a = [(a_{ij}), a_i]$. The square array of f^2 matrices $M_a = (a_{ij})$ will be called the *basis* of T_a. J will be denoted as the set of all transformations which can be obtained in this way, for a fixed integer f, from the range $\Re^n$ within modulo 26.

Now, let T_a with the schedule $P_a = [(a_{ij}), a_i]$ be a transformation belonging to the set J. Concentrating on the *basis* $M_a = [a_{ij}]$ of T_a, the parentheses are removed from all the f^2 matrices in the square array $[a_{ij}]$. The result is a square matrix G_a in modulo 26 of the order $g = fn$. The matrix G_a will be called the *frame matrix* of T_a. It is evident that G_a belongs to the range $\Re^g$ in modulo 26.

Lemma. *Let T_a, T_b, T_c be transformations in J, and let their frame matrices be G_a, G_b, G_c respectively. Then $G_c = G_a G_b$ if $T_c = T_a T_b$. In other words, the frame matrix of a product of transformations is the corresponding product of the frame matrices of the transformations.*

Consider the set H of all transformations in the set J which have *regular* frame matrices. H is then the set of *regular transformation* in J. H contains the identical transformation, defined by the schedule $Q = [(a_{ij}), a_i]$ in which $a_{ij} = 1_n (i = j), a_{ij} = 0_n (i \neq j), a_i = 0_n$ ($\forall$ index i). Using this fact, the following theorem can be proved:

Theorem. *If T_a is any transformation in H, $\exists$! transformation $T_b \ni$ the schedule of the product $T_a T_b = Q$, and $Q = T_a T_b$.*

This theorem asserts that (1) any *regular* transformation T in J has a unique inverse T^{-1}, and (2) T^{-1} is regular and has T for its inverse.

Proof : Suppose, first, that T_a is any homogeneous transformation in H. The frame matrix, G_a of T_a is regular, and has a unique reciprocal G_a^{-1} in the range $\Re^g$, i.e.

$$G^{-1} = \begin{pmatrix} \frac{G_{11}}{\rho} & \cdots & \frac{G_{n1}}{\rho} \\ \vdots & \ddots & \vdots \\ \frac{G_{1n}}{\rho} & \cdots & \frac{G_{nn}}{\rho} \end{pmatrix} = \frac{1}{\rho} \begin{pmatrix} G_{11} & \cdots & G_{n1} \\ \vdots & \ddots & \vdots \\ G_{1n} & \cdots & G_{nn} \end{pmatrix},$$

where G_{ij} is the cofactor of g_{ij} in the determinant of G, and ρ is the determinant of G modulo 26. Hence, the homogeneous transformation T_b of J which has the frame matrix G_a^{-1} is regular and lies in H. By the lemma stated above, T_b is manifestly a unique inverse to T_a in the set H.

Now, let T_a be any transformation in H. Let $y_i = z_i + a_i (i = 1, 2, \cdots, f)$, these sums being formed in the range $\Re^n$ of matrices. Substituting in the equations of T_a, the equations of a transformation T_c in H are obtained – a transformation converting the sequence $x_1, x2, \cdots, x_n$ into the sequence $z_1, z_2, \cdots, z_n$. Since T_c is also homogeneous, it has a unique inverse T_c^{-1}. Replacing z_i in the equations of T_c^{-1} by $y_i - a_i$, and simplifying (by operations in the range $\Re^n$) the equations of a transformation T_a^{-1} are determined, which is the unique inverse of T_a in H.[4]

Now, consider this cipher message:

```
WXAFR KORNK OOUHM SHINY KJUDO UNNKX RYUAM AWHLP WVRZK GRGYA QGRGA KKDSW FALXH WBTIW

XAKCQ VSGON GGSIJ QOEHU QQMIV OHHKY DIMSW BEEBE V
```

How would one go about decrypting this message, without any prior knowledge of what kind of method was used? Some tools will be needed in order to solve this cipher message. It is known that the 26 letters of the alphabet do not occur with equal frequency. Thus, the probabilities $p_A, p_B, \cdots, p_Z$ are not equal. All have positive values between 0 and 1, and their sum is 1:

$$\sum_{i=A}^{i=Z} p_i = 1.$$

The amount by which p_A differs from the average probability, $\frac{1}{26}$, is $p_A - \frac{1}{26}$. This is similar for each letter. The sum of these deviations cannot be used to determine the *measure of roughness* of the cipher message because the sum is 0, as shown below:

$$\sum_{i=A}^{i=Z} \Big(p_i - \frac{1}{26}\Big) = \sum_{i=A}^{i=Z} p_i - \sum_{i=A}^{i=Z} \frac{1}{26} = 1 - 26\frac{1}{26} = 0.$$

The way to get around this is to square the *measure of roughness*, or M.R. for short:[5]

$$\begin{aligned}
M.R. &= \sum_{i=A}^{i=Z} \Big(p_i - \frac{1}{26}\Big)^2 \\
&= \sum_{i=A}^{i=Z} \Big[p_i^2 - 2p_i\Big(\frac{1}{26}\Big) + \Big(\frac{1}{26}\Big)^2\Big] \\
&= \sum_{i=A}^{i=Z} p_i^2 - \sum_{i=A}^{i=Z} 2p_i\Big(\frac{1}{26}\Big) + \sum_{i=A}^{i=Z}\Big(\frac{1}{26}^2\Big) \\
&= \sum_{i=A}^{i=Z} p_i^2 - 2\Big(\frac{1}{26}\Big)\sum_{i=A}^{i=Z} p_i + 26\Big(\frac{1}{26}\Big)^2 \\
&= \sum_{i=A}^{i=Z} p_i^2 - 2\Big(\frac{1}{26}\Big) + \frac{1}{26} \\
&= \sum_{i=A}^{i=Z} p_i^2 - \frac{1}{26}
\end{aligned}$$

However, the above equation is only good when the original message is known. There needs to be a way to approximate $\sum_A^Z p_i^2$. Using the probability that two letters chosen at random will be the same, a good

[4] Hill, pgs. 143–145

[5] Sinkov, pg. 65–66

approximation can be found. What needs to be done is to count the pairs of identical letters there are in the cipher message, and then divide by the total number of possible pairs.

Suppose there are x letters in the set. The number of pairs is determined as follows: for the first choice, the selection can be made from x letters. After which, $x-1$ letters remain. This makes a total of $x(x-1)$ possibilities. However, counting this way, each pair has been counted twice, since each pair can be received two different ways. Thus, the number of pairs of letters that can be chosen from a given set of x is $\frac{1}{2}x(x-1)$.

If the observed frequency of A in the cipher message is f_A, then the number of pairs of A's that can be formed from these f_A letters is $\frac{1}{2}f_A(f_A-1))$. It is the same for B, and so on. Thus, the total number of pairs, regardless of the identity of the letter, is the sum

$$\sum_{i=A}^{i=Z} \frac{f_i(f_i-1)}{2}.$$

If the total number of letters is N, then the total possible number of pairs of letters is $\frac{1}{2}N(N-1)$. This leads to the following equation, called the *index of coincidence,*or I.C. for short. [6] It is defined as follows:

$$I.C. = \frac{\sum_A^Z f_i(f_i-1)}{N(N-1)}$$

Using the I.C., we can determine the number of alphabets, m, used in a cipher message:

m	*I.C.*
1	.066
2	.052
5	.044
10	.041
large	.038

Taking the I.C. on the above cipher message, it's equal to a value of .040, which puts it at around 10 alphabets used for the cipher message. It's possible that this number is not accurate, since the message is not very long. It is fairly obvious that the message is polyalphabetic.

The next step is to list the repetitions found within the cipher message and their locations. This will give a better indication as to how many alphabets there could be.

Repetitions	Locations of first letter	Interval	Factors
WXA	1,70	69	3,23
GRG	46,52	6	2,3

The only common factor between the two repetitions is 3, so there's a good chance that there's three alphabets being used, most likely in a matrix form, since the I.C. was so low.

The focus will now be to try to discover the matrix that was used to encipher this message. The ciphertext WXA is a very interesting one because it occurs at the very beginning of the message. The most frequent digraph in the English language is TH, and the next most popular is HE.[7] So, it is a possibility that WXA might be THE. If so, all that would need to be done is to solve the following system of equations:

$$23a_{11} + 24a_{12} + a_{13} \equiv 20 \ (mod\ 26)$$
$$23a_{21} + 24a_{22} + a_{23} \equiv 8 \ (mod\ 26)$$
$$23a_{31} + 24a_{32} + a_{33} \equiv 5 \ (mod\ 26)$$

[6] Sinkov, pg. 68
[7] Ibid, pg. 134

Or, in matrix form:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} 23 \\ 24 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 8 \\ 5 \end{pmatrix} \ (mod\ 26)$$

This would not be an easy task with 3 equations and 9 unknowns. Concentrating on the first equation, we will plug in some numbers to see if we can find something that will work. It can be seen right away that 1, 1 and 1 would work for a_{11}, a_{12} and a_{13}. Plugging those values into the cipher message, every third letter comes out looking like this:

```
WXAFR  KORNK  OOUHM  SHINY  KJUDO  UNNKX  RYUAM  AWHLP  WVRZK  GRGYA  QGRGA
thei    v  o    p    j  x    i  x    w    l  o    q  i    c    f  q    f  w
KKDSW  FALXH  WBTIW  XAKCQ  VSGON  GGSIJ  QOEHU  QQMIV  OHHKY  DIMSW  BEEBE  V
  t    s  c    e  t  hee    w  j    i  p    h    u  t    a  l    c    l  c
```

Although it starts out looking promising, there seem to be too many x's and q's using 1, 1 and 1. Since the q's need to be followed by u's in the English language, this also will not work since the letters that are near the q's appear not to make up any English words. Another set of three numbers needs to be found. After much trial and error, it can be found that $a_{11} = 13$, $a_{12} = 18$ and $a_{13} = 17$ also work. By plugging those values into the cipher message, every third letter comes out looking like this:

```
WXAFR  KORNK  OOUHM  SHINY  KJUDO  UNNKX  RYUAM  AWHLP  WVRZK  GRGYA  QGRGA
theq    c  r    n    x  m    d  e    h    a  d    w  h    e    n  h    n  h
KKDSW  FALXH  WBTIW  XAKCQ  VSGON  GGSIJ  QOEHU  QQMIV  OHHKY  DIMSW  BEEBE  V
  n    n  o    s  t  her    s  t    n  o    t    t  n    s  d    r    s  v
```

This text looks a lot more promising. There are still q's and x's in the message, but there are less of them, and they're more evenly spaced. Let's see what can be done about the second row (a_{21}, a_{22} and a_{23}). By examining the text, a "u" must follow the q, and also looking at the "ther", maybe an "e" would follow that. Thus, we get the following system of equations:

$$\begin{aligned} 23a_{21} + 24a_{22} + a_{23} &\equiv 8 \ (mod\ 26) \\ 6a_{21} + 18a_{22} + 11a_{23} &\equiv 21 \ (mod\ 26) \\ 11a_{21} + 3a_{22} + 17a_{23} &\equiv 5 \ (mod\ 26) \end{aligned}$$

Solving this system gives the values $a_{21} = 19$, $a_{22} = 11$ and $a_{23} = 9$. Putting these values into the message, we can find the second letters out of each group of three:

```
WXAFR  KORNK  OOUHM  SHINY  KJUDO  UNNKX  RYUAM  AWHLP  WVRZK  GRGYA  QGRGA
thequ   ck r  o nf   xj mp   do e  r he   az do   wi h  a ey   nd ho   nd h
KKDSW  FALXH  WBTIW  XAKCQ  VSGON  GGSIJ  QOEHU  QQMIV  OHHKY  DIMSW  BEEBE  V
e no   ny ow   sa t  here   sn th   ng o  r th   tc nb   sa d  b rm   sh ve
```

The message is really starting to take form. By inspection, it looks like the text 'n th ng' could be the word "nothing". Also "qu ck" could be "quack" or "quick", and "wi h" could be "with" or "wish". So, there are a few different sets of equations that could be solved:

$$\begin{aligned} 6a_{31} + 18a_{32} + 11a_{33} &\equiv 1 \ (mod\ 26) \\ 22a_{31} + 19a_{32} + 7a_{33} &\equiv 15 \ (mod\ 26) \ (1) \\ 15a_{31} + 14a_{32} + 7a_{33} &\equiv 9 \ (mod\ 26) \end{aligned} \quad \text{or} \quad \begin{aligned} 6a_{31} + 18a_{32} + 11a_{33} &\equiv 9 \ (mod\ 26) \\ 22a_{31} + 19a_{32} + 7a_{33} &\equiv 15 \ (mod\ 26) \ (2) \\ 15a_{31} + 14a_{32} + 7a_{33} &\equiv 9 \ (mod\ 26) \end{aligned}$$

(using "quack" vs. "quick")

$$\begin{aligned} 23a_{31} + 8a_{32} + 12a_{33} &\equiv 20 \ (mod\ 26) \\ 22a_{31} + 19a_{32} + 7a_{33} &\equiv 15 \ (mod\ 26) \ (3) \\ 15a_{31} + 14a_{32} + 7a_{33} &\equiv 9 \ (mod\ 26) \end{aligned} \quad \text{or} \quad \begin{aligned} 23a_{31} + 8a_{32} + 12a_{33} &\equiv 19 \ (mod\ 26) \\ 22a_{31} + 19a_{32} + 7a_{33} &\equiv 15 \ (mod\ 26) \ (4) \\ 15a_{31} + 14a_{32} + 7a_{33} &\equiv 9 \ (mod\ 26) \end{aligned}$$

(using "with" vs. "wish")

It turns out that systems (2) and (3) have the same solutions: $a_{31} = 4$, $a_{32} = 6$ and $a_{33} = 3$. This gives us the complete decoded message:

```
THE QUICK BROWN FOX JUMPED OVER THE LAZY DOG, WITH A HEY AND A HO, AND A HEY NONNY
NO. WE SAY THERE IS NOTHING MORE THAT CAN BE SAID. BURMA SHAVE.
```

The message is not particularly deep. However, by using the inverse matrix that was found:

$$\begin{pmatrix} 13 & 18 & 17 \\ 19 & 11 & 9 \\ 4 & 6 & 3 \end{pmatrix}$$

the original matrix that was used to encrypt the message can be found:

$$\begin{pmatrix} 3 & 3 & 16 \\ 3 & 19 & 4 \\ 16 & 12 & 21 \end{pmatrix}$$

This is one way that matrices can be used for encrypting messages. The encryption can be made more secure by not using a direct substitution for the alphabet (i.e. A=1, B=2, etc.). Also, the size of the matrix can be increased to make decoding more difficult. The other problem is that when choosing matrices modulo 26, one has to be careful about which matrix to choose, since all of the matrices do not have inverses modulo 26. It might be better to choose a different basis, such as modulo 29, which has no divisors except 1 and 29. That way, the 26 letters can be used with some punctuation characters. All in all, matrices are very useful for encoding messages.

Bibliography

Sinkov, Abraham. *Elementary Cryptanalysis - A Mathematical Approach* New York: Random House, 1968.

Hill, Lester S. "Concerning Certain Linear Transformation Apparatus of Cryptograph." *American Mathematical Monthly* Volume 38, Issue 3 (Mar., 1931): 135-154.