MATH 314 Spring 2018 - Class Notes

2/8/2018

Scribe: Rachael Williams

Summary: Today in class we recapped attacking the Vigenere Cipher and how we can use CoCalc to aid in this. We then moved on to a more secure type of cipher, Block Ciphers. We specifically covered the Hill Cipher.

Recap: Attacking Vigenere Cipher:

- First you need to find the length of the key. In order to do this you will repeatedly shift the ciphertext one space to the left, and look for a spike in the number of coincidences. These spikes generally suggest that that is the length of the key.
- The next step is to break the ciphertext into substrings based on what you think the length of the key is and perform frequency analysis on these substrings.
- We know that in English `"e"` is generally the most frequently used letter, so we will look for the letter that occurs most frequently and guess that `"e"` maps to that letter. Four letters before that is the letter "a" so we can expect a larger number there as well since `"a"` is also frequently occurring in the English language.
- We then use this information to determine the shift and map the each letter from the ciphertext to the letters in the plaintext.
- For a full example of how to use CoCalc to attack the Vigenere Cipher, see the Vigenere Example document in the Handout folder.

Notes: Block Ciphers

To create a more secure cipher we need to come up with a method where changing one letter of the plaintext changes multiple letters of the ciphertext. Block Ciphers break the messages into blocks, and then you encrypt entire blocks at a time.

Hill Cipher(1929)

- The Hill Cipher uses Linear Algebra and Matrices.
- Pick a block length m.
- Pick a key which is an $m \times m$ matrix with entries from $0 - 25$. (We use $\pmod{26}$ so it is convenient to use these numbers, otherwise we would reduce to these numbers anyway.)

- To encrypt a message we break the plaintext into blocks of m letters.
- Each block gets written as a vector $\vec{V}$ of m numbers.
- We will call the key matrix K.
- The output of a row times a column is a vector.

$$E(\vec{V}) \equiv \vec{V}K \pmod{26}$$

Examples:

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$
$$m = 2$$

Encrypt `"june"` using K and m (Breaking the text into blocks of 2).
The first block = `"ju"` $\to < 9, 20 >$.
The second block = `"ne"` $\to < 13, 4 >$.

$$\begin{aligned} E(< 9, 20 >) &= < 9, 20 > \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \\ &= < 9 \times 11 + 20 \times 3, 9 \times 8 + 20 \times 7 > \\ &= < 99 + 60, 72 + 140 > \\ &= < 159, 212 > \pmod{26} \\ &= < 3, 4 > \\ &= \texttt{"DE"} \end{aligned}$$

$$\begin{aligned} E(< 13, 4 >) &= < 13, 4 > \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} \\ &= < 13 \times 11 + 4 \times 3, 13 \times 8 + 4 \times 7 > \\ &= < 155, 132 > \pmod{26} \\ &= < 25, 2 > \\ &= \texttt{"ZC"} \end{aligned}$$

And we get `"june"` $\to$ `"DEZC"`.
Encrypt `"dune"` using the same key matrix. Only one letter of plaintext has changed.
The first block, `"du"` $\to < 3, 20 >$.
The second block, `"ne"` $\to < 13, 4 > \to$ `"ZC"`.

$$E(< 3, 20 >) = < 15, 8 > \to \texttt{"PI"}$$

And we get `"dune"` $\to$ `"PIZC"`.

Changing one letter of plaintext has changed more than one letter of the ciphertext.

Decrypting the Hill Cipher

Our encryption function is $E(\vec{V}) \equiv \vec{V}K \pmod{26}$.

We can say $\vec{V}K \equiv \vec{W} \pmod{26}$.

We need to find a matrix K^{-1} such that $KK^{-1} = I$ where I is the identity matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The rule that we will use is if $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

then $K^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

We will reduce the negative numbers modulo 26 in the matrix to make them positive.

Note: $(ad - bc)$ known as the determinant, must be invertible modulo 26.

In the Hill Cipher the key matrix must have a determinant that has no factors in common with the number 26.

$$D(\vec{W}) \equiv \vec{W}K^{-1} \pmod{26}$$

Examples:

If we know that $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$ then we need to find K^{-1}.

$$\begin{aligned} K^{-1} &= (77 - 24)^{-1} \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \\ &= (1)^{-1} \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \\ &= \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \end{aligned}$$

All of the numbers in the matrix are positive because we did $mod 26$ on the negative numbers.

Decrypt `"DEZC"` using K^{-1}.

The first block = `"DE"` $\to < 3, 4 >$.

The second block = `"ZC"` $\to < 25, 2 >$.

$$
\begin{aligned}
D(<3,4>) &=<3,4> \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \\
&=<3 \times 7 + 4 \times 23, 3 \times 18 + 4 \times 11> \\
&=<21 + 92, 54 + 44> \\
&=<113, 98> \pmod{26} \\
&=<9, 20> \\
&= \texttt{"ju"}
\end{aligned}
$$

$$
\begin{aligned}
E(<25,2>) &=<25,2> \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} \\
&=<25 \times 7 + 2 \times 23, 25 \times 18 + 2 \times 11> \\
&=<13, 4> \\
&= \texttt{"ne"}
\end{aligned}
$$

And we get `"DEZC"` = `"june"`.

Chosen Plaintext Attack

We pick `"ba"` $\rightarrow <1,0>$.

$$
\begin{aligned}
E(<1,0>) &=<1,0> \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\
&\equiv <a, b>
\end{aligned}
$$

Then we pick `"ab"` $\rightarrow <0,1>$.

$$
\begin{aligned}
E(<0,1>) &=<0,1> \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\
&\equiv <c, d>
\end{aligned}
$$

The result is the key matrix.