MATH 314 - Class Notes

2/7/2017

Scribe: David Winter

Summary: During this class, Dr. Cornwell discussed reviewed and expounded more upon the concepts surrounding affine ciphers. He also covered substitution ciphers and the Vigenere Cipher.

Notes:

Review of the Affine Cipher:

- Take a string of characters a_i that makes a list
- The string forms the vector $(a_1, a_2, a_3, ...) = x$
- a_i refers to a number $\pmod{26}$
- There are two numbers α, β that represent two numbers
- α is a number whose greatest common divisor with 26 is 1
- β is any number from 0 to 25
- The formula for encryption is $\alpha \times x + \beta$

Attacking the Affine Cipher:

- There are two unknowns for Eve: α and β
- Need two equations: In other words, we need to know how two of the letters are encrypted

Example:

$a \to 0$
$b \to 1$
If we know that 0 gets encrypted to 13 and 1 gets encrypted to 20, then this tells us that:
$\alpha \times 0 + \beta \equiv 13 \pmod{26}$
and $\alpha \times 1 + \beta \equiv 20 \pmod{26}$
So $\beta \equiv 13 \pmod{26}$ and since $\alpha + \beta \equiv 20 \pmod{26}$
$\alpha + 13 \equiv 20 \pmod{26}$
So $\alpha \equiv 7 \pmod{26}$

Once we know α, β, Then say "y" is in the ciphertext.
$\alpha \times x + \beta \equiv y \pmod{26}$
Using our knowledge of α and β
$x \equiv \alpha^{-}1\big(y - \beta\big) \pmod{26}$

In order for $\alpha^{-}1$ to exist, we need the greatest common divisor of α and 26 to $= 1$.

Example:

Encrypting the word `CAT` using the affine cipher of the form $\alpha \times x + \beta$ where $\alpha = 7$, $x =$ the number of the letter in the text and $\beta = 13$.

The word `CAT` translates to the numbers 2,0,19 from the table in the text.
Following the specified method of encryption:
$7 \times 2 + 13 = 27$
$27 \equiv 1 \pmod{26}$
$7 \times 0 + 13 = 13$
$13 \equiv 13 \pmod{26}$
$7 \times 19 + 13 = 146$
$146 \equiv 16 \pmod{26}$

So the numbers 1,13,16 encrypt to the letters `BNQ`

To Decrypt:
We need the key which is $\alpha = 7$ and $\beta = 13$
$\alpha^{-}1(y - \beta)$
$\alpha^{-}1$ is 15 because $7 \times 15 = 105 \equiv 1 \pmod{26}$
$15(1 - 13) = -180 \equiv 2 \pmod{26}$
$15(13 - 13) = 0 \equiv 0 \pmod{26}$
$15(16 - 13) = 45 \equiv -7 \pmod{26} \equiv 19 \pmod{26}$

So we now have the original word again: `CAT`

The affine cipher is not a very secure way of encrypting messages since it is subject to attack using statistical analysis.

Statistical Analysis Attack on the Affine Cipher:

- Statistically, E is the most common letter appearing in the English language
- So we can take a ciphertext and find the letter that appears most often, say Z
- Most likely (for a long text) that letter was what the letter E was encrypted to
- For example with the letter Z, $\alpha(4) + \beta \equiv 25 \pmod{26}$
- By looking at the stats of other letters, you can pick another commonly appearing letter and match it to another commonly appearing letter in English and get another equation. Then solve for α and β to continue the search for the key.

Substitution Cipher:

- Pick some ordering of letters that will be substituted by other letters in the alphabet or by another symbol
- Example: A $\rightarrow$ X, B $\rightarrow$ B, C $\rightarrow$ G, D $\rightarrow$ L, E $\rightarrow$ Z, F $\rightarrow$ H, ...

- There are 26! ways to do this
- This kind of cipher was used more commonly used before the advent of computers
- Brute force attack still would take quite a large amount of time to break the cipher because of the large number of possible combinations

Using Statistical Analysis to Attack the Substitution Cipher:

- Some examples of encryption in a substitution cipher
- E is always sent to Z.
- T is always sent to G.
- Substitution cipher becomes very weak under statistical analysis
- Newspaper cryptograms use substitution ciphers
- Monoalphabetic ciphers: each letter always gets encrypted to the same letter.

Vigenere Cipher (1553)

- First polyalphabetic cipher invented
- Idea: The key is a word like `CAT` which in numbers is 2,0,19
- Plaintext ((convert to numbers) then repeat the key "under" the plaintext adding in a vertical fashion

Example 1:

0 5 12 1 2 2... +
2 0 19 2 0 19...
After adding these numbers together we get the following numbers for the ciphertext all of which are reduced (mod 26):
2 5 5 3 2 21...

Example 2:

Encrypting the word `Wednesday` using the key `CAT`

22 4 3 13 4 18 3 0 24
+ 2 0 19 2 0 19 2 0 19

Adding these numbers together we get the following numbers for the ciphertext all of which are reduced (mod 26):
24 4 22 15 4 11 5 0 17
These numbers translate to the following ciphertext based on the table in the book: `yewpelfar`

Decrypting and Attacking the Vigenere Cipher:

- Knowing the key, we can decrypt by subtracting instead of adding

- Can't run statistical analysis on this cipher
- Appears to be unpredictable at first sight
- There is no restriction on the key word
- Eve has no idea how long the key is which is a big part of decryption for one attacking this cipher
- Before computers this cipher was called the unbreakable cipher

Two Steps in Attacking this Cipher:

1. Figure out the length of the key
2. Use statistical analysis to find the key

Steps for figuring out the length of the key

1. Write out the ciphertext
2. Shift the ciphertext one to the right, then align below the original
3. Count the number of coincidences
4. Take the already shifted ciphertext, shift one more to the right, find the number of coincidences with the original ciphertext
5. Continue step 4 until you find the greatest number of coincidences and the shift with the highest number of coincidences that is the smallest multiple represents the length of the key.

Fact: When you have shifted the length of the key (or a multiple of that), the number of coincidences significantly increase (about twice as common).

Example:

Original: `vvhqwvvrhmu...`
1st Shift: `vvhqwvvrhm...`
2nd Shift: `vvhqwvvrh...`

Based on the alignment of the letters and the points at which the same letters conincide a the same place in comparison with the original text, is how the number of conincidences are determined.

There are 2 coincidences between the original ciphertext and the 1st shift of the ciphertext.
There are no conincidences between the original ciphertext and the 2nd the shift of the ciphertext.

Once again, the shift with the highest number of coincidences that is the smallest multiple is the length of the key.