Student Name: Vanessa Tan
Student ID: 20225640

GCT561: Scientific Concepts and Thinking

Homework 3: Bayes' Theorem

---

1. Caesar's cipher

   (a) Generate all possible ciphers for ROMAMOPPVGNATE

X	Cipher
0	ROMAMOPPVGNATE
1	SPNBNPQQXHOBVF
2	TQOCOQRRYIPCXG
3	VRPDPRSSZKQDYH
4	XSQEQSTTALREZI
5	YTRFRTVVBMSFAK
6	ZVSGSVXXCNTGBL
7	AXTHTXYYDOVHCM
8	BYVIVYZZEPXIDN
9	CZXKXZAAFQYKEO
10	DAYLYABBGRZLFP
11	EBZMZBCCHSAMGQ
12	FCANACDDITBNHR
13	GDBOBDEEKVCOIS
14	HECPCEFFLXDPKT
15	IFDQDFGGMYEQLV
16	KGEREGHHNZFRMX
17	LHFSFHIIOAGSNY
18	MIGTGIKKPBHTOZ
19	NKHVHKLLQCIVPA
20	OLIXILMMRDKXQB
21	PMKYKMNNSELYRC
22	QNLZLNOOTFMZSD

(b) Give the monogram probability of all letters in the text

Letter	Probability
A	0.0674
B	0.0143
C	0.0347
D	0.0229
E	0.0992
F	0.0077
G	0.0097
H	0.0053
I	0.0957
K	0.0
L	0.0238
M	0.0435
N	0.0537
O	0.0482
P	0.0239
Q	0.0147
R	0.0565
S	0.0656
T	0.0706
V	0.0789
X	0.005
Y	0.0
Z	0.0
_	0.1586

(c) Give the monogram probability of all letters in the text (X = 5)

Letter	Probability
A	0.0706
B	0.0789
C	0.005
D	0.0
E	0.0
F	0.0674
G	0.0143
H	0.0347
I	0.0229
K	0.0992
L	0.0077
M	0.0097
N	0.0053
O	0.0957
P	0.0
Q	0.0238
R	0.0435
S	0.0537
T	0.0482
V	0.0239
X	0.0147
Y	0.0565
Z	0.0656
_	0.1586

In order to get X, we get the most frequent letter then shift it to the next least frequent letter. As an example, the most frequent letter in the enciphered text is E (probability = 0.0992) and the least frequent letter after E is K (probability = 0.0). Counting from E to K, we get X = 5.

(d) One-Time Pad: What are the probabilities for each letter in the alphabet in the enciphered text? Can you explain?

Using a one-time pad, the probability for each letter in the enciphered text is $\frac{1}{23}$. Since the text is enciphered independently using a different letter from the one-time pad, each letter has an equal probability of being selected for each enciphered letter.

Repeat the analysis for the Latin bi-grams.

As shown in the figures below, the probabilities for the original and the enciphered are the same since the bi-grams have an equal probability of being selected for each enciphered bi-gram.

In the original text (before enciphering), give the two conditional probabilities $P(x = "Q" \mid y = "V")$ and $P(y = "V" \mid x = "Q")$ for the bi-gram $xy = "QV"$, then show that the Bayes' theorem holds.

$$P(x = "Q" \mid y = "V") = 0.0003 \tag{1}$$

$$P(y = "V" \mid x = "Q") = 0.9977 \tag{2}$$

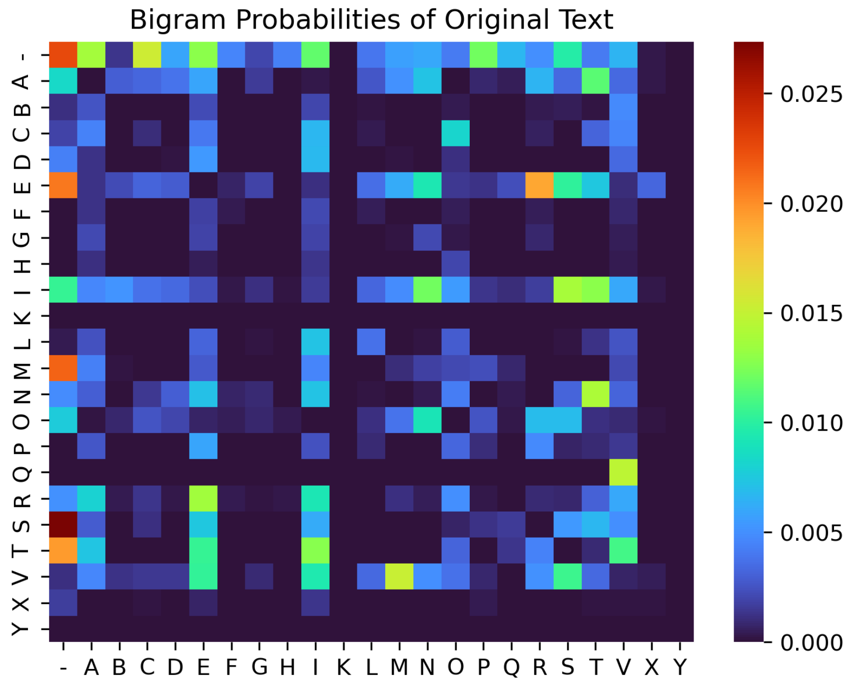

Figure 1: Bi-gram Probabilities of Original Text.

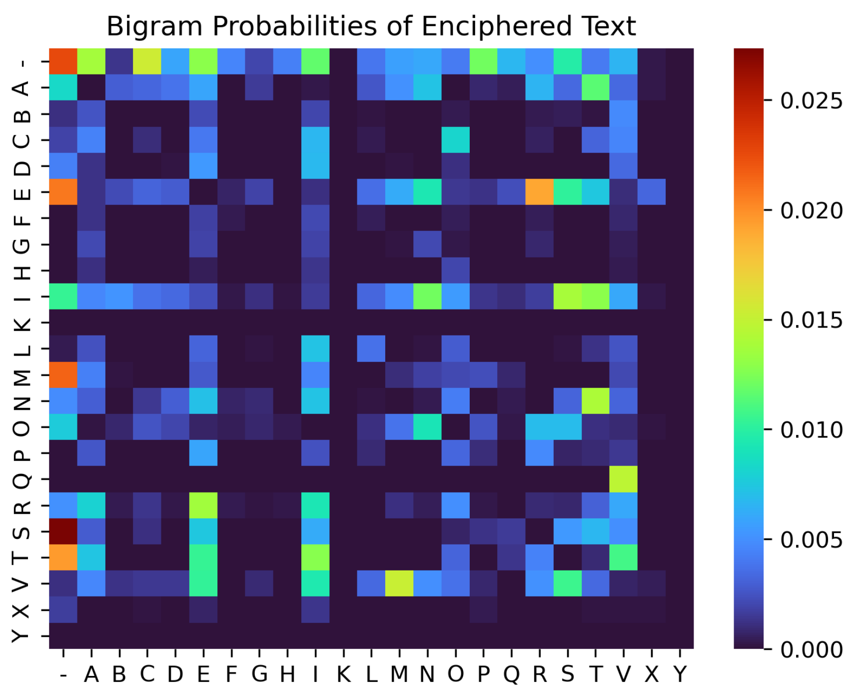

Figure 2: Bi-gram Probabilities of Enciphered Text.

$$P(Q|V) = \frac{P(Q|V)P(Q)}{P(V)} \tag{3}$$

$$P(Q|V)P(V) = P(Q|V)P(Q) \tag{4}$$

$$(0.0003)(0.0789) = (0.9977)(0.0147) \tag{5}$$

$$0 \approx 0.0147 \tag{6}$$

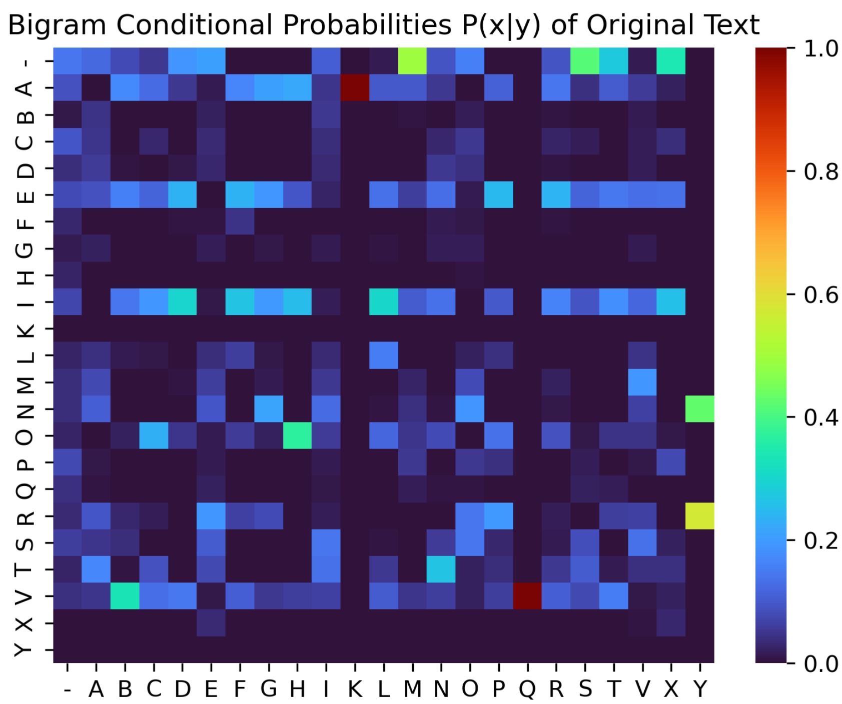

Figure 3: Conditional Probabilities $P(x \mid y)$.

2. Monty Hall

(a) Let us say you guessed it is door 1. What is the probability of winning the car if the door is opened now, and the game ends?

$$P(win) = \frac{1}{3} \tag{7}$$

(b) What are the prior probabilities of each door having the car behind it?

$$P(H_1) = P(H_2) = P(H_3) = \frac{1}{3} \tag{8}$$

(c) Calculate the conditional probabilities

$$P(D_2|H_1) = P(D_3|H_1) = \frac{1}{2} \tag{9}$$

$$P(D_2|H_2) = P(D_3|H_3) = 0 \tag{10}$$

$$P(D_2|H_3) = P(D_3|H_2) = 1 \tag{11}$$

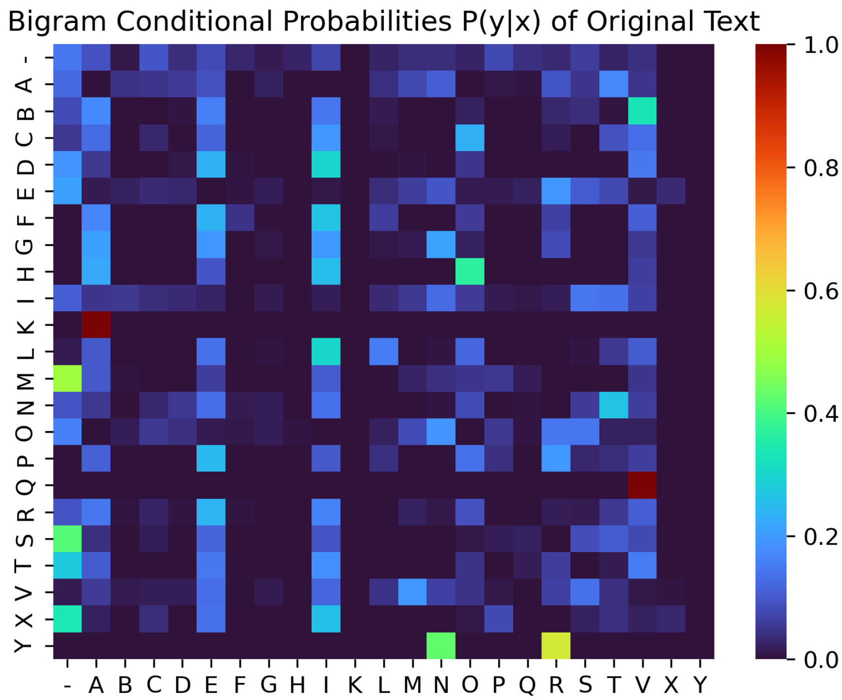

Figure 4: Conditional Probabilities $P(y \mid x)$.

(d) Calculate the posteriors using Bayes' Theorem

$$P(H_i|D_2) = \frac{P(D_2|H_i)P(H_i)}{P(D_2)} = \frac{P(D_2|H_i)P(H_i)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} \tag{12}$$

$$P(H_1|D_2) = \frac{P(D_2|H_1)P(H_1)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(\frac{1}{2})(\frac{1}{3})}{(\frac{1}{2})(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = \frac{\frac{1}{6}}{\frac{1}{2}} = \frac{1}{3} \tag{13}$$

$$P(H_2|D_2) = \frac{P(D_2|H_2)P(H_2)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(0)(\frac{1}{3})}{(\frac{1}{2})(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = 0 \tag{14}$$

$$P(H_3|D_2) = \frac{P(D_2|H_3)P(H_3)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(1)(\frac{1}{3})}{(\frac{1}{2})(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = \frac{\frac{1}{3}}{\frac{1}{2}} = \frac{2}{3} \tag{15}$$

(e) Should you change your mind to door 3 to maximize your chance of winning the car?
Yes, I should choose door 3 since $P(H_3|D_2) > P(H_1|D_2)$.

(f) 1,000,000 doors: After your choice of one door, what is the probability that the car is NOT behind the door of your choice?

$$P(notacar) = 1 - \frac{1}{1000000} = \frac{999999}{1000000} = 0.999999 \tag{16}$$

(g) What is the probability that the car is behind the last remaining door out of the 999,998 doors that you did not choose? What is the wise choice to maximize your chances of winning?

$$P(H_{doors}) = \frac{1}{1000000} = 0.000001 \tag{17}$$

$$P(D_{opened}|H_{chosen}) = \frac{1}{1000000} = 0.000001 \tag{18}$$

$$P(D_{opened}|H_{left}) = 1 - \frac{1}{1000000} = \frac{999999}{1000000} = 0.999999 \tag{19}$$

$$P(H_{chosen}|D_{opened}) = \frac{(0.000001)(0.000001)}{(0.000001)(0.000001) + (0.000001)(0.999999)} = 0.000001 \tag{20}$$

$$P(H_{left}|D_{opened}) = \frac{(0.999999)(0.000001)}{(0.000001)(0.000001) + (0.000001)(0.999999)} = 0.999999 \tag{21}$$

There is a 99.99% that the car is in door that I did not choose. It is a wise decision to switch doors to maximize the chances of winning.

(h) Repeat the calculations for the priors and the posteriors in the earthquake case, and see if you should change your mind to the unopened door 3 to maximize your chances. The earthquake created an equal chance of opening any of the doors.

$$P(H_1) = P(H_2) = P(H_3) = \frac{1}{3} \tag{22}$$

$$P(D_2|H_1) = 1 \tag{23}$$

$$P(D_2|H_2) = 0 \tag{24}$$

$$P(D_2|H_3) = 1 \tag{25}$$

$$P(H_i|D_2) = \frac{P(D_2|H_i)P(H_i)}{P(D_2)} = \frac{P(D_2|H_i)P(H_i)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} \tag{26}$$

$$P(H_1|D_2) = \frac{P(D_2|H_1)P(H_1)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(1)(\frac{1}{3})}{(1)(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = \frac{\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2} \tag{27}$$

$$P(H_2|D_2) = \frac{P(D_2|H_2)P(H_2)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(0)(\frac{1}{3})}{(1)(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = 0 \tag{28}$$

$$P(H_3|D_2) = \frac{P(D_2|H_3)P(H_3)}{\sum_{i=1}^{3} P(D_2|H_i)P(H_i)} = \frac{(1)(\frac{1}{3})}{(1)(\frac{1}{3}) + (0)(\frac{1}{3}) + (1)(\frac{1}{3})} = \frac{\frac{1}{3}}{\frac{2}{3}} = \frac{1}{2} \tag{29}$$

Choosing between door 1 or door 3 does not matter since $P(H_1|D_2) = P(H_3|D_2)$.