Problem 1

We stated without proof in lecture that square matrices formed by permutation of rows of an n-dimension identity matrix are unitary. And being unitary, the inverse of this class of matrix must equal to its transpose. Such matrices have all elements equal to either one or zero, and hence their transpose/inverse have all elements equal to either one or zero. We therefore concluded that such matrices are guaranteed invertible in Z_N.

Consider the case of such an n-dimensional matrix with elements in Z_26, formed by a permutation of an n-dimensional identity matrix. Suppose you wished to form its inverse using Cramer's rule, examining its determinant, and what we termed its "adjugate" (the matrix of its cofactors).

a) What are the possible values that for determinant of this class of matrix, in Z_26? (hint: you may take as given that any such determinant must be a value in Z_26_star. Are all values in Z_26_star achievable as determinant values for this class of matrix, or are the possible determinant values a smaller set?)

1. a. Consider a 2×2 matrix of this class.

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

Fairly simple to see that the only other permutation is:

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

Finding the two possible values of determinant in Z_{26}:

$\det M = 1$
$\det P = 25$ $\Longrightarrow$ generalize to $n \times n$ matrix

ex. 3×3 permutation matrix:

$$P = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Longrightarrow \det P = 25$$

The only two possible values for determinant are 1 and 25.

b) In terms of the transpose of the original matrix, what are the possible adjugate matrices for this class of matrix? Be sure to express your solution in terms of admissible elements in Z_26.

1.b. any given $n \times n$ permutation matrix of this type is unitary

According to Cramer's rule: $A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$

but $A^{-1} = A^T$

So: $\text{adj}(A) = \det(A) \cdot A^T$

c) Note that this question can be answered independently of (a) and (b). For n-dimensional matrix permutation matrices of the type considered here, in in Z_26, what is the cardinality of the associated key space, in terms of the parameter n? Does this result depend here on N=26 , and in general, would it depend on N?

1.c. This type of matrix is formed by permuting rows of an $n \times n$ identity matrix. Each row/column must have only a single 1, the rest of the entries will be 0.

Consider a 4×4 matrix.

For the first row, we have 4 possible ways to place this 1.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ & \vdots & & \end{bmatrix}$$

For the second row, we have 3 ways left

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ & \vdots & & \end{bmatrix} \quad \cdots \text{and so on.}$$

We can write $|K| = 4 \cdot 3 \cdot 2 \cdot 1 = 4!$ ↝ for $n \times n$: $n!$

Problem 2

Consider a Scrabble game. At the start of the game, 98 letter tiles are in a bag, with the frequency of occurrence of each tile type specified below (NOTE: for simplicity, data below ignores actual Scrabble practice of including blank, "wildcard" tiles).

a) Suppose you are the first player, and (contrary to normal Scrabble rules), you draw all seven of your letter tiles immediately, before any other player draws tiles. Evaluate the probability that all seven of your tiles are the letter "E."

b) As in (a), you draw your letter tiles from the bag, before any other players draw. Evaluate the probability that the first three of tiles you draw are the letters, "H," "E," and "N," allowing for any possible order of these three.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	2	2	4	12	2	3	2	9	1	1	4	2	6	8	2	1	6	4	6	4	2	2	1	2	1

2.a. $P(E) = \frac{12}{98}$, Note that we are drawing w/o replacement, so:

$P(\text{second E} \mid \text{first E}) = \frac{11}{97}$

$P(\text{third E} \mid \text{second E}) = \frac{10}{96}$ denominator decreases by 1 each time!

Finally: $P(\text{seven E}) = \prod_{i=0}^{N-1} \left(\frac{12-i}{98-i} \right)$

2.b. Total unordered possibilities of drawing 3 letters:

$${}_{98}C_3 = \binom{98}{3} = \frac{98!}{3!(98-3)!} = 152096$$

Total possibilities of drawing "H", "E", and "N":

$$\binom{2}{1}\binom{12}{1}\binom{6}{1} = 2 \cdot 12 \cdot 6 = 144$$

$$P(H,E,N) = \frac{144}{152096}$$

An alternative approach to 2b:

Consider the $3! = 6$ possible orders of drawing an "H", "E", and "N"

HEN, HNE, EHN, ENH, NEH, NHE $\Rightarrow$ order 1, order 2, ...

Then: $P(\text{order 1}) = \frac{2}{98} \cdot \frac{6}{97} \cdot \frac{12}{96} = \frac{144}{912576}$

$P(\text{order 2}) = \frac{2}{98} \cdot \frac{12}{97} \cdot \frac{6}{96} = \frac{144}{912576}$

$\vdots$

$P(\text{order 6}) = \frac{6}{98} \cdot \frac{2}{97} \cdot \frac{12}{96} = \frac{144}{912576}$

$$P(\text{order 1} \cup \text{order 2} \cup \cdots \cup \text{order 6}) = \frac{144}{912576} + \frac{144}{912576} + \cdots + \frac{144}{912576} = 6 \cdot \frac{144}{912576} = \frac{144}{152096}$$

A note on the Canvas solution:

Question 4 1 / 1 pts

You draw your letter tiles from the bag, before any other players draw. Evaluate the probability that the first three of tiles you draw are the letters, "H," "E," and "N," allowing for any possible order of these three.

Assume we are not replacing any of our drawn tiles back into our bag, and that we are sampling without replacement.

- $\frac{2 \cdot 12 \cdot 6}{98}$
- $\left(\frac{2 \cdot 12 \cdot 6}{98}\right)^3$
- $\frac{2 \cdot 12 \cdot 6}{98!}$
- Correct! $\frac{2 \cdot 12 \cdot 6}{98 \cdot 97 \cdot 96}$

The quantity in the denominator is taken as ${}_{98}P_3$, which takes the order into account.

$${}_{98}P_3 = \frac{98!}{(98-3)!} = \frac{98 \cdot 97 \cdot 96 \cdot 95 \cdot 94 \cdots}{95 \cdot 94 \cdot 93 \cdots} = 98 \cdot 97 \cdot 96 = 912576$$

The answer listed on Canvas is the probability of drawing "H", "E", and "N" one after the other.

Problem 3

Consider a limited alphabet of eight English language upper case characters {A, B, C, D, E, F, S, T}; associate the characters of this alphabet with Z_8. Further suppose that the expected frequency of occurrence of each of these characters is given by

P = [0.2195, 0.0488, 0.0488, 0.0976, 0.2927, 0.0488, 0.0976, 0.1462].

CAUTION IN POSSIBLE USE OF MATLAB: Note the choice here associates Z_8 to letters ***out of normal alphabetic order***. This undermines the usefulness of MATALB's built-in functions char() and double(), unless special care is used. You may still use MATLAB or other software tools to assist in this problem, but use care. This problem remains tractable for hand solution.

a) Consider the following ciphertext (in the alphabet above associated with Z_8):
'TCEFTCCDSACBSDSACF'
Assume this ciphertext was created using a shift cipher in Z_8. For each of the possible shifts in Z_8, compute the resulting frequency of occurrence of each of characters, and the associated empirical probability for each character. Your solution will be in the form of eight arrays, each composed of eight real values, in the same form as P above. In the notation of the Bach notes, you are computing $Q^{(k)}$, k=0, 1, … 7.

3. a. Alphabet {A, B, C, D, E, F, S, T} in Z_8

→ A=0, B=1, ⋯, T=7

Recall: shift cipher

$d_k(y) = y - k \bmod N$

Ciphertext: TCEFTCCDSACBSDSACF, n=18

k=0: $d_k(y) = y$ ⇒ TCEFTCCDSACBSDSACF

$Q^{(0)}$ = [0.1111 0.0556 0.2778 0.1111 0.0556 0.1111 0.1667 0.1111]

k=1: $d_k(y) = y-1$ ⇒ SBDESBBCFTBAFCFTBE

$Q^{(1)}$ = [0.0556 0.2778 0.1111 0.0556 0.1111 0.1667 0.1111 0.1111]

k=2: $d_k(y) = y-2$ ⇒ FACDFAABESATEBESAD

$Q^{(2)}$ = [0.2778 0.1111 0.0556 0.1111 0.1667 0.1111 0.1111 0.0556]

k=3: $d_k(y) = y-3$ ⇒ ETBCETTADFTSDADFTC

$Q^{(3)}$ = [0.1111 0.0556 0.1111 0.1667 0.1111 0.1111 0.0556 0.2778]

k=4: $d_k(y) = y-4$ ⇒ DSABDSSTCESFCTCESB

$Q^{(4)}$ = [0.0556 0.1111 0.1667 0.1111 0.1111 0.0556 0.2778 0.1111]

k=5: $d_k(y) = y-5$ ⇒ CFTXCFFSBDFEBSBDFA

$Q^{(5)}$ = [0.1111 0.1667 0.1111 0.1111 0.0556 0.2778 0.1111 0.0556]

k=6: $d_k(y) = y-6$ ⇒ BESTBEEFACEDAFACET

$Q^{(6)}$ = [0.1667 0.1111 0.1111 0.0556 0.2778 0.1111 0.0556 0.1111]

k=7: $d_k(y) = y-7$ ⇒ ADFSADDETBDCTETBDS

$Q^{(7)}$ = [0.1111 0.1111 0.0556 0.2778 0.1111 0.0556 0.1111 0.1667]

b) For each $Q^{(k)}$, compute its correlation with the given P.

You may assume that the plaintext message corresponds to a sentence composed of English language words, though admittedly with somewhat nonsensical meaning. Utilizing the decipher function corresponding to the maximum correlation shift, do you believe the correlation approach has correctly identified the plaintext message?

3.b. Here, we want the value of k that maximizes correlation w/ P given by $\sum_{i=0}^{N-1} p_i q_i^{(k)}$

From $Q^{(k)}$ we find correlation w.r.t. P by taking dot product:

k	Correlation
0	0.1057
1	0.1043
2	0.1531
3	0.1328
4	0.1152
5	0.0976
6	0.1612
7	0.1301

Problem 4

Use the Jordan formula provided in the Bach notes to evaluate the size of the keyspace for Hill ciphers based on 4x4 matrices, in Z_96. (i.e., compute the number of invertible 4x4 matrices in Z_96). As a special case of Hill ciphers based on 4x4 matrices, in Z_96, we have permutation matrices as a subset of the invertible 4x4 matrices in Z_96. What is the size of the keyspace for Transposition ciphers of block size 4, in Z_96? Note this is essentially a repetition of Problem 1(c). But it is useful here as a comparison of the relative security against key search attacks, for general Hill ciphers, relative to Transposition ciphers.

4. Jordan's formula tells us that there are:

$$N^{n^2} \prod_{p \mid N} (1-1/p)(1-1/p^2)\cdots(1-1/p^n)$$

invertible $n \times n$ matrices over Z_N.

Evaluate keyspace of Hill ciphers based on 4×4 matrices in Z_{96}

$n=4$, $N=96$ (note: prime factorization of $96 = 2^5 \cdot 3$)

Then: $96^{4^2} \cdot (1-\frac{1}{2})(1-\frac{1}{2^2})(1-\frac{1}{2^3})(1-\frac{1}{2^4})(1-\frac{1}{3})(1-\frac{1}{3^2})(1-\frac{1}{3^3})(1-\frac{1}{3^4})$

$\cong 9.022 \times 10^{30}$

From 1c: cardinality of keyspace for permutation matrix given by $n!$.

Refer to Bach's notes for example. This type of matrix, when used as a Hill cipher, accomplishes the task of a transposition cipher.

$\therefore$ For block size 4, cardinality of keyspace $|K| = 4!$