1 Problem 1

A series of messages encrypted using an enigma machine were collected. The following is a list of the first six letters of each message.

BCAADC CAFDBB EFDBAF FBCCCE CEBDFD DABFBD FDECEA ADAEEC

Given this, we can find $P_4 \cdot P_1$. Let’s start with the first message. Each letter in the ciphertext permutes to some value $\theta$.

\begin{align*}
P_1(B) &= \theta_1 \\
P_2(C) &= \theta_2 \\
P_3(A) &= \theta_3 \\
P_4(A) &= \theta_1 \\
P_5(D) &= \theta_2 \\
P_6(C) &= \theta_3
\end{align*}

Let’s now examine the equations involving $\theta_1$.

\begin{align*}
P_1(B) &= \theta_1 \\
P_4(\theta_1) &= A
\end{align*}

We know that the enigma machine never used cycles greater than 2 when permuting, and therefore the inverse of each $P_n$ is itself. We can now substitute $\theta$.

\begin{align*}
P_4(P_1(B)) &= A
\end{align*}
We can repeat this for all other messages received.

\[
P_4(P_1(B)) = A \\
P_4(P_1(C)) = D \\
P_4(P_1(E)) = B \\
P_4(P_1(F)) = C \\
P_4(P_1(C)) = D \\
P_4(P_1(D)) = F \\
P_4(P_1(F)) = C \\
P_4(P_1(A)) = E
\]  

(4)

This creates a cycle for \( P_4 \cdot P_1 \)

\[(BAC)(CDF)\]  

(5)

## 2 Problem 2

Given a set with \( n = 2 \) values, there is only 1 derangement. The set \( (1,2) \) can only be permuted to the following.

\[(2,1)\]  

(6)

Therefore \( D_2 = 1 \).

Given a set with \( n = 3 \) values, there are 2 derangements. The set \( (1,2,3) \) can be permuted to the following.

\[(2,3,1), (3,1,2)\]  

(7)

Therefore \( D_3 = 2 \).

Given a set with \( n = 4 \) values, there are 9 derangements. The set \( (1,2,3,4) \) can be permuted to the following.

\[(2,1,4,3), (2,3,4,1), (2,4,1,3), (3,1,4,2), (3,4,1,2), (3,4,2,1), (4,1,2,3), (4,3,1,2), (4,3,2,1)\]  

(8)
Therefore $D_4 = 9$.

Now that we know the values for each $D_n$, we can now solve for the percentage of derangements that are within a permutation.

For $n = 1$:

$$\frac{D_1}{P_1} = \frac{0}{1} = 0$$  \hspace{1cm} (9)

For $n = 2$:

$$\frac{D_2}{P_2} = \frac{1}{2!} = 0.5$$  \hspace{1cm} (10)

For $n = 3$:

$$\frac{D_3}{P_3} = \frac{2}{3!} = 0.333...$$  \hspace{1cm} (11)

For $n = 4$:

$$\frac{D_4}{P_4} = \frac{9}{4!} = 0.375$$  \hspace{1cm} (12)

3 Problem 3

3.1 Part A

We can find the entropy of a fair die by using the entropy equation below.

$$H(x) = -\sum_x P(x)\log_2 P(x)$$  \hspace{1cm} (13)

We know that a fair die all outcomes are equally likely. There are six sides, and each side has a $\frac{1}{6}$ probability of facing up when rolled.

Given this, we can solve for the entropy, $H(X)$. 

3
\[ H(x) = -\sum_{6}^{1} \log_2 \left( \frac{1}{6} \right) \]
\[ = -\log_2 \left( \frac{1}{6} \right) \]
\[ = \log_2 (6) \]
\[ = 2.58 \]

3.2 Part B

We know that for some joint probability \( P(x, y) \), the entropy \( H(X, Y) \) is \( H(X) + H(Y) \) if the two events are independent of each other.

\[ H(x, y) = H(x) + H(y) \] (15)

Given the entropy of rolling one fair die, \( H(X) \), we can solve for the entropy of rolling two.

\[ H(x) = H(y) = 2.58 \] (16)

\[ H(x, y) = H(x) + H(y) \]
\[ = 2.58 + 2.58 \]
\[ = 5.16 \] (17)

4 Problem 4

4.1 Part A

A bag is full of 5 red marbles, 3 white marbles, and 2 green marbles. The probability of picking each color is as follows.

\[ P(\text{red}) = \frac{5}{10} \]
\[ P(\text{white}) = \frac{3}{10} \]
\[ P(\text{green}) = \frac{2}{10} \] (18)

We can find the entropy of picking one marble using the entropy formula.
\[ H(X) = -\sum_{x} P(x) \log_2 P(x) \]
\[ = -\left[ \frac{5}{10} \log_2 \left( \frac{5}{10} \right) + \frac{3}{10} \log_2 \left( \frac{3}{10} \right) + \frac{2}{10} \log_2 \left( \frac{2}{10} \right) \right] \]
\[ = 1.485 \]  

(19)

Therefore picking one marble has an entropy of 1.485.

We know from previous problems that a joint entropy is the sum of individual entropies if and only if the two events associated with the entropy are independent.

Therefore, if we are to pick to marbles with replacement, we can simply add the entropies of each event together because the events are independent.

\[ H(X, Y) = H(X) + H(Y) \]
\[ = 1.485 + 1.485 \]
\[ = 2.97 \]  

(20)

4.2 Part B

If we pick two marbles with replacement, the events are no longer independent.

\[ H(x, y) = \sum_{x} \sum_{y} P(x, y) \log_2 P(x, y) \]  

(21)

If we first pick a red marble.

\[ P(red, red) = \frac{5}{10} \cdot \frac{4}{9} = \frac{2}{9} \]
\[ P(red, white) = \frac{5}{10} \cdot \frac{3}{9} = \frac{1}{6} \]
\[ P(red, green) = \frac{5}{10} \cdot \frac{2}{9} = \frac{1}{9} \]  

(22)

If we first pick a white marble.

\[ P(white, red) = \frac{3}{10} \cdot \frac{5}{9} = \frac{1}{6} \]
\[ P(white, white) = \frac{3}{10} \cdot \frac{2}{9} = \frac{1}{15} \]
\[ P(white, green) = \frac{3}{10} \cdot \frac{2}{9} = \frac{1}{15} \]  

(23)
If we first pick a green marble.

\[
P(\text{green, red}) = \frac{2}{10} \cdot \frac{5}{9} = \frac{1}{9} \\
P(\text{green, white}) = \frac{2}{10} \cdot \frac{3}{9} = \frac{1}{15} \tag{24} \\
P(\text{green, green}) = \frac{2}{10} \cdot \frac{1}{9} = \frac{1}{45}
\]

If we then plug all of these values into the entropy equation, we produce the following result.

\[
H(X, Y) = 2.951 \tag{25}
\]