Lesson 13: Using Matrix Operations for Encryption

Classwork

Opening

A common way to send coded messages is to assign each letter of the alphabet to a number 1–26 and send the message as a string of integers. For example, if we encode the message "THE CROW FLIES AT MIDNIGHT" according to the chart below, we get the string of numbers

$$20, 8, 5, 0, 3, 18, 15, 23, 0, 6, 12, 9, 5, 19, 0, 1, 20, 0, 13, 9, 4, 14, 9, 7, 8, 20.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	SPACE
14	15	16	17	18	19	20	21	22	23	24	25	26	0

However, codes such as these are easily broken using an analysis of the frequency of numbers that appear in the coded messages.

We can instead encode a message using matrix multiplication. If a matrix E has an inverse, then we can encode a message as follows.

- First, convert the characters of the message to integers between 1 and 26 using the chart above.
- If the encoding matrix E is an $n \times n$ matrix, then break up the numerical message into n rows of the same length. If needed, add extra zeros to make the rows the same length.
- Place the rows into a matrix M.
- Compute the product EM to encode the message.
- The message is sent as the numbers in the rows of the matrix EM.

Exercises

1. You have received an encoded message: $34, 101, 13, 16, 23, 45, 10, 8, 15, 50, 8, 12$. You know that the message was encoded using matrix $E = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

   a. Store your message in a matrix C. What are the dimensions of C?

   b. You have forgotten whether the proper decoding matrix is matrix X, Y, or Z as shown below. Determine which of these is the correct matrix to use to decode this message.

$$X = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \end{bmatrix}, Y = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & \frac{2}{3} \end{bmatrix}, Z = \begin{bmatrix} -\frac{1}{3} & -\frac{1}{3} & \frac{4}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \end{bmatrix}$$

c. Decode the message

2. You have been assigned a group number. The message your group receives is listed below. This message is TOP SECRET! It is of such importance that it has been encoded four times.

Your group's portion of the coded message is listed below.

Group 1:

$1500, 3840, 0, 3444, 3420, 4350, 0, 4824, 3672, 3474, -2592, -6660, 0, -5976, -5940, -7560, 0, -8388, -6372, -6048$

Group 2:

$2424, 3024, -138, 396, -558, -1890, -1752, 1512, -2946, 1458, 438, 540, -24, 72, -90, -324, -300, 270, -510, 270$

Group 3:

$489, 1420, 606, 355, 1151, 33, 1002, 829, 99, 1121, 180, 520, 222, 130, 422, 12, 366, 304, 36, 410$

Group 4:

$-18, 10, -18, 44, -54, 42, -6, -74, -98, -124, 0, 10, -12, 46, -26, 42, -4, -36, -60, -82$

Group 5:

$-120, 0, -78, -54, -84, -30, 0, -6, -108, -30, -120, 114, 42, 0, -12, 42, 0, 36, 0, 0$

Group 6:

$126, 120, 60, 162, 84, 120, 192, 42, 84, 192, -18, -360, -90, -324, 0, -18, -216, -36, -90, -324$

a. Store your message in a matrix C with two rows. How many columns does matrix C have?

b. Begin at the station of your group number, and apply the decoding matrix at this first station.

c. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this second station.

d. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this third station.

e. Proceed to the next station in numerical order; if you are at Station 6, proceed to Station 1. Apply the decoding matrix at this fourth station.

f. Decode your message.

3. Sydnie was in Group 1 and tried to decode her message by calculating the matrix $(D_1 \cdot D_2 \cdot D_3 \cdot D_4)$ and then multiplying $(D_1 \cdot D_2 \cdot D_3 \cdot D_4) \cdot C$. This produced the matrix

$$M = \begin{bmatrix} \frac{10526}{3} & \frac{27020}{3} & 0 & \frac{24242}{3} & 8030 & \frac{30655}{3} & 0 & 11336 & 8616 & 8171 \\ -1455 & -3735 & 0 & -3351 & -3330 & -\frac{8475}{2} & 0 & -4701 & -3573 & -\frac{6177}{2} \end{bmatrix}.$$

a. How did she know that she made a mistake?

b. Matrix C was encoded using matrices E_1, E_2, E_3 and E_4, where D_1 decodes a message encoded by E_1, D_2 decodes a message encoded by E_2 and so on. What is the relationship between matrices E_1 and D_1, between E_2 and D_2, etc.?

c. The matrix that Sydnie received was encoded by $C = E_1 \cdot E_2 \cdot E_3 \cdot E_4 \cdot M$. Explain to Sydnie how the decoding process works to recover the original matrix M, and devise a correct method for decoding using multiplication by a single decoding matrix.

d. Apply the method you devised in part (c) to your group's message to verify that it works.

4. You received a coded message in the matrix $C = \begin{bmatrix} 30 & 30 & 69 \\ 2 & 1 & 15 \\ 9 & 14 & 20 \end{bmatrix}$. However, the matrix D that will decode this message has been corrupted, and you do not know the value of entry d_{12}. You know that all entries in matrix D are integers. Using x to represent this unknown entry, the decoding matrix D is given by $D = \begin{bmatrix} 2 & x & -4 \\ -1 & 2 & 3 \\ 1 & -1 & -2 \end{bmatrix}$. Decode the message in matrix C.

Problem Set

1. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$, $B = \begin{bmatrix} -2 & 7 \\ 3 & -4 \end{bmatrix}$, $C = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix}$, $Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Evaluate the following.
   a. $A + B$
   b. $B + A$
   c. $A + (B + C)$
   d. $(A + B) + C$
   e. $A + I$
   f. $A + Z$
   g. $A \cdot Z$
   h. $Z \cdot A$
   i. $I \cdot A$
   j. $A \cdot B$
   k. $B \cdot A$
   l. $A \cdot C$
   m. $C \cdot A$
   n. $A \cdot B + A \cdot C$
   o. $A \cdot (B + C)$
   p. $A \cdot B \cdot C$
   q. $C \cdot B \cdot A$
   r. $A \cdot C \cdot B$
   s. $\det(A)$
   t. $\det(B)$
   u. $\det(C)$
   v. $\det(Z)$
   w. $\det(I)$
   x. $\det(A \cdot B \cdot C)$
   y. $\det(C \cdot B \cdot A)$

2. For any 2×2 matrix A and any real number k, show that if $kA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then $k = 0$ or $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

3. Claire claims that she multiplied $A = \begin{bmatrix} -3 & 2 \\ 0 & 4 \end{bmatrix}$ by another matrix X and obtained $\begin{bmatrix} -3 & 2 \\ 0 & 4 \end{bmatrix}$ as her result. What matrix did she multiply by? How do you know?

4. Show that the only matrix B such that $A + B = A$ is the zero matrix.

5. A 2×2 matrix of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is a *diagonal* matrix. Daniel calculated

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 5 & -3 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & -6 \end{bmatrix}$$
$$\begin{bmatrix} 2 & 3 \\ 5 & -3 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 10 & -6 \end{bmatrix}$$

and concluded that if X is a diagonal matrix and A is any other matrix, then $X \cdot A = A \cdot X$.

a. Is there anything wrong with Daniel's reasoning? Prove or disprove that if X is a diagonal 2×2 matrix, then $X \cdot A = A \cdot X$ for any other matrix A.

b. For 3×3 matrices, Elda claims that only diagonal matrices of the form $X = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix}$ satisfy $X \cdot A = A \cdot X$ for any other 3×3 matrix A. Is her claim correct?

6. Calvin encoded a message using $E = \begin{bmatrix} 2 & 2 \\ -1 & 3 \end{bmatrix}$, giving the coded message $4, 28, 42, 56, 2, -6, -1, 52$. Decode the message, or explain why the original message cannot be recovered.

7. Decode the message below using the matrix $D = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 2 \\ 1 & 2 & 1 \end{bmatrix}$:

$$22, 17, 24, 9, -1, 14, -9, 34, 44, 64, 47, 77.$$

8. Brandon encoded his name with the matrix $E = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$, producing the matrix $C = \begin{bmatrix} 6 & 33 & 15 & 14 \\ 12 & 66 & 30 & 28 \end{bmatrix}$. Decode the message, or explain why the original message cannot be recovered.

9. Janelle used the encoding matrix $E = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$ to encode the message "FROG" by multiplying $C = \begin{bmatrix} 6 & 18 \\ 15 & 7 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 24 & 30 \\ 22 & 37 \end{bmatrix}$. When Taylor decoded it, she computed $M = \begin{bmatrix} -1 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 24 & 30 \\ 22 & 37 \end{bmatrix} = \begin{bmatrix} 20 & 44 \\ 2 & -7 \end{bmatrix}$. What went wrong?