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 – 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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | SPACE |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

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 has an inverse, then we can encode a message as follows.

* First, convert the characters of the message to integers between and using the chart above.
* If the encoding matrix is an matrix, then break up the numerical message into rows of the same length. If needed, add extra zeros to make the rows the same length.
* Place the rows into a matrix .
* Compute the product to encode the message.
* The message is sent as the numbers in the rows of the matrix

Exercises

1. You have received an encoded message: ,,,,,,,,,,, You know that the message was encoded using matrix .
   1. Store your message in a matrix . What are the dimensions of ?
   2. You have forgotten whether the proper decoding matrix is matrix ,, or as shown below. Determine which of these is the correct matrix to use to decode this message.
   3. 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:

, , , , , , , , , , , , , , , , , , ,

Group 2:

, , , ,, , , , , , , , , , , , , , ,

Group 3:

,, ,,, ,, ,,,,,,, , ,,,,

Group 4:

, , ,, ,, , , ,,,, ,, , , , , ,

Group 5:

,,,, , , , ,, , , ,,,,, ,,,

Group 6:

, ,, , ,, , ,,, , , ,,,, ,, ,

* 1. Store your message in a matrix with two rows. How many columns does matrix have?
  2. Begin at the station of your group number, and apply the decoding matrix at this first station.
  3. 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.
  4. 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.
  5. 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.
  6. Decode your message.

1. Sydnie was in Group 1 and tried to decode her message by calculating the matrix and then multiplying. This produced the matrix  
   1. How did she know that she made a mistake?
   2. Matrix was encoded using matrices ,, and , where decodes a message encoded by , decodes a message encoded by and so on. What is the relationship between matrices and , between and , etc.?
   3. The matrix that Sydnie received was encoded by . Explain to Sydnie how the decoding process works to recover the original matrix , and devise a correct method for decoding using multiplication by a single decoding matrix.
   4. Apply the method you devised in part (c) to your group’s message to verify that it works.
2. You received a coded message in the matrix . However, the matrix that will decode this message has been corrupted, and you do not know the value of entry . You know that all entries in matrix are integers. Using to represent this unknown entry, the decoding matrix is given by . Decode the message in matrix .

Problem Set

1. Let , ,, , and . Evaluate the following.
2. For any matrix and any real number , show that if , then or .
3. Claire claims that she multiplied by another matrix and obtained as her result. What matrix did she multiply by? How do you know?
4. Show that the only matrix such that is the zero matrix.
5. A matrix of the form is a *diagonal* matrix. Daniel calculated

and concluded that if is a diagonal matrix and is any other matrix, then

* 1. Is there anything wrong with Daniel’s reasoning? Prove or disprove that if is adiagonal matrix, then for any other matrix
  2. For matrices, Elda claims that only diagonal matrices of the form satisfy for any other matrix . Is her claim correct?

1. Calvin encoded a message using giving the coded message ,,,,, ,,. Decode the message, or explain why the original message cannot be recovered.
2. Decode the message below using the matrix

, , , , , , , , , , ,

1. Brandon encoded his name with the matrix , producing the matrix Decode the message, or explain why the original message cannot be recovered.
2. Janelle used the encoding matrix to encode the message “FROG” by multiplying  
    When Taylor decoded it, she computed  
   . What went wrong?