units. Of course, as before, we are using "=" to mean the corresponding entries are congruent mod N.

The inverse transformation that expresses P in terms of C can be found by subtracting B from both sides and then applying A^{-1} to both sides:

$$P = A^{-1}C - A^{-1}B.$$

This is also an affine transformation $P = A'C + B'$, where $A' = A^{-1}$ and $B' = -A^{-1}B$. Notice that we must assume that A is an invertible matrix in order to be able to decipher uniquely.

Suppose we know that our adversary is using an affine enciphering transformation of digraph-vectors with an N-letter alphabet. To determine A and B (or to determine $A' = A^{-1}$ and $B' = -A^{-1}B$), we need at least *three* digraph pairs. Suppose we know that the ciphertext digraphs C_1, C_2, C_3 correspond to the plaintext digraphs P_1, P_2, P_3:

$$\begin{aligned} P_1 &= A'C_1 + B' \\ P_2 &= A'C_2 + B' \\ P_3 &= A'C_3 + B'. \end{aligned}$$

To find A' and B' we can proceed as follows. Subtract the last equation from the first two, and then make a 2×2–matrix P from the two columns $P_1 - P_3$ and $P_2 - P_3$ and a 2×2–matrix C from the two columns $C_1 - C_3$ and $C_2 - C_3$. We obtain the matrix equation $P = A'C$, which can be solved for A' (provided that C is invertible) as we did in the case of linear enciphering transformations. Finally, once we find $A' = A^{-1}$, we can determine B' from any of the above three equations, e.g., $B' = P_1 - A'C_1$.

Exercises

1. Use frequency analysis to decrypt the following message, which was encoded in the 26-letter alphabet using a Vigenère cipher with a 3-letter key-word. Do this in the following way. To find the first letter of the key-word, work with the sequence consisting of every third letter starting with the first. Do not assume that the most frequently occurring letter is necessarily the ciphertext for "E". List the four most frequently occurring letters, and try out the possibility that each one in turn is the encryption of "E". If one of the other three frequently occurring letters would then have to be the encryption, say, of "Z" or "Q", then you know that you made a wrong choice for "E". By an elimination process, find the letter that must be "E" and then the key-word letter which produces that translation. In this way find the key-word and decipher the message: