MAT 222 Linear Algebra and Numerical Methods
Week 3
Lecture Notes 2

Murat Karaçayır

Akdeniz University
Department of Mathematics

27th February 2025

Gauss-Jordan Elimination for $n \times n$ Systems

- From now on, let us focus our attention to $n \times n$ systems.
- In our previous examples, Gauss-Jordan elimination always reduced the coefficient matrix to a matrix having a certain form if the coefficient matrix has rank n.
- This was $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ for $n = 3$ and $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ for $n = 4$. A short notation is $\operatorname{diag}(1, 1, \dots, 1)$.
- This is no coincidence: If the rank of the coefficient matrix is n, then every row contains a leading entry in the echelon form and that leading entry can be made equal to 1.
- Gauss-Jordan elimination always produces a matrix of the above form when applied to an $n \times n$ matrix of rank n.

Gauss-Jordan Elimination for $n \times n$ Systems

- Let us now examine Gauss-Jordan elimination in more detail.
- Let $A = \begin{bmatrix} 1 & -2 & 3 \\ 2 & -5 & 10 \\ -1 & 2 & -2 \end{bmatrix}$. Let us then consider a system whose coefficient matrix is A and right-hand side $\mathbf{b}$ is arbitrary.

$$\begin{aligned} x - 2y + 3z &= b_1 \\ 2x - 5y + 10z &= b_2 \\ -x + 2y - 2z &= b_3 \end{aligned}$$

- We will apply Gauss-Jordan elimination to the augmented matrix $\left[\begin{array}{ccc|c} 1 & -2 & 3 & b_1 \\ 2 & -5 & 10 & b_2 \\ -1 & 2 & -2 & b_3 \end{array}\right]$.
- The required row operations are $-2R_1 + R_2, 1R_1 + R_3, -1R_2, 4R_3 + R_2, -3R_3 + R_1, 2R_2 + R_1$ in that order. (Please check)
- These operations, when performed in the same order, transforms the right-hand side vector to $\begin{bmatrix} 10b_1 - 2b_2 + 5b_3 \\ 6b_1 - b_2 + 4b_3 \\ b_1 + b_3 \end{bmatrix}$. (Please check)

Gauss-Jordan Elimination for $n \times n$ Systems

- Gauss-Jordan elimination for this problem is summarized as follows:

$$\left[\begin{array}{rrr|l} 1 & -2 & 3 & b_1 \\ 2 & -5 & 10 & b_2 \\ -1 & 2 & -2 & b_3 \end{array}\right] \longrightarrow \left[\begin{array}{ccc|l} 1 & 0 & 0 & 10b_1 - 2b_2 + 5b_3 \\ 0 & 1 & 0 & 6b_1 - b_2 + 4b_3 \\ 0 & 0 & 1 & b_1 + b_3 \end{array}\right].$$

- The augmented part can be written as follows:

$$b_1 \begin{bmatrix} 10 \\ 6 \\ 1 \end{bmatrix} + b_2 \begin{bmatrix} -2 \\ -1 \\ 0 \end{bmatrix} + b_3 \begin{bmatrix} 5 \\ 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

- Thus, the row operations that reduced A to $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ has the effect of multiplying by the matrix $\begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix}$ on $\mathbf{b}$.

Gauss-Jordan Elimination for $n \times n$ Systems

- In short, we have $\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$.
- Row operations are performed on an entire row at a time, so the same should also be valid for columns of **A**.

$$\begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} -2 \\ -5 \\ 2 \end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} -2 \\ -5 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} 3 \\ 10 \\ -2 \end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 10 \\ -2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

- These three identites involving matrix-vector product can be packed into a single identity by means of a new definiton.

Matrix Multiplication

Matrix multiplication

Let A be an $m \times n$ matrix and let B be an $n \times p$ matrix whose columns are $\mathbf{v}_1, \mathbf{v_2} \ldots, \mathbf{v}_p$. Then the multiplication of A and B produces a matrix whose columns are the matrix-vector product of A and the columns of B, in the same order. We denote it by

$$A \cdot B = A \cdot \left[\begin{array}{c|c|c|c} \mathbf{v}_1 & \mathbf{v}_2 & \ldots & \mathbf{v}_p \end{array} \right] = \left[\begin{array}{c|c|c|c} A\mathbf{v}_1 & A\mathbf{v}_2 & \ldots & A\mathbf{v}_p \end{array} \right].$$

The product $A \cdot B$ can also be denoted by AB and is an $m \times p$ matrix.

- If number of columns of $A \neq$ number of rows of B, then the product AB is not defined.
- As an example, consider $A = \begin{bmatrix} 3 & -1 & 2 \\ \frac{1}{2} & 4 & -2 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 4 \\ 5 & 1 \\ -1 & -3 \end{bmatrix}$.
- We have $\begin{bmatrix} 3 & -1 & 2 \\ \frac{1}{2} & 4 & -2 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 23 \end{bmatrix}$ and $\begin{bmatrix} 3 & -1 & 2 \\ \frac{1}{2} & 4 & -2 \end{bmatrix} \begin{bmatrix} 4 \\ 1 \\ -3 \end{bmatrix} = \begin{bmatrix} 5 \\ 12 \end{bmatrix}$.
- As a result, $AB = \begin{bmatrix} 3 & -1 & 2 \\ \frac{1}{2} & 4 & -2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 5 & 1 \\ -1 & -3 \end{bmatrix} = \begin{bmatrix} -1 & 5 \\ 23 & 12 \end{bmatrix}$.

Matrix Multiplication

- In the previous example, we had

$$\begin{bmatrix}1\\2\\-1\end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix}10 & -2 & 5\\6 & -1 & 4\\1 & 0 & 1\end{bmatrix}\begin{bmatrix}1\\2\\-1\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix},$$

$$\begin{bmatrix}-2\\-5\\2\end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix}10 & -2 & 5\\6 & -1 & 4\\1 & 0 & 1\end{bmatrix}\begin{bmatrix}-2\\-5\\2\end{bmatrix} = \begin{bmatrix}0\\1\\0\end{bmatrix},$$

$$\begin{bmatrix}3\\10\\-2\end{bmatrix} \xrightarrow{\text{G-J Elimination}} \begin{bmatrix}10 & -2 & 5\\6 & -1 & 4\\1 & 0 & 1\end{bmatrix}\begin{bmatrix}3\\10\\-2\end{bmatrix} = \begin{bmatrix}0\\0\\1\end{bmatrix}.$$

- Now, we can describe these three identites in one line as follows:

$$\begin{bmatrix}10 & -2 & 5\\6 & -1 & 4\\1 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & -2 & 3\\2 & -5 & 10\\-1 & 2 & -2\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}.$$

- Thus, Gauss-Jordan elimination on A can be expressed by a single matrix multiplication performed on A.

Matrix Multiplication

- Note that there are other ways to define matrix multiplication.
- One way is to use **vector-matrix** product as a building block as opposed to matrix-vector product.
- Namely, if $\mathbf{v} = [a_1 \quad a_2 \quad \ldots \quad a_n]$ and A is a matrix whose rows are $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n$, respectively. Then vector-matrix product of $\mathbf{v}$ and A is the linear combination $a_1\mathbf{r}_1 + a_2\mathbf{r}_2 + \ldots + a_n\mathbf{r}_n$.
- For example, if $\mathbf{v} = [2 \quad -1 \quad 4]$ and $B = \begin{bmatrix} 1 & 4 \\ 0 & -1 \\ 3 & -2 \end{bmatrix}$, then

$$\begin{aligned} \mathbf{v}B &= 2\begin{bmatrix}1 & 4\end{bmatrix} + (-1)\begin{bmatrix}0 & -1\end{bmatrix} + 4\begin{bmatrix}3 & -2\end{bmatrix} \\ &= \begin{bmatrix}2 & 8\end{bmatrix} + \begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}12 & -8\end{bmatrix} = \begin{bmatrix}14 & 1\end{bmatrix}. \end{aligned}$$

- This vector-matrix product can be used to give an alternative definiton of matrix multiplication in an obvious way: Namely, if A is an $m \times n$ matrix whose rows are $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ and B is an $n \times p$ matrix, than AB is defined to be the matrix whose rows are $\mathbf{u}_1 B, \mathbf{u}_2 B, \ldots, \mathbf{u}_m B$, respectively.
- **Exercise:** Multiply the matrices A and B in the previous page by this new method.

Identity Matrix

- Recall that an $n \times n$ matrix with rank n is transformed to $\operatorname{diag}(1, 1, \ldots, 1)$ by Gauss-Jordan elimination. Let us denote it by $\mathbf{I}_n$ or simply by $\mathbf{I}$.
- This matrix, when multiplied by another matrix of compatible size, leaves the matrix as it is.
- For example, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -1 & 4 \\ 10 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -1 & 4 \\ 10 & 3 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 & 3 \\ 2 & -1 & 0 \\ 3 & 0 & 2 \\ 4 & 3 & 7 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & -1 & 0 \\ 3 & 0 & 2 \\ 4 & 3 & 7 \end{bmatrix}$.
- In general, we have $A\mathbf{I} = A$ and $\mathbf{I}B = B$ whenever A and B are matrices of suitable size.
- The matrix $\mathbf{I}_n$ is known to be the identity matrix of size n.
- Thus, we can restate our former observation as follows: If A is an $n \times n$ matrix of rank n, the row-reduced echelon form of A is $\mathbf{I}_n$.

Gauss-Jordan Elimination and Identity Matrix

- Suppose A is an $n \times n$ matrix of rank n. We have seen that
  (1) Gauss-Jordan elimination reduces A to the identity $\mathbf{I}_n$.
  (2) The row operations performed on A during Gauss-Jordan elimination can be represented by a single matrix multiplication on A.
- Schematically we have:
  (i) $A \xrightarrow{\text{Gauss-Jordan elimination}} CA$
  (ii) $A \xrightarrow{\text{Gauss-Jordan elimination}} \mathbf{I}$
- Therefore it must be true that $CA = \mathbf{I}$.

Inverse of a matrix

For a square matrix A, if $CA = AC = \mathbf{I}$, then C is called the inverse of A and is denoted by A^{-1}.

- So Gauss-Jordan elimination can be utilized to obtain the inverse of a matrix, whenever this inverse exists.

Not Every Matrix has an Inverse

- Matrices that have an inverse are called invertible and those that do not have an inverse are called noninvertible or singular.
- As a side note, we observe that not every square matrix is invertible.
- For example, the matrices $\begin{bmatrix} 2 & -1 \\ -6 & 3 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 4 & 8 \\ 2 & -2 & -1 \end{bmatrix}$ are not invertible.
- For these two matrices, the reduced echelon forms are $\begin{bmatrix} 1 & -1/2 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & 2/3 \\ 0 & 1 & 7/6 \\ 0 & 0 & 0 \end{bmatrix}$, respectively.
- This is typical: A square matrix that is noninvertible has at least one nonzero row in its echelon form.
- A restatement of this fact is as follows: An $n \times n$ matrix is invertible if and only if its rank is n.

Inverse Matrix and the Solution of a Linear System

- Given an $n \times n$ system $A\mathbf{x} = \mathbf{b}$, if A is invertible, then this inverse can be used to solve the system in a straightforward way.
- To see this, just multiply both sides of the system by A^{-1}.
  $A^{-1}A\mathbf{x} = A^{-1}\mathbf{b} \longrightarrow \left(A^{-1}A\right)\mathbf{x} = A^{-1}\mathbf{b} \longrightarrow \mathbf{I}\mathbf{x} = A^{-1}\mathbf{b} \longrightarrow \mathbf{x} = A^{-1}\mathbf{b}$
- This shows that once we have the inverse of the coefficient matrix, the problem of solving the system reduces to performing a matrix-vector multiplication.
- This also implies the following: If A is invertible, the system $A\mathbf{x} = \mathbf{b}$ has a unique solution for every right-hand side $\mathbf{b}$.
- What remains is to devise methods to compute the inverse of a matrix.

Computing the Inverse: Method 1

- In fact we have already described a method to compute the inverse of an $n \times n$ invertible matrix A.
- Namely, we take a symbolic column vector $\mathbf{b}$ of size n and perform Gauss-Jordan elimination on the augmented matrix $\left[\begin{array}{c|c} A & \mathbf{b} \end{array}\right]$.
- When A is reduced to $\mathbf{I}$, the augmented part $\mathbf{b}$ will have been reduced to some other symbolic vector. This vector can be expressed as some matrix C multiplied by $\mathbf{B}$.
- For this matrix C we have $CA = \mathbf{I}$. So C is a left inverse of A. It can be shown that $AC = \mathbf{I}$ also holds. So $C = A^{-1}$.
- In our previous example $A = \begin{bmatrix} 1 & -2 & 3 \\ 2 & -5 & 10 \\ -1 & 2 & -2 \end{bmatrix}$ and Gauss-Jordan elimination reduces $\mathbf{b}$ to $\begin{bmatrix} 10b_1 - 2b_2 + 5b_3 \\ 6b_1 - b_2 + 4b_3 \\ b_1 + b_3 \end{bmatrix} = \begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$
- So the inverse of A is $\begin{bmatrix} 10 & -2 & 5 \\ 6 & -1 & 4 \\ 1 & 0 & 1 \end{bmatrix}$.

Computing the Inverse: Method 2

- This method of finding the inverse involves operations on symbolic expressions, so a modification is required to make it better-suited for computer programming.
- Suppose that A is given and we want to find C such that $AC = \mathbf{I}$.
- Recall the definiton of matrix multiplication: The first column of AC is A multiplied by the first column of C, the second column of AC is A multiplied by the second column of C, and so on.
- Thus, if the columns of C are $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$, the following should be true:

$$A\mathbf{c}_1 = A\begin{bmatrix} c_{1,1} \\ c_{2,1} \\ \vdots \\ c_{n,1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, A\mathbf{c}_2 = A\begin{bmatrix} c_{1,2} \\ c_{2,2} \\ \vdots \\ c_{n,2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, A\mathbf{c}_n = A\begin{bmatrix} c_{1,n} \\ c_{2,n} \\ \vdots \\ c_{n,n} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

- Above we have n equation systems. The entries in the first column of C are the unknowns of the first system, the entries in the second column of C are the unknowns of the second system, and so on.
- These n systems have the same coefficient matrix A. This means they can be solved simultaneously to obtain every entry of C.

Computing the Inverse: Method 2

- As an example, consider the system $\begin{array}{r} 3x+y-z=3 \\ -x+2y-2z=-8 \\ x-5y+z=5 \end{array}$. Let us find the inverse of the coefficient matrix $A = \begin{bmatrix} 3 & 1 & -1 \\ -1 & 2 & -2 \\ 1 & -5 & 1 \end{bmatrix}$.
- We will solve three systems:

$$A\begin{bmatrix} c_{1,1} \\ c_{2,1} \\ c_{3,1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, A\begin{bmatrix} c_{1,2} \\ c_{2,2} \\ c_{3,2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, A\begin{bmatrix} c_{1,3} \\ c_{2,3} \\ c_{3,3} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

- These three systems have a common coefficient matrix so the row operations required to reduce them to row-reduced echelon form are completely the same. So they can be solved simultaneously.
- We will apply Gauss-Jordan elimination on $\left[\begin{array}{rrr|rrr} 3 & 1 & -1 & 1 & 0 & 0 \\ -1 & 2 & -2 & 0 & 1 & 0 \\ 1 & -5 & 1 & 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{c|c} A & \mathbf{I} \end{array}\right]$. The resulting matrix on the right-hand side will be the inverse of A.

- $$\left[\begin{array}{rrr|rrr} 3 & 1 & -1 & 1 & 0 & 0 \\ -1 & 2 & -2 & 0 & 1 & 0 \\ 1 & -5 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{R_1 \leftrightarrow R_3} \left[\begin{array}{rrr|rrr} 1 & -5 & 1 & 0 & 0 & 1 \\ -1 & 2 & -2 & 0 & 1 & 0 \\ 3 & 1 & -1 & 1 & 0 & 0 \end{array}\right]$$
$$\xrightarrow[-3R_1+R_3]{1R_1+R_2} \left[\begin{array}{rrr|rrr} 1 & -5 & 1 & 0 & 0 & 1 \\ 0 & -3 & -1 & 0 & 1 & 1 \\ 0 & 16 & -4 & 1 & 0 & -3 \end{array}\right] \xrightarrow{\frac{16}{3}R_2+R_3} \left[\begin{array}{rrr|rrr} 1 & -5 & 1 & 0 & 0 & 1 \\ 0 & -3 & -1 & 0 & 1 & 1 \\ 0 & 0 & -28/3 & 1 & 16/3 & 7/3 \end{array}\right]$$
$$\xrightarrow[-\frac{3}{28}R_3]{-\frac{1}{3}R_2} \left[\begin{array}{rrr|rrr} 1 & -5 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1/3 & 0 & -1/3 & -1/3 \\ 0 & 0 & 1 & -3/28 & -4/7 & -1/4 \end{array}\right].$$
- The forward elimination phase is complete. In addition we have made every leading entry equal to 1. Let us do the remaining part.
- $$\xrightarrow[-1R_3+R_1]{-\frac{1}{3}R_3+R_2} \left[\begin{array}{rrr|rrr} 1 & -5 & 0 & 3/28 & 4/7 & 5/4 \\ 0 & 1 & 0 & 1/28 & -1/7 & -1/4 \\ 0 & 0 & 1 & -3/28 & -4/7 & -1/4 \end{array}\right]$$
$$\xrightarrow{5R_2+R_1} \left[\begin{array}{rrr|rrr} 1 & 0 & 0 & 2/7 & -1/7 & 0 \\ 0 & 1 & 0 & 1/28 & -1/7 & -1/4 \\ 0 & 0 & 1 & -3/28 & -4/7 & -1/4 \end{array}\right]$$
- The resulting 3×3 matrix on the right is the inverse of A.

Computing the Inverse: Method 2

- So we have obtained $C = \begin{bmatrix} 2/7 & -1/7 & 0 \\ 1/28 & -1/7 & -1/4 \\ -3/28 & -4/7 & -1/4 \end{bmatrix}$ as the inverse of A.
- You can verify that
$$AC = \begin{bmatrix} 3 & 1 & -1 \\ -1 & 2 & -2 \\ 1 & -5 & 1 \end{bmatrix} \begin{bmatrix} 2/7 & -1/7 & 0 \\ 1/28 & -1/7 & -1/4 \\ -3/28 & -4/7 & -1/4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$
- You can also verify that $CA = \mathbf{I}$. So we have $C = A^{-1}$.
- We can use A^{-1} to solve the given linear system.
$$\mathbf{x} = A^{-1}\mathbf{b} = \begin{bmatrix} 2/7 & -1/7 & 0 \\ 1/28 & -1/7 & -1/4 \\ -3/28 & -4/7 & -1/4 \end{bmatrix} \begin{bmatrix} 3 \\ -8 \\ 5 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 3 \end{bmatrix}$$
- So the solution of the system is $x = 2, y = 0, z = 3$.
- The summary of the method is as follows:
$$\left[\; A \;\middle|\; \mathbf{I} \;\right] \xrightarrow{\text{Gauss-Jordan Elimination}} \left[\; \mathbf{I} \;\middle|\; A^{-1} \;\right]$$

Operation Cost of Finding the Inverse

- It can be shown that finding the inverse of an $n \times n$ matrix using Method 2 requires n^3 multiplications.
- In addition, one has to perform an additional matrix multiplication to solve a system using the inverse.
- This makes this method impractical to solve a single system of equations.
- Another disadvantage is that it cannot be applied to systems that have infinitely many solutions. Because the coefficient matrix does not have an inverse in such cases.
- Still there are certain advantages of working with inverse matrices.

An Application of Inverse Matrices: Hill Cipher

- Inverse matrices has an easy application in cryptography, which was invented by Lester S. Hill in 1929 and known as "Hill cipher".
- The idea is to convert the plaintext (the message to be sent) to a matrix and encrypt it by multiplying it with a matrix (called the "key).
- The receiver of the message, who knows the key, can then use the inverse matrix to decipher the encrypted message.
- Schematically, we have

$$\text{(Plaintext) } B \xrightarrow{\textit{Encryption}} \text{(Ciphertext) } AB \xrightarrow{\textit{Decryption}} \text{(Plaintext) } A^{-1}AB = B$$

- The message is converted to a matrix by an agreed-upon labeling such as $A = 0, B = 1, C = 2, \dots, Z = 25$ etc. Yet it is more secure to use a random permutation of the alphabet.
- If the key matrix A is $n \times n$, then the message is split into groups of n characters. Any missing characters in the end may be filled by an additional character such as $\#$ (26).

An Application of Inverse Matrices: Hill Cipher

- For example, let us encrypt the message "IL NOME DELLA ROSA". Let us not use blank characters so that it is "ILNOMEDELLAROSA".
- Let us use the key matrix $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$. (Note that it should be invertible)
- Using the usual numbering of the alphabet, the message becomes
  8 11 13 14 12 4 3 4 11 11 0 17 14 18 0
- Now we group these in 2×1 column vectors as $\begin{bmatrix} 8 \\ 11 \end{bmatrix}, \begin{bmatrix} 13 \\ 14 \end{bmatrix}, \ldots$ etc.

  The "0" at the end is alone so we group it with a "#": $\begin{bmatrix} 0 \\ 26 \end{bmatrix}$.
- Thus we have the plaintext matrix
  $$B = \begin{bmatrix} 8 & 13 & 12 & 3 & 11 & 0 & 14 & 0 \\ 11 & 14 & 4 & 4 & 11 & 17 & 18 & 26 \end{bmatrix}.$$
- The ciphertext matrix becomes
  $$AB = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 8 & 13 & 12 & 3 & 11 & 0 & 14 & 0 \\ 11 & 14 & 4 & 4 & 11 & 17 & 18 & 26 \end{bmatrix} =$$
  $$\begin{bmatrix} 30 & 40 & 20 & 11 & 33 & 34 & 50 & 52 \\ 41 & 55 & 24 & 15 & 44 & 51 & 68 & 78 \end{bmatrix}.$$

An Application of Inverse Matrices: Hill Cipher

- Then we replace each number by their modulo-27 equivalents:
$$AB = \begin{bmatrix} 3 & 13 & 20 & 11 & 6 & 7 & 23 & 25 \\ 14 & 1 & 24 & 15 & 17 & 24 & 14 & 24 \end{bmatrix}.$$
- The codewords corresponding to columns are do,nb,uy,lp,gr, hy,xo,zy. Therefore the receiver receives the message "DONBUYLPGRHYXOZY".
- The receiver should convert the ciphertext to a matrix. Thus he/she obtains the matrix $AB = \begin{bmatrix} 3 & 13 & 20 & 11 & 6 & 7 & 23 & 25 \\ 14 & 1 & 24 & 15 & 17 & 24 & 14 & 24 \end{bmatrix}$.
- The receiver, knowing that the key matrix is $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$, computes the inverse of the key matrix, which is $A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$.
- So the receiver computes
$$A^{-1}(AB) = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 13 & 20 & 11 & 6 & 7 & 23 & 25 \\ 14 & 1 & 24 & 15 & 17 & 24 & 14 & 24 \end{bmatrix} =$$
$$\begin{bmatrix} -19 & 37 & 12 & 3 & -16 & -27 & 41 & 27 \\ 11 & -12 & 4 & 4 & 11 & 17 & -9 & -1 \end{bmatrix}.$$

- Modulo 27, this is equal to $B = \begin{bmatrix} 8 & 13 & 12 & 3 & 11 & 0 & 14 & 0 \\ 11 & 14 & 4 & 4 & 11 & 17 & 18 & 26 \end{bmatrix}$.
- The receiver then converts each column to letters as $\begin{bmatrix} 8 \\ 11 \end{bmatrix} \rightarrow$ il, $\begin{bmatrix} 13 \\ 14 \end{bmatrix} \rightarrow$ no, $\ldots$, $\begin{bmatrix} 0 \\ 26 \end{bmatrix} \rightarrow$ a#
- The receiver understands that the message was "ILNOMEDELLAROSA".
- **Exercise:** Suppose you receive the message "BHLXDBUHCG". This time the key matrix is $A = \begin{bmatrix} 2 & 5 \\ 3 & 8 \end{bmatrix}$. Decipher it using the Hill cipher. (Take the modulus number to be 27)

- **Exercise:** Consider the following systems of equations:

$$\begin{aligned} 2x - 3y + z &= 2 \\ x + y - z &= -1 \\ -x + y - 3z &= 0 \end{aligned} \quad , \quad \begin{aligned} 2x - 3y + z &= 6 \\ x + y - z &= 4, \\ -x + y - 3z &= 5 \end{aligned}$$

$$\begin{aligned} 2x - 3y + z &= 0 \\ x + y - z &= 1 \\ -x + y - 3z &= -3 \end{aligned} \quad \text{and} \quad \begin{aligned} 2x - 3y + z &= -1 \\ x + y - z &= 0 \\ -x + y - 3z &= 0 \end{aligned} \quad .$$

Compute the inverse of the coefficient matrix and use this inverse to solve all four systems.