10. Inverse Matrix

Definition A square matrix M is *invertible* (or *nonsingular*) if there exists a matrix M^{-1} such that

$$M^{-1}M = I = M^{-1}M.$$

Inverse of a 2×2 Matrix Let M and N be the matrices:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad N = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Multiplying these matrices gives:

$$MN = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (ad-bc)I$$

Then $M^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, so long as $ad - bc \neq 0$.

Three Properties of the Inverse

1. If A is a square matrix and B is the inverse of A, then A is the inverse of B, since $AB = I = BA$. Then we have the identity:

$$(A^{-1})^{-1} = A$$

2. Notice that $B^{-1}A^{-1}AB = B^{-1}IB = I = ABB^{-1}A^{-1}$. Then:

$$(AB)^{-1} = B^{-1}A^{-1}$$

   Then much like the transpose, taking the inverse of a product *reverses* the order of the product.

3. Finally, recall that $(AB)^T = B^TA^T$. Since $I^T = I$, then $(A^{-1}A)^T = A^T(A^{-1})^T = I$. Similarly, $(AA^{-1})^T = (A^{-1})^TA^T = I$. Then:

$$(A^{-1})^T = (A^T)^{-1}$$

   As such, we could even$M^{-1}V$ write A^{-T} for the inverse transpose of A.

Finding Inverses

Suppose M is a square matrix and $MX = V$ is a linear system with unique solution X_0. Since there is a unique solution, $M^{-1}V$, then the reduced row echelon form of the linear system has an identity matrix on the left:

$$\begin{pmatrix} M \mid V \end{pmatrix} \sim \begin{pmatrix} I \mid M^{-1}V \end{pmatrix}$$

Solving the linear system $MX = V$ then tells us what $M^{-1}V$ is.

To solve many linear systems at once, we can consider augmented matrices with a matrix on the right side instead of a column vector, and then apply Gaussian row reduction to the left side of the matrix. Once the identity matrix is on the left side of the augmented matrix, then the solution of each of the individual linear systems is on the right.

To compute M^{-1}, we are interested in solving the collection of systems $MX = e_k$, where e_k is the column vector of zeroes with a 1 in the kth entry. Putting the e_k's together into an identity matrix, we get:

$$\begin{pmatrix} M \mid I \end{pmatrix} \sim \begin{pmatrix} I \mid M^{-1}I \end{pmatrix} = \begin{pmatrix} I \mid M^{-1} \end{pmatrix}$$

Example Find $\begin{pmatrix} -1 & 2 & -3 \\ 2 & 1 & 0 \\ 4 & -2 & 5 \end{pmatrix}^{-1}$.

Start by writing the augmented matrix, then apply row reduction to the left side.

$$\begin{aligned}
\left(\begin{array}{ccc|ccc} -1 & 2 & -3 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 \\ 4 & -2 & 5 & 0 & 0 & 1 \end{array}\right) &\sim \left(\begin{array}{ccc|ccc} 1 & -2 & 3 & 1 & 0 & 0 \\ 0 & 5 & -6 & 2 & 1 & 0 \\ 0 & 6 & -7 & 4 & 0 & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & \frac{3}{5} & \frac{-1}{4} & \frac{2}{5} & 0 \\ 0 & 1 & \frac{-6}{5} & \frac{2}{5} & \frac{1}{5} & 0 \\ 0 & 0 & \frac{1}{5} & \frac{4}{5} & \frac{-6}{5} & 1 \end{array}\right) \\
&\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & -5 & 4 & 0 \\ 0 & 1 & 0 & 10 & -7 & 6 \\ 0 & 0 & 1 & 8 & -6 & 5 \end{array}\right)
\end{aligned}$$

At this point, we know M^{-1} assuming we didn't goof up. However, row reduction is a lengthy and arithmetically involved process, so we should *check our answer,* by confirming that $MM^{-1} = I$ (or if you prefer $M^{-1}M = I$):

$$MM^{-1} = \begin{pmatrix} -1 & 2 & -3 \\ 2 & 1 & 0 \\ 4 & -2 & 5 \end{pmatrix} \begin{pmatrix} -5 & 4 & 0 \\ 10 & -7 & 6 \\ 8 & -6 & 5 \end{pmatrix}$$

The product of the two matrices is indeed the identity matrix, so we're done.

Linear Systems and Inverses

If M^{-1} exists and is known, then we can immediately solve linear systems associated to M.

Example Consider the linear system:

$$\begin{array}{rrrl} -x & +2y & -3z & = 1 \\ 2x & +y & & = 2 \\ 4x & -2y & +5z & = 0 \end{array}$$

The associated matrix equation is $MX = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$. Then:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 & 2 & -3 \\ 2 & 1 & 0 \\ 4 & -2 & 5 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -5 & 4 & 0 \\ 10 & -7 & 6 \\ 8 & -6 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ -4 \\ -4 \end{pmatrix}$$

Then $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ -4 \\ -4 \end{pmatrix}$.

In summary, when M^{-1} exists, then $MX = V \Rightarrow X = M^{-1}V$.

Homogeneous Systems

Theorem 0.1. *A square matrix M is invertible if and only if the system $MX = 0$ has no non-zero solutions.*

Proof. First, suppose that M^{-1} exists. Then $MX = 0 \Rightarrow X = M^{-1}0 = 0$. Thus, if M is invertible, then $MX = 0$ has no non-zero solutions.

On the other hand, $MX = 0$ always has the solution $X = 0$. If no other solutions exist, then M can be put into reduced row echelon form with every variable a pivot. In this case, M^{-1} can be computed using the process in the previous section. $\square$

Bit Matrices

In computer science, information is recorded using binary strings of data. For example, the following string contains an English word:

$$011011000110100101101110011001010110000101110010$$

A *bit* is the basic unit of information, keeping track of a single one or zero. Computers can add and multiply individual bits very quickly.

Consider the set $\mathbb{Z}_2 = \{0, 1\}$ with addition and multiplication given by the following tables:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Notice that $-1 = 1$, since $1 + 1 = 0$.

It turns out that $\mathbb{Z}_2$ is just as good as the real or complex numbers (they are all *fields*), so we can apply all of the linear algebra we have learned thus far to matrices with $\mathbb{Z}_2$ entries. A matrix with entries in $\mathbb{Z}_2$ is sometimes called a *bit matrix*.

Example $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ is an invertible matrix over $\mathbb{Z}_2$:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

This can be easily verified by multiplying:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

References

Hefferon: Chapter Three, Section IV.2
Wikipedia: Invertible Matrix

Review Questions

1. Let M be a square matrix. Explain why the following statements are equivalent:

   i. $MX = V$ has a *unique* solution for every column vector V.

   ii. M is non-singular.

   (Show that $(i) \Rightarrow (ii)$ and $(ii) \Rightarrow (i)$.)

2. Find formulas for the inverses of the following matrices, when they are not singular:

   i. $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$

   ii. $\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$

   When are these matrices singular?

3. Write down all 2×2 bit matrices and decide which of them are singular. For those which are not singular, pair them with their inverse.