2.4 — MATRIX INVERSE AND TRANSPOSE
UNIVERSITY OF MASSACHUSETTS AMHERST
MATH 235 — SPRING 2014

Definition 1. If A is an $m \times n$ matrix, the *transpose* of A is the $n \times m$ matrix, denoted A^T, whose columns are the rows of A.

Example 2. Let $A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ -2 & 4 \end{bmatrix}$. Compute $A^T, B^T, AB, (AB)^T, A^TB^T, B^TA^T$.

Theorem 3. *Wherever these sums and products are defined,*
(a) $(A^T)^T = A$.
(b) $(A + B)^T = A^T + B^T$.
(c) $(kA)^T = kA^T$ *for any scalar* k.
(d) $(AB)^T = B^T A^T$.

Example 4. Prove that $(ABC)^T = C^T B^T A^T$ using properties of matrices.

Definition 5. An $n \times n$ matrix A is *invertible* if there is an $n \times n$ matrix B such that $AB = BA = I_n$, where I_n is the $n \times n$ identity matrix. We call B the *inverse* of A.

Theorem 6. *An $n \times n$ matrix A is invertible if and only if* $\operatorname{rref}(A) = I_n$. *Equivalently,* $\operatorname{rank}(A) = n$.

Example 7. Which of the following matrices are invertible?

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 3 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & 0 & 0 \end{bmatrix}$$

Theorem 8. *If A is invertible, then its inverse is unique.*

Proof. Idea: Suppose that B and C are both inverses of A. We want to show that ...

□

Theorem 9. *Let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. *If $ad - bc \neq 0$, then A is invertible and*

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

If $ad - bc = 0$, then A is not invertible.

Proof. Idea: Show that $\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then show that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is not invertible if $ad - bc = 0$.

□

Theorem 10. *If A is an $n \times n$ invertible matrix, the equation $A\vec{x} = \vec{b}$ has a unique solution: $\vec{x} = A^{-1}\vec{b}$.*

Example 11. Use the inverse of $A = \begin{bmatrix} -7 & 3 \\ 5 & -2 \end{bmatrix}$ to solve the system $\left\{ \begin{array}{c} -7x_1 + 3x_2 = 2 \\ 5x_1 - 2x_2 = 1 \end{array} \right\}$.

Theorem 12. *Suppose that A and B are invertible. Then*
(a) A^{-1} is invertible, and $(A^{-1})^{-1} = A$.
(b) AB is invertible, and $(AB)^{-1} = B^{-1}A^{-1}$.
(c) A^T is invertible, and $(A^T)^{-1} = (A^{-1})^T$.

Proof. Parts (b) and (c):

□

Algorithm for finding A^{-1} Write A and I side-by-side in an augmented matrix $\begin{bmatrix} A & I \end{bmatrix}$ and row reduce. If A is invertible, then $\begin{bmatrix} A & I \end{bmatrix}$ will reduce to $\begin{bmatrix} I & A^{-1} \end{bmatrix}$.

Example 13. Find the inverse of $A = \begin{bmatrix} 2 & 0 & 0 \\ -3 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ if it exists.

ADDITIONAL EXERCISES

(1) Compute the inverses of the invertible matrices in Example 7.

(2) Prove that if A, B, and C are invertible matrices, then $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$.

(3) For which values is k is the matrix $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & k \\ 1 & 4 & k^2 \end{bmatrix}$ invertible?

(4) Linear transformations may be used to encrypt messages in the following way. First assign a number to each letter.

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
14	15	16	17	18	19	20	21	22	23	24	25	26

Then we choose a 2×2 invertible matrix T with which to encrypt our message. The encryption process is the following:

- Break your message into two letter chunks.
- Write each pair of letters as a column vector of two numbers, where the top number corresponds to the first letter, and the bottom number corresponds to the second letter.
- Multiply each vector on the left by the matrix T; the outputs give the encrypted message.

For example, to encrypt the message "CODE" using the matrix $T = \begin{bmatrix} 6 & -1 \\ -1 & 1 \end{bmatrix}$, we break "CODE" into to chunks, "CO" and "DE", which are represented by the vectors $\begin{bmatrix} 3 \\ 15 \end{bmatrix}$ and $\begin{bmatrix} 4 \\ 5 \end{bmatrix}$. Now multiply by T:

$$\begin{bmatrix} 6 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 3 \\ 12 \end{bmatrix}, \quad \begin{bmatrix} 6 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 19 \\ 1 \end{bmatrix},$$

and convert the outputs into the encrypted message: $\begin{bmatrix} 3 \\ 12 \end{bmatrix} \to$ "CL", $\begin{bmatrix} 19 \\ 1 \end{bmatrix} \to$ "SA". Hence "CODE" becomes "CLSA".

Your task (should you choose to accept): Under a different linear transformation, "KEYS" is encrypted as "EFSF". Use this information to decipher the message "OJRCADEBIESB".