Matrix Inverses and Cryptography

Finite Math

10 April 2017

Matrix Equations

Theorem

Assume that all products and sums are defined for the indicated matrices A, B, C, I, and 0 (where 0 stands for the zero matrix). Then

- *Addition Properties*
  1. *Associative*
  $$(A + B) + C = A + (B + C)$$
  2. *Commutative*
  $$A + B = B + A$$
  3. *Additive Identity*
  $$A + 0 = 0 + A = A$$
  4. *Additive Inverse*
  $$A + (-A) = (-A) + A = 0$$

Matrix Equations

Theorem

Assume that all products and sums are defined for the indicated matrices A, B, C, I, and 0 (where 0 stands for the zero matrix). Then

- *Multiplication Properties*
  1. *Associative Property*
  $$A(BC) = (AB)C$$
  2. *Multiplicative Identity*
  $$AI = IA = A$$
  3. *Multiplicative Inverse*
  If A is a square matrix and A^{-1} exists, then $AA^{-1} = A^{-1}A = I$

Matrix Equations

Theorem

Assume that all products and sums are defined for the indicated matrices A, B, C, I, and 0 (where 0 stands for the zero matrix). Then

- *Combined Properties*
  1. *Left Distributive*
     $$A(B+C) = AB + AC$$
  2. *Right Distributive*
     $$(B+C)A = BA + CA$$

Matrix Equations

Theorem

Assume that all products and sums are defined for the indicated matrices A, B, C, I, and 0 (where 0 stands for the zero matrix). Then

- *Equality*
  1. *Addition*
     If $A = B$, then $A + C = B + C$
  2. *Left Multiplication*
     If $A = B$, then $CA = CB$
  3. *Right Multiplication*
     If $A = B$, then $AC = BC$

Solving Matrix Equations

We can use the rules above to solve various matrix equations. In the next 3 examples, we will assume all necessary inverses exists.

Solving Matrix Equations

We can use the rules above to solve various matrix equations. In the next 3 examples, we will assume all necessary inverses exists.

Example

Suppose A is an $n \times n$ matrix and B and X are $n \times 1$ column matrices. Solve the matrix equation for X

$$AX = B.$$

Solving Matrix Equations

We can use the rules above to solve various matrix equations. In the next 3 examples, we will assume all necessary inverses exists.

Example

Suppose A is an $n \times n$ matrix and B and X are $n \times 1$ column matrices. Solve the matrix equation for X

$$AX = B.$$

Example

Suppose A is an $n \times n$ matrix and B, C, and X are $n \times 1$ matrices. Solve the matrix equation for X

$$AX + C = B.$$

Now You Try It!

Example

Suppose A and B are $n \times n$ matrices and C is an $n \times 1$ matrix. Solve the matrix equation for X

$$AX - BX = C.$$

What size matrix is X?

Matrix Equations and Systems of Linear Equations

We can also solve systems of equations using the above ideas. These apply in the case that the system has the same number of variables as equations and the coefficient matrix of the system is invertible.

Matrix Equations and Systems of Linear Equations

We can also solve systems of equations using the above ideas. These apply in the case that the system has the same number of variables as equations and the coefficient matrix of the system is invertible. If that is the case, for the system

$$
\begin{array}{ccccccccc}
a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\
a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\
\vdots & + & \vdots & + & \ddots & + & a_{1n}x_n & = & \vdots \\
a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nn}x_n & = & b_n
\end{array}
$$

Matrix Equations and Systems of Linear Equations

We can also solve systems of equations using the above ideas. These apply in the case that the system has the same number of variables as equations and the coefficient matrix of the system is invertible. If that is the case, for the system

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & + & \vdots & + & \ddots & + & a_{1n}x_n & = & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nn}x_n & = & b_n \end{array}$$

we can create the matrix equation

$$AX = B$$

Matrix Equations and Systems of Linear Equations

we can create the matrix equation

$$AX = B$$

Matrix Equations and Systems of Linear Equations

we can create the matrix equation

$$AX = B$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{1n} \end{bmatrix}, X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \text{ and } B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Matrix Equations and Systems of Linear Equations

we can create the matrix equation

$$AX = B$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{1n} \end{bmatrix}, X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \text{ and } B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Then, if A is invertible (as is the case when the system is consistent and independent, i.e., exactly one solution), we have

$$X = A^{-1}B.$$

Solving Systems of Equations Using Matrices

Example

Solve the system of equations using matrix methods

$$\begin{array}{ccccc} x & + & 2y & = & k_1 \\ x & + & 3y & = & k_2 \end{array}$$

where

(a) $k_1 = 1, k_2 = 3$

(b) $k_1 = 3, k_2 = 5$

(c) $k_1 = -2, k_2 = 1$

Now You Try It!

Example

Solve the system of equations using matrix methods

$$\begin{array}{rcrcl} 2x & + & y & = & k_1 \\ 5x & + & 3y & = & k_2 \end{array}$$

where

(a) $k_1 = 2, k_2 = 13$

(b) $k_1 = 2, k_2 = 4$

(c) $k_1 = 1, k_2 = -3$

Now You Try It!

Example

Solve the system of equations using matrix methods

$$\begin{array}{rcrcl} 2x & + & y & = & k_1 \\ 5x & + & 3y & = & k_2 \end{array}$$

where

(a) $k_1 = 2$, $k_2 = 13$

(b) $k_1 = 2$, $k_2 = 4$

(c) $k_1 = 1$, $k_2 = -3$

Solution

(a) $x = -7$ *and* $y = 16$, *(b)* $x = 2$ *and* $y = -2$, *(c)* $x = 6$ *and* $y = -11$