Math 107 Lecture 15

Gaussian Elimination and Applications to Cryptography

by Dr. Kurianski
on October 16, 2024

» Announcements and Objectives

Announcements

* Skill Check 4 is next Wed (10/23, 110 mins)
* Pre-Notes due before start of next lecture
* Assignments Due Friday (10/18):
    * HW7 Handwritten Questions
    * HW7 Coding Problems
    * HW7 MATLAB File Upload

Objectives

* Write systems of linear equations as augmented matrices
* Solve systems of linear equations using row reduction
* Use Gaussian elimination to solve systems of linear equations

Gaussian Elimination

» Elementary row operations

1. Add scalar multiple of one row to second and replace second row with the sum (ex: $3R_1 + R_2 \to R_2$)
2. Multiply one row by a nonzero scalar (ex: $-\frac{1}{2}R_3 \to R_3$)
3. Swap rows (ex: $R_1 \leftrightarrow R_2$)

» Reduced row-echelon form

Definition: A matrix is in **reduced row-echelon form** if its entries satisfy the following conditions:

1. The first nonzero entry in each row is 1 (called the leading 1).
2. Each leading 1 comes in a column to the right of the leading 1s in the rows above it.
3. Rows of all 0s come at the bottom of the matrix.
4. If a column contains a leading 1, then all other entries in that column are 0.

» Reduced row-echelon form

Definition: A matrix is in **reduced row-echelon form** if its entries satisfy the following conditions:

1. The first nonzero entry in each row is 1 (called the leading 1).
2. Each leading 1 comes in a column to the right of the leading 1s in the rows above it.
3. Rows of all 0s come at the bottom of the matrix.
4. If a column contains a leading 1, then all other entries in that column are 0.

Note: If a matrix satisfies 1-3 only, it is said to be in **row-echelon form**. If it satisfies all 4, then it is in **reduced row-echelon form**.

» Row-echelon form

Poll

Question: Which of the following matrices are in reduced row-echelon form? (Select all that apply.)

(a) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

(d) $\begin{bmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(e) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

» Gaussian elimination

Steps

Goal: Put the matrix in reduced row-echelon form using elementary row operations.

Steps:

1. Create a leading 1.
2. Use this leading 1 to put 0s below it. (Forward steps)
3. Repeat above steps until all possible rows have leading 1s.
4. Put 0s above these leading 1s. (Backward steps)

» Gaussian elimination

Example 1

Solve the following system of equations using reduced row reduction on the augmented matrix. Check your work by performing each row operation in MATLAB.

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ 2x_1 + 3x_2 + 7x_3 &= 0 \\ x_1 + 3x_2 - 2x_3 &= 17 \end{aligned}$$

» Gaussian elimination

Example 2

$$
\begin{aligned}
-3x_1 - 3x_2 + 9x_3 &= 12 \\
2x_1 + 2x_2 - 4x_3 &= -2 \\
-2x_2 - 4x_3 &= -8
\end{aligned}
$$

» Gaussian elimination

Example 3

$$
\begin{aligned}
2x + y - z &= 4\\
x - y + 2z &= 12\\
2x + 2y - z &= 9
\end{aligned}
$$

Solving Systems in MATLAB

» Solving Systems in MATLAB

Recall that a system of linear equations can be written as a matrix equation

$$A\vec{x} = \vec{b}$$

where A is the coefficient matrix, $\vec{x}$ is the vector of unknowns, and $\vec{b}$ is the vector of right-hand side values.

Steps for solving:

1. Write down augmented matrix [A b]
2. Find the reduced row-echelon form the augmetned matrix (use Gaussian elimination)
3. If the system has exactly one solution, then the solution $\vec{x}$ is the last column of the matrix from step 2.

» Example from last time

Example:

$$\begin{aligned} -3x_1 - 3x_2 + 9x_3 &= 12 \\ 2x_1 + 2x_2 - 4x_3 &= -2 \\ -2x_2 - 4x_3 &= -8 \end{aligned}$$

MATLAB Syntax: `rref(A)` - returns the reduced row-echelon form of the matrix A

» Example 2

Example:

$$
\begin{aligned}
2x_1 + x_2 - x_3 &= 4 \\
x_1 - x_2 + 2x_3 &= 12 \\
2x_1 + 2x_2 - x_3 &= 9
\end{aligned}
$$

Cryptography

» Cryptography

What is it and how is it used?

What is it?

* Encrypted (coded) messages transmitted to a receiver which can decrypt (decode) and read the message.

How is it used?

* Credit card transactions
* Passwords
* Secure web browsing
* ATMs

» Caesar cipher

Activity

1. Enumerate the letters in alphabetical order

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

2. Turn a word into a vector of associated numbers. For example, 'cat' becomes $\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix}$.
3. Add 3 to each element to create an encrypted word. For example,

$$\begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix} \to \begin{bmatrix} 5 \\ 3 \\ 22 \end{bmatrix}$$