Matrix Operations and Congruences

Priyank Kalla

Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

January 22, 2024

Matrix Review

- Please review addition, multiplication and determinants $det(\boldsymbol{A})$ of matrices
- Denote a $m \times n$ matrix $\boldsymbol{A} = (a_{ij})_{m\times n}$, $\boldsymbol{B} = (b_{ij})_{m\times n}$
- $\boldsymbol{A} \pm \boldsymbol{B} = (a_{ij}) \pm (b_{ij})$
- $r \cdot \boldsymbol{A} = (r \cdot a_{ij})$ where r is a scalar
- $\boldsymbol{A} + \boldsymbol{B} = \boldsymbol{B} + \boldsymbol{A}$; $(\boldsymbol{A} + \boldsymbol{B}) + \boldsymbol{C} = \boldsymbol{A} + (\boldsymbol{B} + \boldsymbol{C})$; and $r(\boldsymbol{A} + \boldsymbol{B}) = r\boldsymbol{A} + r\boldsymbol{B}$
- $\boldsymbol{Z}$ is the 0 matrix and $\boldsymbol{I} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is the identity matrix

Matrix Multiplication

- Row vector $(a_1, a_2, \ldots, a_p)$ and column vector $(b_1, b_2, \ldots, b_p)^T = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_p \end{pmatrix}$, then their product is the number: $a_1 b_1 + a_2 b_2 + \cdots + a_p b_p$.
- Matrix Product: $\boldsymbol{A}_{m \times p} \cdot \boldsymbol{B}_{p \times n} = \boldsymbol{C}_{m \times n}$, where each ij-entry of $\boldsymbol{C}$ is the product of the i^{th} row of $\boldsymbol{A}$ and the j^{th} column of $\boldsymbol{B}$. Here $1 \leq i \leq m, 1 \leq j \leq n$.
- In general $\boldsymbol{A} \cdot \boldsymbol{B} \neq \boldsymbol{B} \cdot \boldsymbol{A}$: matrix multiplication is not always commutative
- $(\boldsymbol{AB})\boldsymbol{C} = \boldsymbol{A}(\boldsymbol{BC})$
- $\boldsymbol{A}(\boldsymbol{B} + \boldsymbol{C}) = \boldsymbol{AB} + \boldsymbol{AC}$
- $\boldsymbol{A} \cdot \boldsymbol{I} = \boldsymbol{IA} = \boldsymbol{A}$

Solving Linear Equations

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

These equations canbe put in Matrix Form:

$$
\begin{aligned}
\boldsymbol{A}\overline{x} &= \overline{b} \\
\overline{x} &= \boldsymbol{A}^{-1} \cdot \overline{b}
\end{aligned}
$$

Multiplicative Inverses

- Multiplicative Inverse of a matrix: defined only for square matrix
- Inverses: $\boldsymbol{A} \times \boldsymbol{B} = \boldsymbol{B} \times \boldsymbol{A} = \boldsymbol{I}$
- A square matrix may or may not have an inverse, but a non-square matrix does not have an inverse
- Multiplicative inverse of (square) $\boldsymbol{A}$ exists only if $det(\boldsymbol{A})$ has an inverse in the ring.
- There are efficient algorithms to compute determinants and inverses of matrices: *please review them*.
- Integers (infinite set $\mathbb{Z}$) have no inverses, no integer matrices have no inverses, unless their determinant is ± 1.
- In Crypto: we use matrices over $\mathbb{Z}_n$ – called residue matrices

Cofactors, Adjugate and Inverse

Cofactor of an element $a_{ij} \in \boldsymbol{A}$ is a number $C_{ij} = (-1)^{i+j} M_{ij}$
M_{ij} is the minor of the element a_{ij}

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Minor of $a_{12} = \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$ (determinant)
Minor of a_{ij} is the determinant obtained by removing i-th row and j-th column of $\boldsymbol{A}$

Cofactor, Adjugate and Inverse

$C_{ij} = (-1)^{i+j} M_{ij}$

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$\text{Minor}(\boldsymbol{A}) = \begin{bmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{bmatrix}$$

$$\boldsymbol{C} = \text{Cof}(\boldsymbol{A}) = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix}$$

- Adjugate of $\boldsymbol{A}$ = transpose of the cofactor matrix $\boldsymbol{C}$ of $\boldsymbol{A}$: $Adj(\boldsymbol{A}) = \boldsymbol{C}^T$

Remember the following results:

$Det(\boldsymbol{A}) \cdot \boldsymbol{I} = Adj(\boldsymbol{A}) \cdot \boldsymbol{A}$ and therefore Inverse: $\boldsymbol{A}^{-1} = \frac{1}{det(\boldsymbol{A})} Adj(\boldsymbol{A})$.

Residue Matrices

- Cryptography uses residue matrices where every operation is performed in $\mathbb{Z}_n$, i.e. computed $\pmod{n}$: Add, subtract of multiply elements $\pmod{n}$
- You can use the SINGULAR Computer Algebra Tool to perform matrix operations in $\mathbb{Z}_n$
- The SINGULAR tool is installed in the CADE lab, and also available for free download from `https://www.singular.uni-kl.de`. See info on Canvas.

Matrix Inverses in $\mathbb{Z}_n$

A square matrix $\boldsymbol{A}$ has an inverse in $\mathbb{Z}_n$ iff $gcd(det(A), n) = 1$.

Given a demo of Singular in Class!

Application: Solve Linear Congruences

$$\begin{aligned} 3x + 5y + 7z &\equiv 3 \pmod{16} \\ x + 4y + 13z &\equiv 5 \pmod{16} \\ 2x + 7y + 3z &\equiv 4 \pmod{16} \end{aligned}$$

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \pmod{16}$$

$$\boldsymbol{A} \cdot \overline{x} \equiv \overline{b} \pmod{16}$$

$$\overline{x} \equiv \boldsymbol{A}^{-1}\overline{b} \pmod{16}$$

Solution to this congruence: $x = 15, y = 4, z = 14$. Solve using Singular!

Solve Linear Congruence Systems: Non-Invertible Matrix

$$\boldsymbol{A} \cdot \overline{x} \equiv \overline{b} \pmod{n}$$
$$\overline{x} \equiv \boldsymbol{A}^{-1}\overline{b} \pmod{n}$$

- When $\boldsymbol{A}^{-1}$ exists in $\mathbb{Z}_n$, then the above congruence has a unique solution, which can be computed above.
- When $\boldsymbol{A}^{-1}$ does not exist, then the system may have no solutions, or multiple solutions.

Theorem (The number of solutions to a linear congruence system)

Given the linear congruence $\boldsymbol{A}x \equiv b \pmod{m}$, the number of solutions η is bounded by $\eta \leq \mathrm{GCD}(det(A), m)$.

Solution Count

Theorem (The number of solutions to a linear congruence system [1])

Given the linear congruence $\boldsymbol{A}x \equiv b \pmod{m}$, the number of solutions η is bounded by $\eta \leq \mathrm{GCD}(det(A), m)$.

Proof.

$$
\begin{aligned}
\boldsymbol{A}x &\equiv b \pmod{m} \\
Adj(\boldsymbol{A}) \cdot \boldsymbol{A}x &\equiv Adj(\boldsymbol{A})b \pmod{m} \\
Det(\boldsymbol{A})x &\equiv Adj(\boldsymbol{A})b \pmod{m} \qquad (1)
\end{aligned}
$$

Eqn. (1) has solutions if and only if the determinant $GCD(Det(\boldsymbol{A}), m)$ divides <u>all the elements</u> in $Adj(\boldsymbol{A})b$. Then $\eta \leq \mathrm{GCD}(det(\boldsymbol{A}), m)$. Otherwise, the system has no solutions. When $GCD(Det(\boldsymbol{A}), m) = 1$ then $\eta = 1$. □

The reason for $\eta \leq GCD(det(\boldsymbol{A}), m)$

$$\boldsymbol{A}x \equiv b \pmod{m}$$
$$Adj(\boldsymbol{A}) \cdot \boldsymbol{A}x \equiv Adj(\boldsymbol{A})b \pmod{m}$$
$$Det(\boldsymbol{A})x \equiv Adj(\boldsymbol{A})b \pmod{m}$$

- We multiply the congruence by $Adj(\boldsymbol{A})$
- Multiplying a congruence relation with an integer may introduce more solutions:
- $2x \equiv 6 \pmod{8}$: solution $x = 3, 7$
- $4x \equiv 4 \pmod{8}$: solution $x = 1, 3, 5, 7$
- In a "system of congruences", some of these extra solutions may not lift.

How to Solve?

- Many algorithms to solve
- Basic idea: solve the system using Gaussian elimination.
- For row reductions, i.e. to perform elimination, we cannot always use division, due to lack of inverses in $\mathbb{Z}_n$.
- For elimination, we have to use MULT, ADD, SUB operations on rows. However, multiplication by numbers not coprime to the modulus may create extraneous non-solutions.

Explain with Example: Triangularization

Consider the system of linear congruences $\pmod{16}$

$$
\begin{aligned}
2x + 5y + 7z &\equiv 3 \pmod{16} \\
x + 4y + 13z &\equiv 5 \pmod{16} \\
2x + 7y + 3z &\equiv 4 \pmod{16}
\end{aligned}
$$

$$
\begin{bmatrix} 2 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \pmod{16}
$$

$$
\boldsymbol{A} \cdot x \equiv b \pmod{16}
$$

$det(\boldsymbol{A}) = 14$, which has no onverse in $\mathbb{Z}_{16}$.

$Adj(\boldsymbol{A}) \cdot b = \begin{bmatrix} 9 \\ 9 \\ 5 \end{bmatrix}$: No solution, because $GCD(14, 16) = 2 \nmid 9, 5$.

Triangularization with Congruences

Construct the augmented matrix with the output column vector. Note: Perform these computations $\pmod{16}$:

$$\begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 1 & 4 & 13 & \vdots & 5 \\ 2 & 7 & 3 & \vdots & 4 \end{bmatrix}$$

Cannot divide row r_3 by 2 in $\mathbb{Z}_{16}$. Do: $r_3 = r_3 - r_1$:

$$\begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 1 & 4 & 13 & \vdots & 5 \\ 0 & 2 & 12 & \vdots & 1 \end{bmatrix}$$

Triangularize $\pmod{16}$

$$\begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 1 & 4 & 13 & \vdots & 5 \\ 0 & 2 & 12 & \vdots & 1 \end{bmatrix} \xrightarrow{r_2=2r_2} \begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 2 & 8 & 10 & \vdots & 10 \\ 0 & 2 & 12 & \vdots & 1 \end{bmatrix} \xrightarrow{r_2=r_2-r_1}$$

$$\begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 0 & 3 & 3 & \vdots & 7 \\ 0 & 2 & 12 & \vdots & 1 \end{bmatrix} \xrightarrow{r_3=3r_3, r_2=2r_2} \begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 0 & 6 & 6 & \vdots & 14 \\ 0 & 6 & 4 & \vdots & 3 \end{bmatrix} \xrightarrow{r_3=r_3-r_2}$$

$$\begin{bmatrix} 2 & 5 & 7 & \vdots & 3 \\ 0 & 6 & 6 & \vdots & 4 \\ 0 & 0 & 14 & \vdots & 5 \end{bmatrix} \pmod{16}$$

Last congruence: $14z \equiv 5 \pmod{16}$ has no solutions. See HW for congruences with multiple solutions.

M. Nilsson and R. Nyqvist. *Number of Solutions of Linear Congruence Systems*, Math arXive: arXiv:1208.3550v3, https://arxiv.org/abs/1208.3550v3.