MATH 201: Linear Algebra
Week 4

Today:

1. Matrix multiplication (quickly)
2. Inverses!
3. Image and Kernel

Matrix Products

Definition:

a. Let B be an $n \times p$ matrix and A a $q \times m$ matrix. The product BA is defined if and only if $p = q$.

b. If B is an $n \times p$ matrix and A is a $p \times m$ matrix then BA is the matrix of the linear transformation $T(\vec{x}) = (A \circ B)(\vec{x}) = B(A(\vec{x}))$.

* Why is this the same as the "row times column" rule?

$$\begin{bmatrix} 3 & 2 & 1 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 4 & 5 & 6 \\ 2 & 7 & 0 & 1 \\ 3 & 2 & 4 & 5 \end{bmatrix} = \begin{bmatrix} (3\cdot1)+(2\cdot2)+(1\cdot3) & (3\cdot4)+(2\cdot7)+(1\cdot2) & \bullet & \bullet \\ (4\cdot1)+(5\cdot2)+(6\cdot3) & (4\cdot4)+(5\cdot7)+(6\cdot2) & \bullet & \bullet \end{bmatrix}$$

$2 \times \boxed{3} \longleftrightarrow \boxed{3} \times 4$

(2×4)

$$\begin{bmatrix} 3 & 2 & 1 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 4 & 5 & 6 \\ 2 & 7 & 0 & 1 \\ 3 & 2 & 4 & 5 \end{bmatrix} = \begin{bmatrix} (3\cdot1)+(2\cdot2)+(1\cdot3) & (3\cdot4)+(2\cdot7)+(1\cdot2) & \bullet & \bullet \\ (4\cdot1)+(5\cdot2)+(6\cdot3) & (4\cdot4)+(5\cdot7)+(6\cdot2) & 6 & \bullet \end{bmatrix}$$

$2 \times 3 \longleftrightarrow 3 \times 4$ $\quad (2 \times 4)$

A $\quad B$ $\quad A \cdot B$

$T_A : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ $\qquad T_B : \mathbb{R}^4 \longrightarrow \mathbb{R}^3$

$(T_B \circ T_A) : \mathbb{R}^4 \xrightarrow{T_B} \mathbb{R}^3 \xrightarrow{T_A} \mathbb{R}^2$

$T_{AB} : \mathbb{R}^4 \longrightarrow \mathbb{R}^2$

The matrix multiplication $A \cdot B$ corresponds to the composition $(T_B \circ T_A)$

Linear Transformation

Def 1: A function $T : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ such that

1. $T(\vec{x} + \vec{y}) = T(\vec{x}) + T(\vec{y})$
2. $T(k\vec{x}) = k\,T(\vec{x})$

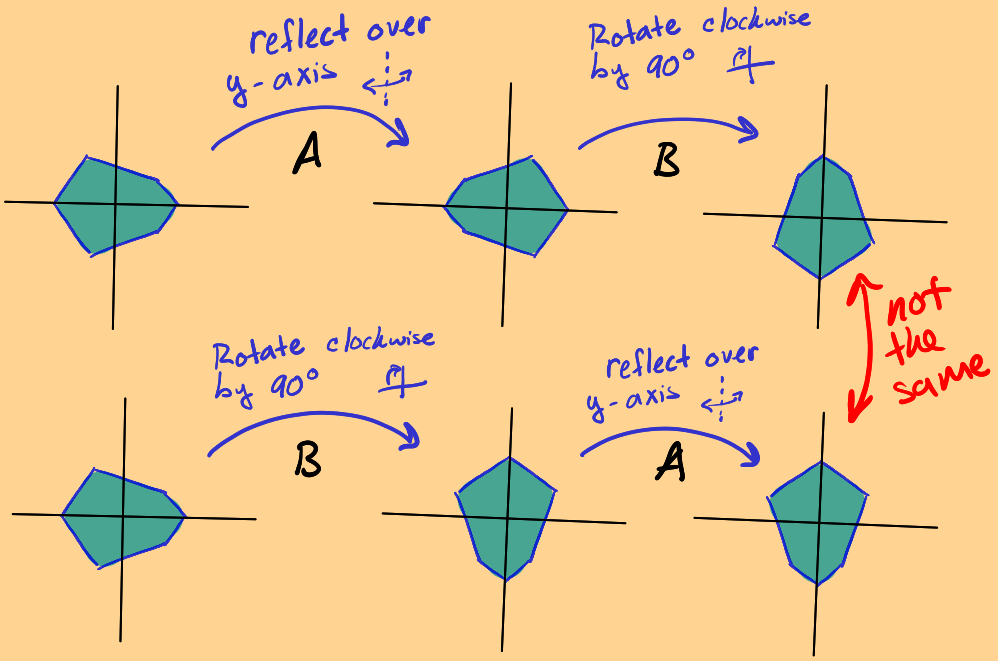
↕ equivalent.

Def 2: A function $T : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ such that there exists an $n \times m$ matrix satisfying

$$T(\vec{x}) = A\vec{x} \quad \forall \ \vec{x} \in \mathbb{R}^m$$

"for all"

Theorem: Matrix multiplication is non-commutative!



* Which matrices commute with <u>all</u> others?

* For various shapes, which symmetries commute?

$A \cdot B \neq BA$

Exercise: Find two matrices A, B such that

1. AB <u>and</u> BA are defined
2. $AB \neq BA$

Break: Come back at 5:10

Other Properties...

$I_n = \begin{bmatrix} 1 & & 0 \\ & 1 & \\ 0 & & 1 \end{bmatrix}$ "identity matrix"

* Identity	$A \cdot I = I \cdot A = A$
* Associativity	$(AB)C = A(BC)$
* Distributive Property	$A(C + D) = AC + AD$
* Commutativity of scalar multiplication	$(kA)B = A(kB)$

$(n \times p) \cdot (q \times m)$ — the same

Definition: $T: X \longrightarrow Y$ is called *invertible* if $T(x) = y$ has a <u>unique</u> solution $x \in X$ for each $y \in Y$.

* This is also called "one-to-one"

In this case, the function $T^{-1}: Y \longrightarrow X$ defined by

$$T^{-1}(y) = x \iff y = T(x)$$

is called the *inverse*.

- $T^{-1}(T(x)) = x$ and $T(T^{-1}(x)) = x$
- If $L: Y \longrightarrow X$ and $L(T(x)) = T(L(x))$ then $L = T^{-1}$
- $(T^{-1})^{-1} = T$

Definition: A matrix is called *invertible* if $T(x) = Ax$ is inveritble.

Conditions for invertibility: An <u>n x n</u> matrix A is invertible iff

1. $\text{rref}(A) = I_n$
2. $\text{rank}(A) = n$

Theorem: Let A be $n \times n$.

a) If A is invertible, $A\vec{x} = \vec{b}$ has the unique solution $\vec{x} = A^{-1}\vec{b}$.
If A is not invertible, $A\vec{x} = \vec{b}$ has infinitely many or no solutions.

b) Consider the special case where $\vec{b} = \vec{0}$. Then $A\vec{x} = \vec{b}$ is <u>always</u> solved by $\vec{x} = \vec{0}$. If A is invertible then $\vec{x} = \vec{0}$ is the <u>only</u> solution.
If A is not invertible, then $A\vec{x} = \vec{0}$ has infinitely many solutions.

A is inv. iff $A\vec{x} = \vec{0} \Rightarrow \vec{x} = \vec{0}$

kernel:

A is inv. $\iff$ $\ker(A) = \{\vec{0}\}$

How do we find the inverse?

- Compute $\text{rref}[A \mid I_n]$

If you get $[I_n \mid B]$
- A is invertible
- $B = A^{-1}$

If you don't get $[I_n \mid B]$ then A is <u>not</u> invertible.

Properties

- $(BA)^{-1} = A^{-1}B^{-1}$
- $AA^{-1} = A^{-1}A = I_n$

Examples.

- Is $A = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$ invertible? If so, find the inverse.
- Suppose $ABC = (AB)C = I_n$. Show B is invertible and compute B^{-1} in terms of A and C.
- Prove: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible iff $ad - bc \neq 0$.
- Prove: If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible then

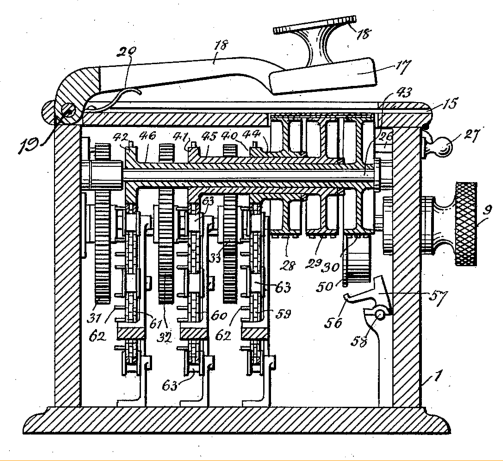
$$A^{-1} = \underbrace{\frac{1}{ad-bc}}_{\text{determinant}} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Cryptography

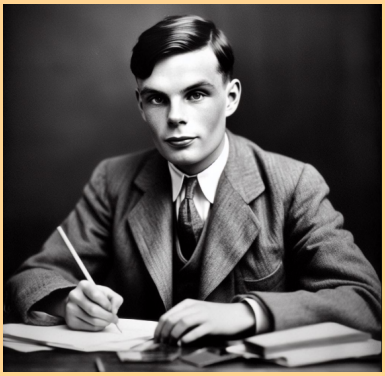
Message

↓ Really cool math...

Secret Code



Hill Cipher Machine



Alan Turing

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Each letter corresponds to a number modulo 26.

$$38 - 26 = 12$$

FIRE $\rightsquigarrow \begin{bmatrix} 5 \\ 8 \\ 17 \\ 4 \end{bmatrix}$ $\quad \begin{bmatrix} 5 \\ 8 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \end{bmatrix}$

key

$$\begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 5 \\ 8 \end{bmatrix} = \begin{bmatrix} 10+8 \\ 5-8 \end{bmatrix} = \begin{bmatrix} 18 \\ -3 \end{bmatrix} = \begin{bmatrix} S \\ X \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 34+4 \\ 17-4 \end{bmatrix} = \begin{bmatrix} 38 \\ 13 \end{bmatrix} = \begin{bmatrix} M \\ N \end{bmatrix}$$

Encoded message: SXMN

$$A \begin{bmatrix} F \\ I \end{bmatrix} = \begin{bmatrix} S \\ X \end{bmatrix}$$

$$A^{-1} \begin{bmatrix} S \\ X \end{bmatrix} = \begin{bmatrix} F \\ I \end{bmatrix}$$