Matrices

Alex Shaffer

Matrices

- Matrices are collections of numbers organized into a rectangular array.
- A matrix with n rows and m columns is a $\mathrm{n} \times m$ matrix.
- $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is an example of a 2x2 matrix.

Matrix Addition

- Matrices have a special type of algebra with its own multiplication and addition.
- To add matrices, we just add elements in the same position.
  - You can only add matrices of the same dimensions together.
  - $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$

Matrix Scalar Multiplication

- In the context of matrix algebra, a scalar is just a number.
  - You can multiply matrices by scalars, and it just distributes out to all of its elements.
  - $3 \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 9 & 12 \end{pmatrix}$

Matrix Multiplication

- You can multiply matrices of dimension $n \times k$ by $k \times m$
  - They must both have the same inner dimension.
  - This produces a matrix of dimension $n \times m$
  - The order of the multiplication matters. Unlike multiplying numbers matrices do not always commute.
  - To do the multiplication you multiply element-wise rows from the first matrix with columns from the second matrix and add those values up.
    - The value from row 1 column 2 will be places in position (1, 2) in the resulting matrix.

Matrix Multiplication Examples

- $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 1\cdot 2 & 1\cdot 2 + 1\cdot 1 \\ 1\cdot 1 + (-1)\cdot 2 & 1\cdot 2 + (-1)\cdot 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ -1 & 1 \end{pmatrix}$

- $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 6 \\ 6 & 6 \end{pmatrix}$

The Identity Matrix

- When multiplying numbers, 1 is the identity.
  - This just means multiplying by one leave the value unchanged.
  - The identity for addition is 0.
- For matrix multiplication the identity matrix is:
  - $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for 2×2
  - $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ for 3×3
  - That pattern continues

Matrix Determinant

- For a square matrix, the determinant is a property of that matrix. It has geometric properties associated corresponding linear transformations. If you are curious watch this.
  - For us we will only worry about 2×2 matrix determinants.
  - For the matrix $\mathrm{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ its determinant written $\det(M) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \mathrm{ad} - \mathrm{bc}.$

Inverse Matrices

- Some square matrices have inverses.
  - If M is a matrix with is an inverse, and M^{-1} is its inverse. Then $\mathrm{M}^{-1}\mathrm{M} = MM^{-1} = I$.
  - Inverse matrices can be challenging to calculate we will only concern ourselves with 2×2 matrices.
  - Matrix inverse only exists if the determinant is 1.
  - For a 2×2 matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we get $M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
  - Let's check for ourselves that this is right.
    - $\frac{1}{ad-bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} ad - bc & -ab + ab \\ cd - cd & ad - bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Inverse Matrix Example

- Consider the matrix $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$
  - $\det(M) = 4 - 6 = -2$
  - $M^{-1} = \frac{-1}{2}\begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$

Vectors

- Vectors have lots of definitions based on the context but usually roughly refer to the same type of object with some definitions just being more general that others.
  - In physics a vector is referred to as something with magnitude and direction.
  - In linear algebra a vector is an element of a vector space.
  - In differential geometry a vector is a rank 1 contravariant tensor.
- For us a vector will be a $n \times 1$ matrix.
  - $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is a 2×1 vector.

Matrix-Vector Multiplication

- Just a special case of matrix-matrix multiplication.
  - $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 0 \\ 2 \cdot 1 + (-1) \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$
- Sometimes we will encode plaintext/ciphertext as a vector.

The Hill Cipher

- The hill cipher uses square invertible matrices as keys.
  - For a key matrix K of size $n \times n$. We can encode blocks of n letter (represented as integers).
  - The determinant of the matrix must be coprime with 26.
  - $E(x) = Kx \pmod{26}$
    - where x is a vector of length n.
- Decryption uses a decryption key $K^{-1}\ (mod\ 26)$
  - $D(x) = K^{-1}x\ (mod\ 26)$

Hill Cipher Encryption Example

- Let's use the encryption matrix.
  - $K = \begin{pmatrix} b & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$
- Consider the plaintext example: "Hello world"
  - We have an even number of total letters; we will encrypt 2 at a time.
    - Converted to numbers: [7, 4, 11, 11, 14, ' ', 22, 14, 17, 11, 3]

Hill Encryption Continued

- Now to do out matrix vector multiplication:
  - $\begin{pmatrix}1 & 1\\2 & 3\end{pmatrix}\begin{pmatrix}7\\4\end{pmatrix}$(mod 26) = $\begin{pmatrix}11\\26\end{pmatrix}$(mod 26) = $\begin{pmatrix}11\\0\end{pmatrix}$
  - $\begin{pmatrix}1 & 1\\2 & 3\end{pmatrix}\begin{pmatrix}11\\11\end{pmatrix}$ (mod 26) = $\begin{pmatrix}22\\55\end{pmatrix}$(mod 26) = $\begin{pmatrix}22\\3\end{pmatrix}$
  - $\begin{pmatrix}1 & 1\\2 & 3\end{pmatrix}\begin{pmatrix}14\\22\end{pmatrix}$ (mod 26) = $\begin{pmatrix}36\\94\end{pmatrix}$(mod 26) = $\begin{pmatrix}10\\16\end{pmatrix}$
  - $\begin{pmatrix}1 & 1\\2 & 3\end{pmatrix}\begin{pmatrix}14\\17\end{pmatrix}$ (mod 26) = $\begin{pmatrix}31\\79\end{pmatrix}$(mod 26) = $\begin{pmatrix}5\\1\end{pmatrix}$
  - $\begin{pmatrix}1 & 1\\2 & 3\end{pmatrix}\begin{pmatrix}11\\3\end{pmatrix}$ (mod 26) = $\begin{pmatrix}14\\31\end{pmatrix}$(mod 26) = $\begin{pmatrix}14\\5\end{pmatrix}$
- lawdk qfbof

Hill Decryption

- Now let's invert our in encryption matrix:
  - $K = \begin{pmatrix} b & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \rightarrow K^{-1}(mod\ 26) = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}(mod\ 26) =$

    $\begin{pmatrix} 3 & 25 \\ 24 & 1 \end{pmatrix}$
  - Now we want to decrypt: "lawdk qfbof"