Linear System of Equations

- (lowkey review of MATH 221)
- linear system of equation

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

  - x_j are variables and we want to solve for them; while a_j are coefficients
  - each eq above is a linear eq (nothing is squared)
  - we want to solve for a set of sols (if any exists) for $x_1, \ldots h_n$ such that all m equations are satisfied
- writing the system in matrix form

$$\underbrace{\begin{bmatrix} a_{11} & a_{12} & \ldots a_{1n} & \\ a_{21} & a_{22} & \ldots a_{2n} & \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots a_{mn} & \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}}_{x} = \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}}_{b}$$

$$Ax = b$$

  - $A = (m \times n), x = (n \times 1), b = (m \times 1)$
- <u>fact</u>: every linear system with m equations, n unknowns (all real values) can be expressed as a matrix equations $Ax = b$ where $A \in \mathbb{R}^{m \times n}$, $x \in \mathbb{R}^n$, $b \in \mathbb{R}^m$
- **<u>Gaussian Elimination (GE)</u>**: how we solve for linear equations
  1. Form the "augmented matrix" from $Ax = b$

$$[A \mid b]$$

  2. Do row reduction using elementary row operations until the augmented matrix is in row echelon form (REF)
- elementary row operations:
  1. add multiple of a row to another
  2. multiply a row be a non-zero scalar
  3. interchange two rows
- <u>row echelon form</u>

$$\left[\begin{array}{cccccc|c} 0 & 0 & \blacksquare & x & x & x & b_1 \\ 0 & 0 & 0 & 0 & \blacksquare & x & b_2 \\ 0 & 0 & 0 & 0 & 0 & \blacksquare & b_3 \end{array}\right]$$

  - all non-zero rows at the bottom
  - first non-zero entry (called a <u>pivot</u>) in any row is to the right of the pivot in any row above it
  - note: if all pivot entries are 1 and all entries above the pivot are 0, then we have a matrix in <u>reduced row echelon form</u> (RREF)
  - example: TODO (maybe)
- **<u>rank</u>** (of a matrix): the number of non-zero rows in REF of a matrix
  - this number is unique to the matrix
  - can also be defined as the number of linearly independent rows OR the number of pivots
  - **theorems**
    1. The system $Ax = b$ has no solutions (the system is inconsistent) when $\text{rank}(A) < \text{rank}([A \mid b])$
    2. Suppose A is $(m \times n)$, then $Ax = b$ has a unique solution iff $\text{rank}(A) = \text{rank}([A \mid b]) = n$ (number of columns/variables)
    3. Iff $\text{rank}(A) = \text{rank}([A \mid b]) < n$, then there are $n - \text{rank}(A)$ free variables and the system has ∞ solutions
- special case: square matrix
  - suppose A is a $(n \times n)$ matrix and $\text{rank}(A) = n$, then $Ax = b$ has a unique solution regardless of b
  - in fancier terms: the map $f : x \in \mathbb{R}^n \to Ax \in \mathbb{R}^n$ is an invertible function (or: linear transformation)
    - $\to$ i.e for every $y \in \mathbb{R}^n$, there exists $x \, in\mathbb{R}^n$ such that $Ax = y$
  - so, we define the inverse of A as: $y = Ax \longrightarrow x = A^{-1}y$
  - facts about this inverse
    1. A^{-1} is also an $(n \times n)$ matrix
    2. $(A^{-1})^{-1}$ exists and is equal to A
    3. for square matrices w/ non-zero determinant, you can find its inverse
- recall: the identity matrix

$$\begin{aligned} I_n &= (n \times n) \text{ Identity Matrix} \\ &= \text{ matrix w/ 0s everywhere, 1s on the diagonal} \end{aligned}$$

  - I_n takes on the role of "the number one" in matrix computation, that is

$$\begin{aligned} I_n \times x &= x & & x \, in\mathbb{R}^n \\ I_n \times A &= A & & A \in \mathbb{R}^{m \times n} \\ A \times A^{-1} &= I_n & & \text{(only if A is square-invertible)} \end{aligned}$$

- <u>theorem</u>: Suppose $A \in \mathbb{R}^{m \times n}$ and $\text{rank}(A) = n$ (full rank), then
  1. A^{-1} exists is an $(n \times n)$ matrix
  2. $A(A^{-1}) = (A^{-1})A = I_n$
  - <u>points is</u>: when solving linear system $Ax = b$ w/ an invertible A, solution given by $x = A^{-1}b$
- **<u>Finding the Inverse</u>**: typically do $[A \mid I_n]$ then do GE to REF which gives $[I_n \mid A^{-1}]$
  - (so reduce until you get I_n on the LHS, whatever on the RHS is the inverse)
  - example: TODO

LU Decomposition

- computational motivation: suppose we want to solve many large linear system $Ax = b; Ax = c; Ax = d, \ldots$ where A is a common (the same) but the RHS $b, c, d, \ldots$ are different
  - for each linear system, we need to do GE to get to REF

$$\begin{aligned} &[\ A \mid b\ ] \longrightarrow \ldots \\ &[\ A \mid c\ ] \longrightarrow \ldots \\ &[\ A \mid d\ ] \longrightarrow \ldots \end{aligned}$$

    however, the **steps** to do GE to get to REF <u>only depend on A</u>
  - goal: record the steps of GE and use it repeatedly with however many different RHS we have (this is what LU aims to do)

- What is LU decomposition? It is a factorization of A in the form

$$
\begin{aligned}
A &= LU \\
U &= \text{REF}(A) \\
L &= \text{matrix that encodes steps of GE}
\end{aligned}
$$

  - L is a unit lower triangular matrix and U is called an upper triangular matrix (see below)
- definitions
  1. Lower triangular matrix: all entries above the main diagonal are 0

$$
\begin{bmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \\ * & * & * \end{bmatrix} \quad \begin{bmatrix} * & 0 & 0 & 0 \\ * & * & 0 & * \\ * & * & * & 0 \end{bmatrix} \quad \begin{bmatrix} * & 0 \\ * & * \\ * & * \\ * & * \end{bmatrix}
$$

     - in other words $a_{ij} = 0 \; \forall \; i < j$
     - the stars can be anything
  2. Unit lower triangular matrix: it's a square lower triangular matrix with all ones on the main diagonal
     - stars can still be anything
  3. Upper triangular & unit upper triangular matrix: same as lower but just opposite
- row operation matrices: matrices that perform row operations when mutiplied with another matrix
  1. Swapping Rows: you take the identity matrix, then you apply the row operation **to the identity matrix**
     - ex. swap row 2 and 3 for the matrix A below

$$
P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}
$$

     (we swapped row 2 and 3 of the identity matrix)
  2. Multiply row i by a scalar s: we have $A \longrightarrow DA$ where D is I_n where the i-th diagonal entry is replaced with s
  3. Add c times row j to row i ($i \neq j$): replace the entry in the i-th row and j-th column with the value c
     - we basically do `A[i][j] = c`
     - example: TODO
     - note: for this matrix, its matrix is particularly easy to get, just flip the c entry to $-c$
- want: compute the LU decomposition of a matrix (if it exists)
  - solution: do Gaussian Elimination
  - that is:

$$
\begin{aligned}
A \longrightarrow E_1(A) \longrightarrow E_2(E_1(A)) \longrightarrow \ldots \longrightarrow \text{REF}(A) \\
\therefore \underbrace{\text{REF}(A)}_{U} = E_j \cdot E_{j-1} \cdot \ldots \cdot E_2 \cdot E_1 \cdot A
\end{aligned}
$$

$$
\begin{aligned}
U &= (E_j \ldots E_2 E_1)A \\
\therefore A &= (E_j \ldots E_2 E_1)^{-1} U \\
&= \underbrace{(E_1{}^{-1} E_2{}^{-1} \ldots E_j{}^{-1})}_{L} U
\end{aligned}
$$

  - example: find the LU decomposition of

$$
\begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 4 \\ -1 & 0 & 1 \end{bmatrix}
$$

solution:

$$
\begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 4 \\ -1 & 0 & 1 \end{bmatrix} \xrightarrow{-3R_1+R_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ -1 & 0 & 1 \end{bmatrix}
$$

$$
\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ -1 & 0 & 1 \end{bmatrix} \xrightarrow{R_1+R_3} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} = \text{REF}(A) = U
$$

thus we have

$$
E_1 = -3R_1 + R_2 = \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
$$

$$
E_2 = R_1 + R_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}
$$

$$
\begin{aligned}
U &= E_1 E_2 A \\
\therefore A &= E_2{}^{-1} E_1{}^{-1} U \\
&= \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_{E_1{}^{-1}} \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}}_{E_2{}^{-1}} \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix}}_{U} \\
&= \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix} = LU
\end{aligned}
$$

  - the steps above is general and can be stated as a theorem
- **theorem**: if a matrix A can be reduced to REF by GE without swapping rows, then A has an LU decomposition
  - def: we say A has an LU decomposition if $A = LU$ where L is unit lower triangular and U is upper triangular.
- using LU decomposition to solve linear systems: the usual set up is that we have the same A but multiple different b's - currently we have

$$
Ax = b \Longrightarrow (LU)x = b
$$

  1. Let $Ux = y$, so we solve $Ly = b$ for $y \longrightarrow$ should be easy bc L is a lower unit triangular matrix (use forward sub)
  2. Solve $y = Ux$ for $x \longrightarrow$ can do backward sub
  - example: let

$$
\begin{aligned}
A &= \begin{bmatrix} 2 & 4 & 4 \\ -1 & -1 & 3 \\ 3 & 4 & 5 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 \\ -1/2 & 1 & 0 \\ 3/2 & -2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 9 \end{bmatrix} \quad \text{(no work shown)}
\end{aligned}
$$

    1. Let $LUx = b$, set $Ux = y$ and solve $Ly = b$

$$
\begin{bmatrix} 1 & 0 & 0 \\ -1/2 & 1 & 0 \\ 3/2 & -2 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 6 \end{bmatrix}
$$

       Solving, we can see that $y = [y_1, y_2, y_3] = [2, 3, 9]$
    2. Solve $Ux = y$ for x

$$
\begin{bmatrix} 2 & 4 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 9 \end{bmatrix}
$$

       Solving, we can get $x = [1, -2, 6]$
- other useful facts about LU
  - $\text{rank}(A) = \text{rank}(U)$
  - if A is square, $\det(A) = \det(U) =$ product of diag entry of$U$

Error Analysis

Vector Norms

- norms of vectors: norms on $\mathbb{R}^n$ assigns a magnitude (size) to vectors in $\mathbb{R}^n$
  - ex. $n = 1$: in $\mathbb{R}$ the absolute value of x, $|x|$ does the job
  - ex. $n = 2$: let $\vec{x} =< x_1, x_2 >$, the typical norm is the Euclidean norm (aka 2-norm)

$$\|x\| = \sqrt{|x_1^2| + |x_2^2|}$$

  → note that the 2-norm can be used in n-dimension

- definition: a function $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}^n$ is a norm iff
  1. $\|x\| > 0, \ \forall \ x \in \mathbb{R}^n$
  2. $\|x\| = 0$ if and only if $x = \vec{0}$ (the zero-vector)
  3. $\|cx\| = |c| \cdot \|x\|, \ \forall \ c \in \mathbb{R}, \ \ \forall \ x \in \mathbb{R}^n$
  4. $\|x + y\| \leq \|x\| + \|y\|$ (known as the triangle inequality)
- examples of other norms
  - 1-norm: it's the sum of all the absolute value of the components (aka Manhattan Distance)

$$\|x\|_1 = |x_1| + |x_2| + \ldots + |x_n|$$

  - p-norm: let $1 \leq p < \infty$ on $\mathbb{R}^n$

$$\|x\|_p := \left(\sum_{j=1}^{n} |x_j|^p \right)^{1/p}$$

  → note: when $p = 2$ that's the Euclidean norm and $p = 1$ then it's the 1-norm

  - ∞-norm:

$$\|x\|_\infty = \max\{|x_1|, \ldots, |x_n|\}$$

- remark: with any given norm, we can define the "distance" between 2 points in $\mathbb{R}^n$ (say x and y) as

$$\text{dist(x, y)} := \|x - y\|_t \qquad \text{where } t \text{ can be any norm}$$

- different norms can have different "geometry"
  - in $n = 2$ (we're in $\mathbb{R}^2$), we can def the unit circle in 2 ways

$$\begin{aligned} S_2 &:= \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x^2 + y^2 = 1, \quad x, y \in \mathbb{R} \right\} \\ &= \left\{ x \in \mathbb{R}^2 : \|x\|_2 = 1 \right\} \\ &= \text{all vector } \vec{x} \text{ such that the 2-norm of } \vec{x} \text{ is } 1 \end{aligned}$$

  - now if we wanted to define the "unit circle" as a 1-norm

$$S_1 = \left\{ x \in \mathbb{R}^2 : \|x\|_1 = 1 \right\}$$

  - so here "circle" no longer has the same geometric representation that we usually think of, instead we can define it as $\vec{x} \in \mathbb{R}^2 : \|x\|_p = 1$ for any norm p

Matrix Norms

- want: measure the magnitude (size) of a matrix in meaningful way
- definition of a norm is the same as before - they need to satisfy the 4 properties
- Frobenius (or Hibery-Schmidt) Norm: like the 2-norm for vectors

$$\text{let } A = [a_{ij}]_{m \times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

$$\|A\|_F = \|A\|_S = \sqrt{\sum_{j=1}^{n} \sum_{i=1}^{m} |a_{ij}|^2}$$

- Operator Norm: intuitively, it's calculating the maximum "stretching" capability of the matrix across all possible non-zero vectors
  - when you multiply a matrix and vector, you transform the vector - you stretch it by some factor

$$\|A\|_{\text{op}} = \|A\| = \max \left\{ \frac{\|Ax\|_2}{\|x\|_2} \right\}$$

  - we can also re-write the definition in another manner

$$\begin{aligned} \|A\|_{\text{op}} &= \max_{\|x\|=1} \|Ax\| \\ \|A^{-1}\|_{\text{op}} &= \frac{1}{\min\limits_{\|x\|=1} \|Ax\|_2} \end{aligned}$$

  - so $\|A\|$ is the maximum stretch of a unit vector by the linear transformation A while $\|A^{-1}\|$ is the reciprocal of the minimum stretch of a unit vector by the linear transformation A
  - operator norms have some special properties
    1. $\|A\| > 0$
    2. $\|A\| = 0$ iff A is a non-zero matrix
    3. $\|cA\| = |c|\|A\|$
    4. $\|A + B\| \leq \|A\| + \|B\|$
    5. $\|AB\| \leq \|A\| \cdot \|B\|$ (new)
    6. $\|Ax\|_2 \leq \|A\|_{\text{op}} \cdot \|x\|$
- solving operator norm: we will cover general case later, for now we'll only cover special cases
  - diagonal matrices: let D be a diagonal matrix, then the norm is the max magnitude of the diagonal entries

$$\|D\| = \max\{|d_{jj}|\}$$

  - permutation matrices: let P be the perm matrix (matrix obtained by shuffling rows of I)

$$\begin{aligned} \|P\| &= 1 && \text{for any permutation matrix} \\ \|PA\| &= \|A\| && \text{if } P \text{ is a permutation matrix} \end{aligned}$$

Condition Number

- we want to answer the question "how stable" is the solution with respect to small changes in b
- **definition**: the condition of a nonsingular (invertible) square matrix A is

$$\begin{aligned} \text{cond}(A) &= \|A\| \times \|A^{-1}\| \\ &= \frac{\text{max stretch of a unit vector}}{\text{min stretch of a unit vector}} \end{aligned}$$

  if A is singular, we have $\text{cond}(A) = \infty$

- **definition**: given a vector b and a small change Δb, the relative change (or relative error) is $\dfrac{\|\Delta b\|}{\|b\|}$

- **theorem**: Let A be a nonsingular matrix and consider the linear system $Ax = b$. If a small change Δb corresponds to a change Δx in the sense that $A(x + \Delta x) = (b + \Delta b)$ - we define the error bound

$$\frac{\|\Delta x\|}{\|x\|} \leq \text{cond}(A)\frac{\|\Delta b\|}{\|b\|}$$

  - this means that if A has a large condition number, then small changes in b may result in very large changes in x (solution x is sensitive to errors in Δb)
- for permutation matrix P

$$\begin{aligned} \text{cond}(P) &= 1 \\ \text{cond}(PA) &= \text{cond}(A) \end{aligned}$$

Interpolation

- interpolating function provides information about values between points and beyond the range of the data
  - note that there are infinitely many different ways to interpolate a set of data
- **definition**: given data $[(t_0, y_0), \dots, (t_d, y_d)]$, an interpolating function (or interpolant) is a function $f(t)$ such that $f(t_k) = y_k$ for $k = 0, \dots, d$

Polynomial Interpolation

- a polynomial of degree (at most) d is a function of the form

$$p(t) = c_0 + c_1 t + \dots c_d t^d, \quad c_i \in \mathbb{R}$$

  - note that there are $d + 1$ variables (because of c_0 as well)
  - we want to solve for c_i
- we have $d+1$ variables to solve for $\longrightarrow$ every data point gives an equation

$$P(t_j) = y_j$$

$$\text{i.e.} \quad \begin{aligned} P(t_0) &= c_0 + c_1 t_0 + \dots + c_d (t_0)^d = y_0 \\ P(t_1) &= c_0 + c_1 t_1 + \dots + c_d (t_1)^d = y_1 \\ &\vdots \\ P(t_d) &= c_0 + c_1 t_d + \dots + c_d (t_d)^d = y_d \end{aligned}$$

- re-write above into matrix form

$$\begin{bmatrix} 1 & t_0 & (t_0)^2 & \dots & (t_0)^d \\ & \ddots & & & \\ & & \ddots & & \\ & & & \ddots & \\ (t_d)^0 & (t_d)^1 & (t_d)^2 & \dots & (t_d)^d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_d \end{bmatrix}$$

  - problem of interpolation: **solve $\mathbf{Ac} = \mathbf{y}$ for $\mathbf{c}$**
- sidenote: Vandermonde matrix
  - the matrix A above is a Vandermonde matrix, generated by $t_0, t_1, \dots, t_d$
  - ex. Vandermonde matrix generated by $-2, 3, 5$

$$\begin{bmatrix} (-2)^0 & (-2)^1 & (-2)^2 \\ (3)^0 & (3)^1 & (3)^2 \\ (5)^0 & (5)^1 & (5)^2 \end{bmatrix}$$

  - **theorem**: let A be the Vandermonde matrix, then

$$\det(A) = \prod_{0 \leq i < j \leq d} (t_j - t_i)$$

    in simple terms: for a Vandermonde matrix constructed from numbers $x_1, x_2, \dots, x_n$, the determinant of the matrix, the determinant is the product of the differences between each pair of these numbers
  - in terms of interpolation: if the determinant of the Vandermonde matrix is zero, it implies that at least two x-coordinates used to construct the matrix are the same, this means generating a interpolant is impossible
- note: while invertible, the condition number of the Vandermonde matrix gets very large as d increases
  - as d increases, poly interpolation is not numerically stable
  - intuitively: more data = higher degree polynomial = very sensitive and oscillating function $\rightarrow$ not very useful

Cubic Spline Interpolation

- general idea: between every pair of adjacent points (t_i, t_{i+1}), we want to fit a cubic function then glue them together
- **definition**: consider $N + 1$ points $(t_0, y_0) \dots, (t_N, y_N)$, a **cubic spline** is a function $p(t)$ defined piecewise (made up of many parts) by N cubic polynomials $p_1(t), \dots, p_N(t)$ where

$$p_k(t) = a_k(t - t_{k-1})^3 + b_k(t - t_{k-1})^2 + c_k(t - t_{k-1}) + d_k$$

- we need to solve for (a_j, b_j, c_j, d_j) for $j = 1, 2, \dots, N \rightarrow$ we require $4N$ unknowns, thus we have to impose conditions to get $4N$ equations
  1. Interpolation at left endpoints (yield N equations)

$$p_k(t_{k-1}) = y_{k-1}, \qquad k = 1, \dots, N$$

     (basically saying left endpoint of this polynomial need to match the data)
  2. Interpolation at right endpoints (yield N equations)

$$p_k(t_k) = y_k, \qquad k = 1, \dots, N$$

  3. Continuity of $p'(t)$ (yield $N - 1$ equations)

$${p'}_k(t_k) = {p'}_{k+1}(t_k), \qquad k = 1, \dots, N - 1$$

  4. Continuity of p'' (yield $N - 1$ equations)

$${p''}_k(t_k) = {p''}_{k+1}(t_k), \qquad k = 1, \dots, N - 1$$

  5. Natural spline condition (yield 2 equations)

$${p''}_1(t_0) = {p''}_N(t_N) = 0$$

     note: there are different choices to get these extra 2 equations (i.e "not-a-knot" condition)
- **theorem**: for $N + 1$ points $(t_0, y_0), \dots (t_N, y_N)$ where $t_i \neq t_j$ for all $i \neq j$, a unique "natural" cubic spline $p(t)$ that interpolates these points can be constructed
  - term "natural" here means second derivatives of the spline at the endpoints are zero
  - can represent the cubic spline $p(t)$ by the coefficient matrix

$$C = \begin{bmatrix} a_1 & a_2 & \dots & a_N \\ b_1 & b_2 & \dots & b_N \\ c_1 & c_2 & \dots & c_N \\ d_1 & d_2 & \dots & d_N \end{bmatrix}$$

    where the k-th column of C consists of the coefficients for the k cubic polynomial in the spline, i.e

$$p_k(t) = a_k(t - t_{k-1})^3 + b_k(t - t_{k-1})^2 + c_k(t - t_{k-1}) + d_k$$

- turns out that we get the solutions to the first set of equations for free

$$d_k = y_{k-1} \quad \text{for } k = 1, \ldots, N$$

- the coefficients $a_1, b_1, c_1, \ldots, a_N, b_N, c_N$ are the solutions to the linear system

$$H = \left[\begin{array}{c|c|c|c|c} A(L_1) & B & & & \\ \hline & A(L_2) & B & & \\ \hline & & \ddots & \ddots & \\ \hline & & & A(L_{N-1}) & B \\ \hline T & & & & V \end{array}\right]$$

$$H \cdot \begin{bmatrix} a_1 \\ b_1 \\ c_1 \\ \vdots \\ a_N \\ b_N \\ c_N \end{bmatrix} = \begin{bmatrix} y_1 - y_0 \\ 0 \\ 0 \\ \vdots \\ y_N - y_{N-1} \\ 0 \\ 0 \end{bmatrix}$$

where $L_k = t_k - t_{k-1}$ = the length of the sub-interval $[t_{k-1}, t_k]$ and

$$A(L) = \begin{bmatrix} L^3 & L^2 & L \\ 3L^2 & 2L & 1 \\ 6L & 2 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -2 & 0 \end{bmatrix}$$

$$T = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad V = \begin{bmatrix} {L_N}^3 & {L_N}^2 & L_N \\ 0 & 0 & 0 \\ 6L_N & 2 & 0 \end{bmatrix}$$

- note: condition number of the matrix for constructing the natural cubic spline does not increase as drastically with the number of points like Vandermonde

Subspaces

- note: term vector refers to elements of $\mathbb{R}^n$ and scalar s refers to elements in $\mathbb{R}$
- **definition**: a subset $S \subseteq \mathbb{R}^n$ is a **subspace** iff $\forall\, u, v \in S,\ \forall\, a \in \mathbb{R}$
  1. $u + v \in S$ (S is closed under addition)
  2. $a \times u \in S$ (S is closed under scalar multiplication)

  another way to write this is (equiv to both statements above)

  $$\forall\, u, v \in S,\ \forall\, a \in \mathbb{R}, \quad au + bv \in S$$

  - remark: if S is a subspace, then $\vec{0}$ must be in S
- **definition**: given $\{v_1, v_2, \ldots, v_k\} \in \mathbb{R}^n,\ c_j \in \mathbb{R}$
  - the sum $\sum_{i=1}^k c_j v_j$ is a **linear combination** of $v_1, \ldots, v_k$
  - the set of all linear combination of $\{v_1, \ldots, v_k\}$ is its **span**

  $$\text{span}\{v_1, \ldots, v_k\} = \left\{ \sum_{j=1}^k c_j v_j, \quad c_j \in \mathbb{R} \right\}$$

    → in other words, it is the set of all vectors that can be obtained by scaling and adding these vectors together

    → for any $v_1, \ldots v_k \in \mathbb{R}^k$, span$\{v_1, \ldots, v_k\}$ is a subspace
  - $\{v_1, \ldots v_k\}$ is **linearly dependent** if there exists a case where $\sum_{i=1}^k c_j v_j = 0$ but not all c_j are 0

    → equivalently: at least 1 v_j can be expressed as linear combo of other vectors
  - $\{v_1, \ldots v_k\}$ is **linearly independent** if it is not linearly dependent

    → equivalently: $\sum_{j=1}^k c_j v_j = \vec{0} \iff c_j = 0$ for all j
- note: we can write linear combination as matrix multiplication (put each vector v_i as column of V)

$$\sum_{j=1}^k c_j v_j = \underbrace{[v_1 \mid v_2 \mid \ldots \mid v_k]}_{V} \underbrace{\begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix}}_{c}$$

  - this means that you can use the rank to check for linear independence
  - example: check if $\{[1,1,1]^T, [1,1,0]^T, [1,0,0]^T\}$ is linearly independent

  $$V = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \xrightarrow{\text{RREF}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

  This matrix has full rank so it is linearly independent (if less then it's dependent) - note that we could have done REF instead of RREF
- **definition**: a set $\{v_1, v_2, \ldots, v_k\} \subseteq S$ is a **basis** of S if
  1. span$\{v_1, \ldots, v_k\} = S$ (the set of vector spans S)
  2. $\{v_1, \ldots, v_k\}$ is linearly independent
  - in other words, the vectors in the basis can generate (or span) the entire space by linear combinations
  - so any vector in the vector space can be expressed as a unique linear combination of the basis vectors
  - remark: if $\{v_1, \ldots, v_k\}$ is linearly independent, then it is a basis for its span
  - equivalently: a set $\{v_1, v_2, \ldots, v_k\} \subseteq S$ is a **basis** of S iff
    1. $\forall\ u \in S,\ \exists\ c_1, c_2 \ldots c_k \in \mathbb{R}$ s.t $u = \sum_{j=1}^k c_j v_j$ (basically the span requirement above)
    2. the choice of c_j in 1) is unique (i.e only 1 way of expressing any vector)
  - remarks
    1. given a subspace, the choice of a basis is not unique
    2. however, given a subspace S, the number of vector in any basis of S must be the same - this number of vectors is called the dimension of S
    3. **theorem**: in a k-dim subspace S, any k linearly independent vectors for a basis for S

  Example: Find a basis and the dimension of S = span(u_1, u_2, u_3, u_4)

  $$u_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} u_2 = \begin{bmatrix} 2 \\ -3 \\ 1 \\ 0 \end{bmatrix} u_3 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} u_4 = \begin{bmatrix} 2 \\ -1 \\ 1 \\ 2 \end{bmatrix}$$

  important: the pivot columns indicates which u_i is indep.

  Let $U = [u_1\ u_2\ u_3\ u_4]$

  $$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & -3 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 2 \end{bmatrix} \xrightarrow{\text{RREF}} \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -5 & 2 & -3 \\ 0 & 0 & 2/5 & -2/5 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

  So we can say that $\{u_1, u_2, u_3\}$ is the basis for S and thus $\dim(S) = 3$
- if we found out that U = span$\{u_1, u_2, \ldots, u_k\}$ has dimension d, then any d linearly independent vector from the set $\{u_1, u_2, \ldots, u_k\}$ will form the basis for U

Null Spaces & Ranges

- recall: a matrix $A \in \mathbb{R}^{m\times n}$ can be interpreted as a linear map (function transformation) from $\mathbb{R}^n$ to $\mathbb{R}^m$

$$A : \mathbb{R}^n \longrightarrow \mathbb{R}^m \qquad \text{or} \qquad A : x \in \mathbb{R}^n \longrightarrow Ax \in \mathbb{R}^m$$

  - note: A is linear iff $\forall\ x_1, x_2 \in \mathbb{R}^n,\ \forall\ s_1, s_2 \in \mathbb{R}$

$$A(sx_1 + sx_2) = s_1 Ax_2 + s_2 Ax_2$$

- **definition**: <u>**null spaces**</u> of A

$$\begin{aligned} N(A) &= \{x \in \mathbb{R}^n : Ax = \vec{0}\} \subseteq \mathbb{R}^n \\ &= \text{solution set of } Ax = 0 \end{aligned}$$

  - fact: $N(A)$ is a subspace of $\mathbb{R}^n$
  - example: given A, find basis of $N(A)$ $\rightarrow$ means solve $Ax = 0$ (technically, want to solve for the basis of $N(A)$)

$$A = \begin{bmatrix} 1 & 3 & 3 & 10 \\ 2 & 6 & -1 & -1 \\ 1 & 3 & 1 & 4 \end{bmatrix} \xrightarrow{\text{RREF}} \begin{bmatrix} 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

x_1, x_3 are pivots and x_2, x_4 are free variables

let $x_2 = s, x_3 = t \rightarrow x_3 = -3t, x_1 = -3s - t$

$$\therefore N(A) = \left\{ \begin{bmatrix} -3s - t \\ s \\ -3t \\ t \end{bmatrix} : s, t \in \mathbb{R} \right\} = \left\{ s \begin{bmatrix} -3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} -1 \\ 0 \\ -3 \\ 1 \end{bmatrix} \right\}$$

$$= \text{span} \left\{ \begin{bmatrix} -3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ -3 \\ 1 \end{bmatrix} \right\} \text{ is the basis of } N(A)$$

  - geometrically, think of it as the "directions" or "vectors" that get mapped to zero by A when you apply it
  - it represents the subspace of vectors that get "collapsed" or "squished" to the origin when applied to A

- **definition**: <u>**range of** A</u> - assume that A is $m \times n$

$$\begin{aligned} R(A) &:= \{Ax : x \in \mathbb{R}^n\} \subseteq \mathbb{R}^m \\ &= \text{span}\{a_1, \ldots, a_k\} \\ &= \text{set of all possible linear combinations of its col} \\ &= \text{col}(A) = \text{"column space" of } A \end{aligned}$$

  - fact: $R(A)$ is a subspace of $\mathbb{R}^n$

- some important facts: let $A \in \mathbb{R}^{m\times n}$
  1. $\text{rank}(A) = \#$ of pivots $\leq \min(m, n)$
  2. $\dim(R(A)) = \#$ of pivots $= \text{rank}(A)$ (because the number linearly independent columns gives the basis)
  3. $\dim(N(A)) = \#$ of free variable $= n - \text{rank}(A)$

  - all things above lead to **Rank-Nullity Theorem**: For any $m \times n$ matrix A, $\dim(R(A)) + \dim(N(A)) = n$

- special case: if we have the LU decomposition of A and we want to find $R(A)$ and $N(A)$
  - <u>**theorem**</u>: let $A = LU$ be the LU decomposition of A and let $\text{rank}(A) = r$, then the first r <u>columns</u> of L forms the basis for $R(A) \longrightarrow$ that is, $R(A) = \text{span}\{l_1, \ldots, l_r\}$
  - and since L is invertible, we have

$$N(A) = N(LU) = N(U)$$

    so we just have to find $N(U)$ (meaning solve for $Ux = \vec{0}$)

    $\rightarrow$ proposition: suppose B is invertible $m \times n$ and A is any $m \times n$ matrix, then $N(BA) = N(A)$

- some remarks on A^T

$$A = [a_{ij}]_{m\times n} \qquad A^T = [a_{ji}]_{n\times m} \qquad (\text{rows} \rightarrow \text{columns})$$

  - $R(A^T) = R(U^T) =$ the first r <u>rows</u> of U

Orthogonality

- **definition**: the <u>**inner product**</u> (dot product) of two vectors $x = [x_1, \ldots, x_n]^T$ and $y = [y_1, \ldots, y_n]^T$ in $\mathbb{R}^n$ is

$$\begin{aligned} < x, y > &:= x \cdot y = x_1y_1 + x_2y_2 + \ldots + x_ny_n \\ &= \sum_{i=1}^{n} x_iy_i \end{aligned}$$

- important properties
  1. we can express it in matrix notation

$$< x, y >= x^T y = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

  2. $< x, y >=< y, x >$ (only true for real numbers)
  3. $< x, cy + dz >= c < x, y > +d < x, z >$ where $c, d \in \mathbb{R}$ and $x, y, z \in \mathbb{R}^n$
  4. $< x, Ay >=< A^T x, y >$ (memorize, always true for reals and any matrix A)
  5. the inner product induces the 2-norm (can write the 2-norm as inner product)

$$< x, x >= \sum_{i=1}^{n} x_i^2 = \|x\|_2^2$$

  6. $|< x, y >| \leq \|x\|_2 \cdot \|y\|_2$ (Cauchy–Schwarz inequality)
  7. $< x, y >= \|x\|_2 \cdot \|y\|_2 \cdot \cos\theta$ where θ is angle b/t x & y

- **some more definitions**
  1. two vectors x and y in $\mathbb{R}^n$ are said to be orthogonal iff $< x, y >= 0$ (because $\cos(\pi/2) = 0$)
  2. vector set $x_1, x_2, \ldots, x_k \in \mathbb{R}^n$ are said to be orthogonal if $< x_i, x_j >= 0\ \forall\ i \neq j$
     - if in addition to being orthogonal, these vectors also have $\|x_j\|_2 = 1$, then they are called orthnormal
     - in other words, they are orthonormal if

$$< x_i, x_j > = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} =: \delta_{ij}$$

     - ex. the set of standard basis in $\mathbb{R}^n$, $\{e_1, e_2, \ldots, e_n\}$ are orthonormal (i.e $< e_i, e_j >= \delta_{ij}$)
  3. if x, y are orthogonal, we write $x \perp y$

- **Pythagorean theorem**: let $x_1, \ldots, x_k$ be orthogonal in R^n, then

$$\|x_1 + x_2 + \ldots + x_n\|^2 = \|x_1\|^2 + \|x_2\|^2 + \ldots + \|x_n\|^2$$

Orthogonal Subspaces

- **definition**: 2 subspaces S_1 and S_2 are orthogonal iff

$$\forall u \in S_1, \forall v \in S_2, < u, v >= 0$$

  - ex. in 3D space, imagine each subspace as a plane, 2 subspaces can be perpendicular if they intersect at a right angle, forming an "L" shape (hyper-planes in higher dims)
  - geometrically, this implies that these subspaces don't share any common directionality, they span different dimensions of the overall vector space

- **theorem**: 2 subspaces S_1 & S_2 are orthogonal iff there exists a basis $B = \{b_1, \ldots, b_k\}$ for S_1 and $C = \{c_1, \ldots, c_l\}$ for S_2 that's mutually orthogonal; i.e

$$< b_i, c_j >= 0 \qquad \begin{aligned} &\forall i = 1, \ldots, k \\ &\forall j = 1, \ldots, l \end{aligned}$$

  - note: if one such pair of basis exist, then any basis for each subspace will also satisfy this property
  - example: the following will work as $B \perp C$

$$\begin{aligned} S_1 &= \text{span}\{e_1, e_2\} & S_2 &= \text{span}\{e_3\} \\ B &= \{e_1, e_2\} & C &= \{e_3\} \end{aligned}$$

  - note: the property above is equivalent to

$$B^T C = \vec{0} \quad \text{where } B = [b_1 | \ldots | b_k] \ \ \& \ \ C = [c_1 | \ldots | c_l]$$

- **definition**: let U be a subspace of a vector space W (i.e $U \subseteq W$), we define the <u>orthogonal complement of U</u> as

$$U^\perp = \{x \in W : x \perp U\}$$

  - (all vectors that are orthogonal to every vector in U)
  - note: $U^\perp$ is the largest subspace that is orthogonal to U
  - intuitively, it consists of all vectors that do not "point into" or "lie within" the subspace U
  - ex. let $U = \text{span}\{e_1, e_3, e_4\}$, then $U^\perp = \text{span}\{e_2, e_5\}$ as $e_2, e_5 \perp U$
  - remarks
    1. given subspace $U \subseteq W$, we have

$$\dim(U) + \dim(U^\perp) = \dim(W)$$

    2. $(U^\perp)^\perp = U$
    3. if B is a basis for $U$and C is a basis for $U^\perp$, then $B \cup C$ is a basis for W
    4. given $U, U^T \subseteq W$ and $x \in W$, we can express

$$x = x_u + x_{u^\perp} \qquad x_u \in U, x_{u^\perp} \in U^\perp$$

       → this is called an orthogonal decomposition
       → further: given x, the choice is x_u and $x_{u^\perp}$ is unique
       → say x_u is the orthogonal projection of x onto U
       → so any vector $x \in W$ can be uniquely decomposed into its project onto U and its projection onto $U^\perp$

- **theorem**: let A be a $m \times n$ matrix, then
  1. $N(A) = [R(A^T)]^\perp$
  2. $N(A^T) = [R(A)]^\perp$

Orthogonal Projections

- **definition**: **projection of vector x onto a vector u** is

$$\text{proj}_u v = \frac{\langle x, u \rangle}{\langle u, u \rangle} u$$

  - it is the vector that represents the component of x that lies on in the direction of v
  - geometrically, the projection of x onto v is the point along the direction of v where the shadow of x falls
  - remarks
    1. $\text{proj}_u(x) = \langle \hat{u}, x \rangle \cdot \hat{u}$ where $\hat{u} = \dfrac{u}{\|u\|}$ = unit projection of u
    2. using matrix notation

$$\begin{aligned} \text{proj}_u(x) &= \frac{uu^T}{\|u\|^2} x \\ &= P_u x \end{aligned}$$

       call P_v the orthogonal projection matrix onto span v

  - example: Let $v = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$ and $x = \begin{bmatrix} 5 \\ 7 \\ 3 \end{bmatrix}$. Compute P_v and the projection of x onto v

$$\begin{aligned} P_v &= \frac{vv^T}{\|v\|^2} \qquad\qquad \|v\|^2 = 1^2 + 2^2 + 0^2 = 5 \\ &= \frac{1}{5} \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \end{bmatrix} \\ &= \frac{1}{5} \begin{bmatrix} 1 & 2 & 0 \\ 2 & 4 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} \text{proj}_v(x) = P_v x &= \begin{bmatrix} 1/5 & 2/5 & 0 \\ 2/5 & 4/5 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 5 \\ 7 \\ 3 \end{bmatrix} \\ &= \begin{bmatrix} 19/5 \\ 2/5 \\ 0 \end{bmatrix} \end{aligned}$$

  - properties of P_v
    1. $P_v(P_v x) = P_v(x)$ (additional projections doesn't do anything, $(P_v)^k = P_v$)
    2. $(P_v)^T = P_v$
  - additionally: let $P_v = P$ for notation purposes
    1. $\langle x, Py \rangle = \langle Px, y \rangle$
    2. $\langle Px, P_y \rangle = \langle Px, y \rangle$
    3. $R(P) = \text{span}\{v\}$
    4. $N(P) = \text{span}\{v\}^\perp$

Orthonormal Basis & Gram–Schmidt

- we say $\{w_1, w_2, \ldots, w_m\}$ is an orthonormal basis (ONB) for a subspace U if
  1. $\{w_1, \ldots, w_m\}$ is a basis for U
  2. $\{w_1, \ldots, w_m\}$ is orthonormal

  i.e. $\langle w_i, w_j \rangle = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$

- why is ONB important: let $\{w_1, w_2, \ldots, w_m\}$ be ONB for U, then for any $x \in U$, there exist a unique set of scalars $\{c_1, c_2, \ldots c_m\}$ s.t
  1. $x = \sum_{i=1}^m c_j w_j$ (this is nothing special, simply the basis definition - usually solve system of equations to find c_i)
  2. $c_j = \langle w_j, x \rangle$ (special to ONB)
  3. $\|x\|^2 = \sum |x_j|^2$ (Parseval Equality – holds for all basis)

- **Gram-Schmidt Orthogonalization Algorithm**: let $\{v_1, v_2, \dots, v_n\}$ be a basis of a subspace U, we want to find the ONB

$$
\begin{aligned}
u_1 &= v_1 \\
u_2 &= v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 \\
u_3 &= v_3 - \frac{\langle v_3, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 - \frac{\langle v_3, u_2 \rangle}{\langle u_2, u_2 \rangle} u_2 \\
&\vdots \\
u_n &= v_n - \sum_{j=1}^{n-1} \frac{\langle v_n, u_j \rangle}{\langle u_j, u_j \rangle} u_j \\
&= v_n - \sum_{j=1}^{n-1} P_{v_j}(u_n)
\end{aligned}
$$

Then $\{u_1, u_2, \dots, u_n\}$ is an orthogonal basis of U.
If you normalize them, i.e. $e_i = \dfrac{u_i}{\|u_i\|}$ then $\{e_1, e_2, \dots, e_n\}$ is an orthonormal basis of U

  - example:

    Construct ONB for $U = \text{span}\left\{ \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 3 \\ -1 \end{bmatrix} \right\}$

    Apply GS:

$$
v_1 = u_1 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}
$$

$$
\begin{aligned}
v_2 = u_2 - P_{u_1}(u_2) &= \begin{bmatrix} 1 \\ 1 \\ 3 \\ -1 \end{bmatrix} - \frac{\langle v_i, u_2 \rangle}{\|v_1\|^2} v_1 \\
&= \begin{bmatrix} 1 \\ 1 \\ 3 \\ -1 \end{bmatrix} - \frac{4}{4} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 2 \\ 0 \end{bmatrix}
\end{aligned}
$$

    After normalizing, we have

$$
w_1 = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \qquad w_2 = \frac{1}{2\sqrt{2}} \begin{bmatrix} 0 \\ 2 \\ 2 \\ 0 \end{bmatrix}
$$

  - note: can use GS even if given vec not linearly independent

Projection onto Subspaces

- **definition**: let $U \subseteq R^n$ be a subspace with ONB $\{w_1, \dots, w_m\}$, then

$$
\begin{aligned}
\text{proj}_U(x) &:= \text{proj}_{w_1}(x) + \text{proj}_{w_2}(x) + \dots \text{proj}_{w_m}(x) \\
&= \left(w_1 {w_1}^T + w_2 {w_2}^T + \dots w_m {w_m}^T \right) x \\
&= P \times x
\end{aligned}
$$

  - where P is the ortho projector onto U (it is a matrix)
  - (second line works because w_j is a unit vector)
- properties of P:
  1. $P^2 = P$
  2. $P^T = P$
- **definition**: a matrix P is an ortho projection matrix iff $(P^2 = P) \wedge (P^T = P)$
- **fact**: if P is an ortho projector onto U, then $Q = I - P$ is the ortho projector onto $U^\perp$
  - while P projects any vector onto U, Q projects any vector onto $U^\perp$
- **fact**: let $U \in \mathbb{R}^n$ be a subspace, let P_U be the ortho projector onto U
  1. $x - P_u(x) \in U^\perp$
     - if you take any vector x and subtract its projection onto U, the result is a vector that is orthogonal to U
     - because the projection captures all of x's components that are in U, so what remains must be orthogonal to U
  2. $\|x - P_u(x)\| \le \|x - y\| \quad \forall\, y \in U$
     - basically saying the orthogonal projection of x onto U ($P_U(x)$) is the closest point in U to x
- **fact**: let U be a subspace in $\mathbb{R}^n$, let $\{w_1, w_2, \dots, w_m\}$ be an ONB for U, then we can express the ortho projector onto U in different ways
  1. $P_U = \sum_{i=1}^n w_i w_i^T$
  2. define $B = [w_1 \mid w_2 \mid \dots \mid w_m]$, then $P_U = BB^T$

QR Decomposition

- big idea: If A is a $m \times n$ matrix with rank(A), then the decomposition $A = QR$ provides orthonormal bases of both $R(A)$ and $R(A)^\perp$
- **definition**: a matrix A is called orthogonal if $A^T A = AA^T = I$, it has properties:
  1. A is square and invertible ($A^{-1} = A^T$)
  2. $\|Ax\| = \|x\|$ (norm preserving or has norm of 1)
  3. columns of A are orthonormal
  4. rows of A are orthonormal
- some examples of orthogonal matrices
  - I_n is orthogonal matrix
  - rotation matrices are orthogonal matrices
  - reflection matrix wrt subspaces are orthogonal
    - → reflection of x across U $\text{ref}_U(x) = (I - 2P_{U^\perp})x$
    - → for any ortho projector P, the reflection matrix is $I - 2P$ and it's also orthogonal
- **QR Decomposition**: Let A be an $m \times n$ matrix with rank$(A) = n$
  1. Write $A = [a_1 \mid \dots \mid a_n]$
  2. Apply Gram-Schmidt to $\{a_1, \dots a_n\}$ and construct $\{w_1, w_2, \dots, w_n\}$ that's an ONB for $R(A)$
     - recall that $a_k \in \text{span}\{w_1, \dots, w_k\}$ by construction
  3. Rewrite to express each column a_j of A as linear combination of the ONB

$$
\begin{aligned}
A &= Q_1 R_1 \\
Q_1 &= \underbrace{\begin{bmatrix} w_1 & \cdots & w_n \end{bmatrix}}_{m \times n}
\end{aligned}
$$

$$
R_1 = \underbrace{\begin{bmatrix} \langle w_1, a_1 \rangle & \langle w_1, a_2 \rangle & \dots & \langle w_1, a_n \rangle \\ & \langle w_2, a_2 \rangle & \dots & \langle w_2, a_n \rangle \\ & & \ddots & \\ & & & \langle w_n, a_n \rangle \end{bmatrix}}_{n \times n}
$$

(this is called the **thin QR decomposition** of A)

4. Obtain the full QR decomposition of A by writing

$$A = QR = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix} \begin{bmatrix} R_1 \\ 0 \end{bmatrix}$$

where Q is an $m \times m$ orthogonal matrix and R is a $m \times n$ upper triangular matrix

- $Q_2 = \begin{bmatrix} w_{n+1} & w_{n+2} & \dots & w_m \end{bmatrix}$ where $\{w_{n+1}, \dots, w_m\}$ is any ONB of the orthogonal complement $R(A)^{\perp}$
- since $R(A)^{\perp} = N(A^T)$, we just solve $A^T w = 0$ for Q_2

- **theorem**: let $A = QR$ be the full QR decomposition of the matrix A and let $Q = \begin{bmatrix} Q_1 & Q_2 \end{bmatrix}$
  1. the columns of Q_1 form ONB for $R(A)$
  2. the columns of Q_2 form ONB for $R(A)^{\perp}$

$$\begin{aligned} \text{proj}_{R(A)}(x) &= Q_1 {Q_1}^T x \\ Q_1 {Q_1}^T &= \text{ortho projector onto } R(A) \\ \text{proj}_{R(A)^{\perp}} &= Q_2 {Q_2}^T x \\ Q_2 {Q_2}^T &= \text{ortho projector onto } R(A)^{\perp} \end{aligned}$$

Least Squares Approximation

- **theorem**: let A be an $m \times n$ matrix with and $m > n$ and $\text{rank}(A) \geq n$ – the least squares approximation of the system $Ax \approx b$ is the solution of the system

$$\begin{aligned} A^T A x^{\star} &= A^T b \\ x^{\star} = x_{LS} &= (A^T A)^{-1} A^T b \end{aligned}$$

The system is called the normal equations.

- the LSE (in our current set-up) always has a solution
- any solution u of LSE minimze $\|Au - b\|_2$
- if $A^T A$ is invertible then LSE has a unique sol (called x_{LS})
  $\rightarrow$ $A^T A$ is invertible iff $\text{rank}(A) = \#$ of col $= n$
- as an alternative to QR decomposition, we can find the ortho-projector onto $R(A)$

$$\begin{aligned} A(x_{LS}) &= \text{proj}_{R(A)}(b) \qquad \text{by design} \\ A\left[(A^T A)^{-1} A^T b\right] &= \text{proj}_{R(A)}(b) \\ A(A^T A)^{-1} A^T &= \text{ortho projector onto } R(A) \end{aligned}$$

- example: solve the following using LSE

$$\underbrace{\begin{bmatrix} 1 & -1 & 4 \\ 1 & 4 & -2 \\ 1 & 4 & 2 \\ 1 & -1 & 0 \end{bmatrix}}_{A} x = \underbrace{\begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}}_{b}$$

$$A^T A = \begin{bmatrix} 4 & 6 & 4 \\ 6 & 34 & -4 \\ 4 & -4 & 24 \end{bmatrix} \qquad A^T b = \begin{bmatrix} 10 \\ 15 \\ 6 \end{bmatrix}$$

$$(A^T A)^{-1} = \begin{bmatrix} 0.5 & -0.1 & -0.1 \\ -0.1 & 0.05 & 0.025 \\ -0.1 & 0.025 & 0.0625 \end{bmatrix}$$

$$x_{LS} = (A^T A)^{-1} A^T b = \begin{bmatrix} 2.9 \\ -0.1 \\ -0.25 \end{bmatrix}$$

- solving LSE using QR decomp: using the same set-up as above and let $A = Q_1 R_1$ be the thin QR decomposition

$$\begin{aligned} R_1 x &= Q_1^T y \\ x_{LS} &= R^{-1} Q_1^T y \end{aligned}$$

further, the residual is given by

$$\|Ax - b\| = \|Q_2^T b\|$$

(note, most of the time, it's easier to solve $R_1 x = Q_1^T y$ using augmented matrix - inverses are tricky)

- fitting models to data: suppose we have m points $\{(t_1, y_1), (t_2, y_2), \dots (t_m, y_m)\}$ and we want the to find a line $y = c_1 + c_2 t + c_3 t^2$ that best fits the data (minimize SSE)

$$A = \begin{bmatrix} 1 & t_1 & (t_1)^2 \\ 1 & t_2 & (t_2)^2 \\ \vdots & \vdots & \vdots \\ 1 & t_m & (t_m)^2 \end{bmatrix} \qquad c = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \qquad y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}$$

and we want to solve $Ac \approx y$ using the LSE

- this generalize to any function on t that's defined in the best fit equation
- we assume $m \geq n$ and the function $f_1, f_2, \dots, f_n$ are linearly independent (so $\text{rank}(A) = n$)

Eigenvalues

- **definition**: let A be an $n \times n$ matrix, a scalar $\lambda \in \mathbb{R}$ and a non-zero vector $v \in \mathbb{R}^n$ is called an **eigenvalue/eigenvector pair** if

$$Av = \lambda v$$

- how to find eigevenvalues of a given matrix A

$$\begin{aligned} Av &= \lambda v \\ Av &= \lambda I v \\ Av - \lambda I v &= 0 \\ (A - \lambda I)v &= 0 \end{aligned}$$

  - **def**: $c_A(\lambda) = \det(A - \lambda I)$ is the characteristic polynomial of A
  - **theorem**: eigenvalues of A is the root of $c_A(\lambda)$ (set $c_A(\lambda) = 0$)
    $\rightarrow$ note: via fundamental theorem of algebra, $c_A(\lambda)$ will have n roots (possible repeated, possibly complex)

- finding corresponding eigenvector: once we have eigenvalue λ_j, since $v \in N(A - \lambda_j I)$ (see above)

$$\text{solve for } v: \qquad (A - \lambda_j I)v = 0$$

  - any vector in the basis of $N(A - \lambda_j I)$ is the corresponding eigenvector to λ_j
  - we defined $E_{\lambda_j} := N(A - \lambda_j I)$ as the eigenspace of λ_j

- example: find a eigenvalue/eigenvector pair for A

$$A = \begin{bmatrix} 3 & -6 & -7 \\ 1 & 8 & 5 \\ 1 & 2 & 1 \end{bmatrix}$$

$$\begin{aligned} c_A(\lambda) = \det(A) &= (\lambda - 2)(\lambda - 4)(\lambda - 6) = \\ \therefore \lambda &= 2, 4, 6 \end{aligned}$$

for $\lambda = 2$, we can find the corresponding eigenvector

$$\begin{aligned} E_{\lambda_1} = N(A - 2I) &= \begin{bmatrix} 1 & -6 & -7 \\ 1 & 6 & 5 \\ -1 & -2 & -1 \end{bmatrix} \\ &= \text{span}\left\{ \begin{bmatrix} -1 \\ -1 \\ -1 \end{bmatrix} \right\} \end{aligned}$$

- **theorem**: if all eigenvalue of $n \times n$ matrix is distinct, then the corresponding eigenvector are linearly independent and form a basis for $\mathbb{R}^n$
  - such a basis is called a eigenbasis
- multiplicity of eigenvalue: say $c_A(\lambda) = (\lambda - \lambda_1)^2(\lambda - \lambda_2)^3(\lambda - \lambda_3)$ where $\lambda_1 \neq \lambda_2 \neq \lambda_3$
  - algebraic multiplicity of $\lambda_1, \lambda_2, \lambda_3$

$$m_1 = 2 \qquad\qquad m_2 = 3 \qquad\qquad m_3 = 1$$

  - geometric multiplicity of $\lambda_1, \lambda_2, \lambda_3$

$$d_j := \dim(E_{\lambda_j}) \qquad\qquad j = 1, 2, 3$$

    $\rightarrow$ note: $1 \leq d_j \leq m_j$
    $\rightarrow$ when $d_j < m_j$, that's called a defective eigenvalue
- **theorem**: there exists an eigenbasis corresponding to A if $d_j = m_j$ for each eigenvalue of A

Diagonalization

- setting for this section
  - A is $n \times n$
  - $\lambda_1, \lambda_2, \ldots, \lambda_3$: eigenvalues of A
  - $\{v_1, v_2, \ldots, v_n\}$: eigenbasis of A such that $Av_j = \lambda_j v_j$
- **definition**: A matrix is **diagonalizable** if there exists an invertible matrix P and a diagonal matrix D such that

$$A = PDP^{-1}$$

- **theorem**: if A is diagonalizable, then we can construct P with the eigenvectors as the columns and D with the eigenvalues in the diagonal

$$P = \begin{bmatrix} | & | & | & | \\ v_1 & v_2 & \ldots & v_n \\ | & | & | & | \end{bmatrix} \quad D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

$$A = PDP^{-1}$$

- **theorem**: if A has distinct eigenvalues, it is diagonalizable
- application of diagonalization: power of matrices

$$\text{Suppose we have } A = PDP^{-1}$$
$$A^k = PD^kP^{-1}$$

  - the formula above also hold for negative k if all egienvalues are non-zero
  - equivalently, it holds for negative k if A is diagonalizable and invertible
  - note: $D^{-1} = 1/\lambda_j$ for all diagonal values

Spectral Theorem

- **definition**: a square matrix A is symmetric if $A^T = A$
  - proposition: all eigenvalues of a real symmetric matrix A are real
  - proposition: let A be a real symmetric matrix, and suppose λ_1, λ_2 are distinct eigenvalues with respective eigenvectors v_1, v_2; then $v_1 \perp v_2$
- **theorem**: let A be a real symmetric matrix, then there exists an orthogonal matrix P and diagonal matrix D such that $A = PDP^T$
  - in other words, A is orthogonally diagonalizable
  - note: $P^{-1} = P^T$ for orthogonal matrices
- important remark: let A be any real $m \times n$ matrix, then we have
  1. A^TA and AA^T will both be real symmetric matrices (try transposing each of them and see)
  2. both A^TA and AA^T are orthgonally diagonalizable (via Spectral theorem)

Single Value Decomposition

- **theorem**: let A be a $m \times n$ real matrix, then there exists and orthogonal matrix P $(m \times n)$, Q $(n \times n)$ and a "diagonal" matrix Σ such that $A = P\Sigma Q^T$

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_R & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

  - so the diagonal values only goes up until index r, after that you fill it with 0s
  - the values $\sigma_1 \geq \sigma_2 \geq \ldots \sigma_r > 0$ (they are ordered) and are the non-zero singular values of A
  - where $r = \min(m, n)$
- some propositions/observations
  1. if λ is a non-zero eigenvalue of AA^T, λ is also the eigenvalue of A^TA
  2. all eigenvalues of A^TA and AA^T (they are the same) are non-negative
  3. if λ is a non-zero eigenvalue of AA^T (and thus of A^TA), then λ has the same level of repetition in A^TA and AA^T
     - or $\dim(N(AA^T - \lambda I)) = \dim(N(A^TA - \lambda I))$
- **theorem**: let $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_r > 0$ by the (ordered) non-zero eigenvalues of AA^T (or A^TA), then the non-zero singular value of A is

$$\sigma_k = \sqrt{\lambda_k}$$

- SVD construction: let A be $m \times n$ and real
  1. Find singular value for Σ $(m \times m)$:
     (a) find eigenvalue of either A^TA or AA^T, order them
     (b) set $\sigma_k = \sqrt{\lambda_k}$
  2. Construct the matrix Q $(n \times n)$
     (a) set the corresponding eigenvectors as columns

$$Q = \begin{bmatrix} | & | & | & | \\ v_1 & v_2 & \ldots & v_n \\ | & | & | & | \end{bmatrix}$$

     (b) you also have to normalize the q_i such that $\|q_k\|_2 = 1$
  3. Construct the matrix P $(n \times n)$
     (a) let p_k be the columns of P, then we can take

$$p_k = \frac{1}{\sigma_k} Aq_k$$

     this will give you the first r columns of P
     (b) for the remaining $m - r$ columns, complete $p_1, \ldots p_m$ to an ONB (remember thin QR to full QR)
- application of SVD
  1. $\|A\|_{op} = \sigma_1$ (the largest singular value of A)
  2. $\|A\|_F = (\sigma_1^2 + \sigma_2^2 + \ldots + \sigma_r^2)^{1/2}$
  3. $\text{rank}(A) = r$ (number of non-zero singular value)

4. if A is $n \times n$ and invertible, then all singular values of A is positive, thus Σ is invertible, and A^{-1}

$$\begin{aligned} A &= P\Sigma Q^T \\ A^{-1} &= Q\Sigma^{-1}P^T \qquad \text{because } Q,\ P \text{ are orthogonal} \\ \Sigma^{-1} &= \begin{bmatrix} 1/\sigma_1 & 0 & \cdots & 0 & 0 \\ 0 & 1/\sigma_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1/\sigma_R & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

   - note: this is not a SVD of A^{-1}, because the columns of Σ is not ordered, but if you reorder them (reverse the column order for all matrices), you'll get the SVD

5. $\|A^{-1}\|_{op} = \dfrac{1}{\sigma_r}$
6. $\text{cond}(A) = \|A\|_{op} \times \|A^{-1}\|_{op} = \dfrac{\sigma_1}{\sigma_r}$
7. assume $P = \begin{bmatrix} p_1 & \cdots & p_m \end{bmatrix}$ and $Q = \begin{bmatrix} q_1 & \cdots & q_n \end{bmatrix}$, then
   - $\{p_1, \ldots, p_r\}$ is an orthonormal basis of $R(A)$
   - $\{p_{r+1}, \ldots, p_m\}$ is an orthonormal basis of $N(A^T)$
   - $\{q_1, \ldots, q_r\}$ is an orthonormal basis of $R(A^T)$
   - $\{q_{r+1}, \ldots, q_n\}$ is an orthonormal basis of $N(A)$.

SVD Expansion

- **theorem**: let A be a $m \times n$ matrix such that rank(A) $= r$ and $A = P\Sigma Q^T$ is the SVD; then the SVD expansion of A is

$$A = \sum_{k=1}^{r} \sigma_k p_k q_k^T$$

  where $p_1, \ldots, p_r$ are the first r columns of P, and $q_1, \ldots, q_r$ are the first r columns of Q

- **definition**: let $A = P\Sigma Q^T$, then truncated SVD expansion of rank s of A is

$$A_s = \sum_{k=1}^{s} \sigma_k p_k q_k^T$$

   - A_s is a rank s approximation of A
   - A_s is the best rank s approximation of A wrt the Frobenius norm

Principal Component Analysis

- problem: you're given $x_1, x_2, \ldots x_n \in \mathbb{R}^P$
   - (can assume they are centered (i.e $\sum x_k = 0$) but if not replace each points with $\tilde{x}_k = x_k - \bar{x}$)
   - we can form the data matrix that looks like

$$X = \begin{bmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_n^T \end{bmatrix}$$

   - we want to find the unit vector w_1 that maximizes $\sum_{k=1}^{n} |\langle x_k, w_1 \rangle|$
   - interpretation: the first weight vector w_1 points in the direction which captures the most information (ie. the maximum variance) of the data, and the second weight vector w_2 is orthogonal to w_1

- **theorem**: we can pick the weight vectors w_i as

$$w_i = q_i$$

  where q_i is the k-th column of Q in SVD decomposition of X

Pseudoinverse

- **fact**: if A is $n \times n$ and invertible, then there's an $n \times n$ matrix such that $AA^{-1} = I$ and $A^{-1}A = I$ (i.e right inverse and left inverse is the same)
   - we want to generalize the notion of inverse to some approximate sense to non-square matrices as well

- **def**: let A be an $m \times n$ matrix with SVD $A = P\Sigma Q^T$, we define the pseudoinverse $A^\dagger$

$$A^\dagger = Q\Sigma^\dagger P^T \qquad \Sigma^\dagger = \begin{bmatrix} 1/\sigma_1 & 0 & \cdots & 0 & 0 \\ 0 & 1/\sigma_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1/\sigma_R & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

theorem:

1. if A is invertible, $A^\dagger = A^{-1}$
2. if A is $m \times n$, $m \leq n$ and rank$(A) = m$ then $AA^\dagger = I_m$ (right inverse)
3. if A is $m \times n$, $n \leq m$ and rank$(A) = n$ then $A^\dagger A = I_n$ (left inverse)

- general properties
   1. $AA^\dagger A = A$ and $A^\dagger AA^\dagger = A^\dagger$
   2. $AA^\dagger$ is the projection matrix onto $R(A)$ and $A^\dagger A$ is the projection onto $R(A^T)$
   3. let A be an $m \times n$ matrix with rank$(A) = n$ and let $b \in \mathbb{R}^m$, the LSE approximation of $Ax \approx b$ is given by

$$x = A^\dagger b \qquad\qquad A^\dagger = \sum_{k=1}^{r} \frac{1}{\sigma_i} q_i p_i^T$$

Discrete Fourier Transform

Complex Vectors

- we define the symbol i such that

$$i^2 = -1 \qquad\qquad i = \sqrt{-1}$$

- **def**: a complex number is of the form

$$z = a + ib$$

   - we say that $Re(z) = a$ is the real part of z
   - and say that $Im(z) = b$ is the imaginary part of z

- **def**: polar form of a complex number $z = a + ib$

$$\begin{aligned} z &= re^{i\theta} \\ r &= \sqrt{a^2 + b^2} \\ \theta &= \tan^{-1}(b/a) \end{aligned}$$

- **Euler's formula**: $e^{i\theta} = \cos\theta + i\sin\theta$
- **definition**: let $z = a + ib$ and $z = re^{i\theta}$ in polar form
   1. the modulus of z is $|z| = r = \sqrt{a^2 + b^2}$
   2. the angle (or argument) of z is arg(z) $= \theta = \tan^{-1}(b/a)$
   3. the conjugate of z is $\bar{z} = a - ib = re^{-i\theta}$

   - properties of conjugate
      1. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$
      2. $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$
      3. $\overline{z_1 / z_2} = \overline{z_1} / \overline{z_2}$

- properties of modulus
  1. $|z_1 z_2| = |z_1||z_2|$
  2. $|cz| = |c||z|$
  3. $|z_1/z_2| = |z_1|/|z_2|$
- properties of $e^{i\theta}$
  1. $e^{i\theta_1} \times e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$
  2. $|e^{i\theta}|^2 = 1 \longrightarrow |e^{i\theta}| = 1$
  3. $(e^{i\theta})^n = e^{i\theta n}$
  4. $e^{i\theta}$ is 2π periodic meaning $e^{i2\pi k} = 1$ for $k \in \mathbb{Z}$

- **def**: complex vector space
  - a complex vector space $\mathbb{C}^n$ is the set of vectors of length n with complex entries $v_1, \dots v_n$
  - the conjugate of a vector $v \in \mathbb{C}^n$ is given by the conjugate of each entry $\overline{v}_1, \dots, \overline{v}_n$
- **def**: the standard inner product of vectors $u, v \in \mathbb{C}^n$ is

$$\langle u, v\rangle = u^T\overline{v} = u_1\overline{v_1} + \ldots + u_n\overline{v_n}$$

  - properties: let $u, v \in \mathbb{C}^n$ and let $c \in \mathbb{C}$
    1. $\langle cu, v\rangle = c\langle u, v\rangle$
    2. $\langle u, cv\rangle = \overline{c}\langle u, v\rangle$
    3. $\langle u, v\rangle = \overline{\langle v, u\rangle}$
    4. $\langle v, v\rangle \geq 0$ for all v and it's only 0 if $v = \vec{0}$
- **def**: the norm of $v \in \mathbb{C}^n$ is

$$\|v\| = \sqrt{\langle v, v\rangle} = \sqrt{|v_1|^2 + \ldots + |v_n|^2}$$

- **def**: the complex vectors $u, v \in \mathbb{C}^n$ are orthogonal if $\langle u, v\rangle = 0$
- **def**: the conjugate transpose of a complex A is $A^\star = (\overline{A})^T$
  - we can note that $\langle Au, v\rangle = \langle u, A^\star v\rangle$
- **def**: A complex matrix A is hermitian if $A = A^\star$, they have the following properties
  1. $\langle Au, v\rangle = \langle u, Av\rangle$ for $u, v \in \mathbb{C}^n$
  2. A has real eigenvalues
  3. diagonal entries of A are real
  - notice it's very similar to properties of a real symmetric matrix
- **def**: A complex matrix A is unitary if $A^{-1} = A^\star$, unitary matrices have the following properties (to check see if $AA^\star \stackrel{?}{=} I$)
  1. if A is real, then A is orthogonal
  2. $\langle Ax, Ay\rangle = \langle x, y\rangle$
  3. their columns and rows are orthonormal
  - notice properties are the same as orthogonal, just generalize to complex too now
- **general spectral theorem**: every hermitian matrix is unitary diagonalizable

Roots of Unity

- **def**: an Nth root of unity is a complex number w wuch that $w^N = 1$
- proposition: let $w_N = e^{2\pi i/N}$, then w_N is an Nth root of unity
  - further, $\{1, w_N, (w_N)^2, \dots, (w_N)^{N-1}\}$ are all Nth roots of unity - that is $\{{w_N}^k : 0 \leq k \leq N-1\}$
- proposition: let $w_N = e^{2\pi i/N}$
  1. $(w_N)^N = (w_N)^0 = 1$ (it repeats once you're past $N-1$)
  2. $\overline{w}_N = (w_N)^{-1} = (w_N)^{N-1}$
     - this means that $(1, N-1), (2, N-2), (3, N-3), \dots$ are conjugate pairs of each other
  3. let s be an integer such that $0 < s < N$

$$\sum_{k=0}^{N-1} ({w_N}^k)^s = 0$$

     - this means that the sum of all N-th root of unity ($w_N^k, 0 \leq k \leq N-1$) raised to a power s is always 0

The Fourier Basis

- first, we'll use 0-indexing now (like Python) going forward
- the standard basis of $\mathbb{C}^N$ is $\{e_0, \dots, e_{N-1}\}$ where e_k is the vector with all 0s except 1 in index k
  - ex. for $N = 3$

$$e_0 = \begin{bmatrix}1\\0\\0\end{bmatrix} \qquad e_1 = \begin{bmatrix}0\\1\\0\end{bmatrix} \qquad e_2 = \begin{bmatrix}0\\0\\1\end{bmatrix}$$

- **def**: let N be a positive integer and let $w_N = e^{2\pi i/N}$, the fourier basis of $\mathbb{C}^N$ is $\{f_0, \dots, f_{N-1}\}$

$$f_k = \begin{bmatrix}1\\ {w_N}^k\\ {w_N}^{2k}\\ \dots\\ {w_N}^{(N-1)k}\end{bmatrix}$$

(all the Nth root of unity raised to power of k)
  - basically, they're a set of orthogonal functions that are used in the Fourier transform
  - they are like standard basis (in a sense) - Fourier basis functions span the function space for periodic signals, just as the standard basis spans $\mathbb{R}^n$
  - example: for $N = 3$, $w_3 = e^{2\pi/3} = (-1 + i\sqrt{3})/2$ and the Fourier basis of $\mathbb{C}^3$ is

$$f_0 = \begin{bmatrix}1\\1\\1\end{bmatrix} \qquad f_1 = \begin{bmatrix}1\\(-1+i\sqrt{3})/2\\(-1-i\sqrt{3})/2\end{bmatrix}$$

$$f_2 = \begin{bmatrix}1\\(-1-i\sqrt{3})/2\\(-1+i\sqrt{3})/2\end{bmatrix}$$

- proposition:
  1. the Fourier basis $\{f_0, \dots, f_{N-1}\}$

$$\langle f_k, f_l\rangle = \begin{cases} N & \text{if } k = l \\ 0 & \text{otherwise}\end{cases}$$

     so the Fourier basis is an **orthogonal basis** of $\mathbb{C}^N$
  2. $\|f_k\|_2 = \sqrt{N}$ (all of them have the same norm)
  3. let $0 < k < N$

$$\overline{f}_k = f_{N-k}$$

     - example: $N = 8$

$$f_7 = \overline{f_1} \qquad f_6 = \overline{f_2} \qquad f_5 = \overline{f_3} \qquad \dots$$

     - you can see this kind of symmetry in the entries too (i.e $\overline{f_k[i]} = f_k[N-i]$)
     - if N is even, then $f_{N/2}$ is a real vector

Discrete Fourier Transform

- **def**: let $x \in \mathbb{C}^N$, the **discrete Fourier transform** of x is

$$\text{DFT}(x) = F_N(x)$$

where F_N is the **Fourier matrix**

$$F_N = \begin{bmatrix} \overline{f_0}^T \\ \overline{f_1}^T \\ \vdots \\ \overline{f}_{N-1}^T \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \overline{w}_N & \overline{w}_N^2 & \dots & \overline{w}_N{}^{N-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & \overline{w}_N{}^{N-1} & \overline{w}_N{}^{2(N-1)} & \dots & \overline{w}_N{}^{(N-1)^2} \end{bmatrix}$$

  - DFT is a mathematical transformation used to analyze the frequency components of a discrete signal
  - takes a signal represented in the time domain (as a sequence of samples) and transforms it into the frequency domain (as a set of frequencies and corresp amplitudes)
  - ex. say you have a signal, such as a sound recording, the DFT tells you what notes (frequencies) are playing and how loud (amplitude) they are
  - DFT decomposes the signal into its constituent sinusoidal waves, each with a certain frequency, amplitude, and phase
- note: you can also expand x in terms of the Fourier basis

$$x = \frac{1}{N}\begin{bmatrix} f_0 & \dots & f_{N-1} \end{bmatrix} \begin{bmatrix} \overline{f}_0^T \\ \overline{f}_1^T \\ \vdots \\ \overline{f}_{N-1}^T \end{bmatrix} x = \frac{1}{N} \cdot \overline{F}_N^T \cdot F_N x$$

  - this means the DFT(x) is the vector of coefficients of x wrt the Fourier basis (up to multiplication of N)

$$\text{DFT}(x) = \begin{bmatrix} \langle x, f_0 \rangle \\ \langle x, f_1 \rangle \\ \vdots \\ \langle x, f_{N-1} \rangle \end{bmatrix}$$

- notation: the DFT used to study signal (sound, image) that can be represented as vector $x \in \mathbb{C}^N$ and we use the notation

$$x = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix} \qquad x[n] = x_n \text{ (i.e indexing)}$$

- for a vector y, we define the inverse DFT of y

$$\text{IDFT}(y) = \frac{1}{N}\overline{F}_N^T y$$

and this will invert the DFT of y
  - the process of taking a frequency domain signal and reconstructing the original time domain signal from it (reverse operation of the DFT)
  - ex. the DFT is like breaking a song into individual notes, the IDFT is like putting those notes back together to recreate the original song

- <u>proposition</u>: let x be a real signal (that is $x[k] \in \mathbb{R}$ for all k) and let $y = \text{DFT}(x)$

$$\overline{y[k]} = y[N-k]$$

- **def**: sinusoids
  - let $t = \left(0, \frac{1}{N}, \frac{2}{N}, \dots, \frac{N-1}{N}\right)^T$
  - a sinusoids is a vector $x \in \mathbb{C}^N$ of the form

$$x = A\cos(2\pi kt + \phi)$$

$$A = \text{amplitude}$$
$$k = \text{frequency}$$
$$\phi = \text{phase}$$

  - <u>prop</u>: we can say that for any sinusoids x

$$x = A\cos(2\pi kt + \phi) \quad k \in \{1, 2, \dots, N-1\}$$

$$\text{DFT}(x) = \frac{AN}{2}(e^{i\phi}e_k + e^{-i\theta}e_{N-k})$$

    → note: $e^{i\phi}$ is Euler's number, e_k is the standard basis (meaning we only care about certain entries)
    → equivalently, we can say

$$A\cos(2\pi kt + \phi) = \frac{A}{2}e^{i\phi}f_k + \frac{A}{2}e^{-i\phi}f_{N-k}$$

- Example: Find DFT of x if

$$x = 3\cos\left(4\pi t - \frac{\pi}{2}\right) \qquad t = [0, 1/8, \dots, 7/8]^T$$

  - we can see that $A = 3, k = 2, \phi = -\pi/2$
  - because $k = 2$, we know that only index 2 and $N - k = 6$ entries of the DFT(x) will be non-zero, i.e

$$\text{DFT}(x) = \begin{bmatrix} 0 \\ 0 \\ \frac{AN}{2}(e^{i\phi}e_k) \\ 0 \\ 0 \\ 0 \\ \frac{AN}{2}(e^{-i\theta}e_{N-k}) \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{3(8)}{2}e^{-\frac{\pi}{2}i} \\ 0 \\ 0 \\ 0 \\ \frac{3(8)}{2}e^{\frac{\pi}{2}i} \\ 0 \end{bmatrix}$$

- Example: Calculate $y = \text{IDFT}(Y)$ where

$$Y = [\ 0,\ 0,\ 2,\ 3i, -3i,\ 2, 0\ ]^T \in \mathbb{C}^7$$

  - we can recognize that $Y[k] = \overline{Y[N-k]}$ for all k and thus we can conclude that the signal is real
  - we can think of Y as: (only care about non-zero pairs)

$$Y = Y_1 + Y_2$$
$$Y_1 = [\ 0,\ 0,\ 2,\ 0,\ 0,\ 2, 0\ ]^T$$
$$Y_2 = [\ 0,\ 0,\ 0,\ 3i, -3i,\ 0, 0\ ]^T$$

  similarly, we can do the same for y

$$y = y_1 + y_2$$

  - finding $y_1 = \text{IDFT}(Y_1)$: we only have to focus on $Y_1[2] = 2$ because the other is just the complex conjugate

$$k = 2 \qquad \longrightarrow y_1 = A\cos(2\pi \times 2t + \phi)$$
$$Y_1[2] = 2 = \frac{AN}{2}e^{i\phi} \qquad \longrightarrow A = \frac{4}{7}, \phi = 0$$
$$\therefore y_1 = \frac{4}{7}\cos(4\pi t)$$

  (note: the second line came from the real part of the decomposition of the DFT above)

- finding y_2

$$k = 3$$

$$Y_2[3] = 3i = \frac{AN}{2} e^{i\phi_2} \qquad \longrightarrow A = \frac{6}{7}, \phi_2 = \frac{\pi}{2}$$

$$\therefore y_2 = \frac{6}{7} \cos(6\pi t + \pi/2)$$

- and finally $y = y_1 + y_2$