A system is homogeneous if setting all variables to 0 produces a solution.

Matrix multiplication: A is M×R and B is R×N : M×N is the size of the product.

If AB = BA, A and B "commute"

Transpose is interchanging the rows and columns of a matrix.

Trace is the sum of the diagonal entries of a matrix.

tr(A+B) = tr(A) + tr(B)

tr(AB) = tr(BA)

Properties

1. A+B = B+A
2. A+(B+C) = (A+B)+C
3. A(BC) = (AB)C
4. A(B+C) = AB+AC
5. AB ≠ BA

Identity Matrices

A square matrix with 1's on the diagonals and 0's everywhere else.

1. AI = A
2. IB = B

Matrix Inverse

$B = A^{-1}$ if :
AB = I and BA = I

If A has an inverse, it's called "invertible" or "non-singular".

Theorem: A matrix has only one inverse. If B and C are inverses of A, B = C.

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

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

Results:

1. $(AB)^{-1} = B^{-1}A^{-1}$
2. A^{-1} is invertible : $(A^{-1})^{-1} = A$
3. $(A^n)^{-1} = (A^{-1})^n$
4. $(kA)^{-1} = \frac{1}{k} \times A^{-1}$
5. AkB = kAB

Transpose Properties

1. $(A^T)^T = A$
2. $(A+B)^T = A^T + B^T$
3. $(kA)^T = kA^T$
4. $(AB)^T = B^TA^T$
5. $(A^{-1})^T = (A^T)^{-1}$
6. A and A^T have the same eigenvalues

If A is invertible, A^T is also invertible.

Elementary Matrices

E is elementary if it can be obtained from I by doing one elementary row operation.

EA performs the original ERO that was performed on E, on A.

Every elementary matric is invertible and its inverse is also elementary.

TFAE [A is square]

i) A is invertible
ii) Ax = 0 has only the trivial solution
iii) The RRF of A is I
iv) A can be written as a product of elementary matrices
v) Ax = b is consistent for every b
vi) Ax = b has exactly one solution for every b.
vii) λ=0 is not an eigenvalue of A

Inversion Algorithm

Series of row operations to get A as RRF, do the same operations on the identity. That identity becomes the inverse.

Consistent means the system has at least 1 solution. Inconsistent means it has no solutions.
Idempotent if $A^2 = A$

Diagonals

If the diagonals are all non-zero, it is invertible.

1) Transpose of an upper triangular is lower triangular
2) Inverse of an upper triangular is upper triangular
3) Product of upper triangular is upper triangular

Symmetry

A is "symmetric" if $A = A^T$

Results:
1) A+B is symmetric
2) kA is symmetric
3) If A is inv and sym, then A^{-1} is sym.

Skew-Symmetric

A is skew-symmetric if $A^T = -A$
1) A^T is also skew-symmetric
2) $A \pm B$ is also skew-symmetric
3) kA is also skew-symmetric

Commute

If AB=BA, then A and B commute.

Result: AB is symmetric iff A and B commute.

Determinants by Row Reduction

Results:
1) If A is nxn and if A has a row or column of zero's, then det(A)=0
2) If A is nxn then $\det(A)=\det(A^T)$

Theorem:
i) A nonzero scalar could be factored out of any row/col of a determinant.

ii) If B is obtained from A by interchanging two rows or columns, then det(B) = – det(A)

iii) If B is made from A by adding to a given row, some multiple of another row, then det(B) = det(A)

Determinants by Cofactor Expansion

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ det(A) = ad-bc

If A is nxn, the "minor" of entry a_{ij} (M_{ij}) is the determinant of the matrix obtained by deleting row I and column j of A.

The "cofactor" of entry a_{ij} is $C_{ij} = (-1)^{i+j} M_{ij}$

If A is nxn then $\det(A) = a_{11}C_{11} + a_{12}C_{12}$ ...

The determinant can be expanded along any row or column

Properties of Determinants

$\det(kA) = k^n \det(A)$

$\det(A+B) \neq \det(A) + \det(B)$

$\det(A^k) = [\det(A)]^k$

Lemma: If E is elementary, then $\det(EB) = \det(E)\times\det(B)$

Theorem: A square is inv iff $\det(A) \neq 0$

Theorem: If E is elementary, then $\det(E) \neq 0$

Eigenvalues and Eigenvectors

λ is an eigenvalue of A with eigenvector **X** if $\mathbf{X} \neq 0$ and $A\mathbf{X} = \lambda\mathbf{X}$

(a) λ is a solution of the characteristic equation $\det(\lambda I - A) = 0$.
(b) The system of equations $(\lambda I - A)x = 0$ has nontrivial solutions.
(c) There is a nonzero vector x such that $Ax = \lambda x$.

How to Find Eigenvalue and Eigenvectors:

Values:
Solve det(λI-A) = 0 for λ
^ "Characteristic Polynomial"

Vectors:
For each λ solve (λI-A)**X** = 0

Result: Any nonzero multiple of an eigenvector **X** is also an eigenvector with the same eigenvalue.

Theorem: If A and B are nxn then
det(AB) = det(A)det(B)
det(AB) = det(BA)

Theorem: If A is inv then
$\det(A^{-1}) = \frac{1}{\det(A)}$

The Adjoint

The adjoint of (nxn) A is the transpose of the matrix of cofactors.
$A^{-1} = \frac{1}{\det(A)} adj(A)$

Diagonalization

If A and B are nxn then B is "similar" to A if there's an inv matrix, P, such that
$B = PAP^{-}$

If A is similar to B, B is similar to A.

Result: If B is similar to A then A and B have the same:
1) Determinant
2) Trace
3) Characteristic Polynomial
4) Eigenvalues
5) A is inv iff B is inv

Result: $A^2\mathbf{X} = \lambda^2\mathbf{X}$

Theorem: An nxn matrix, A, is inv iff λ=0 is ***not*** an eigenvalue of A.

An nxn matrix A is "diagonalizable" if there is an inv matrix P such that $P^{-}AP = D$ where D is some diagonal matrix.

Result: If A is diagonalizable then A^2 is also diagonalizable. A^{-1} is too.

How to Diagonalize a Matrix:

1. Find a basis for each eigenspace and call the resulting eigenvectors P_1, P_2, P_n

2. Let P = [P_1 P_2 … P_n]

3. $P^{-}AP = D = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{bmatrix}$

Note: If there are less than n eigenvectors in step 1, then A is not diagonalizable.

Terminology:

1. The power of the factored characteristic polynomial is called the "Algebraic Multiplicity"

2. The number of eigenvectors in the basis for the eigenspace corresponding to λ is called the "Geometric Multiplicity"

Result: GM ≤ AM

Theorem: A is diagonalizable iff AM = GM for every eigenvalue

Powers of a Matrix:

If there's a matrix P such that $P^{-}AP = D$
$A = PDP^{-}$
$A^2 = PD^2P^{-}$

$$\det(A) = \frac{1}{2}\begin{bmatrix} tr(A) & 1 \\ tr(A^2) & tr(A) \end{bmatrix}$$

If $A^k = 0$ then $(I-A)^{-1} = I + A + A^2 + A^{k-1}$

Differential Equations

An equation involving a function and its derivatives.

How to Solve Y' = AY
1. Find a matrix P that diagonalizes A
2. Find the diagonalized version of A
3. $Y = C_1X_1e^{\lambda 1x} + C_2X_2e^{\lambda 2x} + C_nX_ne^{\lambda nx}$
4. Solve for Y with given initial values

Theorem: If Y'=AY and A is diagonalizable, then $Y = C_1X_1e^{\lambda 1x} + C_2X_2e^{\lambda 2x} + C_nX_ne^{\lambda nx}$. Where X_n are the eigen vectors of A.

Complex Numbers

A complex number is a number of the form a+bi where a and b are real numbers and $i = \sqrt{-1}$ $\quad i^2 = -1$

Define: If Z = a+bi then the modulus of Z is its length in the complex plane and is denoted by $|Z| = \sqrt{a^2 + b^2}$

Define: If Z = a+bi then the conjugate of Z is $\bar{z} = a - bi$

Properties:

1. Modulus of Z ≥ 0
2. Modulus of Z = 0 iff Z = 0 vector
3. $\bar{\bar{z}} = z$

Addition:
$Z_1 = a+bi \qquad Z_2 = c+di$
$Z_1 + Z_2 = (a+c) + (b+d)i$

Multiplication:
$Z_1Z_2 = (ac-bd) + (ab+bc)i$

4. $z\bar{z} = |z|^2$
5. $z = \bar{z}$ iff Z is real (b=0)
6. $\overline{z + w} = \bar{z} + \bar{w}$
7. $\overline{zw} = \bar{z} * \bar{w}$
8. $\overline{\frac{z}{w}} = \frac{\bar{z}}{\bar{w}}$
9. $|zw| = |z||w|$

Division:
$$\frac{z}{w} = \frac{z\bar{w}}{|w|^2}$$

10. $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$

Polar Form of a Complex Number

$Z = r(cos\theta + isin\theta)$

$Z = re^{i\theta}$

$Z^n = r^n e^{i\theta n}$

$\theta = \tan^{-1}(\frac{y}{x}) + sgn(y) \times \frac{\pi}{2}(1 - sgn(x))$

Roots:

$$Z^n = |z|^n(\cos(\theta n + 2k\pi n) + i\sin(\theta n + 2k\pi n))$$

k = 0 , 1 , 2 , 3 , 4 …

Special Case:

$Z^n = a \qquad b^n = a$
$Z^n = b^n e^{2\pi k i}$

Vectors

PQ = Q – P

Linear Combinations:
W is a linear combo of V_1, V_2, V_k if there are scalars such that $W = C_1V_1 + C_2V_2 + C_kV_k$

Length

$$||V|| = \sqrt{V_1^2 + V_2^2 + V_n^2}$$

Properties:
1. ||V||≥0
2. ||V|| = 0 iff V=0 vector
3. ||kV|| = |k|||V||
4. $\frac{1}{||V||}V - \textit{the unit vector}$

Dot Product

$U \cdot V = ||U||||V||cos\theta$

Define: If $U=(u_1, u_2, u_n)$ and $V=(v_1, v_2, v_n)$;

$U \cdot V = u_1v_1 + u_2v_2 + u_nv_n$

Properties:
1. $V \cdot V = ||V||^2$
2. $U \cdot V = V \cdot U$
7. $U \cdot (V+W) = U \cdot V + U \cdot W$

Theorem:
$||U+V|| + ||U-V||^2 = 2(||V||^2 + ||U||^2)$

Theorem:
$U \cdot V = \frac{1}{4}||U+V||^2 - \frac{1}{4}||U-V||^2$

Theorem:
$||U \cdot V|| \leq ||U||||V||$

Theorem:
$||U + V|| \leq ||U|| + ||V||$

Orthogonality

U and V are orthogonal (perpendicular) if
$U \cdot V = 0$

Projections

$$Proj_a U = \frac{U \cdot A}{||A||^2} A$$

$U - Proj_a U$ = Vector component of U perpendicular to A.

$$|Proj_a U| = \frac{U \cdot A}{||A||}$$

Cross Product

$$U \times V = \begin{bmatrix} i & j & k \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{bmatrix}$$

Find the determinant.

Properties:

1. $U \times V$ is orthogonal to both U and V
2. $U \times V = -(V \times U)$
3. $U \times (V+W) = U \times V + U \times W$
4. $U \times U = 0$
5. $U \times 0 = 0$
6. $k(U \times V) = (kU) \times V$

$||U \times V|| = ||U||||V||\sin\theta$

Theorem:
$||U \times V|| = ||U||^2 ||V||^2 - (U \cdot V)^2$

Area of a closed shape can be interpreted by a cross product.

Volume = $|U \cdot (V \times W)|$ $\det(v1,v2,v3)^T$

Real Vector Spaces

Let V be any non-empty set of objects with two operations called "addition" and "scalar multiplication". Then, V_s is called a "vector space" if the following axioms are satisfied:

1. If U and V are in V_s then U+V is in V_s

2. U+V = V+U

3. U + (V+W) = (U+V) + W

4. There is an object in V_s called the zero vector with the property that:
$U + 0_v = U$

5. For each U in V_s there is an object -U in V_s with the property:
$U + (-U) = 0_v$

6. If U is in V_s and K is a scalar, KU is in V_s

7. K(U+V) = KU + KV

8. (K+M)U = KV + MU

9. K(MU) = (KM)U

10. 1(U) = U

Theorem: If V_s is a vector space:

a) -U = (-1)U
b) $0_vU = 0_v$
c) $K0_v = 0_v$
d) If $KU = 0_v$ then K = 0 or U = 0

Subspaces

A subset W_{ss} of a vector space V_s is called a subspace if W_{ss} itself is a vector space using the same addition and multiplication as V_s

Theorem: If W_{ss} is a non-empty subset of V_s, then W_{ss} is a subspace iff:
a) If U and V are in W_{ss}, then U+V is in W_{ss}
b) If K is a scalar and U is in W_{ss}, then KU is in W_{ss}

Define: Let $S = \{w_1, w_2, w_r\}$
The set of all linear combinations of vectors in S is called span(S).
If V = Span(S) then we say that the vectors in S span V.

Theorem: Let $S = \{w_1, w_2, w_r\}$ be a non-empty set in a vector space V_s and let W = Span(S). Then W_{ss} is a subset of V_s.

Linear Independence

Define: Let $S = \{V_1, V_2, V_r\}$, S is called linearly independent if the equation
$K_1V_1 + K_2V_2 + K_rV_r = 0$
has **only** the trivial solution K = 0

Theorem: a) A set with 2 or more vectors is linearly dependant iff at least 1 of the vectors in S can be written as a linear combo of the remaining vectors in S.

b) A set with 2 vectors is linearly dependant iff each vector is a constant multiple of the other.

Coordinates and Basis

Define: If V is a vector space and $S = \{V_1, V_2, V_n\}$ then S is called a basis for V if:

1) S is linearly independent
2) S spans V

Theorem: If $S = \{V_1, V_2, V_n\}$ is a basis for a vector space V_{vs} then every vector in V_s can be written as $V = C_1V_1 + C_2V_2 + C_nV_n$ in exactly one way.

Define: C_1, C_2, C_n in the previous theorem are called the coordinates of V relative to S. The vector (C_1, C_2, C_n) is denoted by $(V)_s$

Gram-Schmidt Process

(R^n only, omit QR-Decomposition)

Notation: $\langle u, v\rangle = u\cdot v$
Inner Product Space = R^n
Inner Product = Dot Product

Define: $S = \{V_1, V_2, V_n\}$ is called "orthogonal" if $V_i \neq 0_v$ (for i=1,2,n) and $V_i \cdot V_j = 0$ whenever $i\neq j$

If, in addition, each vector in S has length 1 then S is "orthonormal"

Theorem: Every orthogonal set is independent

Theorem: If $S = \{V_1, V_2, V_n\}$ is an orthogonal basis for a subspace W of R^n and u is any vector in W then

$$\vec{u} = \frac{\vec{u}\cdot\vec{v_1}}{||\vec{v_1}||^2}\times\vec{v_1} + \cdots + \frac{\vec{u}\cdot\vec{v_n}}{||\vec{v_n}||^2}\times\vec{v_n}$$

Note: If S is orthonormal then:

$$\vec{u} = (\vec{u}\cdot\vec{v_1})\vec{v_1} + \cdots + (\vec{u}\cdot\vec{v_n})\vec{v_n}$$

Theorem: If a set of n vectors in R^n spans R^n or is independent then S is a basis for R^n

Orthogonal Projections

Define: Let W be a subspace of R^n and let $\{V_1, V_2, V_r\}$ be an orthogonal basis for W. If u is in R^n then the $Proj_w u$ is defined by:

$$Proj_w\vec{u} = \frac{\vec{u}\cdot\vec{v_1}}{||\vec{v_1}||^2}\times\vec{v_1} + \cdots + \frac{\vec{u}\cdot\vec{v_r}}{||\vec{v_r}||^2}\times\vec{v_r}$$

Properties:

1. $Proj_w\vec{u}$ is in W (Since W is closed under addition and scalar multiplication)

2. $\vec{u} - Proj_w\vec{u}$ is perpendicular to every vector in W.

3. $Proj_w\vec{u}$ is independent of the choice of orthogonal basis

Gram-Schmidt Process

How to produce an orthogonal basis:

Let $\{u_1, u_2, u_r\}$ be a basis for a subspace W of R^n;

$$v_1 = u_1$$
$$v_2 = u_2 - \frac{u_2\cdot v_1}{||v_1||^2}\times v_1$$
$$v_3 = u_3 - \frac{u_3\cdot v_1}{||v_1||^2}\times v_1 - \frac{u_3\cdot v_2}{||v_2||^2}\times v_2$$
$$v_r = u_r - \cdots - \frac{u_r\cdot v_{r-1}}{||v_{r-1}||^2}\times v_{r-1}$$

Then $\{v_1, v_2, v_r\}$ is an ortho basis for W.

Dimension

Theorem: Let V_{vs} be a vector space and let $\{V_1, V_2, V_n\}$ be any basis.

a) If a set has more than n vectors then it must be dependent
b) if a set has less than n vectors then it cannot span V.

Define: The dimension of a V_{vs} is the number of vectors in any basis for V_{vs}

Theorem: Let V_{vs} have dimension n and let S be a set in V_{vs} with n vectors. Then S is a basis for V_{vs} iff S spans V or S is independent.

Row Space, Column Space, Null Space

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{1n} \\ a_{21} & a_{22} & a_{2n} \\ a_{m1} & a_{m2} & a_{mn} \end{bmatrix}$$

If A is an m×n matrix then the subspace of R^n spanned by the rows of A is called the Row Space of A. The subspace of R^m spanned by the columns of A is called the Column Space of A. The set of all solutions to Ax=0 is called the Null Space of A.

Theorem: Ax=b is consistent iff b is in the column space of A

Bases for Row Space and Column Space

Results:

1. Elementary row ops don't change the row space of a matrix
2. Elementary row ops do change the column space of a matrix

Theorem: Let R be a row-echelon form A

1. The non-zero rows of R form a basis for the RS(A)
2. The columns of A corresponding to the columns of R with the leading ones form a basis for the column space of A.

Result:

Row operations do not change the dependency relations among the columns of a matrix.

Cryptography

Modular Arithmetic

Define: If m is a positive integer and a and b are any integers then [a = b(mod m)] if a-b is an integer multiple of m.

Note: Every integer "a" is equivalent modulo m to exactly one of {0,1,2…m-1} where the number is called the "residue" of a modulo m. The set is called Z_m

Reciprocals Modulo m

Define: If a is in Z_m = {0,1,2…m-1} then a^{-1} in Z_m is called the "reciprocal" or multiplicative inverse of a modulo m if:

$$aa^{-1} = 1\ (mod\ m)$$

Hill 2-Ciphers

Last two pages of written notes.

End.