ENGG5781 Matrix Analysis and Computations
Lecture 1: Basic Concepts

Wing-Kin (Ken) Ma

2023-24 First Term

Department of Electronic Engineering
The Chinese University of Hong Kong

Lecture 1: Basic Concepts

- notation and conventions
- subspace, linear independence, basis, dimension
- rank, determinant, invertible matrices
- vector norms, inner product
- projections onto subspaces, orthogonal complements
- orthonormal basis, Gram Schmidt
- matrix multiplications and representations, block matrix manipulations
- complexity, floating point operations (flops)

Notation and Conventions

$\mathbb{R}$	the set of real numbers, or real space
$\mathbb{C}$	the set of complex numbers, or complex space
$\mathbb{R}^n$	n-dimensional real space
$\mathbb{C}^n$	n-dimensional complex space
$\mathbb{R}^{m\times n}$	set of all $m \times n$ real-valued matrices
$\mathbb{C}^{m\times n}$	set of all $m \times n$ complex-valued matrices
$\mathbf{x}$	column vector
$x_i, [\mathbf{x}]_i$	ith entry of $\mathbf{x}$
$\mathbf{A}$	matrix
$a_{ij}, [\mathbf{A}]_{ij}$	(i,j)th entry of $\mathbf{A}$
$\mathbb{S}^n$	set of all $n \times n$ real symmetric matrices; i.e, $\mathbf{A} \in \mathbb{R}^{n\times n}$ and $a_{ij} = a_{ji}$ for all i, j
$\mathbb{H}^n$	set of all $n \times n$ complex Hermitian matrices; i.e, $\mathbf{A} \in \mathbb{R}^{n\times n}$ and $a_{ij} = a_{ji}^*$ for all i, j

Notation and Conventions

- vector: $\mathbf{x} \in \mathbb{R}^n$ means that $\mathbf{x}$ is a real-valued n-dimensional column vector; i.e.,

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \qquad x_i \in \mathbb{R} \text{ for all } i.$$

  Similarly, $\mathbf{x} \in \mathbb{C}^n$ means that $\mathbf{x}$ is a complex-valued n-dimensional column vector.

- transpose: let $\mathbf{x} \in \mathbb{R}^n$. The notation $\mathbf{x}^T$ means that

$$\mathbf{x}^T = \begin{bmatrix} x_1, & x_2, & \ldots, & x_n \end{bmatrix}.$$

- Hermitian transpose: let $\mathbf{x} \in \mathbb{C}^n$. The notation $\mathbf{x}^H$ means that

$$\mathbf{x}^H = \begin{bmatrix} x_1^*, & x_2^*, & \ldots, & x_n^* \end{bmatrix},$$

  where the superscript $*$ denotes the complex conjugate.

Notation and Conventions

- matrix: $\mathbf{A} \in \mathbb{R}^{m \times n}$ means that $\mathbf{A}$ is real-valued $m \times n$ matrix

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}, \qquad a_{ij} \in \mathbb{R} \text{ for all } i, j.$$

  Similarly, $\mathbf{A} \in \mathbb{C}^{m \times n}$ means that $\mathbf{A}$ is a complex-valued $m \times n$ matrix.

- unless specified, we denote the ith column of a matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$ as $\mathbf{a}_i \in \mathbb{R}^m$; i.e.,

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1, & \mathbf{a}_2, & \ldots, & \mathbf{a}_n \end{bmatrix}.$$

  The same notation applies to $\mathbf{A} \in \mathbb{C}^{m \times n}$.

Notation and Conventions

- transpose: let $\mathbf{A} \in \mathbb{R}^{m \times n}$. The notation $\mathbf{A}^T$ means that

$$\mathbf{A}^T = \begin{bmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & & & \vdots \\ a_{1n} & a_{m2} & \dots & a_{mn} \end{bmatrix} \in \mathbb{R}^{n \times m}.$$

  - or, we have $\mathbf{B} = \mathbf{A}^T \Longleftrightarrow b_{ij} = a_{ji}$ for all i, j.
  - properties:
    * $(\mathbf{AB})^T = \mathbf{B}^T \mathbf{A}^T$
    * $(\mathbf{A}^T)^T = \mathbf{A}$
    * $(\mathbf{A} + \mathbf{B})^T = \mathbf{A}^T + \mathbf{B}^T$

Notation and Conventions

- Hermitian transpose: let $\mathbf{A} \in \mathbb{C}^{m \times n}$. The notation $\mathbf{A}^H$ means that

$$\mathbf{A}^H = \begin{bmatrix} a_{11}^* & a_{21}^* & \dots & a_{m1}^* \\ a_{12}^* & a_{22}^* & \dots & a_{m2}^* \\ \vdots & & & \vdots \\ a_{1n}^* & a_{m2}^* & \dots & a_{mn}^* \end{bmatrix} \in \mathbb{C}^{n \times m}.$$

  - or, we have $\mathbf{B} = \mathbf{A}^T \Longleftrightarrow b_{ij} = a_{ji}^*$ for all i, j.
  - properties (same as transpose):
    * $(\mathbf{AB})^H = \mathbf{B}^H \mathbf{A}^H$
    * $(\mathbf{A}^H)^H = \mathbf{A}$
    * $(\mathbf{A} + \mathbf{B})^H = \mathbf{A}^H + \mathbf{B}^H$

Notation and Conventions

- trace: let $\mathbf{A} \in \mathbb{R}^{n \times n}$. The trace of $\mathbf{A}$ is

$$\mathrm{tr}(\mathbf{A}) = \sum_{i=1}^{n} a_{ii}.$$

  - properties:
    - $\mathrm{tr}(\mathbf{A}^T) = \mathrm{tr}(\mathbf{A})$
    - $\mathrm{tr}(\mathbf{A} + \mathbf{B}) = \mathrm{tr}(\mathbf{A}) + \mathrm{tr}(\mathbf{B})$
    - $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA})$ for $\mathbf{A}, \mathbf{B}$ of appropriate sizes

- matrix power: let $\mathbf{A} \in \mathbb{R}^{n \times n}$. The notation $\mathbf{A}^2$ means $\mathbf{A}^2 = \mathbf{AA}$, and $\mathbf{A}^k$ means

$$\mathbf{A}^k = \underbrace{\mathbf{AA} \cdots \mathbf{A}}_{k \ \mathbf{A}\text{'s}}.$$

Notation and Conventions

- all-one vectors: we use the notation

$$\mathbf{1} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

  to denote a vector of all 1's.

- zero vectors or matrices: we use the notation $\mathbf{0}$ to denote either a vector of all zeros, or a matrix of all zeros.

- unit vectors: unit vectors are vectors that have only one nonzero element and the nonzero element is 1. We use the notation

$$\mathbf{e}_i = \begin{bmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}^T$$

  to denote a unit vector with the nonzero element at the ith entry.

Notation and Conventions

- identity matrix:

$$\mathbf{I} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix},$$

  where, as a convention, the empty entries are assumed to be zero.

- diagonal matrices: we use the notation

$$\mathrm{Diag}(a_1, \ldots, a_n) = \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix}$$

  to denote a diagonal matrix with diagonals $a_1, \ldots, a_n$. We also use the shorthand notation $\mathrm{Diag}(\mathbf{a}) = \mathrm{Diag}(a_1, \ldots, a_n)$.

Notation and Conventions

- A matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$ is said to be
  - square if $m = n$;
  - tall if $m > n$;
  - fat if $m < n$.

- A matrix $\mathbf{A} \in \mathbb{R}^{n \times n}$ is said to be
  - upper triangular if $a_{ij} = 0$ for all $i > j$;
  - lower triangular if $a_{ij} = 0$ for all $i < j$.

  Examples:

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{bmatrix}, \quad \mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 2 & 0 \\ \frac{1}{8} & 3 & 0 \end{bmatrix}.$$

Subspace

A subset $\mathcal{S}$ of $\mathbb{R}^m$ is said to be a subspace if

$$\begin{matrix} \mathbf{x}, \mathbf{y} \in \mathcal{S}, \\ \alpha, \beta \in \mathbb{R} \end{matrix} \quad \Longrightarrow \quad \alpha\mathbf{x} + \beta\mathbf{y} \in \mathcal{S}.$$

- if $\mathcal{S}$ is a subspace and $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathcal{S}$, any linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_n$, i.e., $\sum_{i=1}^n \alpha_i \mathbf{a}_i$ for some $\boldsymbol{\alpha} \in \mathbb{R}^n$, lies in $\mathcal{S}$.

- some quick facts: let $\mathcal{S}_1, \mathcal{S}_2$ be subspaces of $\mathbb{R}^m$.
  - $\mathcal{S}_1 + \mathcal{S}_2$ is a subspace [1]
  - $\mathcal{S}_1 \cap \mathcal{S}_2$ is a subspace

[1] note the notation $\mathcal{X} + \mathcal{Y} = \{\mathbf{x} + \mathbf{y} \mid \mathbf{x} \in \mathcal{X}, \mathbf{y} \in \mathcal{Y}\}$.

Span

The span of a collection of vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{R}^m$ is defined as

$$\mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} = \left\{ \mathbf{y} \in \mathbb{R}^m \;\middle|\; \mathbf{y} = \sum_{i=1}^{n} \alpha_i \mathbf{a}_i,\ \boldsymbol{\alpha} \in \mathbb{R}^n \right\}.$$

- the set of all linear combinations of $\mathbf{a}_1, \ldots, \mathbf{a}_n$
- a subspace
- Question: any span is a subspace. But can any subspace be written as a span?

  Theorem 1.1. Let $\mathcal{S}$ be a subspace of $\mathbb{R}^m$. There exists a positive integer n and a collection of vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathcal{S}$ such that $\mathcal{S} = \mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$.

  – Implication: we can always represent a subspace by a span

Range Space and Nullspace

The range space of $\mathbf{A} \in \mathbb{R}^{m \times n}$ is defined as

$$\mathcal{R}(\mathbf{A}) = \{\mathbf{y} \in \mathbb{R}^m \mid \mathbf{y} = \mathbf{A}\mathbf{x},\ \mathbf{x} \in \mathbb{R}^n\}.$$

- essentially the same as span

The nullspace of $\mathbf{A} \in \mathbb{R}^{m \times n}$ is defined as

$$\mathcal{N}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{A}\mathbf{x} = \mathbf{0}\}.$$

- a nullspace is a subspace (verify as a mini exercise)
- by Theorem 1.1, we can represent a nullspace by $\mathcal{N}(\mathbf{A}) = \mathcal{R}(\mathbf{B})$ for some $\mathbf{B} \in \mathbb{R}^{n \times r}$ and positive integer r.

Linear Independence

A collection of vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{R}^m$ is said to be linearly independent if

$$\sum_{i=1}^{n} \alpha_i \mathbf{a}_i \neq \mathbf{0}, \quad \text{for all } \boldsymbol{\alpha} \in \mathbb{R}^n \text{ with } \boldsymbol{\alpha} \neq \mathbf{0};$$

and linearly dependent otherwise.

- an equivalent way of defining linear dependence: $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{R}^m$ is a linearly dependent vector set if there exists $\boldsymbol{\alpha} \in \mathbb{R}^n$, $\boldsymbol{\alpha} \neq \mathbf{0}$, such that

$$\sum_{i=1}^{n} \alpha_i \mathbf{a}_i = \mathbf{0}.$$

Linear Independence

Some known facts (some easy to show, some not):

- if $\{\mathbf{a}_1, \ldots \mathbf{a}_n\} \subset \mathbb{R}^m$ is linearly independent, then any $\mathbf{a}_j$ *cannot* be a linear combination of the other $\mathbf{a}_i$'s; i.e., $\mathbf{a}_j \neq \sum_{i \neq j} \alpha_i \mathbf{a}_i$ for any α_i's.

- if $\{\mathbf{a}_1, \ldots \mathbf{a}_n\} \subset \mathbb{R}^m$ is linearly dependent, then *there exists* an $\mathbf{a}_j$ such that $\mathbf{a}_j$ is a linear combination of the other $\mathbf{a}_i$'s; i.e., $\mathbf{a}_j = \sum_{i \neq j} \alpha_i \mathbf{a}_i$ for some α_i's.

- if $\{\mathbf{a}_1, \ldots \mathbf{a}_n\} \subset \mathbb{R}^m$ is linearly independent, then $n \leq m$ must hold.

- let $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\} \subset \mathbb{R}^m$ be a linearly independent vector set. Suppose $\mathbf{y} \in \mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$. Then the coefficient $\boldsymbol{\alpha}$ for the representation

$$\mathbf{y} = \sum_{i=1}^{n} \alpha_i \mathbf{a}_i$$

  is unique; i.e., there does *not* exist a $\boldsymbol{\beta} \in \mathbb{R}^n$, $\boldsymbol{\beta} \neq \boldsymbol{\alpha}$, such that $\mathbf{y} = \sum_{i=1}^{n} \beta_i \mathbf{a}_i$.

Linear Independence

Let $\{\mathbf{a}_1, \ldots \mathbf{a}_n\} \subset \mathbb{R}^m$, and denote $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ as an index subset with $k \leq n$ and $i_j \neq i_l$ for all $j \neq l$.

A vector subset $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is called a maximal linearly independent subset of $\{\mathbf{a}_1, \ldots \mathbf{a}_n\}$ if

1. $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is linearly independent;
2. $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is not contained by any other linearly independent subset of $\{\mathbf{a}_1, \ldots \mathbf{a}_n\}$.

- physical meaning: find a set of non-redundant vectors from $\{\mathbf{a}_1, \ldots \mathbf{a}_n\}$

Linear Independence

- example:

$$\mathbf{a}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{a}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{a}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \quad \mathbf{a}_4 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

The linearly independent subets of $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4\}$ are

$$\{\mathbf{a}_1\}, \{\mathbf{a}_2\}, \{\mathbf{a}_3\}, \{\mathbf{a}_4\},$$
$$\{\mathbf{a}_1, \mathbf{a}_2\}, \{\mathbf{a}_1, \mathbf{a}_3\}, \{\mathbf{a}_1, \mathbf{a}_4\}, \{\mathbf{a}_2, \mathbf{a}_3\}, \{\mathbf{a}_2, \mathbf{a}_4\}, \{\mathbf{a}_3, \mathbf{a}_4\},$$
$$\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}, \quad \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_4\}, \quad \{\mathbf{a}_1, \mathbf{a}_3, \mathbf{a}_4\}.$$

But the maximal linearly independent subsets are

$$\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}, \quad \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_4\}, \quad \{\mathbf{a}_1, \mathbf{a}_3, \mathbf{a}_4\}.$$

Linear Independence

Facts:

- $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is a maximal linearly independent subset of $\{\mathbf{a}_1, \ldots \mathbf{a}_n\}$ if and only if $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}, \mathbf{a}_j\}$ is linearly dependent for any $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$

- if $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is a maximal linearly independent subset of $\{\mathbf{a}_1, \ldots \mathbf{a}_n\}$, then

$$\mathrm{span}\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\} = \mathrm{span}\{\mathbf{a}_1, \ldots \mathbf{a}_n\}.$$

Basis

Let $\mathcal{S} \subseteq \mathbb{R}^m$ be a subspace with $\mathcal{S} \neq \{\mathbf{0}\}$.

A vector set $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\} \subset \mathbb{R}^m$ is called a basis for $\mathcal{S}$ if $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ is linearly independent and

$$\mathcal{S} = \mathrm{span}\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}.$$

- examples: let $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ be a maximal linearly independent vector subset of $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. Then, $\{\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_k}\}$ is a basis for $\mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$.

Some facts:

- we may have more than one basis for $\mathcal{S}$
- all bases for $\mathcal{S}$ have the same number of elements; i.e., if $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ and $\{\mathbf{c}_1, \ldots, \mathbf{c}_l\}$ are bases for $\mathcal{S}$, then $k = l$

Dimension of a Subspace

The dimension of a subspace $\mathcal{S}$, with $\mathcal{S} \neq \{\mathbf{0}\}$, is defined as the number of elements of a basis for $\mathcal{S}$. The dimension of $\{\mathbf{0}\}$ is defined as 0.

- $\dim \mathcal{S}$ will be used as the notation for denoting the dimension of $\mathcal{S}$
- physical meaning: effective degrees of freedom of the subspace
- examples:
  - $\dim \mathbb{R}^m = m$
  - if k is the number of maximal linearly independent vectors of $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$, then $\dim \operatorname{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} = k$.

Dimension of a Subspace

Property 1.1. Let $\mathcal{S}, \mathcal{S}_1, \mathcal{S}_2 \subseteq \mathbb{R}^m$ be subspaces.

1. If $\mathcal{S}_1 \subseteq \mathcal{S}_2$, then $\dim \mathcal{S}_1 \leq \dim \mathcal{S}_2$.

2. If $\mathcal{S}_1 \subseteq \mathcal{S}_2$ and $\dim \mathcal{S}_1 = \dim \mathcal{S}_2$, then $\mathcal{S}_1 = \mathcal{S}_2$.

3. $\dim \mathcal{S} = m$ if and only if $\mathcal{S} = \mathbb{R}^m$.

4. $\dim(\mathcal{S}_1 + \mathcal{S}_2) + \dim(\mathcal{S}_1 \cap \mathcal{S}_2) = \dim \mathcal{S}_1 + \dim \mathcal{S}_2$.

5. $\dim(\mathcal{S}_1 + \mathcal{S}_2) \leq \dim \mathcal{S}_1 + \dim \mathcal{S}_2$.

Rank

The rank of a matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$, denoted by $\mathrm{rank}(\mathbf{A})$, is defined as the number of elements of a maximal linearly independent subset of $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$.

- or, $\mathrm{rank}(\mathbf{A})$ is the maximum number of linearly independent columns of $\mathbf{A}$
- $\dim \mathcal{R}(\mathbf{A}) = \mathrm{rank}(\mathbf{A})$ by definition

Facts:

- $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}^T)$, i.e., the rank of $\mathbf{A}$ is also the maximum number of linearly independent rows of $\mathbf{A}$
- $\mathrm{rank}(\mathbf{A} + \mathbf{B}) \leq \mathrm{rank}(\mathbf{A}) + \mathrm{rank}(\mathbf{B})$
- $\mathrm{rank}(\mathbf{AB}) \leq \min\{\mathrm{rank}(\mathbf{A}), \mathrm{rank}(\mathbf{B})\}$. Also, the equality above holds if the columns of $\mathbf{A}$ are linearly independent and the rows of $\mathbf{B}$ are linearly independent.

Rank

- $\mathbf{A}$ is said to have
  - full column rank if the columns of $\mathbf{A}$ are linearly independent (more precisely, the collection of *all* columns of $\mathbf{A}$ is linearly independent)
    * $\mathbf{A} \in \mathbb{R}^{m \times n}$ being of full-column rank $\Longleftrightarrow m \geq n, \mathrm{rank}(\mathbf{A}) = n$
  - full row rank if the rows of $\mathbf{A}$ are linearly independent
    * $\mathbf{A} \in \mathbb{R}^{m \times n}$ being of full-row rank $\Longleftrightarrow m \leq n, \mathrm{rank}(\mathbf{A}) = m$
  - full rank if $\mathrm{rank}(\mathbf{A}) = \min\{m, n\}$; i.e., it has either full column rank or full row rank
  - rank deficient if $\mathrm{rank}(\mathbf{A}) < \min\{m, n\}$

Invertible Matrices

A square matrix $\mathbf{A}$ is said to be nonsingular or invertible if the columns of $\mathbf{A}$ are linearly independent, and singular otherwise.

- alternatively, we say $\mathbf{A}$ is singular if $\mathbf{A}\mathbf{x} = \mathbf{0}$ for some $\mathbf{x} \neq \mathbf{0}$.

The inverse of an invertible $\mathbf{A}$, denoted by $\mathbf{A}^{-1}$, is a square matrix that satisfies

$$\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}.$$

Invertible Matrices

Facts (for a nonsingular $\mathbf{A}$):

- $\mathbf{A}^{-1}$ always exists and is unique (or there are no two inverses of $\mathbf{A}$)
- $\mathbf{A}^{-1}$ is nonsingular
- $\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$
- $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$
- $(\mathbf{A}\mathbf{B})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$, where $\mathbf{A}, \mathbf{B}$ are square and nonsingular
- $(\mathbf{A}^T)^{-1} = (\mathbf{A}^{-1})^T$
  - as a shorthand notation, we will denote $\mathbf{A}^{-T} = (\mathbf{A}^T)^{-1}$

Determinant

Let $\mathbf{A} \in \mathbb{R}^{m \times m}$. The determinant of $\mathbf{A}$, denoted by $\det(\mathbf{A})$, is defined inductively.

- if $m = 1$, $\det(\mathbf{A}) = a_{11}$.
- if $m \geq 2$, we have the following:
  - let $\mathbf{A}_{ij} \in \mathbb{R}^{(m-1)\times(m-1)}$ be a submatrix of $\mathbf{A}$ obtained by deleting the ith row and jth column of $\mathbf{A}$. Let $c_{ij} = (-1)^{i+j} \det(\mathbf{A}_{ij})$.
  - cofactor expansion:

$$\det(\mathbf{A}) = \sum_{j=1}^{m} a_{ij} c_{ij}, \quad \text{for any } i = 1, \dots, m$$

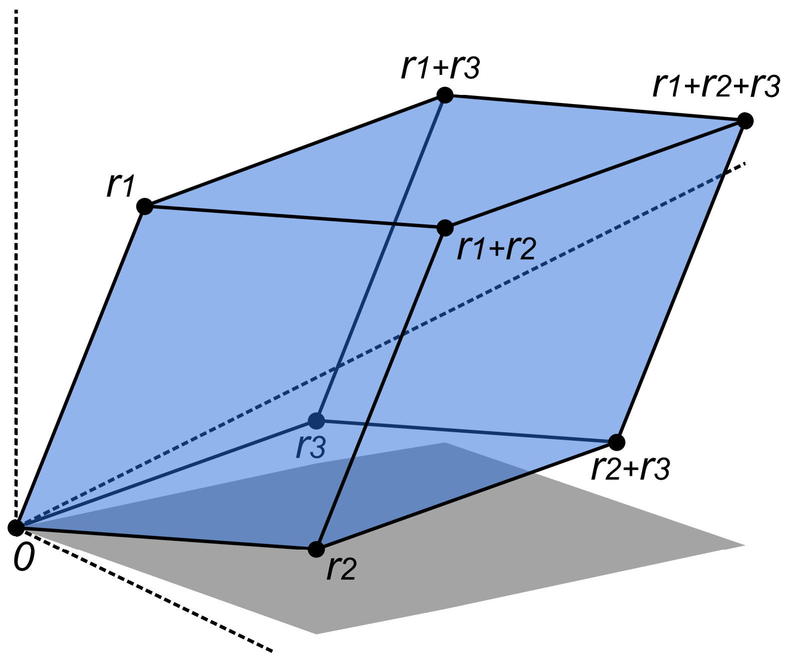
$$\det(\mathbf{A}) = \sum_{i=1}^{m} a_{ij} c_{ij}, \quad \text{for any } j = 1, \dots, m$$

  - remark: c_{ij}'s are called the cofactors, $\det(\mathbf{A}_{ij})$'s are called the minors

Determinant

Some interpretations of determinant:

- (important) $\mathbf{A}\mathbf{x} = \mathbf{0}$ for some $\mathbf{x} \neq \mathbf{0}$ if and only if $\det(\mathbf{A}) = 0$
- $|\det(\mathbf{A})|$ is the volume of the parallelepiped $\mathcal{P} = \{\mathbf{y} = \sum_{i=1}^{m} \alpha_i \mathbf{a}_i \mid \alpha_i \in [0,1] \; \forall i\}$



Source: Wiki. r_1, r_2, r_3 are $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ on $\mathbb{R}^3$.

Determinant

Properties:

- $\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$ for any $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{m \times m}$
- $\det(\mathbf{A}) = \det(\mathbf{A}^T)$
- $\det(\alpha\mathbf{A}) = \alpha^m \det(\mathbf{A})$ for any $\alpha \in \mathbb{R}, \mathbf{A} \in \mathbb{R}^{m \times m}$
- $\det(\mathbf{A}^{-1}) = 1/\det(\mathbf{A})$ for any nonsingular $\mathbf{A}$
- $\det(\mathbf{B}^{-1}\mathbf{AB}) = \det(\mathbf{A})$ for any nonsingular $\mathbf{B}$
- $\mathbf{A}^{-1} = \dfrac{1}{\det(\mathbf{A})}\tilde{\mathbf{A}}$, where $\tilde{a}_{ij} = c_{ji}$ (the cofactor) for all i, j ($\mathbf{A}$ is nonsingular)
  - remark: $\tilde{\mathbf{A}}$ is called the adjoint of $\mathbf{A}$

Determinant

More properties:

- if $\mathbf{A} \in \mathbb{R}^{m \times m}$ is triangular, either upper or lower,

$$\det(\mathbf{A}) = \prod_{i=1}^{m} a_{ii}$$

  - proof: apply cofactor expansion inductively

- if $\mathbf{A} \in \mathbb{R}^{m \times m}$ takes a block upper triangular form

$$\mathbf{A} = \begin{bmatrix} \mathbf{B} & \mathbf{C} \\ \mathbf{0} & \mathbf{D} \end{bmatrix},$$

  where $\mathbf{B}$ and $\mathbf{D}$ are square (and can be of different sizes), then

$$\det(\mathbf{A}) = \det(\mathbf{B}) \det(\mathbf{D}).$$

  The same result also holds when $\mathbf{A}$ takes a block lower triangular form.

Vector Norms

A function $f : \mathbb{R}^n \to \mathbb{R}$ is called a vector norm if

1. $f(\mathbf{x}) \geq 0$ for any $\mathbf{x} \in \mathbb{R}^n$
2. $f(\mathbf{x}) = 0$ if and only if $\mathbf{x} = \mathbf{0}$
3. $f(\mathbf{x} + \mathbf{y}) \leq f(\mathbf{x}) + f(\mathbf{y})$ for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$
4. $f(\alpha\mathbf{x}) = |\alpha| f(\mathbf{x})$ for any $\alpha \in \mathbb{R}$, $\mathbf{x} \in \mathbb{R}^n$

- used to measure the length of a vector
- we usually use the notation $\|\cdot\|$ to denote a norm
- also used to measure the distance of two vectors, specifically, via $\|\mathbf{x} - \mathbf{y}\|$ where $\mathbf{x}, \mathbf{y}$ are the two vectors

Vector Norm

Examples of norm:

- 2-norm or Euclidean norm: $\|\mathbf{x}\|_2 = \sqrt{\sum_{i=1}^{n} |x_i|^2} = (\mathbf{x}^T\mathbf{x})^{1/2}$

- 1-norm or Manhattan norm: $\|\mathbf{x}\|_1 = \sum_{i=1}^{n} |x_i|$

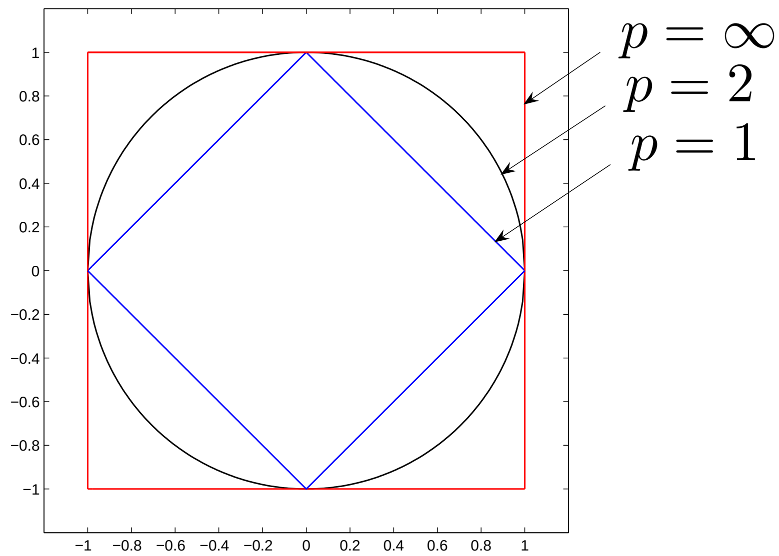
- ∞-norm: $\|\mathbf{x}\|_\infty = \max_{i=1,\ldots,n} |x_i|$

- p-norm, $p \geq 1$: $\|\mathbf{x}\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{\frac{1}{p}}$

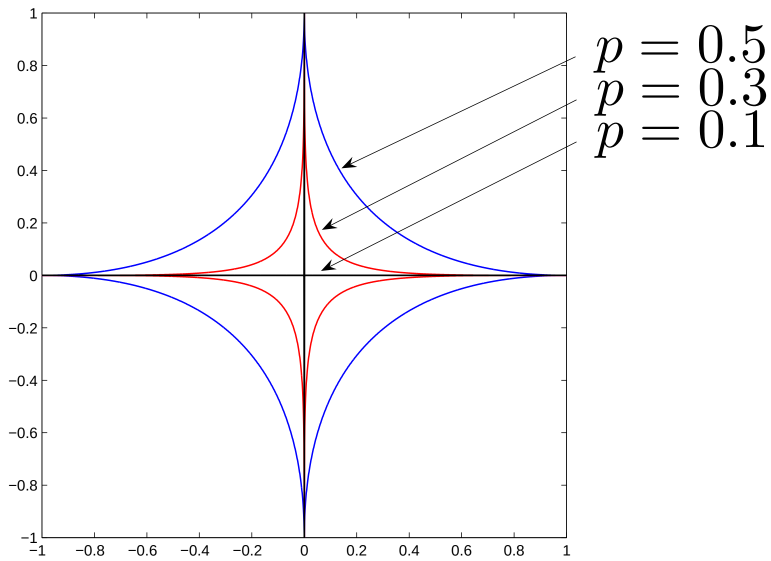
ℓ_p Function

Let

$$f_p(\mathbf{x}) = \left(\sum_{i=1}^{n} |x_i|^p \right)^{\frac{1}{p}}, \qquad p > 0.$$



(a) Region of $f_p(\mathbf{x}) = 1$, $p \geq 1$.



(b) Region of $f_p(\mathbf{x}) = 1$, $p \leq 1$.

- f_p is *not* a norm for $0 < p < 1$
- when $p \to 0$, f_p is like the cardinality function $\mathrm{card}(\mathbf{x}) = \sum_{i=1}^{n} \mathbb{1}\{x_i \neq 0\}$, where $\mathbb{1}\{x \neq 0\} = 1$ if $x \neq 0$ and $\mathbb{1}\{x \neq 0\} = 0$ if $x = 0$.

Inner Product and Angle

The inner product of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is defined as

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} y_i x_i = \mathbf{y}^T \mathbf{x}.$$

- $\mathbf{x}, \mathbf{y}$ are said to be orthogonal to each other if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$
- $\mathbf{x}, \mathbf{y}$ are said to be parallel if $\mathbf{x} = \alpha \mathbf{y}$ for some α
  - for parallel $\mathbf{x}, \mathbf{y}$ we have $\langle \mathbf{x}, \mathbf{y} \rangle = \pm \|\mathbf{x}\|_2 \|\mathbf{y}\|_2$

The angle between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is defined as

$$\theta = \cos^{-1}\left(\frac{\mathbf{y}^T \mathbf{x}}{\|\mathbf{x}\|_2 \|\mathbf{y}\|_2} \right).$$

- $\mathbf{x}, \mathbf{y}$ are orthogonal if $\theta = \pm \pi/2$
- $\mathbf{x}, \mathbf{y}$ are parallel if $\theta = 0$ or $\theta = \pm \pi$

Important Inequalities for Inner Product

Cauchy-Schwarz inequality:

$$|\mathbf{x}^T\mathbf{y}| \leq \|\mathbf{x}\|_2\|\mathbf{y}\|_2.$$

Also, the above equality holds if and only if $\mathbf{x} = \alpha\mathbf{y}$ for some $\alpha \in \mathbb{R}$.

- proof: suppose $\mathbf{y} \neq \mathbf{0}$; the case of $\mathbf{y} = \mathbf{0}$ is trivial. For any $\alpha \in \mathbb{R}$,

$$0 \leq \|\mathbf{x} - \alpha\mathbf{y}\|_2^2 = (\mathbf{x} - \alpha\mathbf{y})^T(\mathbf{x} - \alpha\mathbf{y}) = \|\mathbf{x}\|_2^2 - 2\alpha\mathbf{x}^T\mathbf{y} + \alpha^2\|\mathbf{y}\|_2^2. \qquad (*)$$

Also, the equality above holds if and only if $\mathbf{x} = \beta\mathbf{y}$ for some β. Let

$$f(\alpha) = \|\mathbf{x}\|_2^2 - 2\alpha\mathbf{x}^T\mathbf{y} + \alpha^2\|\mathbf{y}\|_2^2.$$

The function f is minimized when $\alpha = (\mathbf{x}^T\mathbf{y})/\|\mathbf{y}\|_2^2$. Plugging this α back to $(*)$ leads to the desired result.

Important Inequalities for Inner Product

Hölder inequality:

$$|\mathbf{x}^T\mathbf{y}| \leq \|\mathbf{x}\|_p \|\mathbf{y}\|_q,$$

for any p, q such that $1/p + 1/q = 1$, $p \geq 1$.

- examples:
  - $(p,q) = (2,2)$: Cauchy-Schwarz inequality
  - $(p,q) = (1,\infty)$: $|\mathbf{x}^T\mathbf{y}| \leq \|\mathbf{x}\|_1 \|\mathbf{y}\|_\infty$. This can be easily verified to be true:

$$|\mathbf{x}^T\mathbf{y}| \leq \textstyle\sum_{i=1}^n |x_i y_i| \leq \max_j |y_j| \left(\sum_{i=1}^n |x_i|\right) = \|\mathbf{x}\|_1 \|\mathbf{y}\|_\infty.$$

Projections on Subspaces

Let $\mathcal{S} \subseteq \mathbb{R}^m$ be a nonempty closed set (not necessarily a subspace).

Let $\mathbf{y} \in \mathbb{R}^m$ be given.

A projection of $\mathbf{y}$ onto $\mathcal{S}$ is any solution to

$$\min_{\mathbf{z} \in \mathcal{S}} \; \|\mathbf{z} - \mathbf{y}\|_2^2$$

- a projection of $\mathbf{y}$ onto $\mathcal{S}$ is any point that is closest to $\mathbf{y}$ and lies in $\mathcal{S}$

- notation: if, for every $\mathbf{y} \in \mathbb{R}^m$, there is always *only one* projection of $\mathbf{y}$ onto $\mathcal{S}$, then we denote

$$\Pi_{\mathcal{S}}(\mathbf{y}) = \arg\min_{\mathbf{z} \in \mathcal{S}} \; \|\mathbf{z} - \mathbf{y}\|_2^2$$

  and $\Pi_{\mathcal{S}}$ is called *the* projection (or projection operator) of $\mathbf{y}$ onto $\mathcal{S}$.

Projections onto Subspaces

Theorem 1.2 (Projection Theorem)**.** Let $\mathcal{S}$ be a subspace of $\mathbb{R}^m$.

1. for every $\mathbf{y} \in \mathbb{R}^m$, there exists a unique vector $\mathbf{y}_s \in \mathcal{S}$ that minimizes $\|\mathbf{z} - \mathbf{y}\|_2^2$ over $\mathbf{z} \in \mathcal{S}$. Thus, we can use the notation $\Pi_{\mathcal{S}}(\mathbf{y}) = \arg\min_{\mathbf{z} \in \mathcal{S}} \ \|\mathbf{z} - \mathbf{y}\|_2^2$.

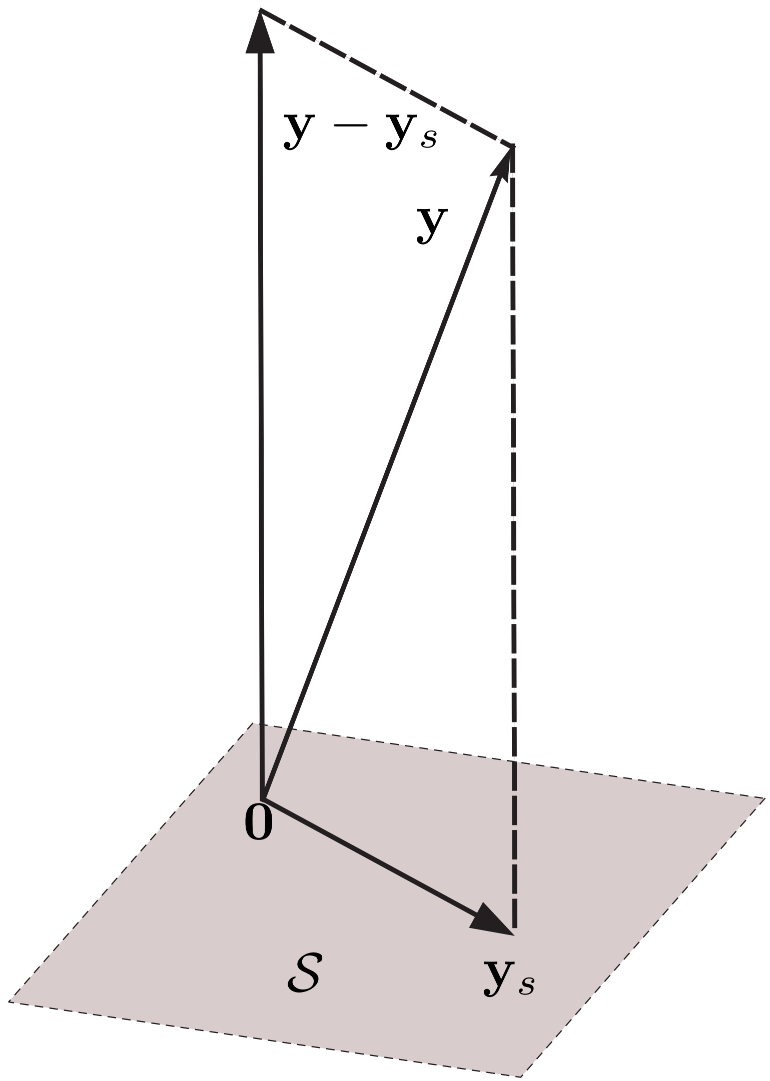
2. given $\mathbf{y} \in \mathbb{R}^m$, we have the equivalence

$$\mathbf{y}_s = \Pi_{\mathcal{S}}(\mathbf{y}) \quad \Longleftrightarrow \quad \mathbf{y}_s \in \mathcal{S}, \quad \mathbf{z}^T(\mathbf{y}_s - \mathbf{y}) = 0 \text{ for all } \mathbf{z} \in \mathcal{S}.$$

- a special case of the projection theorem for convex sets
  - the latter plays a key role in convex optimization

- the subspace projection theorem above is very useful, as we will see

Projections onto Subspaces



Orthogonal Complements

Let $\mathcal{S} \subseteq \mathbb{R}^m$ be a nonempty closed set.

The orthogonal complement of $\mathcal{S}$ is defined as

$$\mathcal{S}^\perp = \{\mathbf{y} \in \mathbb{R}^m \mid \mathbf{z}^T\mathbf{y} = 0 \text{ for all } \mathbf{z} \in \mathcal{S}\}.$$

- $\mathcal{S}^\perp$ is a subspace (easy to verify)
- any $\mathbf{z} \in \mathcal{S}, \mathbf{y} \in \mathcal{S}^\perp$ are orthogonal
- either $\mathcal{S} \cap \mathcal{S}^\perp = \{\mathbf{0}\}$ or $\mathcal{S} \cap \mathcal{S}^\perp = \emptyset$
- some facts for subspaces:
  - $\mathcal{R}(\mathbf{A})^\perp = \mathcal{N}(\mathbf{A}^T)$ (also easy to verify)
  - $\mathcal{N}(\mathbf{A}) = \mathcal{R}(\mathbf{A}^T)^\perp$

Orthogonal Complements

What happens to the orthogonal complement if $\mathcal{S}$ is a subspace?

Theorem 1.3. Let $\mathcal{S} \subseteq \mathbb{R}^m$ be a subspace.

1. for every $\mathbf{y} \in \mathbb{R}^m$, there exists a unique $(\mathbf{y}_s, \mathbf{y}_c) \in \mathcal{S} \times \mathcal{S}^\perp$ such that

   $$\mathbf{y} = \mathbf{y}_s + \mathbf{y}_c.$$

   Also, such a $(\mathbf{y}_s, \mathbf{y}_c)$ is $\mathbf{y}_s = \Pi_{\mathcal{S}}(\mathbf{y}), \mathbf{y}_c = \mathbf{y} - \Pi_{\mathcal{S}}(\mathbf{y})$.

2. the projection of $\mathbf{y}$ onto $\mathcal{S}^\perp$ can be determined by $\Pi_{\mathcal{S}^\perp}(\mathbf{y}) = \mathbf{y} - \Pi_{\mathcal{S}}(\mathbf{y})$.

- proof sketch: by the projection theorem. We can rephrase the projection theorem as

  $$\mathbf{y}_s \in \mathcal{S},\ \mathbf{y} - \mathbf{y}_s \in \mathcal{S}^\perp \quad \Longleftrightarrow \quad \mathbf{y}_s \in \Pi_{\mathcal{S}}(\mathbf{y}).$$

  This leads us to Statement 1 of Theorem 1.3.

Orthogonal Complements

Consequences of Theorem 1.3:

Property 1.2. Let $\mathcal{S} \subseteq \mathbb{R}^m$ be a subspace.

1. $\mathcal{S} + \mathcal{S}^\perp = \mathbb{R}^m$;
2. $\dim \mathcal{S} + \dim \mathcal{S}^\perp = m$;
3. $(\mathcal{S}^\perp)^\perp = \mathcal{S}$.

- examples: let $\mathbf{A} \in \mathbb{R}^{m \times n}$.
  - $\dim \mathcal{R}(\mathbf{A}) + \dim \mathcal{R}(\mathbf{A})^\perp = m$
  - and then $\dim \mathcal{R}(\mathbf{A}) + \dim \mathcal{N}(\mathbf{A}^T) = m$
  - and then $\dim \mathcal{N}(\mathbf{A}) = n - \dim \mathcal{R}(\mathbf{A}^T) = n - \mathrm{rank}(\mathbf{A}) \geq n - \min\{m, n\}$
    - implication: if $\mathbf{A}$ is fat, the dim. of $\mathcal{N}(\mathbf{A})$ is at least $n - m$

Property 1.3. $\mathcal{S}_1 \cap \mathcal{S}_2 = (\mathcal{S}_1^\perp + \mathcal{S}_2^\perp)^\perp$, where $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathbb{R}^m$ are subspaces.

Orthogonal Bases and Matrices

A collection of nonzero vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{R}^m$ is said to be

- orthogonal if $\mathbf{a}_i^T \mathbf{a}_j = 0$ for all i, j with $i \neq j$
- orthonormal if $\|\mathbf{a}_i\|_2 = 1$ for all i and $\mathbf{a}_i^T \mathbf{a}_j = 0$ for all i, j with $i \neq j$.

The same definition applies to complex $\mathbf{a}_i$'s, but we need to replace "T" with "H".

Examples:

- $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\} \subset \mathbb{R}^m$ is orthonormal; in fact, it's an orthonormal basis for $\mathbb{R}^m$
- any subset of $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ is orthornormal
- (to be learnt) discrete Fourier transform (DFT), Haar transform, etc., form orthonormal bases

Orthogonal Bases and Matrices

Some immediate facts:

- an orthonormal set of vectors is also linearly independent.
- let $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{R}^m$ be an orthonormal set of vectors. Suppose $\mathbf{y} \in \mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. Then the coefficient $\boldsymbol{\alpha}$ for the representation

$$\mathbf{y} = \sum_{i=1}^{n} \alpha_i \mathbf{a}_i$$

  is uniquely given by $\alpha_i = \mathbf{a}_i^T \mathbf{y}$, $i = 1, \ldots, n$.

A not so immediate fact:

- (important) every subspace $\mathcal{S}$ with $\mathcal{S} \neq \{\mathbf{0}\}$ has an orthonormal basis.
  - this will be clear when we consider Gram-Schmidt

Orthogonal Bases and Matrices

A real matrix $\mathbf{Q}$ is said to be

- orthogonal if it is square and its columns are orthonormal (why we call it an orthogonal matrix, but not an orthonormal matrix?)
- semi-orthogonal if its columns are orthonormal
  - a semi-orthogonal $\mathbf{Q}$ must be tall or square

A complex matrix $\mathbf{Q}$ is said to be unitary if it is square and its columns are orthonormal, and semi-unitary if its columns are orthonormal.

Example: consider a transformation $\mathbf{y} = \mathbf{Q}\mathbf{x}$, where

$$\mathbf{Q} = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix},$$

where $\theta \in [0, 2\pi)$. This $\mathbf{Q}$ is orthogonal. Also, it performs rotation and reflection.

Orthogonal Bases and Matrices

Facts:

- $\mathbf{Q}^T\mathbf{Q} = \mathbf{I}$ and $\mathbf{Q}\mathbf{Q}^T = \mathbf{I}$ for orthogonal $\mathbf{Q}$
- $\mathbf{Q}^T\mathbf{Q} = \mathbf{I}$ (but *not* necessarily $\mathbf{Q}\mathbf{Q}^T = \mathbf{I}$) for semi-orthogonal $\mathbf{Q}$
- $\|\mathbf{Q}\mathbf{x}\|_2 = \|\mathbf{x}\|_2$ for orthogonal $\mathbf{Q}$
  - physical meaning: rotation and reflection do not affect the vector length
- for every tall and semi-orthogonal matrix $\mathbf{Q}_1 \in \mathbb{R}^{n \times k}$, there exists a matrix $\mathbf{Q}_2 \in \mathbb{R}^{n \times (n-k)}$ such that $[\ \mathbf{Q}_1\ \mathbf{Q}_2\ ]$ is orthogonal

Orthogonal Bases and Matrices

Question: given a subspace $\mathcal{S}$, how do we know that it has an orthonormal basis?

- we know that every subspace has a basis, c.f. Theorem 1.1
- but the theorem doesn't say if that basis is orthonormal
- we can construct an orthonormal basis from a basis—and one way to do it is the Gram-Schmidt procedure

Gram-Schmidt Procedure

Algorithm: Gram-Schmidt
input: a collection of vectors $\mathbf{a}_1, \dots, \mathbf{a}_n$, presumably linearly independent
$\tilde{\mathbf{q}}_1 = \mathbf{a}_1$, $\mathbf{q}_1 = \tilde{\mathbf{q}}_1 / \|\tilde{\mathbf{q}}_1\|_2$
for $i = 2, \dots, n$
    $\tilde{\mathbf{q}}_i = \mathbf{a}_i - \sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i) \mathbf{q}_j$
    $\mathbf{q}_i = \tilde{\mathbf{q}}_i / \|\tilde{\mathbf{q}}_i\|_2$
end
output: $\mathbf{q}_1, \dots, \mathbf{q}_n$

- Fact: Suppose that $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent. The collection of vectors $\mathbf{q}_1, \dots, \mathbf{q}_n$ produced by the Gram-Schmidt procedure is orthonormal and satisfies

$$\mathrm{span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\} = \mathrm{span}\{\mathbf{q}_1, \dots, \mathbf{q}_n\}.$$

- here we use Gram-Schmidt to identify the existence of an orthonormal basis for a subspace, but it is a numerical algorithm

Gram-Schmidt Procedure

Proof of the fact on the last page:

- assume linearly independent $\mathbf{a}_1, \ldots, \mathbf{a}_n$
- consider $i = 2$.
  - $\tilde{\mathbf{q}}_2$ is a linear combination of $\mathbf{a}_1, \mathbf{a}_2$ and is nonzero:

$$\tilde{\mathbf{q}}_2 = \mathbf{a}_2 - (\mathbf{q}_1^T \mathbf{a}_2)\mathbf{q}_1 = \mathbf{a}_2 - (\mathbf{q}_1^T \mathbf{a}_2 / \|\mathbf{a}_1\|_2)\mathbf{a}_1; \qquad (\dagger)$$

    the linear independence of $\mathbf{a}_1, \mathbf{a}_2$ implies $\tilde{\mathbf{q}}_2 \neq \mathbf{0}$.
  - $\mathbf{a}_2$ is a linear combination of $\mathbf{q}_1, \mathbf{q}_2$: seen from ($\dagger$)
  - consequence: $\mathrm{span}\{\mathbf{a}_1, \mathbf{a}_2\} = \mathrm{span}\{\mathbf{q}_1, \mathbf{q}_2\}$ (why?)
  - $\tilde{\mathbf{q}}_2$ is orthogonal to $\mathbf{q}_1$:

$$\mathbf{q}_1^T \tilde{\mathbf{q}}_2 = \mathbf{q}_1^T (\mathbf{a}_2 - (\mathbf{q}_1^T \mathbf{a}_2)\mathbf{q}_1) = \mathbf{q}_1^T \mathbf{a}_2 - \mathbf{q}_1^T \mathbf{a}_2 = 0.$$

Gram-Schmidt Procedure

- consider $i \geq 2$.
  - $\tilde{\mathbf{q}}_i$ is a linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}$ and is nonzero: by induction, $\mathbf{q}_1, \ldots \mathbf{q}_{i-1}$ are linear combinations of $\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}$. So,

    $$\tilde{\mathbf{q}}_i = \mathbf{a}_i - \textstyle\sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i) \mathbf{q}_j \qquad (\ddagger)$$

    is a linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_i$. The linear independence of $\mathbf{a}_1, \ldots, \mathbf{a}_i$ implies $\tilde{\mathbf{q}}_i \neq \mathbf{0}$.
  - $\mathbf{a}_i$ is a linear combination of $\mathbf{q}_1, \ldots, \mathbf{q}_i$: seen from $(\ddagger)$
  - consequence: $\mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_i\} = \mathrm{span}\{\mathbf{q}_1, \ldots, \mathbf{q}_i\}$
  - $\tilde{\mathbf{q}}_i$ is orthogonal to $\mathbf{q}_1, \ldots, \mathbf{q}_{i-1}$: by induction, $\mathbf{q}_1, \ldots, \mathbf{q}_{i-1}$ are orthonormal. For any $k \in \{1, \ldots, i-1\}$,

    $$\mathbf{q}_k^T \tilde{\mathbf{q}}_i = \mathbf{q}_k^T (\mathbf{a}_i - \textstyle\sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i) \mathbf{q}_j) = \mathbf{q}_k^T \mathbf{a}_i - \mathbf{q}_k^T \mathbf{a}_i = 0.$$

Gram-Schmidt Procedure

More comments:

- the step

$$\tilde{\mathbf{q}}_i = \mathbf{a}_i - \textstyle\sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i) \mathbf{q}_j$$

  can be shown to be equivalent to

$$\tilde{\mathbf{q}}_i = \Pi_{\mathrm{span}\{\mathbf{q}_1,\ldots,\mathbf{q}_{i-1}\}^\perp}(\mathbf{a}_i) = \Pi_{\mathrm{span}\{\mathbf{a}_1,\ldots,\mathbf{a}_{i-1}\}^\perp}(\mathbf{a}_i);$$

  this will be seen in the LS lecture.

- the Gram-Schmidt procedure can be modified in various ways
  - e.g., it can be modified to do linear independence test, or to find a maximal linearly independent vector subset

Matrix Product Representations

Let $\mathbf{A} \in \mathbb{R}^{m\times k}$, $\mathbf{B} \in \mathbb{R}^{k\times n}$, and consider

$$\mathbf{C} = \mathbf{A}\mathbf{B}.$$

- column representation:

$$\mathbf{c}_i = \mathbf{A}\mathbf{b}_i, \quad i = 1, \ldots, n$$

(I didn't say anything so I assume you know that $\mathbf{c}_i$ and $\mathbf{b}_i$ are the ith column of $\mathbf{C}$ and $\mathbf{B}$, resp.)

- inner-product representation: redefine $\mathbf{a}_i \in \mathbb{R}^k$ as the ith row of $\mathbf{A}$.

$$\mathbf{A}\mathbf{B} = \begin{bmatrix} \mathbf{a}_1^T \\ \vdots \\ \mathbf{a}_m^T \end{bmatrix} \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_n \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1^T\mathbf{b}_1 & \cdots & \mathbf{a}_1^T\mathbf{b}_n \\ \vdots & & \vdots \\ \mathbf{a}_m^T\mathbf{b}_1 & \cdots & \mathbf{a}_m^T\mathbf{b}_n \end{bmatrix}$$

Thus,

$$c_{ij} = \mathbf{a}_i^T\mathbf{b}_j, \quad \text{for any } i, j.$$

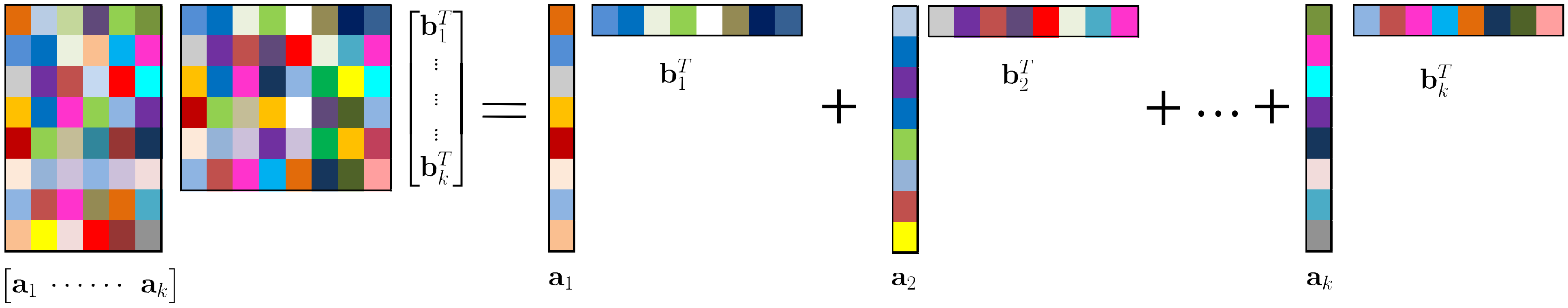
Matrix Product Representations

- outer-product representation: redefine $\mathbf{b}_i \in \mathbb{R}^k$ as the ith row of $\mathbf{B}$.

$$\mathbf{C} = \mathbf{A}(\mathbf{I})\mathbf{B} = \mathbf{A}\left(\sum_{i=1}^{k} \mathbf{e}_i\mathbf{e}_i^T\right)\mathbf{B} = \sum_{i=1}^{k} \mathbf{A}\mathbf{e}_i\mathbf{e}_i^T\mathbf{B}$$

Thus,

$$\mathbf{C} = \sum_{i=1}^{k} \mathbf{a}_i\mathbf{b}_i^T$$



Matrix Product Representations

- a matrix of the form $\mathbf{X} = \mathbf{a}\mathbf{b}^T$ for some $\mathbf{a}, \mathbf{b}$ is called a rank-one outer product. It can be verified that $\mathrm{rank}(\mathbf{X}) \leq 1$, and $\mathrm{rank}(\mathbf{X}) = 1$ if $\mathbf{a} \neq \mathbf{0}, \mathbf{b} \neq \mathbf{0}$.

- the outer-product representation $\mathbf{C} = \sum_{i=1}^{k} \mathbf{a}_i \mathbf{b}_i^T$ is a sum of k rank-one outer products

- does it mean that $\mathrm{rank}(\mathbf{C}) = k$?
  - $\mathrm{rank}(\mathbf{C}) \leq \sum_{i=1}^{k} \mathrm{rank}(\mathbf{a}_i \mathbf{b}_i^T) \leq k$ is true [2]
  - but the above equality is generally not attained; e.g., $k = 2$, $\mathbf{a}_1 = \mathbf{a}_2$, $\mathbf{b}_1 = -\mathbf{b}_2$ leads to $\mathbf{C} = \mathbf{0}$
  - $\mathrm{rank}(\mathbf{C}) = k$ only when $\mathbf{A}$ has full-column rank and $\mathbf{B}$ has full-row rank (requires a proof)

---

[2] use the rank inequality $\mathrm{rank}(\mathbf{A} + \mathbf{B}) \leq \mathrm{rank}(\mathbf{A}) + \mathrm{rank}(\mathbf{B})$.

Block Matrix Manipulations

Sometimes it may be useful to manipulate matrices in a block form.

- let $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{x} \in \mathbb{R}^n$. By partitioning

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{A}_2 \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix}$$

  where $\mathbf{A}_1 \in \mathbb{R}^{m \times n_1}, \mathbf{A}_2 \in \mathbb{R}^{m \times n_2}, \mathbf{x}_1 \in \mathbb{R}^{n_1}, \mathbf{x}_2 \in \mathbb{R}^{n_2}$, with $n_1 + n_2 = n$, we can write

$$\mathbf{A}\mathbf{x} = \mathbf{A}_1\mathbf{x}_1 + \mathbf{A}_2\mathbf{x}_2$$

- similarly, by partitioning

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix},$$

  we can write

$$\mathbf{A}\mathbf{x} = \begin{bmatrix} \mathbf{A}_{11}\mathbf{x}_1 + \mathbf{A}_{12}\mathbf{x}_2 \\ \mathbf{A}_{21}\mathbf{x}_1 + \mathbf{A}_{22}\mathbf{x}_2 \end{bmatrix}$$

Block Matrix Manipulations

- consider $\mathbf{AB}$. By an appropriate partitioning,

$$\mathbf{AB} = \begin{bmatrix} \mathbf{A}_1 & \mathbf{A}_2 \end{bmatrix} \begin{bmatrix} \mathbf{B}_1 \\ \mathbf{B}_2 \end{bmatrix} = \mathbf{A}_1\mathbf{B}_1 + \mathbf{A}_2\mathbf{B}_2$$

- similarly, by an appropriate partitioning,

$$\mathbf{AB} = \begin{bmatrix} \mathbf{A}_1 \\ \mathbf{A}_2 \end{bmatrix} \begin{bmatrix} \mathbf{B}_1 & \mathbf{B}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_1\mathbf{B}_1 & \mathbf{A}_1\mathbf{B}_2 \\ \mathbf{A}_2\mathbf{B}_1 & \mathbf{A}_2\mathbf{B}_2 \end{bmatrix}$$

- we showcase two-block partitioning only, but the same manipulations apply to multi-block partitioning like

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{11} & \cdots & \mathbf{A}_{1q} \\ \vdots & & \vdots \\ \mathbf{A}_{p1} & \cdots & \mathbf{A}_{pq} \end{bmatrix}$$

Extension to $\mathbb{C}^n$

- all the concepts described above apply to the complex case

- we only need to replace every "$\mathbb{R}$" with "$\mathbb{C}$", and every "T" with "H"; e.g.,

$$\text{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} = \{\mathbf{y} \in \mathbb{C}^m \mid \mathbf{y} = \textstyle\sum_{i=1}^n \alpha_i \mathbf{a}_i,\ \boldsymbol{\alpha} \in \mathbb{C}^n\},$$

  $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{y}^H \mathbf{x}$, $\|\mathbf{x}\|_2 = \sqrt{\mathbf{x}^H \mathbf{x}}$, and so forth.

Extension to $\mathbb{R}^{m\times n}$

- the concepts also apply to the matrix case
  - e.g., we may write

$$\text{span}\{\mathbf{A}_1, \ldots, \mathbf{A}_k\} = \{\mathbf{Y} \in \mathbb{R}^{m\times n} \mid \mathbf{Y} = \textstyle\sum_{i=1}^k \alpha_i \mathbf{A}_i,\ \boldsymbol{\alpha} \in \mathbb{R}^k\}.$$

  - sometimes it is more convenient to *vectorize* $\mathbf{X}$ as a vector $\mathbf{x} \in \mathbb{R}^{mn}$, and use the same treatment as in the $\mathbb{R}^n$ case
  - inner product for $\mathbb{R}^{m\times n}$:

$$\langle \mathbf{X}, \mathbf{Y} \rangle = \textstyle\sum_{i=1}^m \sum_{j=1}^n x_{ij} y_{ij} = \text{tr}(\mathbf{Y}^T \mathbf{X}),$$

  - the matrix version of the Euclidean norm is called the Frobenius norm:

$$\|\mathbf{X}\|_F = \sqrt{\textstyle\sum_{i=1}^m \sum_{j=1}^n |x_{ij}|^2} = \sqrt{\text{tr}(\mathbf{X}^T \mathbf{X})}$$

- extension to $\mathbb{C}^{m\times n}$ is just as straightforward as in that to $\mathbb{C}^n$

Complexities of Matrix Computations

- every vector/matrix operation such as $\mathbf{x}+\mathbf{y}$, $\mathbf{y}^T\mathbf{x}$, $\mathbf{A}\mathbf{x}$, $\ldots$ incurs computational costs, and they cost more as the vector and matrix sizes get bigger

- we typically look at floating point arithmetic operations, such as add, subtract, multiply, and divide

Complexities of Matrix Computations

- flops: one flop means one floating point arithmetic operation.

- flop counts of some standard vector/matrix operations:

  for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$,

  - $\mathbf{x} + \mathbf{y}$: n adds, so n flops
  - $\mathbf{y}^T \mathbf{x}$: n multiplies and $n-1$ adds, so $2n-1$ flops
  - $\mathbf{A}\mathbf{x}$: m inner products, so $m(2n-1)$ flops
  - $\mathbf{A}\mathbf{B}$: do "$\mathbf{A}\mathbf{x}$" above p times, so $pm(2n-1)$ flops

Complexities of Matrix Computations

- we are often interested in the *order* of the complexity
- big O notation: given two functions $f(n), g(n)$, the notation

$$f(n) = \mathcal{O}(g(n))$$

  means that there exists a constant $C > 0$ and n_0 such that $|f(n)| \leq C|g(n)|$ for all $n \geq n_0$.

- big O complexities of standard vector/matrix operations:
  - $\mathbf{x} + \mathbf{y}$: $\mathcal{O}(n)$ flops
  - $\mathbf{y}^T\mathbf{x}$: $\mathcal{O}(n)$ flops
  - $\mathbf{A}\mathbf{x}$: $\mathcal{O}(mn)$ flops
  - $\mathbf{A}\mathbf{B}$: $\mathcal{O}(mnp)$ flops
  - (we'll learn it later) solve $\mathbf{y} = \mathbf{A}\mathbf{x}$ for $\mathbf{x}$, with $\mathbf{A} \in \mathbb{R}^{n \times n}$: $\mathcal{O}(n^3)$ flops

Complexities of Matrix Computations

- big O complexities are commonly used, although we should be careful sometimes
- example: suppose you have an algorithm whose exact flop count is

$$f(n) = 3n^3 + 8n^2 + 2n + 1234.$$

  - $\mathcal{O}(n^3)$ flops
  - big O makes sense for large n; n^3 dominates as n is large
  - but be careful: for small n, it's 1234 that consumes more

- example: suppose you have two algorithms for the same problem. Their exact flop counts are

$$f_1(n) = n^3, \quad f_2(n) = \frac{1}{2}n^3.$$

  - their big O complexities are the same: $\mathcal{O}(n^3)$
  - but two times faster is two times faster!

Complexities of Matrix Computations

- example: suppose our algorithm deals with complex vector and matrix operations. Define one flop as one real flop.
  - one complex add $=$ 2 real adds $=$ 2 flops
  - one complex multiply $=$ 4 real multiplies $+$ 2 real adds $=$ 6 flops

    $\vdots$

  When we report big O complexity, the scaling factors above are not seen

Exercise: Count the Complexity of Gram Schmidt

- recall the Gram-Schmidt procedure recursively computes

$$\tilde{\mathbf{q}}_i = \mathbf{a}_i - \textstyle\sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i)\mathbf{q}_j, \quad \mathbf{q}_i = \tilde{\mathbf{q}}_i / \|\tilde{\mathbf{q}}_i\|_2, \quad i = 1, \ldots, n.$$

- consider iteration i.
  - every $\mathbf{q}_j^T \mathbf{a}_i$, $j = 1, \ldots, i = 1$, takes $\mathcal{O}(m)$
  - then, computing $\tilde{\mathbf{q}}_i = \mathbf{a}_i - \sum_{j=1}^{i-1} (\mathbf{q}_j^T \mathbf{a}_i)\mathbf{q}_j$ is almost the same as the operation "$\mathbf{A}\mathbf{x}$"; it takes $\mathcal{O}(mi)$
  - $\tilde{\mathbf{q}}_i = \tilde{\mathbf{q}}_i / \|\tilde{\mathbf{q}}_i\|_2$ requires $\mathcal{O}(m)$ (one divide, one $\sqrt{\cdot}$, one inner product $\tilde{\mathbf{q}}_i^T \tilde{\mathbf{q}}_i$)
  - total complexity for iteration i: $(i-1) \times \mathcal{O}(m) + \mathcal{O}(mi) + \mathcal{O}(m) = \mathcal{O}(mi)$
- total complexity of the whole algorithm:

$$\mathcal{O}(m \textstyle\sum_{i=1}^{n} i) = \mathcal{O}(m \frac{n(n+1)}{2}) = \mathcal{O}(mn^2)$$

Complexities of Matrix Computations

- Discussion: flop counts do not always translate into the actual efficiency of the execution of an algorithm, say, in terms of actual running time.

- things like pipelining, FPGA, parallel computing (multiple GPUs, multiple servers, cloud computing), etc., can make the story different.

- flop counts also ignore memory usage and other overheads...

- that said, we need at least a crude measure of how computationally costly an algorithm would be, and counting the flops serves that purpose.

How to Save Computations

- computational complexities depend much on how we design and write an algorithm
- generally, it is about
  - top-down, analysis-guided, designs: often seen in class, often look elegant
  - street-smart, possibly bottom-up, tricks: usually *not* taught much in class, also not commonplace in papers (unless you download and read somebody's code), subtly depends on your problem at hand, but a bunch of small differences can make a big difference, say in actual running time
- here we give several, but by no means all, tips for saving computations

How to Save Computations

- apply matrix operations wisely

- example: try this on MATLAB

```
>> A=randn(5000,2); B=randn(2,10000); C=randn(10000,10000);
>>
>> tic; D= A*B*C; toc
Elapsed time is 12.238567 seconds.
>> tic; D= (A*B)*C; toc     % ask MATLAB to do AB first
Elapsed time is 12.640961 seconds.
>> tic; D= A*(B*C); toc     % ask MATLAB to do BC first
Elapsed time is 0.222270 seconds.
```

How to Save Computations

- let us analyze the complexities in the last example
  - $\mathbf{A} \in \mathbb{R}^{m \times n}, \mathbf{B} \in \mathbb{R}^{n \times p}, \mathbf{C} \in \mathbb{R}^{p \times p}$, with $n \ll \min\{m, p\}$. We want to compute $\mathbf{D} = \mathbf{ABC}$.
  - if we compute $\mathbf{AB}$ first, and then $\mathbf{D} = (\mathbf{AB})\mathbf{C}$, the flop count will be

$$\mathcal{O}(mnp) + \mathcal{O}(mp^2) = \mathcal{O}(m(n+p)p) \approx \mathcal{O}(mp^2)$$

  - if we compute $\mathbf{BC}$ first, and then $\mathbf{D} = \mathbf{A}(\mathbf{BC})$, the flop count will be

$$\mathcal{O}(np^2) + \mathcal{O}(mnp) = \mathcal{O}((m+p)np).$$

  - the 2nd option is preferable if n is much smaller than m, p

How to Save Computations

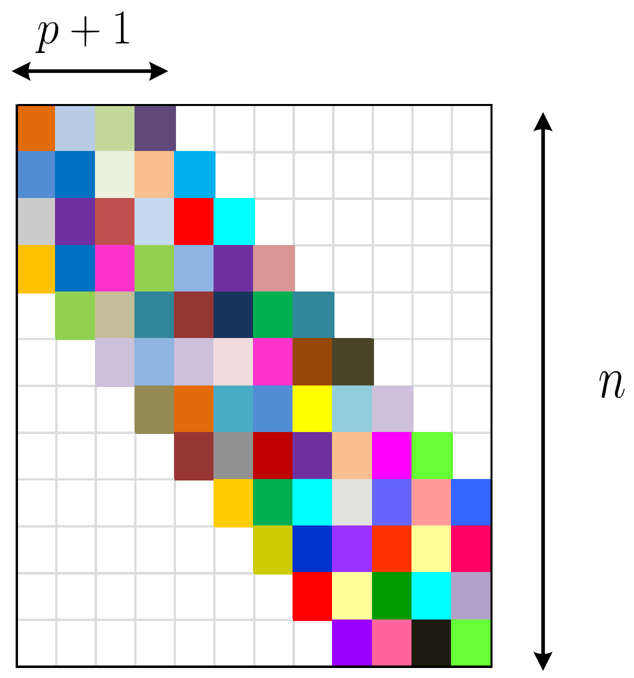
- use structures, if available

- example: let $\mathbf{A} \in \mathbb{R}^{n \times n}$ and suppose that

$$a_{ij} = 0 \;\text{ for all } i, j \text{ such that } |i - j| > p,$$

for some integer $p > 0$.

  - such a structured $\mathbf{A}$ is called band diagonal
  - if we don't use structures, computing $\mathbf{Ax}$ requires $\mathcal{O}(n^2)$

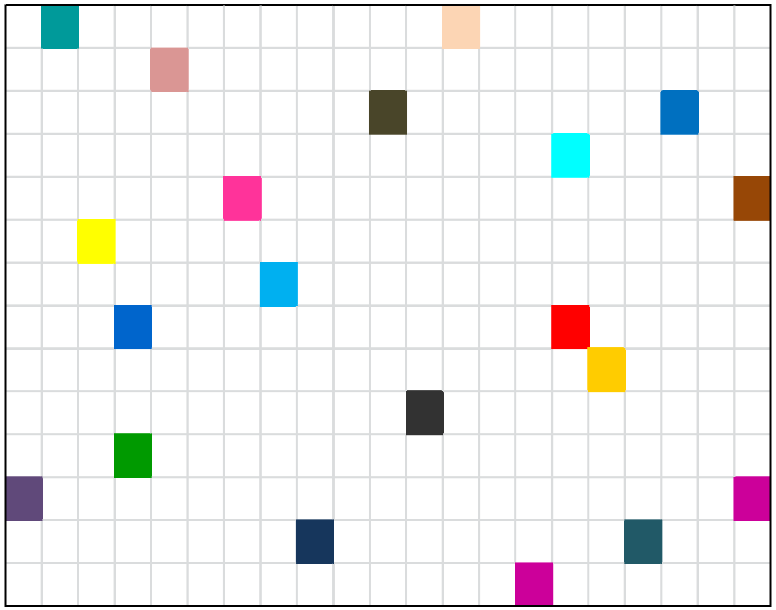


  - if we use the band diagonal structures, we can compute $\mathbf{Ax}$ with $\mathcal{O}(pn)$

How to Save Computations

- use sparsity, if available

- a vector or matrix is said to be sparse if it contains many zero elements
  - we assume unstructured sparsity



How to Save Computations

- let $\mathrm{nnz}(\mathbf{x})$ denote the number of nonzero elements of a vector $\mathbf{x}$; the same notation applies to matrices

- flop counts: for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\mathbf{B} \in \mathbb{R}^{n \times p}$,

  - $\mathbf{x} + \mathbf{y}$: from 0 and $\min\{\mathrm{nnz}(\mathbf{x}), \mathrm{nnz}(\mathbf{y})\}$ flops $\Longrightarrow \mathcal{O}(\min\{\mathrm{nnz}(\mathbf{x}), \mathrm{nnz}(\mathbf{y})\})$
  - $\mathbf{y}^T\mathbf{x}$: from 0 to $2\min\{\mathrm{nnz}(\mathbf{x}), \mathrm{nnz}(\mathbf{y})\}$ flops $\Longrightarrow \mathcal{O}(\min\{\mathrm{nnz}(\mathbf{x}), \mathrm{nnz}(\mathbf{y})\})$
  - $\mathbf{A}\mathbf{x}$, $\mathbf{x}$ being dense: from $\mathrm{nnz}(\mathbf{A})$ to $2\mathrm{nnz}(\mathbf{A})$ flops $\Longrightarrow \mathcal{O}(\mathrm{nnz}(\mathbf{A}))$
  - $\mathbf{AB}$: no simple expression for the flops, but at most
    $$2\min\{\mathrm{nnz}(\mathbf{A})p, \mathrm{nnz}(\mathbf{B})m\} \text{ flops} \Longrightarrow \mathcal{O}(\min\{\mathrm{nnz}(\mathbf{A})p, \mathrm{nnz}(\mathbf{B})m\})$$

- reference: S. Boyd and L. Vandenberghe, *Introduction to Applied Linear Algebra – Vectors, Matrices, and Least Squares*, 2018. Available online at https://web.stanford.edu/~boyd/vmls/vmls.pdf.