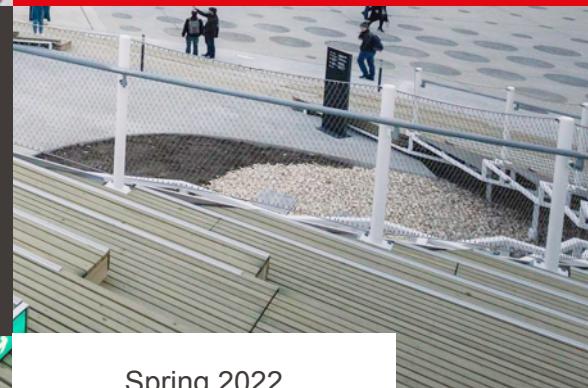




Prof Pierre
Vanderghenst

Spring 2022



Notations

\mathbb{R}^n the set of n-tuples or column vectors

$$x \in \mathbb{R}^n \quad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ \vdots \\ x_n \end{pmatrix} \quad x_i \in \mathbb{R}$$

vectors are always column vectors and row vectors are transposed, i.e y^T

\mathbb{C}^n likewise with complex-valued entries

\bar{x} is the vector of complex conjugates

x^H is the transposed and conjugate vector

Notations

$\mathbb{R}^{m,n}$ is the set of real-valued m -by- n matrices (m rows, n columns)

$$A \in \mathbb{R}^{m,n}, \quad (A)_{ij} = a_{ij} \in \mathbb{R} \quad (A^T)_{ij} = a_{ji}$$

$\mathbb{C}^{m,n}$ likewise with complex-valued entries

$$(A^H)_{ij} = \overline{a_{ji}} \in \mathbb{C}$$

$A = A^T$ symmetric matrix

$A = A^H$ hermitian matrix

Multiplications: matrix-matrix, matrix-vector, vector-vector

A and B are compatible for multiplication $A \in \mathbb{R}^{m \times p}$ $B \in \mathbb{R}^{p \times n}$ $AB \in \mathbb{R}^{m \times n}$

Everything is matrix-matrix! But some useful particular cases

Real and Hermitian dot products, inner products or scalar products

$$x, y \in \mathbb{R}^n \rightarrow x^T y = y^T x \in \mathbb{R} \quad x, y \in \mathbb{C}^n \rightarrow x^H y = \overline{y^H x} \in \mathbb{C}$$

Outer products

$$x \in \mathbb{R}^m \ y \in \mathbb{R}^n \rightarrow xy^T \in \mathbb{R}^{m \times n} \quad x \in \mathbb{C}^m \ y \in \mathbb{C}^n \rightarrow xy^H \in \mathbb{C}^{m \times n}$$

both “products” will play fundamental roles later on !

Two views of matrix-vector mult

$$A \in \mathbb{R}^{m \times n} \quad x \in \mathbb{R}^n$$

Column view: $A = [a_1, \dots, a_n]$, $a_i \in \mathbb{R}^m$ the **columns** of A

$$Ax = \begin{pmatrix} | & & | & & | \\ a_1 & \dots & a_n & \dots & x_1 \\ | & & | & & \vdots \\ a_1 & \dots & a_n & \dots & x_n \end{pmatrix} = \sum_{i=1}^n x_i a_i \in \mathbb{R}^m$$

linear combination
of columns

Row view: $A = [a^1 \dots a^m]$, $a^i \in \mathbb{R}^n$ the **rows** of A (seen as transposed vectors!)

$$Ax = \begin{pmatrix} - & a^1 & - \\ \vdots & \vdots & \vdots \\ - & a^m & - \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (a^1)^T x \\ \vdots \\ (a^m)^T x \end{pmatrix}$$

m-tuple of products of
rows of A with x

Scalar (inner) products, orthogonality

$$x, y \in \mathbb{R}^n$$

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

$$\langle x, x \rangle = 0 \text{ iff } x = 0$$

$$x, y \in \mathbb{C}^n$$

$$\langle x, y \rangle_H \equiv x^H y = \sum_{i=1}^n \overline{x_i} y_i$$

$$\langle x, x \rangle_H = 0 \text{ iff } x = 0$$

Orthogonal vectors: $\langle x, y \rangle = 0$ or $\langle x, y \rangle_H = 0$

Orthogonal matrices: $A \in \mathbb{R}^{n \times n}$ such that $A^T A = A A^T = I_n$

Unitary matrices: $A \in \mathbb{C}^{n \times n}$ such that $A^H A = A A^H = I_n$

Vector Spaces

(essentially finite dimensional ones)

Motivation: abstraction of the more intuitive euclidean case, but allows to work with other interesting objects such as functions

A vector space over a field \mathbb{F} is a set of *vectors* \mathcal{V}

two operations $+$: $\mathcal{V} \times \mathcal{V} \mapsto \mathcal{V}$ vector addition

\cdot : $\mathbb{F} \times \mathcal{V} \mapsto \mathcal{V}$ mult. by a scalar

Vector Spaces

A vector space over a field \mathbb{F} is a set of *vectors* \mathcal{V}

two operations $+$: $\mathcal{V} \times \mathcal{V} \mapsto \mathcal{V}$

\cdot : $\mathbb{F} \times \mathcal{V} \mapsto \mathcal{V}$

$(\mathcal{V}, +)$ is an abelian group

$$(\alpha\beta) \cdot u = \alpha(\beta \cdot u) \quad \forall \alpha, \beta \in \mathbb{F} \text{ and } \forall u \in \mathcal{V}$$

$$(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u \quad \forall \alpha, \beta \in \mathbb{F} \text{ and } \forall u \in \mathcal{V}$$

$$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v \quad \forall \alpha \in \mathbb{F} \text{ and } \forall u, v \in \mathcal{V}$$

$$1 \cdot u = u, \quad \forall u \in \mathcal{V} \text{ and } 1 \text{ is neutral element of product over } \mathbb{F}$$

Examples

$$\mathcal{V} = \mathbb{R}^n \text{ and } \mathbb{F} = \mathbb{R} \quad u + v = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix} \quad \alpha \cdot u = \begin{pmatrix} \alpha u_1 \\ \vdots \\ \alpha u_n \end{pmatrix}$$

The set of polynomials of order n with coefficients in \mathbb{F}

$$\mathcal{V} = \mathbb{R}^{m \times n} \text{ and } \mathbb{F} = \mathbb{R} \quad (A + B)_{ij} = a_{ij} + b_{ij} \text{ and } (\alpha \cdot A)_{ij} = \alpha a_{ij}$$

Rem: when there is no risk of confusion we will save the product sign for other operations and simply write αu or αA

Subspaces

Part of a vector space that is closed under the natural operations.

Will play a major role when we discuss (in particular) linear applications.

More formally:

$(\mathcal{V}, \mathbb{F})$ a vector space. $\mathcal{W} \subseteq \mathcal{V}$, $\mathcal{W} \neq \emptyset$.

$(\mathcal{W}, \mathbb{F})$ is a subspace of $(\mathcal{V}, \mathbb{F})$ IFF

$$\alpha w_1 + \beta w_2 \in \mathcal{W} \quad \forall w_1, w_2 \in \mathcal{W} \text{ and } \forall \alpha, \beta \in \mathbb{F}$$

Rem: it is equivalent to saying it is itself a vector space

Linear independence

Motivation: Somehow measure the “size” of a vector space or of a subspace

$X \equiv \{v_1, \dots, v_k\}$, $v_i \in \mathcal{V}$ a collection of k vectors

Suppose there exists scalars $\alpha_1, \dots, \alpha_k \in \mathbb{F}$ not all zeros such that

$$\alpha_1 v_1 + \dots + \alpha_k v_k = 0$$

For instance $\alpha_1 \neq 0$ then: $v_1 = -\frac{\alpha_2}{\alpha_1} v_2 - \dots - \frac{\alpha_k}{\alpha_1} v_k$

At least one vector in X can be expressed as a linear combination of the others

X is a linearly dependent set of vectors

Linear independence

X is a **linearly independent** set of vectors if the equation

$$\alpha_1 v_1 + \dots + \alpha_k v_k = 0$$

can only be satisfied for $\alpha_1 = \dots = \alpha_k = 0$

Examples: Pauli matrices

Monomials form a linearly independent family of vectors for the vector space of finite order polynomials

Span, Basis, Dimension

Where linear independence gets us where we wanted

Let X be a collection of vectors $v_i \in \mathcal{V}$

The **span** of X is the set of all vectors that can be represented as lin. comb. of X

$$\text{Sp}(X) = \{v : v = \alpha_1 v_1 + \dots + \alpha_k v_k, \alpha_i \in \mathbb{F}\}$$

X is a **basis** for \mathcal{V} IFF

X is a linearly independent set, and

$$\text{Sp}(X) = \mathcal{V}$$

Span, Basis, Dimension

X is a **basis** for \mathcal{V} IFF

X is a linearly independent set, and

$$\text{Sp}(X) = \mathcal{V}$$

This means you can write $v = X\alpha$, $\forall v \in \mathcal{V}$ with unique coefficients α

The number of elements in a basis is independent of the basis

It is therefore a characteristic of the vector space spanned by the basis called its **dimension** (note the space can be infinite dimensional)

Sums, intersections of subspaces

Let $\mathcal{R}, \mathcal{S} \in (\mathcal{V}, \mathbb{F})$

$$\mathcal{R} + \mathcal{S} = \{r + s : r \in \mathcal{R}, s \in \mathcal{S}\}$$

Subspaces! $\mathcal{R} \cup \mathcal{S}$ not necessarily subspace

$$\mathcal{R} \cap \mathcal{S} = \{v : v \in \mathcal{R} \text{ and } v \in \mathcal{S}\}$$

$$\mathcal{R}_1 + \cdots + \mathcal{R}_k \subseteq \mathcal{V} \quad \bigcap_{k \in A} \mathcal{R}_k \subseteq \mathcal{V}$$

The direct sum of two subspaces is a subspace $\mathcal{T} = \mathcal{R} \oplus \mathcal{S}$

$$\begin{array}{l} \mathcal{R} \cap \mathcal{S} = 0 \\ \mathcal{R} + \mathcal{S} = \mathcal{T} \end{array} \quad \xrightarrow{\hspace{1cm}} \quad \begin{array}{l} t = r + s \text{ uniquely } \forall t \in \mathcal{T}, r \in \mathcal{R}, s \in \mathcal{S} \\ \dim(\mathcal{T}) = \dim(\mathcal{R}) + \dim(\mathcal{S}) \end{array}$$

Inner product, orthogonality

Vector spaces over \mathbb{R} or \mathbb{C} are sometimes endowed with an inner product

$$\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{F} \quad \forall u, v, w \in \mathcal{V} \text{ and } \alpha \in \mathbb{F}$$

$$\langle \alpha u, v \rangle = \alpha \langle u, v \rangle$$

$$\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$$

$$\langle u, v \rangle = \overline{\langle v, u \rangle}$$

$$\langle u, u \rangle \geq 0 \quad \langle u, u \rangle = 0 \Rightarrow u = 0$$

Important example: Euclidean “dot” product

$$u, v \in \mathbb{R}^n \quad \langle u, v \rangle = u^T v$$

$$= \sum_{i=1}^n u_i v_i$$

A set of non-zero vectors $\{v_1, \dots, v_k\}$ is **orthogonal** if $\langle v_i, v_j \rangle = 0$ for $i \neq j$

It is **orthonormal** if $\langle v_i, v_j \rangle = \delta_{ij}$

Orthogonal complements

Let the set $\mathcal{S} \subseteq \mathcal{V}$. The **orthogonal complement** is defined as:

$$\mathcal{S}^\perp = \{v \in \mathcal{V} : \langle v, s \rangle = 0 \quad \forall s \in \mathcal{S}\}$$

Some properties for $\mathcal{R}, \mathcal{S} \subseteq \mathcal{V}$

$$\mathcal{S}^\perp \subseteq \mathcal{V}$$

$$\mathcal{R} \subseteq \mathcal{S} \text{ IFF } \mathcal{S}^\perp \subseteq \mathcal{R}^\perp$$

$$\mathcal{S} \oplus \mathcal{S}^\perp = \mathcal{V}$$

$$(\mathcal{R} + \mathcal{S})^\perp = \mathcal{R}^\perp \cap \mathcal{S}^\perp$$

$$(\mathcal{S}^\perp)^\perp = \mathcal{S}$$

$$(\mathcal{R} \cap \mathcal{S})^\perp = \mathcal{R}^\perp + \mathcal{S}^\perp$$

The Discrete Fourier Basis

The set of k -dimensional complex-valued vectors $v_k[n] = e^{j2\pi \frac{kn}{N}}$
 $k, n \in 0, \dots, N-1$

Is an orthogonal basis of \mathbb{C}^N called the **Discrete Fourier Basis**

Change of basis: $f = \sum_{k=0}^{N-1} (v_k^H f) v_k$

$F[k] = v_k^H f = \sum_{n=0}^{N-1} e^{-j2\pi \frac{kn}{N}} f[n]$ **Discrete Fourier Transform**