CS724: Topics in Algorithms
Norms and Inner Products - II
Slide Set 5

Prof. Dan A. Simovici

The set $\mathbb{C}^{m \times n}$ is a linear space. Therefore, it is natural to consider norms defined on matrices. We discuss two basic methods for defining norms for matrices.

- The first approach treats matrices as vectors (through the vec mapping).
- The second, regards matrices as representations of linear operators, and defined norms for matrices starting from operator norms.

Definition

The *$(m \times n)$-vectorization mapping* is the mapping $\text{vec} : \mathbb{C}^{m \times n} \longrightarrow \mathbb{C}^{mn}$ defined by

$$\text{vec}(A) = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix},$$

obtained by reading A column-wise.

The following equality is immediate for a matrix $A \in \mathbb{C}^{m \times n}$:

$$\text{vec}(A) = \begin{pmatrix} A\mathbf{e}_1 \\ A\mathbf{e}_2 \\ \vdots \\ A\mathbf{e}_n \end{pmatrix}.$$

The vectorization mapping vec is an isomorphism between the linear space $\mathbb{C}^{m \times n}$ and the linear space $\mathbb{C}^{mn}$, as can be easily verified.

Example

For the matrix I_n we have

$$\text{vec}(I_n) = \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}.$$

Definition

Let ν be a vector norm on the space $\mathbb{R}^{mn}$. The *vectorial matrix norm* $\mu^{(m,n)}$ *on* $\mathbb{R}^{m\times n}$ is the mapping $\mu^{(m,n)} : \mathbb{R}^{m\times n} \longrightarrow \mathbb{R}_{\geqslant 0}$ defined by

$$\mu^{(m,n)}(A) = \nu(\text{vec}(A)),$$

for $A \in \mathbb{R}^{m\times n}$.

Vectorial norms of matrices are defined without regard for matrix products.

Theorem

If $f : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ is a linear operator, ν and ν' are corms on $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively, there exists a non-negative constant such that

$$\nu'(f(x)) \leqslant M\nu(x)$$

for every $x \in \mathbb{C}^m$.

Definition

Let $f : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ is a linear operator, and let ν and ν' be norms on $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively. The operatorial norm of f is the number

$$\mu(f) = \inf\{M \in \mathbb{R}_{\geqslant 0} \mid \nu'(f(x)) \leqslant M\nu(x) \text{ for every } \boldsymbol{x} \in \mathbb{C}^m\}.$$

Theorem

The mapping ν is a norm on the space of linear operators $Hom(\mathbb{C}^m, \mathbb{C}^n)$.

Since μ depends on both ν and ν' it is denoted by $N(\nu, \nu')$.

Theorem

Let $f : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ *and* $g : \mathbb{C}^n \longrightarrow \mathbb{C}^p$ *be two linear operators and let* ν, ν', ν'' *be norms on* $\mathbb{C}^m, \mathbb{C}^n$ *and* $\mathbb{C}^p$*, respectively. Define* $\mu = N(\nu, \nu')$*,* $\mu' = N(\nu', \nu'')$*, and* $\mu'' = N(\nu, \nu'')$*. We have*

$$\mu''(gf) \leqslant \mu(f)\mu'(g).$$

Proof

For $\boldsymbol{x} \in \mathbb{C}^m$ we have $\nu'(f(x) \leqslant (\mu(f) + \epsilon')\nu(\boldsymbol{x})$ for every $\epsilon' > 0$/ Similarly, for $\boldsymbol{y} \in \mathbb{C}^n$ e have $\nu''(g(y)) \leqslant (\mu'(g) + \epsilon'')\nu'(\boldsymbol{y})$ for every $\epsilon'' > 0$. These inequalities imply

$$\nu''(g(f(\boldsymbol{x}))) \leqslant (\nu'(g) + \epsilon'')\nu'(f(x)) \leqslant (\nu'(g) + \epsilon'')(\nu(f(x)) + \epsilon')\nu(\boldsymbol{x}),$$

hence

$$\mu''(gf) \leqslant (\mu'(g) + \epsilon'')(\mu(f) + \epsilon')$$

for every ϵ' and ϵ'', hence $\mu''(gf) \leqslant \mu(f)\mu'(g)$.

Definition

A *consistent family of matrix norms* is a family of functions $\mu^{(m,n)} : \mathbb{C}^{m\times n} \longrightarrow \mathbb{R}_{\geqslant 0}$, where $m, n \in \mathbb{P}$ that satisfies the following conditions:

- $\mu^{(m,n)}(A) = 0$ if and only if $A = O_{m,n}$;
- $\mu^{(m,n)}(A + B) \leqslant \mu^{(m,n)}(A) + \mu^{(m,n)}(B)$ (the *subadditivity property*);
- $\mu^{(m,n)}(aA) = |a|\mu^{(m,n)}(A)$;
- $\mu^{(m,p)}(AB) \leqslant \mu^{(m,n)}(A)\mu^{(n,p)}(B)$ for every matrix $A \in \mathbb{R}^{m\times n}$ and $B \in \mathbb{R}^{n\times p}$ (the *submultiplicative property*).

If the format of the matrix A is clear from context or is irrelevant, then we shall write $\mu(A)$ instead of $\mu^{(m,n)}(A)$.

Example

Let $P \in \mathbb{C}^{n \times n}$ be an idempotent matrix, that is, a matrix P such that $P^2 = P$. If μ is a matrix norm, then either $\mu(P) = 0$ or $\mu(P) \geqslant 1$. Indeed, since P is idempotent we have $\mu(P) = \mu(P^2)$. By the submultiplicative property, $\mu(P^2) \leqslant (\mu(P))^2$, so $\mu(P) \leqslant (\mu(P))^2$. Consequently, if $\mu(P) \neq 0$, then $\mu(P) \geqslant 1$.

Some vectorial matrix norms turn out to be actual matrix norms; others fail to be matrix norms. This point is illustrated by the next examples.

Example

Consider the vectorial matrix norm μ_1 induced by the vector norm ν_1. We have $\mu_1(A) = \sum_{i=1}^{n} \sum_{j=1}^{m} |a_{ij}|$ for $A \in \mathbb{R}^{m\times n}$. Actually, this is a matrix norm. To prove this fact consider the matrices $A \in \mathbb{R}^{m\times p}$ and $B \in \mathbb{R}^{p\times n}$. We have:

$$
\begin{aligned}
\mu_1(AB) &= \sum_{i=1}^{m}\sum_{j=1}^{n}\left|\sum_{k=1}^{p} a_{ik}b_{kj}\right| \leqslant \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p} |a_{ik}b_{kj}| \\
&\leqslant \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k'=1}^{p}\sum_{k''=1}^{p} |a_{ik'}||b_{k''j}| \\
&\quad \text{(because we added extra non-negative terms to the sums)} \\
&= \left(\sum_{i=1}^{m}\sum_{k'=1}^{p} |a_{ik'}|\right)\cdot\left(\sum_{j=1}^{n}\sum_{k''=1}^{p} |b_{k''j}|\right) \\
&= \mu_1(A)\mu_1(B).
\end{aligned}
$$

We denote this vectorial matrix norm by the same notation as the corresponding vector norm, that is, by $\| A \|_1$.

The vectorial norm μ_2 (also known as the *Frobenius norm*) is induced by the vector norm ν_2. It is also a matrix norm. Indeed, we have

$$
\begin{aligned}
(\mu_2(AB))^2 &= \sum_{i=1}^{m} \sum_{j=1}^{n} \left| \sum_{k=1}^{p} a_{ik} b^{kj} \right|^2 \\
&\leqslant \sum_{i=1}^{m} \sum_{j=1}^{n} \left(\sum_{k=1}^{p} |a_{ik}|^2 \sum_{\ell=1}^{p} |b^{\ell j}|^2 \right) \\
& \quad \text{(by Cauchy-Schwarz Inequality)} \\
&\leqslant (\mu_2(A))^2 (\mu_2(B))^2.
\end{aligned}
$$

$\mu_2(A)$ is denoted also by $\| A \|_F$ (F from Frobenius).

Example

For real matrices we have $\parallel A \parallel_F^2 = \text{trace}(AA') = \text{trace}(A'A)$.
For complex matrices the corresponding equality is

$$\parallel A \parallel_F^2 = \text{trace}(AA^{\mathsf{H}}) = \text{trace}(A^{\mathsf{H}}A).$$

Note that $\parallel A^{\mathsf{H}} \parallel_F^2 = \parallel A \parallel_F^2$ for every A.

Example

The vectorial norm μ_∞ induced by the vector norm ν_∞ is denoted by $\parallel A \parallel_\infty$ and is given by

$$\parallel A \parallel_\infty = \max_{i,j} |a_{ij}|$$

for $A \in \mathbb{C}^{n\times n}$. This is *not* a matrix norm. Indeed, let a, b be two positive numbers and consider the matrices

$$A = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \text{ and } B = \begin{pmatrix} b & b \\ b & b \end{pmatrix}.$$

We have $\parallel A \parallel_\infty = a$ and $\parallel B \parallel_\infty = b$. However, since

$$AB = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix},$$

we have $\parallel AB \parallel_\infty = 2ab$ and the submultiplicative property of matrix norms is violated.

Theorem

Let μ be the matrix norm on $\mathbb{C}^{n\times n}$ induced by the vector norm ν. We have $\nu(A\boldsymbol{u}) \leqslant \mu(A)\nu(\boldsymbol{u})$ for every $\boldsymbol{u} \in \mathbb{C}^n$.

Proof.

The inequality is obviously satisfied when $\boldsymbol{u} = \boldsymbol{0}_n$. Therefore, we may assume that $\boldsymbol{u} \neq \boldsymbol{0}_n$ and let $\boldsymbol{x} = \frac{1}{\nu(\boldsymbol{u})}\boldsymbol{u}$. Clearly, $\nu(\boldsymbol{x}) = 1$ and

$$\nu\left(A\frac{1}{\nu(\boldsymbol{u})}\boldsymbol{u}\right) \leqslant \mu(A)$$

for every $\boldsymbol{u} \in \mathbb{C}^n - \{\boldsymbol{0}_n\}$. This implies immediately the desired inequality. □

If μ is a matrix norm induced by a vector norm on $\mathbb{R}^n$, then $\mu(I_n) = \sup\{\nu(I_n\mathbf{x}) \mid \nu(\mathbf{x}) \leqslant 1\} = 1$. This necessary condition can be used for identifying matrix norms that are not induced by vector norms.

The operator matrix norm induced by the vector norm $\| \cdot \|_p$ is denoted by $|||\cdot|||_p$.

Example

To compute $\|A\|_1 = \sup\{\| Ax \|_1 \mid \| x \|_1 \leqslant 1\}$, where $A \in \mathbb{R}^{n\times n}$, suppose that the columns of A are the vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$, that is

$$\boldsymbol{a}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}.$$

Let $\boldsymbol{x} \in \mathbb{R}^n$ be a vector whose components are $x_1, \ldots, x_n$. Then, $\boldsymbol{Ax} = x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n$, so

$$\begin{aligned} \| A\boldsymbol{x} \|_1 &= \| x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n \|_1 \\ &\leqslant \sum_{j=1}^{n} |x_j| \, \| \boldsymbol{a}_j \|_1 \\ &\leqslant \max_j \| \boldsymbol{a}_j \|_1 \sum_{j=1}^{n} |x_j| \\ &= \max_j \| \boldsymbol{a}_j \|_1 \cdot \| \boldsymbol{x} \|_1 . \end{aligned}$$

Example cont'd

Example

Let $\boldsymbol{e}_j$ be the vector whose components are 0 with the exception of its j^{th} component that is equal to 1. Clearly, we have $\| \boldsymbol{e}_j \|_1 = 1$ and $\boldsymbol{a}_j = A\boldsymbol{e}_j$. This, in turn implies $\| \boldsymbol{a}_j \|_1 = \| A\boldsymbol{e}_j \|_1 \leqslant |||A|||_1$ for $1 \leqslant j \leqslant n$. Therefore, $\max_j \| \boldsymbol{a}_j \|_1 \leqslant |||A|||_1$, so

$$|||A|||_1 = \max_j \| \boldsymbol{a}_j \|_1 = \max_j \sum_{i=1}^{n} |a_{ij}|.$$

In other words, $|||A|||_1$ equals the maximum column sum of the absolute values.

Example

Consider now a matrix $A \in \mathbb{R}^{n\times n}$. We have

$$\begin{aligned}
\| A\boldsymbol{x} \|_\infty &= \max_{1\leqslant i\leqslant n} \left|\sum_{j=1}^{n} a_{ij}x_j\right| \\
&\leqslant \max_{1\leqslant i\leqslant n} \sum_{j=1}^{n} |a_{ij}x_j| \\
&\leqslant \max_{1\leqslant i\leqslant n} \| \boldsymbol{x} \|_\infty \sum_{j=1}^{n} |a_{ij}|.
\end{aligned}$$

Consequently, if $\| \boldsymbol{x} \|_\infty \leqslant 1$ we have $\| A\boldsymbol{x} \|_\infty \leqslant \max_{1\leqslant i\leqslant n} \sum_{j=1}^{n} |a_{ij}|$. Thus, $\|A\|_\infty \leqslant \max_{1\leqslant i\leqslant n} \sum_{j=1}^{n} |a_{ij}|$.

Example cont'd

Example

The converse inequality is immediate if $A = O_{n,n}$. Therefore, assume that $A \neq O_{n\times n}$, and let $(a_{p1}, \ldots, a_{pn})$ be any row of A that has at least one element distinct from 0. Define the vector $\boldsymbol{z} \in \mathbb{R}^n$ by

$$z_j = \begin{cases} \frac{|a_{pj}|}{a_{pj}} & \text{if } a_{pj} \neq 0, \\ 1 & \text{otherwise,} \end{cases}$$

for $1 \leqslant j \leqslant n$. It is clear that $z_j \in \{-1, 1\}$ for every j, $1 \leqslant j \leqslant n$ and, therefore, $\| \boldsymbol{z} \|_\infty = 1$. Moreover, we have $|a_{pj}| = a_{pj} z_j$ for $1 \leqslant j \leqslant n$. Therefore, we can write:

$$\begin{aligned} \sum_{j=1}^n |a_{pj}| &= \sum_{j=1}^n a_{pj} z_j \leqslant \left| \sum_{j=1}^n a_{pj} z_j \right| \leqslant \max_{1 \leqslant i \leqslant n} \left| \sum_{j=1}^n a_{ij} z_j \right| \\ &= \| A\boldsymbol{z} \|_\infty \leqslant \max\{\| A\boldsymbol{x} \|_\infty \mid \| \boldsymbol{x} \|_\infty \leqslant 1\} = |||A|||_\infty. \end{aligned}$$

UMASS BOSTON

Example cont'd

Example

Since this holds for every row of A, it follows that $\max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |a_{ij}| \leqslant \|A\|_\infty$, which proves that

$$\|A\|_\infty = \max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |a_{ij}|.$$

In other words, $\|A\|_\infty$ equals the maximum row sum of the absolute values.

Example

Let $D = \text{diag}(d_1, \ldots, d_n) \in \mathbb{C}^{n \times n}$ be a diagonal matrix. If $\boldsymbol{x} \in \mathbb{C}^n$ we have

$$D\boldsymbol{x} = \begin{pmatrix} d_1 x_1 \\ \vdots \\ d_n x_n \end{pmatrix},$$

so

$$\begin{aligned} \|D\|_2 &= \max\{\| D\boldsymbol{x} \|_2 \mid \| \boldsymbol{x} \|_2 = 1\} \\ &= \max\{\sqrt{(d_1 x_1)^2 + \cdots + (d_n x_n)^2} \mid x_1^2 + \cdots + x_n^2 = 1\} \\ &= \max\{|d_i| \mid 1 \leqslant 1 \leqslant n\}. \end{aligned}$$

Certain norms are invariant with respect to multiplication by unitary matrices. We refer to these norms as *unitarily invariant norms*.

Theorem

Let $U \in \mathbb{C}^{n\times n}$ be a unitary matrix. The following statements hold:

- $\| U\mathbf{x} \|_2 = \| \mathbf{x} \|_2$ *for every* $\mathbf{x} \in \mathbb{C}^n$;
- $|\!|\!| UA |\!|\!|_2 = |\!|\!| A |\!|\!|_2$ *for every* $A \in \mathbb{C}^{n\times p}$;
- $\| UA \|_F = \| A \|_F$ *for every* $A \in \mathbb{C}^{n\times p}$.

Proof

For the first part of the theorem note that

$$\| U\mathbf{x} \|_2^2 = (U\mathbf{x})^{\mathsf{H}} U\mathbf{x} = \mathbf{x}^{\mathsf{H}} U^{\mathsf{H}} U\mathbf{x} = \mathbf{x}^{\mathsf{H}}\mathbf{x} = \| \mathbf{x} \|_2^2,$$

because $U^{\mathsf{H}} A = I_n$.
The second part of the theorem is shown next:

$$\begin{aligned} \|UA\|_2 &= \max\{\| (UA)\mathbf{x} \|_2 \mid \| \mathbf{x} \|_2 = 1\} \\ &= \max\{\| U(A\mathbf{x}) \|_2 \mid \| \mathbf{x} \|_2 = 1\} \\ &= \max\{\| A\mathbf{x} \|_2 \mid \| \mathbf{x} \|_2 = 1\} \\ &\quad \text{(by Part (i))} \\ &= \|A\|_2. \end{aligned}$$

Proof cont'd

For the Frobenius norm note that

$$\| UA \|_F = \sqrt{\text{trace}((UA)^{\mathsf{H}} UA)} = \sqrt{\text{trace}(A^{\mathsf{H}} U^{\mathsf{H}} UA)} = \sqrt{\text{trace}(A^{\mathsf{H}} A)} = \| A \|_F$$

Corollary

If $U \in \mathbb{C}^{n \times n}$ is a unitary matrix, then $\|U\|_2 = 1$.

Proof.

Since $\|U\|_2 = \sup\{\| U\mathbf{x} \|_2 \mid \| \mathbf{x} \|_2 \leqslant 1\}$, we have

$$\|U\|_2 = \sup\{\| \mathbf{x} \|_2 \mid \| \mathbf{x} \|_2 \leqslant 1\} = 1.$$

□

Corollary

Let $A, U \in \mathbb{C}^{n\times n}$. *If* U *is an unitary matrix, then*

$$\| U^{\mathsf{H}} A U \|_F = \| A \|_F .$$

Proof.

Since U is a unitary matrix, so is U^{H}. By a previous Theorem,

$$\| U^{\mathsf{H}} A U \|_F = \| AU \|_F = \| U^{\mathsf{H}} A^{\mathsf{H}} \|_F^2 = \| A^{\mathsf{H}} \|_F^2 = \| A \|_F^2,$$

which proves the corollary. □

Example

Let $S = \{\mathbf{x} \in \mathbb{R}^n \mid \parallel \mathbf{x} \parallel_2 = 1\}$ be the surface of the sphere in $\mathbb{R}^n$. The image of S under the linear transformation h_U that corresponds to the unitary matrix U is S itself. Indeed, $\parallel h_U(\mathbf{x}) \parallel_2 = \parallel \mathbf{x} \parallel_2 = 1$, so $h_U(\mathbf{x}) \in S$ for every $\mathbf{x} \in S$. Also, note that h_U restricted to S is a bijection because $h_{U^{\mathsf{H}}}(h_U(\mathbf{x})) = \mathbf{x}$ for every $\mathbf{x} \in \mathbb{R}^n$.

Theorem

Let $A \in \mathbb{R}^{n\times n}$. We have $\|A\|_2 \leqslant \| A \|_F$.

Proof.

Let $\boldsymbol{x} \in \mathbb{R}^n$. We have

$$A\boldsymbol{x} = \begin{pmatrix} \boldsymbol{r}_1\boldsymbol{x} \\ \vdots \\ \boldsymbol{r}_n\boldsymbol{x} \end{pmatrix},$$

where $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n$ are the rows of the matrix A. Thus,

$$\frac{\| A\boldsymbol{x} \|_2}{\| \boldsymbol{x} \|_2} = \frac{\sqrt{\sum_{i=1}^n (\boldsymbol{r}_i\boldsymbol{x})^2}}{\| \boldsymbol{x} \|_2}.$$

By Cauchy-Schwarz inequality we have: $(\boldsymbol{r}_i\boldsymbol{x})^2 \leqslant \| \boldsymbol{r}_i \|_2^2 \| \boldsymbol{x} \|_2^2$, so $\frac{\|A\boldsymbol{x}\|_2}{\|\boldsymbol{x}\|_2} \leqslant \sqrt{\sum_{i=1}^n \| \boldsymbol{r}_i \|_2^2} = \| A \|_F$. This implies $\|A\|_2 \leqslant \| A \|_F$. □

UMASS BOSTON

Definition

Let L be a $\mathbb{C}$-linear space. An *inner product* on L is a function $f : L \times L \longrightarrow \mathbb{C}$ that has the following properties:

- $f(a\mathbf{x} + b\mathbf{y}, \mathbf{z}) = af(\mathbf{x}, \mathbf{z}) + bf(\mathbf{y}, \mathbf{z})$ (linearity in the first argument);
- $f(\mathbf{x}, \mathbf{y}) = \overline{f(\mathbf{y}, \mathbf{x})}$ for $\mathbf{y}, \mathbf{x} \in L$ (conjugate symmetry);
- if $\mathbf{x} \neq \mathbf{0}$, then $f(\mathbf{x}, \mathbf{x})$ is a positive real number (positivity),
- $f(\mathbf{x}, \mathbf{x}) = 0$ if and only if $\mathbf{x} = \mathbf{0}$ (definiteness),

for every $\mathbf{x}, \mathbf{y}, \mathbf{z} \in L$ and $a, b \in \mathbb{C}$.
The pair (L, f) is called an *inner product space*.

An alternative terminology for real inner product spaces is *Euclidean spaces*, and *Hermitian spaces* for complex inner product spaces.

For the second argument of an inner product we have the property of *conjugate linearity*, that is,

$$f(\mathbf{z}, a\mathbf{x} + b\mathbf{y}) = \bar{a}f(\mathbf{z}, \mathbf{x}) + \bar{b}f(\mathbf{z}, \mathbf{y})$$

for every $\mathbf{x}, \mathbf{y}, \mathbf{z} \in L$ and $a, b \in \mathbb{C}$. Indeed, by the conjugate symmetry property we can write

$$\begin{aligned} f(\mathbf{z}, a\mathbf{x} + b\mathbf{y}) &= \overline{f(a\mathbf{x} + b\mathbf{y}, \mathbf{z})} \\ &= \overline{af(\mathbf{x}, \mathbf{z}) + bf(\mathbf{y}, \mathbf{z})} \\ &= \bar{a}\overline{f(\mathbf{x}, \mathbf{z})} + \bar{b}\overline{f(\mathbf{y}, \mathbf{z})} \\ &= \bar{a}f(\mathbf{z}, \mathbf{x}) + \bar{b}f(\mathbf{z}, \mathbf{y}). \end{aligned}$$

Observe that conjugate symmetry property on inner products implies that for $\boldsymbol{x} \in L$, $f(\boldsymbol{x}, \boldsymbol{x})$ is a real number because $f(\boldsymbol{x}, \boldsymbol{x}) = \overline{f(\boldsymbol{x}, \boldsymbol{x})}$.
When L is a real linear space the definition of the inner product becomes simpler because the conjugate of a real number a is a itself. Namely, for real linear spaces, the conjugate symmetry is replaced by the plain symmetry property,

$$f(\boldsymbol{x}, \boldsymbol{y}) = f(\boldsymbol{y}, \boldsymbol{x}),$$

for $\boldsymbol{x}, \boldsymbol{y} \in L$ and f is linear in both arguments.

Let $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ be a basis in the complex n-dimensional inner product space L. If $\boldsymbol{x} = \sum_{i=1}^n x^i \boldsymbol{w}_i$ and $\boldsymbol{y} = \sum_{j=1}^n y^j \boldsymbol{w}_j$, then

$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^n \sum_{j=1}^n x^i \overline{y^j} f(\boldsymbol{w}_i, \boldsymbol{w}_j),$$

due to the bilinearity of the inner product. If we denote $f(\boldsymbol{w}_i, \boldsymbol{w}_j)$ by g_{ij}, then $f(\boldsymbol{x}, \boldsymbol{y})$ can be written as

$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^n \sum_{j=1}^n x^i \overline{y^j} g_{ij} \qquad (1)$$

for $\boldsymbol{x}, \boldsymbol{y} \in L$.
If L is a real inner product space L, then

$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^n \sum_{j=1}^n x^i y^j g_{ij}$$

To simplify notations, if there is no risk of confusion, we denote the inner product $f(\boldsymbol{u}, \boldsymbol{v})$ as $(\boldsymbol{u}, \boldsymbol{v})$.

Definition

Two vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{C}^n$ are said to be *orthogonal* with respect to an inner product if $(\boldsymbol{u}, \boldsymbol{v}) = 0$. This is denoted by $x \perp y$.
An *orthogonal set of vectors* in an inner product space L equipped with an inner product is a subset W of L such that for every $\boldsymbol{u}, \boldsymbol{v} \in W$ we have $\boldsymbol{u} \perp \boldsymbol{v}$.

Theorem

Any inner product on a linear space L generates a norm on that space defined by $\parallel \mathbf{x} \parallel = \sqrt{(\mathbf{x}, \mathbf{x})}$ for $\mathbf{x} \in L$.

Proof

Let L be a $\mathbb{C}$-linear space. We need to verify that the norm satisfies the conditions of Definition. Applying the properties of the inner product we have

$$\begin{aligned} \| \boldsymbol{x} + \boldsymbol{y} \|^2 &= (\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{y}) \\ &= (\boldsymbol{x}, \boldsymbol{x}) + 2(\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{y}) \\ &= \| \boldsymbol{x} \|^2 + 2(\boldsymbol{x}, \boldsymbol{y}) + \| \boldsymbol{y} \|^2 \\ &\leqslant \| \boldsymbol{x} \|^2 + 2 \| \boldsymbol{x} \| \| \boldsymbol{y} \| + \| \boldsymbol{y} \|^2 \\ &= (\| \boldsymbol{x} \| + \| \boldsymbol{y} \|)^2. \end{aligned}$$

Because $\| \boldsymbol{x} \| \geqslant 0$ it follows that $\| \boldsymbol{x} + \boldsymbol{y} \| \leqslant \| \boldsymbol{x} \| + \| \boldsymbol{y} \|$, which is the subadditivity property.

If $a \in \mathbb{C}$, then

$\| a\boldsymbol{x} \| = \sqrt{(a\boldsymbol{x}, a\boldsymbol{x})} = \sqrt{a\bar{a}(\boldsymbol{x}, \boldsymbol{x})} = \sqrt{|a|^2(\boldsymbol{x}, \boldsymbol{x})} = |a|\sqrt{(\boldsymbol{x}, \boldsymbol{x})} = |a| \, \| \boldsymbol{x} \|$.

From the definiteness property of the inner product it follows that $\| \boldsymbol{x} \| = 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.

UMASS BOSTON

The norm induced by the inner product $f(\boldsymbol{x}, \boldsymbol{y}) = x^i \overline{y^j} g_{ij}$ is

$$\parallel \boldsymbol{x} \parallel^2 = f(\boldsymbol{x}, \boldsymbol{x}) = x^i \overline{x^j} g_{ij}.$$

Theorem

If W is a set of orthogonal vectors in a n-dimensional $\mathbb{C}$-linear space L and $\mathbf{0} \notin W$, then W is linearly independent.

Proof.

Let $\boldsymbol{c} = a^1\boldsymbol{w}_1 + \cdots + a^n\boldsymbol{w}_n$ a linear combination in L such that $a^1\boldsymbol{w}_1 + \cdots + a^n\boldsymbol{w}_n = \mathbf{0}$. Since $(\boldsymbol{c}, \boldsymbol{w}_i) = a_i \parallel \boldsymbol{w}_i \parallel^2 = 0$, we have $a_i = 0$ because $\parallel \boldsymbol{w}_i \parallel^2 \neq 0$, and this holds for every i, where $1 \leqslant i \leqslant n$. Thus, W is linearly independent. □

Definition

An *orthonormal set of vectors* in an inner product space L equipped with an inner product is an orthogonal subset W of L such that for every $\boldsymbol{u}$ we have $\| \boldsymbol{u} \| = 1$, where the norm is induced by the inner product.

Corollary

If W is an orthonormal set of vectors in an n-dimensional $\mathbb{C}$-linear space L and $|W| = n$, then W is a basis in L.

If $W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ is an orthonormal basis in $\mathbb{C}^n$ we have

$$g_{ij} = (\boldsymbol{w}_i, \boldsymbol{w}_j) = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j, \end{cases}$$

which means that the inner product of the vectors $\boldsymbol{x} = x^i \boldsymbol{w}_i$ and $\boldsymbol{y} = y^j \boldsymbol{w}_j$ is given by:

$$(\boldsymbol{x}, \boldsymbol{y}) = x^i \overline{y^j} (\boldsymbol{w}_i, \boldsymbol{w}_j) = x^i \overline{y^i}. \tag{2}$$

Consequently, $\| \boldsymbol{x} \|^2 = \sum_{i=1}^n |x^i|^2$.
The inner product of $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ is

$$(\boldsymbol{x}, \boldsymbol{y}) = x^i y^j (\boldsymbol{w}_i, \boldsymbol{w}_j) = x^i y^i. \tag{3}$$

Not every norm can be induced by an inner product. A characterization of this type of norms in linear spaces is presented next.
This equality shown in the next theorem is known as the *parallelogram equality*.

Theorem

Let L be a real linear space. A norm $\| \cdot \|$ is induced by an inner product if and only if

$$\| \mathbf{x} + \mathbf{y} \|^2 + \| \mathbf{x} - \mathbf{y} \|^2 = 2(\| \mathbf{x} \|^2 + \| \mathbf{y} \|^2),$$

for every $\mathbf{x}, \mathbf{y} \in L$.

Proof

Suppose that the norm is induced by an inner product. In this case we can write for every $\mathbf{x}$ and $\mathbf{y}$:

$$\begin{aligned} \parallel \mathbf{x}+\mathbf{y} \parallel^2 = (\mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y}) &= (\mathbf{x},\mathbf{x}) + 2(\mathbf{x},\mathbf{y}) + (\mathbf{y},\mathbf{y}), \\ \parallel \mathbf{x}-\mathbf{y} \parallel^2 = (\mathbf{x}-\mathbf{y}, \mathbf{x}-\mathbf{y}) &= (\mathbf{x},\mathbf{x}) - 2(\mathbf{x},\mathbf{y}) + (\mathbf{y},\mathbf{y}). \end{aligned}$$

Thus,

$$(\mathbf{x}+\mathbf{y}, \mathbf{x}+\mathbf{y}) + (\mathbf{x}-\mathbf{y}, \mathbf{x}-\mathbf{y}) = 2(\mathbf{x},\mathbf{x}) + 2(\mathbf{y},\mathbf{y}),$$

which can be written in terms of the norm generated as the inner product as

$$\parallel \mathbf{x}+\mathbf{y} \parallel^2 + \parallel \mathbf{x}-\mathbf{y} \parallel^2 = 2(\parallel \mathbf{x} \parallel^2 + \parallel \mathbf{y} \parallel^2).$$

The proof of the reverse implication is omitted.

Definition

Let $\boldsymbol{w} \in \mathbb{R}^n - \{\boldsymbol{0}\}$ and let $a \in \mathbb{R}$. The *hyperplane* determined by $\boldsymbol{w}$ and a is the set

$$H_{\boldsymbol{w},a} = \{\boldsymbol{x} \in \mathbb{R}^n \mid \boldsymbol{w}'\boldsymbol{x} = a\}.$$

If $\mathbf{x}_0 \in H_{\mathbf{w},a}$, then $\mathbf{w}'\mathbf{x}_0 = a$, so $H_{\mathbf{w},a}$ is also described by the equality

$$H_{\mathbf{w},a} = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{w}'(\mathbf{x} - \mathbf{x}_0) = 0\}.$$

Any hyperplane $H_{\mathbf{w},a}$ partitions $\mathbb{R}^n$ into three sets:

$$\begin{aligned} H^{>}_{\mathbf{w},a} &= \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{w}'\mathbf{x} > a\}, \\ H^{0}_{\mathbf{w},a} &= H_{\mathbf{w},a}, \\ H^{<}_{\mathbf{w},a} &= \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{w}'\mathbf{x} < a\}. \end{aligned}$$

The sets $H^{>}_{\mathbf{w},a}$ and $H^{<}_{\mathbf{w},a}$ are the *positive* and *negative open* half-spaces determined by $H_{\mathbf{w},a}$, respectively. The sets

$$\begin{aligned} H^{\geqslant}_{\mathbf{w},a} &= \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{w}'\mathbf{x} \geqslant a\}, \\ H^{\leqslant}_{\mathbf{w},a} &= \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{w}'\mathbf{x} \leqslant a\}. \end{aligned}$$

are the *positive* and *negative closed* half-spaces determined by $H_{\mathbf{w},a}$, respectively.

If $\boldsymbol{x}_1, \boldsymbol{x}_2 \in H_{\boldsymbol{w},a}$ we say that the vector $\boldsymbol{x}_1 - \boldsymbol{x}_2$ is located in the hyperplane $H_{\boldsymbol{w},a}$. In this case $\boldsymbol{w} \perp \boldsymbol{x}_1 - \boldsymbol{x}_2$. This justifies referring to $\boldsymbol{w}$ as the *normal to the hyperplane* $H_{\boldsymbol{w},a}$. Observe that a hyperplane is fully determined by a vector $\boldsymbol{x}_0 \in H_{\boldsymbol{w},a}$ and by $\boldsymbol{w}$.

Let $\boldsymbol{x}_0 \in \mathbb{R}^n$ and let $H_{\boldsymbol{w},a}$ be a hyperplane. We seek $\boldsymbol{x} \in H_{\boldsymbol{w},a}$ such that $\| \boldsymbol{x} - \boldsymbol{x}_0 \|_2$ is minimal. Finding $\boldsymbol{x}$ amounts to minimizing the function $f(\boldsymbol{x}) = \| \boldsymbol{x} - \boldsymbol{x}_0 \|_2^2 = \sum_{i=1}^n (x_i - x_{0i})^2$ subjected to the constraint $\boldsymbol{w}_1 \boldsymbol{x}_1 + \cdots + w_n \boldsymbol{x}_n - a = 0$. Using the Lagrangian $\Lambda(\boldsymbol{x}) = f(\boldsymbol{x}) + \lambda(\boldsymbol{w}'\boldsymbol{x} - a)$ and the multiplier λ we impose the conditions

$$\frac{\partial \Lambda}{\partial x_i} = 0 \text{ for } 1 \leqslant i \leqslant n$$

which amount to

$$\frac{\partial f}{\partial x_i} + \lambda w_i = 0$$

for $1 \leqslant i \leqslant n$. These equalities yield $2(x_i - x_{0i}) + \lambda \boldsymbol{w}_i = 0$, so we have $x_i = x_{0i} - \frac{1}{2}\lambda \boldsymbol{w}_i$.

Consequently, we have $\boldsymbol{x} = \boldsymbol{x}_0 - \frac{1}{2}\lambda\boldsymbol{w}$. Since $\boldsymbol{x} \in H_{\boldsymbol{w},a}$ this implies

$$\boldsymbol{w}'\boldsymbol{x} = \boldsymbol{w}'\boldsymbol{x}_0 - \frac{1}{2}\lambda\boldsymbol{w}'\boldsymbol{w} = a.$$

Thus,

$$\lambda = 2\frac{\boldsymbol{w}'\boldsymbol{x}_0 - a}{\boldsymbol{w}'\boldsymbol{w}} = 2\frac{\boldsymbol{w}'\boldsymbol{x}_0 - a}{\parallel \boldsymbol{w} \parallel_2^2}.$$

We conclude that the closest point in $H_{\boldsymbol{w},a}$ to $\boldsymbol{x}_0$ is

$$\boldsymbol{x} = \boldsymbol{x}_0 - \frac{\boldsymbol{w}'\boldsymbol{x}_0 - a}{\parallel \boldsymbol{w} \parallel_2^2}\boldsymbol{w}.$$

The smallest distance between $\mathbf{x}_0$ and a point in the hyperplane $H_{\mathbf{w},a}$ is given by

$$\| \mathbf{x}_0 - \mathbf{x} \| = \frac{|\mathbf{w}'\mathbf{x}_0 - a|}{\| \mathbf{w} \|_2}.$$

If we define the distance $d(H_{\mathbf{w},a}, \mathbf{x}_0)$ between $\mathbf{x}_0$ and $H_{\mathbf{w},a}$ as this smallest distance we have

$$d(H_{\mathbf{w},a}, \mathbf{x}_0) = \frac{|\mathbf{w}'\mathbf{x}_0 - a|}{\| \mathbf{w} \|_2}. \quad (4)$$

Lemma

Let $A \in \mathbb{C}^{n\times n}$. *If* $\mathbf{x}^H A\mathbf{x} = 0$ *for every* $\mathbf{x} \in \mathbb{C}^n$, *then* $A = O_{n,n}$.

Proof

If $\boldsymbol{x} = \boldsymbol{e}_k$, then $\boldsymbol{x}^{\mathsf{H}} A \boldsymbol{x} = a_{kk}$ for every k, $1 \leqslant k \leqslant n$, so all diagonal entries of A equal 0. Choose now $\boldsymbol{x} = \boldsymbol{e}_k + \boldsymbol{e}_j$. Then,

$$\begin{aligned}
&(\boldsymbol{e}_k + \boldsymbol{e}_j)^{\mathsf{H}} A (\boldsymbol{e}_k + \boldsymbol{e}_j) \\
&= \boldsymbol{e}_k^{\mathsf{H}} A \boldsymbol{e}_k + \boldsymbol{e}_k^{\mathsf{H}} A \boldsymbol{e}_j + \boldsymbol{e}_j^{\mathsf{H}} A \boldsymbol{e}_k + \boldsymbol{e}_j^{\mathsf{H}} A \boldsymbol{e}_j \\
&= \boldsymbol{e}_k^{\mathsf{H}} A \boldsymbol{e}_j + \boldsymbol{e}_j^{\mathsf{H}} A \boldsymbol{e}_k \\
&= a_{kj} + a_{jk} = 0.
\end{aligned}$$

Proof cont'd

Similarly, if we choose $\boldsymbol{x} = \boldsymbol{e}_k + i\boldsymbol{e}_j$ we obtain:

$$\begin{aligned} & (\boldsymbol{e}_k + i\boldsymbol{e}_j)^{\mathrm{H}} A(\boldsymbol{e}_k + i\boldsymbol{e}_j) \\ &= (\boldsymbol{e}_k^{\mathrm{H}} - i\boldsymbol{e}_j^{\mathrm{H}}) A(\boldsymbol{e}_k + i\boldsymbol{e}_j) \\ &= \boldsymbol{e}_k^{\mathrm{H}} A\boldsymbol{e}_k - i\boldsymbol{e}_j^{\mathrm{H}} A\boldsymbol{e}_k + i\boldsymbol{e}_k^{\mathrm{H}} A\boldsymbol{e}_j + \boldsymbol{e}_j^{\mathrm{H}} A\boldsymbol{e}_j \\ &= -ia_{jk} + ia_{kj} = 0. \end{aligned}$$

The equalities $a_{kj} + a_{jk} = 0$ and $-a_{jk} + a_{kj} = 0$ imply $a_{kj} = a_{jk} = 0$. Thus, all off-diagonal elements of A are also 0, hence $A = O_{n,n}$.

Theorem

A matrix $U \in \mathbb{C}^{n\times n}$ *is unitary if* $\parallel U\mathbf{x} \parallel_2 = \parallel \mathbf{x} \parallel_2$ *for every* $\mathbf{x} \in \mathbb{C}^n$.

Proof

If U is unitary we have

$$\| U\mathbf{x} \|_2^2 = (U\mathbf{x})^{\mathsf{H}} U\mathbf{x} = \mathbf{x}^{\mathsf{H}} U^{\mathsf{H}} U\mathbf{x} = \| \mathbf{x} \|_2^2$$

because $U^{\mathsf{H}} U = I_n$. Thus, $\| U\mathbf{x} \|_2 = \| \mathbf{x} \|_2$.

Conversely, let U be a matrix such that $\| U\mathbf{x} \|_2 = \| \mathbf{x} \|_2$ for every $\mathbf{x} \in \mathbb{C}^n$. This implies $\mathbf{x}^{\mathsf{H}} U^{\mathsf{H}} U\mathbf{x} = \mathbf{x}^{\mathsf{H}}\mathbf{x}$, hence $\mathbf{x}^{\mathsf{H}}(U^{\mathsf{H}} U - I_n)\mathbf{x} = 0$ for $\mathbf{x} \in \mathbb{C}^n$. This implies $U^{\mathsf{H}} U = I_n$, so U is a unitary matrix.

UMASS BOSTON

Corollary

The following statements that concern a matrix $U \in \mathbb{C}^{n\times n}$ are equivalent:

- *U is unitary;*
- $\| U\mathbf{x} - U\mathbf{y} \|_2 = \| \mathbf{x} - \mathbf{y} \|_2$ *for* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$;
- $(U\mathbf{x}, U\mathbf{y}) = (\mathbf{x}, \mathbf{y})$ *for* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$.

UMASS BOSTON

The counterpart of unitary matrices in the set of real matrices are introduced next.

Definition

A matrix $A \in \mathbb{R}^{n \times n}$ is *orthogonal* or *orthonormal* if it is unitary.

In other words, a real matrix $A \in \mathbb{R}^{n \times n}$ is orthogonal if and only if $A'A = AA' = I_n$. Clearly, A is orthogonal if and only if A' is orthogonal.

Theorem

If $A \in \mathbb{R}^{n \times n}$ *is an orthogonal matrix, then* $\det(A) \in \{-1, 1\}$.

Proof.

By a previous Corollary, $|\det(A)| = 1$. Since $\det(A)$ is a real number, it follows that $\det(A) \in \{-1, 1\}$. □

Corollary

Let A be a matrix in $\mathbb{R}^{n\times n}$. The following statements are equivalent:

- *A is orthogonal;*
- *A is invertible and $A^{-1} = A'$;*
- *A' is invertible and $(A')^{-1} = A$;*
- *A' is orthogonal.*

Thus, a matrix A is orthogonal if and only if it preserves the length of vectors.

Definition

A *rotation matrix* is an orthogonal matrix $R \in \mathbb{R}^{n \times n}$ such that $\det(R) = 1$.

A *reflection matrix* is an orthogonal matrix $R \in \mathbb{R}^{n \times n}$ such that $\det(R) = -1$.

In the bidimensional case, $n = 2$, a rotation is a an orthogonal matrix $R \in \mathbb{R}^{2\times 2}$. For

$$R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$$

we have:

$$\begin{aligned} RR' &= \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} \begin{pmatrix} r_{11} & r_{21} \\ r_{12} & r_{22} \end{pmatrix} \\ &= \begin{pmatrix} r_{11}^2 + r_{12}^2 & r_{11}r_{21} + r_{12}r_{22} \\ r_{11}r_{21} + r_{12}r_{22} & r_{21}^2 + r_{22}^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

.

The above equalities imply:

$$
\begin{aligned}
r_{11}^2 + r_{12}^2 &= 1, \\
r_{21}^2 + r_{22}^2 &= 1, \\
r_{11}r_{21} + r_{12}r_{22} &= 0.
\end{aligned}
$$

Also, the orthogonality implies

$$r_{11}r_{22} - r_{12}r_{21} = 1.$$

The equality $r_{11}r_{22} - r_{12}r_{21} = 1$ implies:

$$r_{22}(r_{11}r_{12} + r_{21}r_{22}) - r_{12}(r_{11}r_{22} - r_{12}r_{21}) = -r_{12},$$

or

$$r_{21}(r_{22}^2 + r_{12}^2) = -r_{12},$$

so $r_{21} = -r_{12}$.
If $r_{21} = -r_{21} = 0$, the above equalities imply that either $r_{11} = r_{22} = 1$ or $r_{11} = r_{22} = -1$. Otherwise, the equality $r_{11}r_{12} + r_{21}r_{22} = 0$ implies $r_{11} = r_{22}$.

Since $r_{11}^2 \leqslant 1$ it follows that there exists θ such that $r_{11} = \cos\theta$. This implies that R has the form

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Its effect on a vector

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2$$

is to produce the vector $\boldsymbol{y} = R\boldsymbol{x}$, where

$$\boldsymbol{y} = \begin{pmatrix} x_1\cos\theta - x_2\sin\theta \\ x_1\sin\theta + x_2\cos\theta \end{pmatrix},$$

which is obtained from $\boldsymbol{x}$ by a counterclockwise rotation by the angle θ.

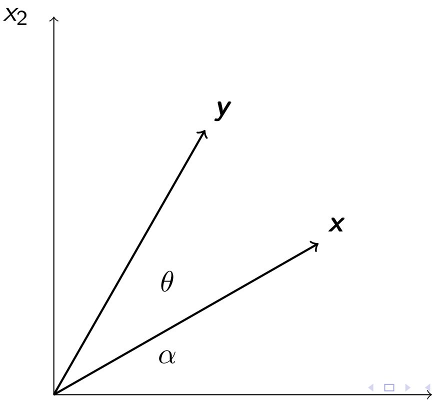
It is easy to see that $\det(R) = 1$, so the term "rotation matrix" is clearly justified for R. To mark the dependency of R on θ we will use the notation

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

If the angle of the vector $\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ with the x_1 axis is α and $\boldsymbol{x}$ is rotated counterclockwise by θ to yield the vector $\boldsymbol{y} = y_1\boldsymbol{e}_1 + y_2\boldsymbol{e}_2$, then $x_1 = r\cos\alpha$, $x_2 = r\sin\alpha$, and

$$\begin{aligned} y_1 &= r\cos(\alpha+\theta) = r\cos\alpha\cos\theta - r\sin\alpha\sin\theta = x_1\cos\theta - x_2\sin\theta, \\ y_2 &= r\sin(\alpha+\theta) = r\sin\alpha\cos\theta + r\cos\alpha\sin\theta = x_1\sin\theta + x_2\cos\theta, \end{aligned}$$

which are the formulas that describe the transformation of $\boldsymbol{x}$ into $\boldsymbol{y}$.



Definition

Let U be an m-dimensional subspace of $\mathbb{C}^n$ and let $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ be an orthonormal basis of this subspace. The *orthogonal projection of the vector $\boldsymbol{x} \in \mathbb{C}^n$ on the subspace U* is the vector $\text{proj}_U(\boldsymbol{x})$ given by:

$$\text{proj}_U(\boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{u}_1)\boldsymbol{u}_1 + \cdots + (\boldsymbol{x}, \boldsymbol{u}_m)\boldsymbol{u}_m.$$

Theorem

Let U be an m-dimensional subspace of $\mathbb{R}^n$ and let $\boldsymbol{x} \in \mathbb{R}^n$. The vector $\boldsymbol{y} = \boldsymbol{x} - proj_U(\boldsymbol{x})$ belongs to the subspace $U^\perp$.

Proof.

Let $B_U = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ be an orthonormal basis of U. Note that

$$\begin{aligned}(\boldsymbol{y}, \boldsymbol{u}_j) &= (\boldsymbol{x}, \boldsymbol{u}_j) - \left(\sum_{i=1}^{m} (\boldsymbol{x}, \boldsymbol{u}_i)\boldsymbol{u}_i, \boldsymbol{u}_j\right) \\ &= (\boldsymbol{x}, \boldsymbol{u}_j) - \sum_{i=1}^{m} (\boldsymbol{x}, \boldsymbol{u}_i)(\boldsymbol{u}_i, \boldsymbol{u}_j) = 0,\end{aligned}$$

due to the orthogonality of the basis B_U. Therefore, $\boldsymbol{y}$ is orthogonal on every linear combination of B_U, that is on the subspace U. □

Theorem

Let U be an m-dimensional subspace of $\mathbb{C}^n$ having the orthonormal basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$.
The orthogonal projection $proj_U$ is given by $proj_U(\boldsymbol{x}) = B_U B_U^{H} \boldsymbol{x}$ for $\boldsymbol{x} \in \mathbb{C}^n$, where $B_U \in \mathbb{R}^{n \times m}$ is the matrix $B_U = (\boldsymbol{u}_1 \ \cdots \ \boldsymbol{u}_m) \in \mathbb{C}^{n \times m}$.

Proof.

We can write

$$\text{proj}_U(\boldsymbol{x}) = \sum_{i=1}^{m} \boldsymbol{u}_i(\boldsymbol{u}_i^{\mathsf{H}}\boldsymbol{x}) = (\boldsymbol{u}_1 \ \cdots \ \boldsymbol{u}_m) \begin{pmatrix} \boldsymbol{u}_1^{\mathsf{H}} \\ \vdots \\ \boldsymbol{u}_m^{\mathsf{H}} \end{pmatrix} \boldsymbol{x} = B_U B_U^{\mathsf{H}} \boldsymbol{x}.$$

□

Since the basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ is orthonormal, we have $B_U^{\mathsf{H}} B_U = I_m$. Observe that the matrix $B_U B_U^{\mathsf{H}} \in \mathbb{C}^{n \times n}$ is symmetric and idempotent because

$$(B_U B_U^{\mathsf{H}})(B_U B_U^{\mathsf{H}}) = B_U (B_U^{\mathsf{H}} B_U) B_U^{\mathsf{H}} = B_U B_U^{\mathsf{H}}.$$

For an m-dimensional subspace U of $\mathbb{C}^n$ we denote by $P_U = B_U B_U^{\mathsf{H}} \in \mathbb{C}^{n \times n}$, where B_U is a matrix of an orthonormal basis of U as defined before. P_U is the *projection matrix* of the subspace U.

Corollary

For every non-zero subspace U, the matrix P_U is a Hermitian matrix, and therefore, a self-adjoint matrix.

Proof.

Since $P_U = B_U B_U^{\mathsf{H}}$ where B_U is a matrix of an orthonormal basis of the subspace S, it is immediate that $P_U^{\mathsf{H}} = P_U$. □

The self-adjointness of P_U means that $(\boldsymbol{x}, P_U \boldsymbol{y}) = (P_U \boldsymbol{x}, \boldsymbol{y})$ for every $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{C}^n$.

Corollary

Let U be an m-dimensional subspace of $\mathbb{C}^n$ having the orthonormal basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$. If $B_U = (\boldsymbol{u}_1 \ \cdots \ \boldsymbol{u}_m) \in \mathbb{C}^{n \times m}$, then for every $\boldsymbol{x} \in \mathbb{C}$ we have the decomposition $\boldsymbol{x} = P_U\boldsymbol{x} + Q_U\boldsymbol{x}$, where $P_U = B_U B_U^H$ and $Q_U = I_n - P_U$, $P_U\boldsymbol{x} \in U$ and $Q_U\boldsymbol{x} \in U^\perp$.

Observe that

$$\begin{aligned} Q_U^2 &= (I_n - P_U P_U^{\mathsf{H}})(I_n - P_U P_U^{\mathsf{H}}) \\ &= I_n - P_U P_U^{\mathsf{H}} - P_U P_U^{\mathsf{H}} + P_U P_U^{\mathsf{H}} P_U P_U^{\mathsf{H}} = Q_U, \end{aligned}$$

so Q_U is an idempotent matrix. The matrix Q_U is the projection matrix on the subspace $U^{\perp}$. Clearly, we have

$$P_{U^{\perp}} = Q_U = I_n - P_U. \tag{5}$$

It is possible to give a direct argument for the independence of the projection matrix P_U relative to the choice of orthonormal basis in U.

It is possible to give a direct argument for the independence of the projection matrix P_U relative to the choice of orthonormal basis in U.

Theorem

Let U be an m-dimensional subspace of $\mathbb{C}^n$ having the orthonormal bases $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ and $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ and let $B_U = (\mathbf{u}_1 \ \cdots \ \mathbf{u}_m) \in \mathbb{C}^{n \times m}$ and $\tilde{B}_U = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_m) \in \mathbb{C}^{n \times m}$. The matrix $B_U^H \tilde{B}_U \in \mathbb{C}^{m \times m}$ is unitary and $\tilde{B}_U \tilde{B}_U^H = B_U B_U^H$.

Proof

Since the both sets of columns of B_U and $\tilde{B}_U$ are bases for U, there exists a unique square matrix $Q \in \mathbb{C}^{m\times m}$ such that $B_U = \tilde{B}_U Q$. The orthonormality of B_U and $\tilde{B}_U$ implies $B_U^{\mathsf{H}} B_U = \tilde{B}_U^{\mathsf{H}} \tilde{B}_U = I_m$. Thus, we can write

$$I_m = B_U^{\mathsf{H}} B_U = Q^{\mathsf{H}} \tilde{B}_U^{\mathsf{H}} \tilde{B}_U Q = Q^{\mathsf{H}} Q,$$

which shows that Q is unitary. Furthermore, $B_U^{\mathsf{H}} \tilde{B}_U = Q^{\mathsf{H}} \tilde{B}_U^{\mathsf{H}} \tilde{B}_U = Q^{\mathsf{H}}$ is unitary and

$$B_U B_U^{\mathsf{H}} = \tilde{B}_U Q Q^{\mathsf{H}} \tilde{B}_U^{\mathsf{H}} = \tilde{B}_U \tilde{B}_U^{\mathsf{H}}.$$

Definition

A matrix $A \in \mathbb{C}^{n\times n}$ is *positive definite* if $\mathbf{x}^{\mathsf{H}}A\mathbf{x}$ is a real positive number for every $\mathbf{x} \in \mathbb{C}^n - \{\mathbf{0}\}$.

Theorem

If $A \in \mathbb{C}^{n \times n}$ is positive definite, then A is Hermitian.

Proof.

Let $A \in \mathbb{C}^{n \times n}$ be a matrix. Since $\mathbf{x}^{\mathsf{H}} A \mathbf{x}$ is a real number it follows that it equals its conjugate, so $\mathbf{x}^{\mathsf{H}} A \mathbf{x} = \mathbf{x}^{\mathsf{H}} A^{\mathsf{H}} \mathbf{x}$ for every $\mathbf{x} \in \mathbb{C}^n$. Therefore, there exists a unique pair of Hermitian matrices H_1 and H_2 such that $A = H_1 + iH_2$, which implies $A^{\mathsf{H}} = H_1^{\mathsf{H}} - iH_2^{\mathsf{H}}$. Thus, we have

$$\mathbf{x}^{\mathsf{H}}(H_1 + iH_2)\mathbf{x} = \mathbf{x}^{\mathsf{H}}(H_1^{\mathsf{H}} - iH_2^{\mathsf{H}})\mathbf{x} = \mathbf{x}^{\mathsf{H}}(H_1 - iH_2)\mathbf{x},$$

because H_1 and H_2 are Hermitian. This implies $\mathbf{x}^{\mathsf{H}} H_2 \mathbf{x} = 0$ for every $\mathbf{x} \in \mathbb{C}^n$, which, in turn, implies $H_2 = O_{n,n}$. Consequently, $A = H_1$, so A is indeed Hermitian. □

UMASS BOSTON

Definition

A matrix $A \in \mathbb{C}^{n \times n}$ is *positive semidefinite* if $\mathbf{x}^{\mathsf{H}} A \mathbf{x}$ is a non-negative real number for every $\mathbf{x} \in \mathbb{C}^n - \{\mathbf{0}\}$.

Positive definiteness (positive semidefiniteness) is denoted by $A \succ 0$ ($A \succeq 0$, respectively).

The definition of positive definite (semidefinite) matrix can be specialized for real matrices as follows.

Definition

A symmetric matrix $A \in \mathbb{R}^{n \times n}$ is *positive definite* if $\boldsymbol{x}' A \boldsymbol{x} > 0$ for every $\boldsymbol{x} \in \mathbb{R}^n - \{\mathbf{0}\}$.
If A satisfies the weaker inequality $\boldsymbol{x}' A \boldsymbol{x} \geqslant 0$ for every $\boldsymbol{x} \in \mathbb{R}^n - \{\mathbf{0}\}$, then we say that A is *positive semidefinite*.
$A \succ 0$ denotes that A is positive definite and $A \succeq 0$ means that A is positive semidefinite.

Note that in the case of real-valued matrices we need to require explicitly the symmetry of the matrix because, unlike the complex case, the inequality $\boldsymbol{x}'A\boldsymbol{x} > 0$ for $\boldsymbol{x} \in \mathbb{R}^n - \{\boldsymbol{0}_n\}$ does *not* imply the symmetry of A. For example, consider the matrix

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

where $a, b \in \mathbb{R}$ and $a > 0$. We have

$$\boldsymbol{x}'A\boldsymbol{x} = (x_1\ x_2) \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = a(x_1^2 + x_2^2) > 0$$

if $\boldsymbol{x} \neq \boldsymbol{0}_2$.

Example

The symmetric real matrix

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

is positive definite if and only if $a > 0$ and $b^2 - ac < 0$. Indeed, we have $\boldsymbol{x}'A\boldsymbol{x} > 0$ for every $\boldsymbol{x} \in \mathbb{R}^2 - \{\mathbf{0}\}$ if and only if $ax_1^2 + 2bx_1x_2 + cx_2^2 > 0$, where $\boldsymbol{x}' = (x_1 \ \ x_2)$; elementary algebra considerations lead to $a > 0$ and $b^2 - ac < 0$.

A positive definite matrix is non-singular. Indeed, if $A\boldsymbol{x} = \boldsymbol{0}$, where $A \in \mathbb{R}^{n\times n}$ is positive definite, then $\boldsymbol{x}^{\mathsf{H}} A\boldsymbol{x} = 0$, so $\boldsymbol{x} = \boldsymbol{0}$. Therefore, A is non-singular.

Example

If $A \in \mathbb{C}^{m\times n}$, then the matrices $A^{\mathsf{H}}A \in \mathbb{C}^{n\times n}$ and $AA^{\mathsf{H}} \in \mathbb{C}^{m\times m}$ are positive semidefinite. For $\boldsymbol{x} \in \mathbb{C}^n$ we have

$$\boldsymbol{x}^{\mathsf{H}}(A^{\mathsf{H}}A)\boldsymbol{x} = (\boldsymbol{x}^{\mathsf{H}}A^{\mathsf{H}})(A\boldsymbol{x}) = (A\boldsymbol{x})^{\mathsf{H}}(A\boldsymbol{x}) = \| A\boldsymbol{x} \|_2^2 \geqslant 0.$$

The argument for AA^{H} is similar.
If $\text{rank}(A) = n$, then the matrix $A^{\mathsf{H}}A$ is positive definite because $\boldsymbol{x}^{\mathsf{H}}(A^{\mathsf{H}}A)\boldsymbol{x} = 0$ implies $A\boldsymbol{x} = \boldsymbol{0}$, which, in turn, implies $\boldsymbol{x} = \boldsymbol{0}$.

Theorem

If $A \in \mathbb{C}^{n \times n}$ is a positive definite matrix, then any principal submatrix $B = A\begin{bmatrix} i_1 & \cdots & i_k \\ i_1 & \cdots & i_k \end{bmatrix}$ is a positive definite matrix.

Proof.

Let $\boldsymbol{x} \in \mathbb{C}^n - \{\mathbf{0}\}$ be a vector such that all components located on positions other than $i_1, \ldots, i_k$ equal 0 and let $\boldsymbol{y} = \boldsymbol{x}\begin{bmatrix} i_1 & \cdots & i_k \\ & 1 & \end{bmatrix} \in \mathbb{C}^k$ be the vector obtained from $\boldsymbol{x}$ by retaining only the components located on positions $i_1, \ldots, i_k$. Since $\boldsymbol{y}^{\mathsf{H}} B \boldsymbol{y} = \boldsymbol{x}^{\mathsf{H}} A \boldsymbol{x} > 0$ it follows that $B \succ 0$. □

Corollary

If $A \in \mathbb{C}^{n \times n}$ is a positive definite matrix, then any diagonal element a_{ii} is a real positive number for $1 \leqslant i \leqslant n$.

Theorem

If $A, B \in \mathbb{C}^{n\times n}$ are two positive semidefinite matrices and a, b are two non-negative numbers, then $aA + bB \succeq 0$.

Proof.

The statement holds because $\mathbf{x}^{\mathsf{H}}(aA + bB)\mathbf{x} = a\mathbf{x}^{\mathsf{H}}A\mathbf{x} + b\mathbf{x}^{\mathsf{H}}B\mathbf{x} \geqslant 0$, due to the fact that A and B are positive semidefinite. □

Definition

Let $L = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ be a sequence of vectors in $\mathbb{R}^n$.
The *Gram matrix of L* is the matrix

$$G_L = (g_{ij}) \in \mathbb{R}^{m \times m}$$

defined by $g_{ij} = \boldsymbol{v}_i' \boldsymbol{v}_j$ for $1 \leqslant i, j \leqslant m$.

If $A_L = (\boldsymbol{v}_1 \ \cdots \ \boldsymbol{v}_m) \in \mathbb{R}^{n \times m}$, then $G_L = A_L' A_L$. Also, note that G_L is a symmetric matrix.

Example

Let

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}.$$

The Gram matrix of the set $L = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is

$$G_L = \begin{pmatrix} 2 & -1 & 2 \\ -1 & 9 & 4 \\ 2 & 4 & 5 \end{pmatrix}.$$

Note that $\det(G_L) = 1$.

Theorem

Let $L = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ be a sequence of m vectors in $\mathbb{R}^n$, where $m \leqslant n$. If L is linearly independent, then the Gram matrix G_L is positive definite.

Proof.

Suppose that L is linearly independent. Let $\boldsymbol{x} \in \mathbb{R}^m$. We have $\boldsymbol{x}' G_L \boldsymbol{x} = \boldsymbol{x}' A_L' A_L \boldsymbol{x} = (A_L \boldsymbol{x})' A_L \boldsymbol{x} = \parallel A_L \boldsymbol{x} \parallel_2^2$. Therefore, if $\boldsymbol{x}' G_L \boldsymbol{x} = 0$, we have $A_L \boldsymbol{x} = \boldsymbol{0}$, which is equivalent to $x_1 \boldsymbol{v}_1 + \cdots + x_n \boldsymbol{v}_n = 0$. Since $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ is linearly independent it follows that $x_1 = \cdots = x_m = 0$, so $\boldsymbol{x} = \boldsymbol{0}$. Thus, A is indeed, positive definite. □

The Gram matrix of an arbitrary sequence of vectors is positive semidefinite, as the reader can easily verify.

Definition

Let $L = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ be a sequence of m vectors in $\mathbb{R}^n$, where $m \leqslant n$. The *Gramian* of L is the number $\det(G_L)$.

Theorem

If $L = (\mathbf{v}_1, \ldots, \mathbf{v}_m)$ is a sequence of m vectors in $\mathbb{R}^n$. Then, L is linearly independent if and only if $\det(G_L) \neq 0$.

Proof.

Suppose that $\det(G_L) \neq 0$ and that L is not linearly independent. In other words, the numbers $a_1, \ldots, a_m$ exists such that at least one of them is not 0 and $a_1\mathbf{x}_1 + \cdots + a_m\mathbf{x}_m = \mathbf{0}$. This implies the equalities

$$a_1(\mathbf{x}_1, \mathbf{x}_j) + \cdots + a_m(\mathbf{x}_m, \mathbf{x}_j) = \mathbf{0},$$

for $1 \leqslant j \leqslant m$, so the system $G_L\mathbf{a} = \mathbf{0}$ has a non-trivial solution in $a_1, \ldots, a_m$. This implies $\det(G_L) = 0$, which contradicts the initial assumption. □

Proof cont'd

Conversely, suppose that L is linearly independent and $\det(G_L) = 0$. Then, the linear system

$$a_1(\boldsymbol{x}_1, \boldsymbol{x}_j) + \cdots + a_m(\boldsymbol{x}_m, \boldsymbol{x}_j) = \boldsymbol{0},$$

for $1 \leqslant j \leqslant m$, has a non-trivial solution in $a_1, \ldots, a_m$. If $\boldsymbol{w} = a_1\boldsymbol{x}_1 + \cdots a_m\boldsymbol{x}_m$, this amounts to $(\boldsymbol{w}, \boldsymbol{x}_i) = 0$ for $1 \leqslant i \leqslant n$. This, in turn, implies $(\boldsymbol{w}, \boldsymbol{w}) = \parallel \boldsymbol{w} \parallel_2^2 = 0$, so $\boldsymbol{w} = 0$, which contradicts the linear independence of L.

The Gram-Schmidt algorithm constructs an orthonormal basis for a subspace U of $\mathbb{C}^n$, starting from an arbitrary basis of $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ of U. The orthonormal basis is constructed sequentially such that $\langle \boldsymbol{w}_1, \ldots, \boldsymbol{w}_k \rangle = \langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle$ for $1 \leqslant k \leqslant m$.

Notations

$U(:, 1:k)$ is the matrix $(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ that contains the first k vectors of the existing basis.
$W(:, 1:k)$ the matrix $(\mathbf{w}_1, \ldots, \mathbf{w}_k)$ that contains the first k vectors of the new orthonormal basis.

Gram-Schmidt Orthogonalization Algorithm

Data: A basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ for a subspace U of $\mathbb{C}^n$

Result: An orthonormal basis $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ for U

$W = O_{n,m}$

$W(:,1) = W(:,1) + \frac{1}{\|U(:,1)\|_2} U(:,1)$

For $(k = 2$ to $m)$ $\{$

$P = I_n - W(:,1:(k-1))W(:,1:(k-1))^{\mathsf{H}}$

$W(:,k) = W(:,k) + \frac{1}{\|PU(:,k)\|_2} PU(:,k)$

$\}$

Return $W = (\boldsymbol{w}_1 \ \cdots \ \boldsymbol{w}_m)$

Theorem

Let $(\mathbf{w}_1, \ldots, \mathbf{w}_m)$ *be the sequence of vectors constructed by the Gram-Schmidt algorithm starting from the basis* $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ *of an m-dimensional subspace* U *of* $\mathbb{C}^n$. *The set* $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ *is an orthogonal basis of* U *and* $\langle \mathbf{w}_1, \ldots, \mathbf{w}_k \rangle = \langle \mathbf{u}_1, \ldots \mathbf{u}_k \rangle$ *for* $1 \leqslant k \leqslant m$.

Proof

In the algorithm the matrix W is initialized as $O_{n,m}$. Its columns will contain eventually the vectors of the orthonormal basis $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m$. The argument is by induction on $k \geqslant 1$.
The base case, $k = 1$, is immediate.
Suppose that the statement of the theorem holds for k, that is, the set $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k\}$ is an orthonormal basis for $U_k = \langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle$ and constitutes the set of the initial k columns of the matrix W, that is, $W_k = W(:, 1 : k)$. Then,

$$P_k = I_n - W_k W_k^{\mathsf{H}}$$

is the projection matrix on the subspace $U_k^{\perp}$, so $P_k \boldsymbol{u}_k$ is orthogonal on every $\boldsymbol{w}_i$, where $1 \leqslant i \leqslant k$. Therefore, $\boldsymbol{w}_{k+1} = W(:, (k+1))$ is a unit vector orthogonal on all its predecessors $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_k$, so $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ is an orthonormal set.

Proof cont'd

The equality $\langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle = \langle \boldsymbol{w}_1, \ldots, \boldsymbol{w}_k \rangle$ clearly holds for $k = 1$. Suppose that it holds for k. Then, we have

$$\begin{aligned} \boldsymbol{w}_{k+1} &= \frac{1}{\| P_k \boldsymbol{u}_{k+1} \|_2} \left(\boldsymbol{u}_{k+1} - W_k W_k^{\mathsf{H}} \boldsymbol{u}_{k+1} \right) \\ &= \frac{1}{\| P_k \boldsymbol{u}_{k+1} \|_2} \left(\boldsymbol{u}_{k+1} - (\boldsymbol{w}_1 \ \cdots \ \boldsymbol{w}_k) W_k^{\mathsf{H}} \boldsymbol{u}_{k+1} \right). \end{aligned}$$

Since $\boldsymbol{w}_1 \ldots, \boldsymbol{w}_k$ belong to the subspace $\langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle$ (by inductive hypothesis), it follows that $\boldsymbol{w}_{k+1} \in \langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{u}_{k+1} \rangle$, so $\langle \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{k+1} \rangle \subseteq \langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle$.

Proof cont'd

For the converse inclusion, since

$$\mathbf{u}_{k+1} = \| P_k \mathbf{u}_{k+1} \|_2 \, \mathbf{w}_{k+1} + (\mathbf{w}_1 \ \cdots \ \mathbf{w}_k) W_k^{\mathsf{H}} \mathbf{u}_{k+1},$$

it follows that $\mathbf{u}_{k+1} \in \langle \mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{w}_{k+1} \rangle$. Thus, $\langle \mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{u}_{k+1} \rangle \subseteq \langle \mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{w}_{k+1} \rangle$.

Example

Let $A \in \mathbb{R}^{3\times 2}$ be the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 3 \end{pmatrix}.$$

It is easy to see that $\text{rank}(A) = 2$. We have $\{\boldsymbol{u}_1, \boldsymbol{u}_2\} \subseteq \mathbb{R}^3$ and we construct an orthogonal basis for the subspace generated by these columns. The matrix W is initialized to $O_{3,2}$.

Example cont'd

we begin by defining

$$\boldsymbol{w}_1 = \frac{1}{\parallel \boldsymbol{u}_1 \parallel_2} \boldsymbol{u}_1 = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix},$$

so

$$W = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 \\ 0 & 0 \\ \frac{\sqrt{2}}{2} & 0 \end{pmatrix},$$

The projection matrix is

$$P = I_3 - W(:,1)W(:,1)' = I_3 - \boldsymbol{w}_1 \boldsymbol{w}_1' = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

The projection of $\mathbf{u}_2$ is

$$P\mathbf{u}_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

and the second column of W becomes

$$\mathbf{w}_k = W(:,2) = \frac{\parallel P\mathbf{u}_2 \parallel_2}{P}\mathbf{u}_2 = \begin{pmatrix} -\frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix}.$$

Thus, the orthonormal basis we are seeking consists of the vectors

$$\begin{pmatrix} \frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix} \text{ and } \begin{pmatrix} -\frac{\sqrt{2}}{2} \\ 0 \\ \frac{\sqrt{2}}{2} \end{pmatrix}.$$

We describe a factorization algorithm for rectangular matrices which allows us to express a matrix as a product of a rectangular matrix with orthogonal columns and un upper triangular invertible matrix (the *thin QR factorization*).

Theorem

(The Thin QR Factorization Theorem) *Let* $A \in \mathbb{C}^{m \times n}$ *be a full-rank matrix such that* $m \geqslant n$*. Then,* A *can be factored as* $A = QR$*, where* $Q \in \mathbb{C}^{m \times n}$*,* $R \in \mathbb{C}^{n \times n}$ *such that*

- *the columns of* Q *constitute an orthonormal basis for* range(A)*, and*
- $R = (r_{ij})$ *is an upper triangular invertible matrix such that its diagonal elements are real non-negative numbers, that is,* $r_{ii} \geqslant 0$ *for* $1 \leqslant i \leqslant n$*.*

Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ be the columns of A. Since $\text{rank}(A) = n$, these columns constitute a basis for $\text{range}(A)$. Starting from this set of columns construct an orthonormal basis $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ for the subspace $\text{range}(A)$ using the Gram-Schmidt algorithm. Define Q as the orthogonal matrix

$$Q = (\boldsymbol{w}_1 \ \cdots \ \boldsymbol{w}_n).$$

By the properties of the Gram-Schmidt algorithm we have $\langle \boldsymbol{u}_1, \ldots, \boldsymbol{u}_k \rangle = \langle \boldsymbol{w}_1, \ldots, \boldsymbol{w}_k \rangle$ for $1 \leqslant k \leqslant n$, so it is possible to write

$$\begin{aligned} \boldsymbol{u}_k &= r_{1k}\boldsymbol{w}_1 + \cdots + r_{kk}\boldsymbol{w}_k \\ &= (\boldsymbol{w}_1 \ \cdots \ \boldsymbol{w}_n) \begin{pmatrix} r_{1k} \\ \vdots \\ r_{kk} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = Q \begin{pmatrix} r_{1k} \\ \vdots \\ r_{kk} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{aligned}$$

We may assume that $r_{kk} \geqslant 0$; otherwise, that is, if $r_{kk} < 0$, replace $\boldsymbol{w}_k$ by $-\boldsymbol{w}_k$. Clearly, this does not affect the orthonormality of the set $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$.

It is clear that $\text{rank}(Q) = n$. Therefore, since $\text{rank}(A) \leqslant \min\{\text{rank}(Q), \text{rank}(R)\}$, it follows that $\text{rank}(R) = n$, so R is an invertible matrix. Therefore, we have $r_{kk} > 0$ for $1 \leqslant k \leqslant n$.

Example

Let us determine a QR factorization for the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 3 \end{pmatrix}.$$

which has rank 2. We constructed an orthonormal basis for range(A) that consists of the vectors

$$\mathbf{w}_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \text{ and } \mathbf{w}_2 = \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Example cont'd

Thus, the orthogonal matrix Q is

$$Q = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

To compute R we need to express $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ as linear combinations of $\boldsymbol{w}_1$ and $\boldsymbol{w}_2$. Since

$$\begin{aligned} \boldsymbol{u}_1 &= \sqrt{2}\boldsymbol{w}_1 \\ \boldsymbol{u}_2 &= 2\sqrt{2}\boldsymbol{w}_1 + \sqrt{2}\boldsymbol{w}_2 \end{aligned}$$

the matrix R is

$$R = \begin{pmatrix} \sqrt{2} & 2\sqrt{2} \\ 0 & \sqrt{2} \end{pmatrix}.$$

Vector norms can be computed using the function `norm` which comes in two signatures: `norm(v)` and `norm(v,p)`. The first variant computes $\| \boldsymbol{v} \|_2$; the second computes $\| \boldsymbol{v} \|_p$ for any p, $1 \leqslant p \leqslant \infty$. In addition, `norm(v,inf)` computes $\| \boldsymbol{v} \|_\infty = \max\{|v_i| \mid 1 \leqslant i \leqslant n\}$, where $\boldsymbol{v} \in \mathbb{R}^n$. If one uses $-\infty$ as the second parameter, then `norm(v,-inf)` returns $\min\{|v_i| \mid 1 \leqslant i \leqslant n\}$.

Example

For the vector

```
v = [2 -3 5 -4]
```

the computation

```
norms = [norm(v,1),norm(v,2),norm(v,2.5),norm(v,inf),norm(v,-inf)]
```

returns

```
norms =

   14.0000    7.3485    6.5344    5.0000    2.0000
```

For matrices whose norm is expensive to compute, an approximative estimation of $\| A \|_2$ can be performed using the function `normest(A)`, or `normest(A,r)`, where r is the relative error; the default for r is 10^{-6}.
The following function implements the Gram-Schmidt algorithm.

```
function [W] = gram(U)
%GRAM implements the classical Gram-Schmidt algorithm
[n,m] = size(U);
W = zeros(n,m);
W(:,1)= (1/norm(U(:,1)))*U(:,1);
for k = 2:1:m
      P = eye(n) - W*W';
      W(:,k) = W(:,k) + (1/norm(P*U(:,k)))* P*U(:,k);
end
end
```

Theorem (Cholesky Decomposition Theorem)

Let $A \in \mathbb{C}^{n \times n}$ *be a Hermitian positive definite matrix. There exists a unique upper triangular matrix* R *with real positive diagonal elements such that* $A = R^H R$.

Corollary

If $A \in \mathbb{C}^{n \times n}$ *is a Hermitian positive definite matrix, then* $\det(A)$ *is a real positive number.*

The Cholesky decomposition of a Hermitian positive definite matrix is computed in MATLAB using the function `chol`. The function call `R = chol(A)` returns an upper triangular matrix R, satisfying the equation $R^{\mathsf{H}} R = A$. If A is not positive definite an error message is generated. The matrix R is computed using the diagonal and the upper triangle of A and the computation makes sense only if A is Hermitian.

Example

Let A be the symmetric positive definite matrix

$$A = \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix}.$$

Then, `R = chol(A)` yields

```
R =
    1.7321         0    1.1547
         0    1.4142    0.7071
         0         0    0.4082
```

The call `L = chol(A,'lower')` returns a lower triangular matrix `L` from the diagonal and lower triangle of matrix A, satisfying the equation $LL^{\mathsf{H}} = A$. When A is sparse, this syntax of `chol` is faster.

Example

For the same matrix A `L = chol(A,'lower')` returns

```
L =
    1.7321         0         0
         0    1.4142         0
    1.1547    0.7071    0.4082
```

For added flexibility, `[R,p] = chol(A)` and `[L,p] = chol(A,'lower')` set `p` to 0 if A is positive definite and to a positive number, otherwise, without returning an error message.

The thin QR decomposition of a matrix $A \in \mathbb{C}^{m \times n}$ is obtained using the function `qr` as in

```
[Q R] = qr(A)
```

To obtain the full decomposition we write

```
[Q R] = qr(A,0)
```