Linear Algebra – Preliminary lectures

Stéphane Marchand-Maillet
(Stephane.Marchand@eurecom.fr)
Department of Multimedia Communications
Institut Eurecom - Sophia-Antipolis
March 1999

Abstract

The following text aims at providing the minimum knowledge in Linear Algebra to the students in order to follow and understand further lectures in *e.g.*, Signal Processing and Telecommunications at Eurecom. This course is by no means supposed to be exhaustive of what is required in subsequent teaching. The references given at the end of this document provide **necessary** complementary reading.

Proofs of theorems within this text are left as exercises. They can be found in the relevant literature and some of them will be detailed in the associated lectures. Some exercises are also suggested and solutions will be detailed during the lectures.

Questions and (constructive) comments about this text are most welcome during the lectures.

Contents

1 Introduction and motivations

1.1 What is Linear Algebra?

- Linear Algebra consists mostly of studying matrix calculus.
- It formalises and gives geometrical interpretation of the resolution of equation systems.
- It creates a formal link between matrix calculus and the use of linear and quadratic transformations.

1.2 Why using Linear Algebra?

Linear Algebra allows for formalising and solving many typical problems in different engineering topics. It is generally the case that (input or output) data from an experiment is given in a discrete form (discrete measurements). Linear Algebra is then useful for solving problems in such a context with applications in topics such as Physics, Fluid Dynamics, Signal Processing and, more generally Numerical Analysis.

1.3 Course outline

This course is divided in four parts whose aims are as follows:

- Vector spaces: Give the necessary formalism for setting the basis.
- Linear transformations: Allow for representations
- Matrix calculus: Basic computation-oriented tools.
- Matrix transforms, solving linear systems: applications.

2 Vector spaces

A fundamental notion is that of **vectors** which in turn define vector spaces.

Definition 1 *Vector.*
A **vector** *of K^n is a n-uple x (also noted $\vec{x}$ or $\underline{x}$ or $\mathbf{x}$) of elements of the field K (e.g., $\mathbb{R}$ or $\mathbb{C}$):*

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix}$$

Definition 2 *Vector space.*
A set of vectors E is a **vector space** *on the field K (e.g., $\mathbb{R}$ or $\mathbb{C}$) if it is supplemented with an internal addition operation $(+)$ and an external product operation $(\times)$*[1] *on $E \times K$ such that $(E, +)$ is a group, i.e., for all vectors $x, y, z \in E$*

- *$x + y \in E$ (E is closed under vector addition),*
- *$(x + y) + z = x + (y + z)$ (associative law of vector addition),*
- *$x + y = y + x$ (commutative law of vector addition),*
- *There exists a unique $0_{\mathrm{E}} \in E$ such that $x + 0_{\mathrm{E}} = x$ (zero vector),*
- *There exists a unique "$-x$" such that $x + (-x) = 0_{\mathrm{E}}$ (existence of additive inverses)*

and for all scalars $\lambda, \mu \in K$,

[1] For the sake of simplicity in the notation, the sign $\times$ will later be dismissed in subsequent equation when multiplying scalar and vectors. However, the difference should be made at this point between scalar-vector multiplication and scalar-scalar multiplication.

- $\lambda \times x = x \times \lambda \in E$ *(E is closed under multiplication with scalars,*
- $\lambda \times (x + y) = \lambda \times x + \lambda \times y$ *(scalar distributes over vector addition),*
- $(\lambda + \mu) \times x = \lambda \times x + \lambda \times x$ *(vector distributes over scalar addition),*
- $\lambda \times (\mu \times x) = (\lambda\mu) \times x$ *(associative law of multiplication by scalar),*
- $1 \times x = x$

Proposition 1 $\lambda \times x = 0_{\mathrm{E}}$ *if and only if either* $\lambda = 0$ *or* $x = 0_{\mathrm{E}}$

Examples of vector spaces include

- The set of polynomials with coefficients from K, $\mathcal{P}(K)$,
- The set of $n \times n$ matrices with elements in K, $\mathcal{M}_{n\times n}(K)$,
- The set of continuous functions on an interval $I \subset K$, $\mathcal{C}^0(I)$

The restriction of a vector space leads to a vector subspace.

Definition 3 *Vector subspace.*
$F \subset E$ *is a* **vector subspace** *of* E *if for all* $x, y \in F$ *and all* $\lambda, \mu \in K$, $\lambda \times x + \mu \times y \in F$.

This definition goes down to saying that multiplying two vectors from a given subspace by any two scalars and adding the newly formed vectors together results in a vector which lies in the initial subspace.
From the above, examples of vector subspaces include

- The set of polynomial with coefficients from K and whose degree is lower than n, $\mathcal{P}_n(K)$,
- The set of continuous functions on an interval $I \subset K$ whose first derivative is also continuous, $\mathcal{C}^1(I)$

2.1 Linear dependence/independence

Definition 4 *Linear combination.*
Given $x_1, \ldots, x_n$ *vectors of* E *and* $\lambda_1, \ldots \lambda_n$ *scalars, the vector* $y \triangleq \sum_{i=1}^{n} \lambda_i \times x_i$ *is called a* **linear combination** *of vectors in* E.

Theorem 1 *The set* F *of all linear combinations of* n *vectors* $x_1, \ldots, x_n$ *of* E *is a vector subspace of* E.

This leads to the notion of **linear (in)dependence**.

Definition 5 *Linear (in)dependence.*
The n *vectors* $\{e_1, \ldots, e_n\}$ *are* **linearly independent** *if and only if*

$$\sum_{i=1}^{n} \lambda_i e_i = 0_{\mathrm{E}} \text{ implies } \lambda_i = 0 \text{ for all } i = 1 \ldots n$$

otherwise, the vectors $\{e_1, \ldots, e_n\}$ *are said to be* **linearly dependent**.

The rank of a set of vector is defined from this concept.

Definition 6 *Rank.*
The **rank** *of a set of vector* F *is the maximal number of linearly independent vectors that one can extract from* F.

Similarly the basis $\mathcal{B}$ is defined as follows.

Definition 7 *Basis.*
$\mathcal{B} = \{e_1, \ldots\} \subset E$ *is a* **basis** *of* E *if and only if any vector from* E *can uniquely be written as a linear combination of elements from* $\mathcal{B}$. *Moreover, if the dimension* n *of* $\mathcal{B}$ *is finite (i.e.,* $\mathcal{B} = \{e_1, \ldots e_n\}$ *then* $\dim E = n$ *and all basis of* E *are of dimension* n. $\mathcal{B}$ *is said to* **generate** E.

Then, the definition of the rank can be extended to apply to a set of vectors.

Remark 1 *The rank of a set of vectors* F *is the dimension of the vector subspace generated by* F.

In summary, the following equivalences can then be set,

Proposition 2 *If* E *is a vector space on* K *and* $\dim E = n$ *and* $\mathcal{B} = \{e_1, \ldots e_n\}$ *is a subset of* n *elements from* E *then,*

$$\mathcal{B} \text{ basis of } E \Leftrightarrow e_1, \ldots e_n \text{ linearly independent } \Leftrightarrow \mathcal{B} \text{ generates } E$$

2.2 Scalar product

Definition 8 *Scalar product.*

A **scalar product** *(or* **dot product** *or* **inner product***) is a symmetric*[2] *positive definite*[3] *bilinear*[4] *form from $E \times E$ to K: $x, y \mapsto < x, y >$ (also noted $x.y$) such that:*

- $< x, y > = < y, x >$ *for all x and y in E (commutativity)*
- $< \lambda x + \mu y, z > = \lambda < x, z > + \mu < y, z >$ *(bilinearity)*
- $< x, x > > 0$ *if $x \neq 0_{\mathrm{E}}$ (positive definiteness)*

Two vectors x and y such that $< x, y > = 0$ are said to be **orthogonal** ($x \perp y$).

The scalar product induces a **norm** noted $||x||$ such that

$$||x||^2 = < x, x >$$

E added with the scalar product is said to be a **pre-Hilbert** space. If E added with the induced norm is complete[5] then E is said to be a **Hilbert space**.

Definition 9 *Orthogonal space.*

Let E be a pre-Hilbert space and F a subset of E. The **orthogonal space** *of F in E is defined as*

$$F^{\perp} \triangleq \{x \in E \text{ such that } < x, y > = 0 \text{ for all } y \in F\}$$

E is therefore equivalently characterised by its **Hilbert decomposition**

$$E = F \oplus F^{\perp}$$

In other words,

For any $x \in E$ there exist a unique pair (x_1, x_2) with $x_1 \in F$ and $x_2 \in F^{\perp}$ such that $x = x_1 + x_2$

3 Linear transformations

Definition 10 *Linear transformation.*

Given E and F two vector spaces on K, $f : E \to F$ is a **linear transformation** *if and only if:*

$$\text{For all } \lambda, \mu \in K \text{ and for all } x, y \in E \times E, f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$$

Then $f \in L(E, F)$, the set of linear transforms from E to F. If $F = E$, f is is said to be an **endomorphism** *of E.*

Linear transforms come with set definitions:

Definition 11 *Kernel, range and rank of a linear transformation.*

- *The* **kernel** *of $f \in L(E, F)$ is defined as*

  $$\ker(f) = \mathrm{Null}(f) = \mathrm{N}(f) = E_0 \triangleq \{x \in E \text{ such that } f(x) = 0_{\mathrm{F}}\}$$

  Note that $\ker(f) \subset E$.

- *The* **range** *of $f \in L(E, F)$ is defined as*

  $$\mathrm{range}(f) \triangleq \{y \in F \text{ such that } \exists x / y = f(x)\}$$

  Note that $\mathrm{range}(f) \subset F$.

[2] $f : E \times E \to F$ is said to be **symmetric** if $f(x, y) = f(y, x)$ for all $x, y \in E \times E$.

[3] $f : E \to F$ is said to be **positive definite** if and only if $f(x, x) > 0$ for any $x \in E$ such that $x \neq 0_{\mathrm{E}}$.

[4] $f : E \times E \to G$ is said to be **bilinear** if $h_y : E \to F$ such that $h_y(x) = f(x, y)$ is linear for all $y \in E$ and $k_x : E \to F$ such that $k_x(y) = f(x, y)$ is linear for all $x \in E$.

[5] A set $(E, ||.||)$ is said to be **complete** whenever any Cauchy series converges within this set *i.e.*, $\forall \varepsilon > 0 \ \exists n$ such that $\forall p, q \geq n \ \ ||x_p - x_q|| < \varepsilon$.

- *The* **rank** *of f is the dimension of its range.*

$$\mathrm{rank}(f) \triangleq \dim(\mathrm{range}(f))$$

This leads to the following important proposition.

Proposition 3 *If E is a vector space of finite dimension then* $\dim(\ker(f))$ *and* $\mathrm{rank}(f)$ *are also finite and*

$$\dim(E) = \dim(\ker(f)) + \mathrm{rank}(f) = \dim(\ker(f)) + \dim(\mathrm{range}(f))$$

3.1 Matrix of a linear transform

Definition 12 *Given E and F two vector spaces with $\mathcal{B}$ and $\mathcal{B}'$ bases of E and F respectively, and $f : E \to F$ a linear transform, the matrix*

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

is defined **with respect to $\mathcal{B}$ and $\mathcal{B}'$** *from the mapping of the elements of $\mathcal{B}$ through f. In other words, if $\mathcal{B} = \{e_1, \dots, e_n\}$ and $\mathcal{B}' = \{e'_1, \dots, e'_m\}$,*

$$f(e_i) = \sum_{j=1}^{m} a_{ij} e'_j$$

This therefore creates an equivalent representation between functional notation and matrix notation

$$y = f(x) \Leftrightarrow Y = AX$$

It is important to emphasise again that the matrix A depends on the choice of the bases $\mathcal{B}$ and $\mathcal{B}'$.

3.2 Related results

The following results call for some definitions given below. This part may be skipped in a first pass.

- From what has been seen earlier, it is clear that the rank of a matrix A is the maximal number of linearly independent columns. It is therefore also the maximal size of a sub-matrix extracted from A whose determinant is non-zero.

- When **changing the basis** $\mathcal{B}$ for another basis $\mathcal{B}$" then the linear transformation stays the same but its matrix A is altered into A' by a **transition matrix** P as follows

$$A' = P^{-1}AP,$$

  where the columns of P are the coordinates of the new basis vectors (vectors of $\mathcal{B}$") in the former basis $\mathcal{B}$. The theory of eigenvectors will detail this application and lead to the characterisation of a "best basis".

4 Matrix calculus

4.1 Basic matrix operations

Given $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$ two $n \times n$ matrices and λ and μ scalars,

- The **trace** of A is defined as $\mathrm{Tr}(A) \triangleq \sum_i a_{ii}$

- $\lambda A + \mu B \triangleq (\lambda a_{ij} + \mu b_{ij})_{ij}$

- $AB \triangleq (\sum_k a_{ik}b_{kj})_{ij}$ (only the number of columns of A needs to be the same as the number of lines of B for the matrix multiplication to be possible),

- Other operations are defined from the elements:

$$A^{\mathsf{T}} = (a_{ji})_{ji} \text{ (transpose) } ; \bar{A} = (\bar{a}_{ij})_{ij} \text{ (conjugate) } ; A^{\mathsf{H}} = (\bar{a}_{ji})_{ji} = \bar{A}^{\mathsf{T}} \text{ (Hermitian)},$$

- Let A_{ij} be the sub-matrix created from A when removing the column and the line containing a_{ij} then, the determinant of A is defined recursively as

$$\det(A) = |A| \triangleq \sum_j (-1)^{i+j} a_{ij} \det(A_{ij})$$

A_{ij} is called a **minor** and $(-1)^{i+j}\det(A_{ij})$ is called a **cofactor** of A.

4.2 Specific matrices

Some particular matrices can be identified:

- **Null** matrix $O_n = (a_{ij})_{ij}$ with $a_{ij} = 0$ for all $i, j = 1 \dots n$,
- **Identity** $I_n = (\delta_{ij})_{ij=1\dots n}$ (where $\delta_{ij} = 1$ if $i = j$, $\delta_{ij} = 0$ otherwise),
- **Upper triangular** matrix $U = (u_{ij})_{ij}$ such that $u_{ij} = 0$ if $i > j$,
- **Lower triangular** matrix $L = (l_{ij})_{ij}$ such that $l_{ij} = 0$ if $i < j$,
- **Diagonal** matrix $D = (d_{ij}\delta_{ij})_{ij}$,
- **Symmetric** matrix $A = A^{\mathsf{T}}$,
- A **block matrix** is a matrix which can be divided into similar parts *i.e.*, :

$$A = \begin{pmatrix} A_{11} & \dots & A_{1b} \\ \vdots & A_{ij} & \vdots \\ A_{b'1} & \dots & A_{b'b} \end{pmatrix}.$$

- A **block diagonal matrix** is a block matrix where $A_{ij} = 0$ if $i \neq j$,
- **Positive definite** matrix: $xAx^{\mathsf{T}} > 0$ for all $x \neq 0_{\mathrm{E}}$,
- **Orthogonal** matrix $A^{\mathsf{T}}A = I$ (A is real),
- **Unitary** matrix $A^{\mathsf{H}}A = I$ (A is complex),
- **Nilpotent** matrix $\exists k_0$ such that $A^k = 0$ for all $k \geq k_0$
- If $\det(A) = 0$ then A, a square $n \times n$ matrix is said to be **singular**, in that case $\operatorname{rank}(A) < n$.
- A and B are **equivalent** then there exist P and Q such that $B = Q^{-1}AP$ (note that A may not be a square matrix),
- A and B are **similar** then there exists P such that $B = P^{-1}AP$ (note that this assumes that A is a square matrix),
- A and B are **congruent** then there exists P non-singular such that $B = P^{\mathsf{T}}AP$ ($B = P^{\mathsf{H}}AP$, if B is complex),

- $A = (a_{ij})_{ij}$ is a **Toepliz** matrix if there exist $2n-1$ scalar r_k, $k = -n+1, \ldots, n-1$ such that $a_{ij} = r_{j-i}$. In that case:

$$A = \begin{pmatrix} r_0 & r_1 & \ldots & r_{n-2} & r_{n-1} \\ r_{-1} & r_0 & \ldots & r_{n-3} & r_{n-2} \\ \vdots & \vdots & & \vdots & \vdots \\ r_{-n+1} & r_{-n+2} & \ldots & r_{-1} & r_0 \end{pmatrix}$$

  Each diagonal or sub-diagonal is formed by only one value.

- A **dyadic** matrix is such that $A = xy^{\mathsf{T}}$ (*i.e.*, it is formed from two vectors)
- If A is a positive definite matrix, B is said to be the **matrix square root** of A if $A = BB^{\mathsf{T}}$,
- P is a **projection matrix** if $P^{\mathsf{T}} = P$ and $P^2 = P$.

4.3 Some properties

- $AB \neq BA$ in general
- $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$
- $\det(AB) = \det(A)\det(B) = \det(BA)$
- $\det(A^{\mathsf{T}}) = \det(A)$
- $\det(A^{-1}) = (\det(A))^{-1}$. Note that A^{-1} exists if and only if A is non-singular.
- If A is a $n \times n$ matrix, $\det(\lambda A) = \lambda^n \det(A)$, for any $\lambda \in K$.
- $\det(A^{\mathsf{H}}) = \overline{\det(A)}$
- If A is a $n \times m$ matrix and B is a $m \times n$ matrix then $\det(I_n - AB) = \det(I_m - BA)$
- If M is a block matrix of the form

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

  then $\det(M) = \det(A)\det(D - CA^{-1}B)$. In particular, if $B = C = 0$ (M is block diagonal), $\det(M) = \det(A)\det(D)$.

- If A is a dyadic matrix then clearly $\mathrm{rank}(A) = 1$.
- **Matrix inversion lemma**: If A and C are respectively $n \times n$ and $m \times m$ non-singular matrices and B and D are respectively $n \times m$ and $m \times n$ matrices, then

$$(A + BCD)^{-1} = A^{-1} - A^{-1}B(DA^{-1}B + C^{-1})^{-1}DA^{-1},$$

  if A^{-1}, C^{-1} and $(DA^{-1}B + C^{-1})^{-1}$ exist.

- If B matrix square root of A, then $\mathrm{range}(B) = \mathrm{range}(A)$.

Exercises:

- Detail all the above properties.
- Calculate explicitly $\det(A^{-1})$ when

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

- Prove that the determinants of the following matrices are zero
  - A matrix with a null-column
  - A matrix with a null-row
  - A matrix with two columns (resp lines) equal.
- Prove that $\det(A) = -\det(B)$ when B is the same as A where 2 columns have been swapped.

5 Eigenspaces

Definition 13 *Eigenvalue, eigenvector.*
Let $f : E \to F$ be a linear transform. λ is an **eigenvalue** *of f if there exists $u \neq 0_{\mathrm{E}}$ such that $f(u) = \lambda u$. In that case u is an* **eigenvector** *of f. The subspace generated by $\{u$ such that $f(u) = \lambda u\}$ is called the* **eigensubspace** *associated with the eigenvalue λ.*

Similarly, eigenconcepts apply to matrix notation:
Given $A \in \mathcal{M}_{n\times n}(\mathrm{I\!R})$, λ is an eigenvalue of A associated with the eigenvector u if and only if $Au = \lambda u$.
From this equivalence, some definitions can be given

Definition 14 *Matrix inertia.*
The **inertia** *of a symmetric matrix is the set of scalars (m, z, p), where m, z and p are the number of negative, zero and positive eigenvalues (counting multiplicities), respectively.*

Definition 15 *Characteristic polynomial.*
Given A a $n \times n$ matrix its **characteristic polynomial** *is given by*

$$P_A(\lambda) \triangleq \det(A - \lambda I)$$

Its is a polynomial in λ of order n and is of the form

$$P_A(\lambda) = (-1)^n\lambda^n + (-1)^{n-1}\mathrm{Tr}(A)\lambda^{n-1} + \ldots + \det(A)$$

The **characteristic equation** of a matrix A is given by

$$P_A(\lambda) = 0$$

and the set $\{\lambda_i\}$ of all eigenvalues of A is defined by the set of solution of the characteristic polynomial. In other words, the eigenvalues of A are the roots of the characteristic polynomial.
The characteristic polynomial applies also to matrices and the following theorem is given.

Theorem 2 *Cayley Hamilton.*
Any matrix satisfies its own characteristic equation,

$$P_A(A) = 0.$$

Proposition 4 *Two congruent matrices have the same inertia. In particular, if $A = P^{\mathsf{T}}BP$ with P non-singular, A is positive definite if and only if B is positive definite.*

Exercises:

- Find the eigenvalues of
$$A = \begin{pmatrix} 4 & -5 \\ 2 & -3 \end{pmatrix}$$
- Find the eigenvalues of a dyadic matrix
- Given $a, b \neq 0$, calculate the eigenvalues of
$$A = \begin{pmatrix} a & b & \ldots & b \\ b & a & \ldots & b \\ & & \ddots & \\ b & \ldots & b & a \end{pmatrix}$$
(Hint: $A = (a-b)I + b(1\ldots1)^{\mathsf{T}}.(1\ldots1)$)
- If P is a projection find the associated eigenvalues.

Remark 2 Important
The equation $Ax = \lambda x$ can be generalised as $AX = X\Lambda$, where the column of X are the eigenvectors of A. This therefore shows that $\Lambda = X^{-1}AX$ so that A is similar to the diagonal matrix Λ formed by its eigenvalues. The transition matrix is such that its columns are the eigenvectors of A.

This generalises to the base change case. When **changing the basis** $\mathcal{B}$ for another basis $\mathcal{B}'$ then the matrix is mapped onto a similar matrix A' by a **transition matrix** P as follows

$$A' = P^{-1}AP,$$

where the columns of P are the coordinates of the new basis vectors (vectors of $\mathcal{B}'$) in the former basis $\mathcal{B}$. Moreover, if A is symmetric then, P is orthogonal (or unitary).

6 Diagonalisation

We recall that B is similar to A if and only if there exists a non-singular matrix P such that $B = P^{-1}AP$.

Theorem 3 *If A and B are similar then $P_A(\lambda) = P_B(\lambda)$. (Proof: Exercise).*

It follows that if A and B are similar, then they have the same eigenvalues. The converse is not true in general (find a counter-example).

Definition 16 *A matrix A is said to be* **diagonalisable** *if it is similar to a diagonal matrix.*

An important theorem follows.

Theorem 4 *If A is a $n \times n$ diagonalisable matrix, then A has n linearly independent eigenvectors.*

Proposition 5

- *Any matrix A symmetric is diagonalisable and its eigenvalues are real.*
- *Any matrix A symmetric positive definite is diagonalisable and its eigenvalues are real and positive.*

Remark 3 *A sufficient condition for A to be diagonalisable is that A has n distinct eigenvalues. This is not a necessary condition.*

Exercise: Calculate A^k when

$$A = \begin{pmatrix} 1-a & a \\ b & 1-b \end{pmatrix}$$

The above therefore show the importance of calculating eigenvalues and eigenvectors. The interpretation of such calculations lies in the base change operation. Changing the basis does not change the linear transform. The new basis formed by eigenvectors is the best basis one can choose for expressing the corresponding linear transform in a simple expression. Since the matrix corresponding to the linear transform is diagonal and since each eigenvector corresponds to a dimension (*i.e.*, variable) within the linear system, all dimensions are therefore "decoupled" by this operation. This in turn allows for the study of each dimension separately. Moreover, once the matrix is diagonal, it is straightforward to define the inverse transformation (*i.e.*, to solve $Ax = b$ where b is known for some *e.g.*, output measurements and A is known from some (linear) black-box characteristics).

It is unfortunately often the case that it is not possible to calculate eigenvalues and eigenvectors explicitly. Techniques for approximating the eigenvalues (and eigenvectors) of a linear transformation exist. They are not detailed here but can be found in most Linear Algebra books (see the **non-exhaustive reference list** within this document). However, for many problems, emphasis is placed on finding x such that $Ax = b$. Finding A^{-1} is useful only when there is the need for solving several systems of the form $Ax_i = b_i$. The next section addresses the problem of solving efficiently $Ax = b$ for several instances of b.

7 Square matrix decomposition

The main aim here is to solve linear systems like $Ax = b$, where A is a square $n \times n$ matrix and x (the unknown) and b (the observations) are column vectors.

7.1 Gaussian elimination

This technique is based on the following theorem.

Theorem 5 *If A is a $n \times n$ matrix, there exists a non-singular matrix M such that MA is triangular.*

It is clear that, if A is mapped onto a triangular matrix, then solving $Ax = b$ becomes trivial. The following algorithm therefore defines incrementally the matrix M such that the resulting matrix $U = AM$ is upper triangular. At each step i, a new matrix A^i is defined ($A^0 = A$). The aim is that the i^{th} column of A^i, $(a^i_{ki})^\mathsf{T}$ ($k = 1 \dots n$) is of the form $\{a^i_{1i}, \dots, a^i_{ii}, 0, \dots, 0\}^\mathsf{T}$. This can be obtained by combining lines i to n of A^{i-1} together.

More specifically, assuming that before step i columns $j = 1$ to $j = i-1$ are of the form $\{a^j_{1j}, \dots, a^j_{jj}, 0, \dots, 0\}^\mathsf{T}$, then

- Set $p = \frac{1}{a^{i-1}_{ii}}$
- Set $l^i_k = l^{i-1}_k - p a^{i-1}_{ki} l^{i-1}_i$ for all $k = i+1 \dots n$
- Set $b^i_k = b^{i-1}_k - p a^{i-1}_{ki} b^{i-1}_i$ (keep b consistent).

This is iterated for all $i = 1, \dots, n-1$. The result is a the equivalent system $A^{n-1}x = b^{n-1}$, where $A^{n-1} = U$ is an upper triangular matrix.

One problem lies in the step where p (the **pivot**) is calculated. If $a^{i-1}_{ii} = 0$, p is not defined. One may therefore swap the lines so that $a^{i-1}_{ji} \neq 0$. In that case, the same operation is to be applied on b^{i-1} for the system to be equivalent.

This algorithm allows to solve **one** particular system $Ax = b$. If different systems $Ax_i = b_i$ then the following LU decomposition is to be applied.

Theorem 6 *If A is non-singular there exist L and U, respectively lower and upper triangular matrices such that $A = LU$ and $L_{ii} = 1$ for all $i = 1, \dots, n$.*

Since $U = L^{-1}A$, the matrix L actually stores the transformations made on A for obtaining U. The **Gaussian elimination** procedure allows for computing and storing L online so that different systems can be solved from this decomposition. $Ax_i = b_i$ implies $LUx_i = b_i$. By first solving $Ly = b_i$ and then $Ux_i = y$ only triangular matrices are considered. For the complete algorithm see *e.g.*, [4, 5]

Remark 4 *Having $A = LU$ allows for obtaining $A = L'\Lambda U'$, where $L' = L$, Λ diagonal matrix such that $\Lambda_{ii} = U_{ii}$ and $U' = \Lambda^{-1}U$. This is typically called the* **LDU** *decomposition of A.*

Remark 5

- *Let M be the block matrix*
$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$
then its block LU (resp LDU) decomposition is
$$M = \begin{pmatrix} I & 0 \\ CA^{-1} & I \end{pmatrix} \begin{pmatrix} A & B \\ 0 & D - CA^{-1}B \end{pmatrix} = \begin{pmatrix} I & 0 \\ CA^{-1} & I \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & D - CA^{-1}B \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ 0 & I \end{pmatrix}.$$
- *For 2×2 block triangular matrices,*
$$\begin{pmatrix} I & 0 \\ A & I \end{pmatrix}^{-1} = \begin{pmatrix} I & 0 \\ -A & I \end{pmatrix} \text{ and } \begin{pmatrix} I & A \\ 0 & I \end{pmatrix}^{-1} = \begin{pmatrix} I & -A \\ 0 & I \end{pmatrix}$$

Exercise: Express
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1}$$
as a function of A, B, C D and their inverses.

7.2 Cholesky decomposition

We recall that a positive definite matrix A is such that $x^{\mathsf{T}}Ax > 0$ for all $x \neq 0_{\mathrm{E}}$. It is therefore clear that all eigenvalues of a positive definite matrix are positive[6]. Cholesky decomposition is based on the following extension of this property.

Theorem 7 *If A is an $n \times n$ symmetric positive definite matrix, then there exists G a lower triangular matrix with positive diagonal elements such that $A = G^{\mathsf{T}}G$ and this decomposition is unique.*

Explicit formulae for calculating g_{ij} for all i, j can be found in [4, 5]. The algorithm is therefore readily defined when giving these expressions. Note that the above Gaussian elimination may also perform the Cholesky decomposition.

Proposition 6 *We first note that if $A = G^{\mathsf{T}}G$, then G is a particular matrix square root of A. Clearly, any matrix $B = QG$, where Q is an orthogonal matrix is a matrix square root of A.*

Proof: Exercise.

Remark 6 *If M is a symmetric positive definite block matrix*

$$M = \begin{pmatrix} A & B \\ B^{\mathsf{T}} & D \end{pmatrix},$$

(A and D are symmetric) then,

$$M = L\Lambda L^{\mathsf{T}} = \begin{pmatrix} I & 0 \\ B^{\mathsf{T}}A^{-1} & I \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & D - B^{\mathsf{T}}A^{-1}B \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ 0 & I \end{pmatrix}.$$

Therefore M is congruent to Λ so that it is positive definite if and only if A is positive definite and $D - B^{\mathsf{T}}A^{-1}B$ is positive definite. Moreover,

$$M^{-1} = \begin{pmatrix} I & -A^{-1}B \\ 0 & I \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & (D - B^{\mathsf{T}}A^{-1}B)^{-1} \end{pmatrix} \begin{pmatrix} I & 0 \\ -B^{\mathsf{T}}A^{-1} & I \end{pmatrix}$$

7.3 Jordan matrices

In the case where the rank of matrix A is lower than n (*i.e.*, only $m < n$ eigenvectors are linearly independent), A can still be written in a particular block diagonal form.

Theorem 8 *If* $\mathrm{rank}(A) = m$, *then A is similar to a block diagonal matrix J (called* **Jordan form** *of A) such that*

$$J = \begin{pmatrix} J_1 & 0 & \\ 0 & \ddots & 0 \\ & 0 & J_m \end{pmatrix}$$

where J_i is a $n_i \times n_i$ block of the form

$$J_i = \begin{pmatrix} \lambda_i & 1 & & 0 & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & 0 & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix}$$

and n_i is dimension of the eigensubspace associated with the eigenvalue λ_i (i.e., it is the multiplicity of the eigenvalue λ_i).

Remark 7 *Note that if the characteristic polynomial of A has n distinct roots, the Jordan form turns into a diagonal matrix.*

[6] Hint: x eigenvector of A then $Ax = \lambda x$. Therefore $x^{\mathsf{T}}Ax = \lambda x^{\mathsf{T}}x = \lambda||x||^2 > 0$ if $x \neq 0_{\mathrm{E}}$.

7.4 Gram-Schmidt orthogonalisation

The aim of the technique presented here is to map a set of n linearly independent vectors into an orthonormal basis. We first characterise linearly independent vectors.

Definition 17 *Gram determinant.*

n vectors $\{x_1, \ldots, x_n\}$ are linearly independent if and only if their corresponding Gram determinant $\det(G)$ *is non-zero, where*

$$G \triangleq \begin{pmatrix} < x_1, x_1 > & \ldots & < x_1, x_n > \\ \vdots & \ddots & \vdots \\ < x_n, x_1 > & \ldots & < x_n, x_n > \end{pmatrix}$$

G is called the **Gram matrix** *associated with $\{x_1, \ldots, x_n\}$. Clearly, G is symmetric positive definite.*

Now, n linearly independent vectors span a space whose dimension is n. This space can be represented by the set of n vectors $\{e_1, \ldots, e_n\}$ such that $< e_i, e_j >= \delta_{ij}$. In that case, any vector y is represented by its coordinates $\{y_i =< e_i, y >\}$ defined such that

$$y = \sum_i < e_i, y > e_i$$

The aim here is therefore to map the n vectors $\{x_1, \ldots, x_n\}$ onto the vectors $\{e_1, \ldots, e_n\}$. This is called the **Gram-Schmidt orthogonalisation**.

The idea is to incrementally construct the set $\{e_1, \ldots, e_n\}$ as follows.

- Normalise x_1 to define e_1.
- Given $\{e_1, \ldots, e_{i-1}\}$, e_i is defined by subtracting from x_i its projection on the space spanned by $\{e_1, \ldots, e_{i-1}\}$ and normalising the result

$$p_i = \sum_{k=1}^{i-1} < x_i, e_k > e_k \text{ and } e_i = \frac{x_i - p_i}{\|x_i - p_i\|}$$

More specifically, the following algorithm creates the set $\{e_1, \ldots, e_n\}$ from a generic set of vectors $\{x_1, \ldots, x_n\}$.

1. $C \leftarrow \{x_1, \ldots, x_n\}$
2. $m \leftarrow 1$, $t \leftarrow 0$, $y \leftarrow x_1$, $C \leftarrow C - \{x_1\}$
3. $t \leftarrow n + 1$, $e_t \leftarrow y/\|y\|$
4. If C is empty, then end.
5. Else $m \leftarrow m + 1$, $y \leftarrow x_m - \sum_{k=1}^{t} < x_m, e_k > e_k$, $C \leftarrow C - \{x_m\}$
6. If $y = 0$ repeat 4. (This may happen if one of the initial vectors is null).
7. Else go to 3.

As a result, m gives the dimension of the space spanned by $\{x_1, \ldots, x_n\}$ (and therefore the number of orthonormal vectors e_i found).

7.5 QR decomposition

The aim here is to formalise the Gram-Schmidt orthogonalisation for mapping a matrix onto an orthogonal matrix. This is based on the following theorem.

Theorem 9 *Any $n \times m$ matrix A whose columns are linearly independent can be written as $A = QR$ where the columns of Q are orthonormal and R is an upper triangular invertible matrix. Moreover, if $m = n$, then Q is an orthogonal matrix.*

The idea here is to use this scheme for solving a system $Ax = b$. In the case where matrices are square, Q is orthogonal so that $Q^{\mathsf{T}} = Q^{-1}$. Therefore

$$Ax = b \Leftrightarrow QRx = b \Leftrightarrow Rx = Q^{\mathsf{T}}b$$

The latter system is straightforward to solve since R is an upper triangular matrix.

Similarly to the LU decomposition, the Gram-Schmidt orthogonalisation technique is used for calculating Q and R. Q is formed by the new orthonormal vectors and R stores the successive transformations made on the columns of A to obtain the columns of Q. The incremental nature of this technique results in the fact the R is triangular.

7.6 Singular value decomposition (SVD)

The following method allows to determine useful characteristics of non-square matrices. It follows from the following theorem.

Theorem 10 *If A is a real $m \times n$ matrix, there exist two square orthogonal matrices U $(m \times m)$ and V $(n \times n)$ such that*

$$U^{\mathsf{T}}AV = \Sigma \triangleq \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_p \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix},$$

where $p = \min(m, n)$ and $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_p \geq 0$ are called the **singular values** *of A and the columns u_i of U and v_i of V are the left and right* **singular vectors** *of A.*

If we define r such that

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \dots = \sigma_p = 0$$

then

- $\text{rank}(A) = r$,
- $\ker(A)$ is the subspace generated by $\{v_{r+1}, \dots, v_n\}$,
- $\text{range}(A)$ is the subspace generated by $\{u_1, \dots, u_r\}$,
- and the SVD expansion of A is defined as

$$A \triangleq \sum_{i=1}^{r} \sigma_i u_i v_i^{\mathsf{T}}.$$

The computation of the SVD is based on the following developments.

If $U^{\mathsf{T}}AV = \Sigma$ then,

$$(U^{\mathsf{T}}AV)^{\mathsf{T}}U^{\mathsf{T}}AV = \Sigma^{\mathsf{T}}\Sigma = \begin{pmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_p^2 \end{pmatrix} = (V^{\mathsf{T}}A^{\mathsf{T}}U)(U^{\mathsf{T}}AV)$$

Therefore, since U and V are orthogonal,

$$V^{\mathsf{T}}(A^{\mathsf{T}}A)V = \Sigma^{\mathsf{T}}\Sigma = \begin{pmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_p^2 \end{pmatrix} \text{ and } U^{\mathsf{T}}(AA^{\mathsf{T}})U = \Sigma\Sigma^{\mathsf{T}} = \begin{pmatrix} \sigma_1^2 & & & & 0 \\ & \ddots & & & \\ & & \sigma_p^2 & & \\ & & & 0 & \\ & 0 & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

Finally,

$$A^\top A = V\Sigma^\top\Sigma V^\top = V\begin{pmatrix} \sigma_1^2 & & 0 \\ & \ddots & \\ 0 & & \sigma_p^2 \end{pmatrix} V^\top \text{ and, } AA^\top = U\Sigma\Sigma^\top U^\top$$

The computation of the singular value decomposition is therefore simply done by calculating the eigenvalues and eigenvectors of $A^\top A$ ($n \times n$). This gives V as eigenvector matrix and $\{\sigma_1^2, \ldots, \sigma_p^2\}$ as eigenvalues. U is similarly computed from the eigensystem corresponding to $A^\top A$ ($m \times m$).

Remark 8 *It is often the case that $n \ll m$. In that case finding the eigenvalues of $A^\top A$ is far easier than finding the eigensystem of $A^\top A$. Since often only the singular values are of interest, the calculation only concentrates on $A^\top A$.*

7.7 Pseudo-inverse

Given the equation system $Ax = b$, one would ideally like to calculate $x = A^{-1}b$. In the case where A^{-1} does not exist, we define a matrix $A^\#$ (also noted A^+) called the **pseudo-inverse** of A, such that,

$$x = A^\# b = A^+ b.$$

It should be an inverse in a weaker sense and we define it such that:

- $AA^\# A = A$ (as opposed to $AA^{-1} = I$)
- $A^\# AA^\# = A^\#$ (as opposed to $A^{-1}A = I$)

One can easily verify that if we define

$$A^\# = (A^\top A)^{-1} A^\top$$

The properties are satisfied. It can be shown that the above definition derives from the solution of the system "projected" into the range of A (range(A)). In other words, the solution $x^* = A^+ b$ characterised is such that $b^* = Ax^*$ is the projection of b on range(A) (minimum square error (MSE) solution). The projection matrix such that $b^* = Pb$ is then

$$P = A(A^\top A)^{-1} A^\top.$$

Proof: Exercise. (Hint: This can be shown by defining $\varepsilon = b - Ax$ and characterising x^* as the $\operatorname{Arg\,min} \|\varepsilon\|$[7]).

8 Quadratic forms

This section introduce bilinear and quadratic functions and their relationship with matrices.

Definition 18 *Let Φ be a bilinear symmetric form on $E = K^n$. Φ is an application from $E \times E$ to K such that for all x, y,*

$$\Phi(x, y) = \sum_{i,j} a_{ij} x_i y_j \text{ and } a_{ij} = a_{ji}$$

We define Ψ as

$$\Psi(x) \triangleq \Phi(x, x) = \sum_i a_{ii} x_i^2 + 2\sum_{i<j} a_{ij} x_i x_j$$

Ψ is called the **quadratic form** *associated with Φ.*

Clearly, $\Phi(x, y) = x^\top Ay$ so that $A = (a_{ij})_{ij}$ is the matrix associated with Φ in the canonic basis. Similarly, $\Psi(x) = x^\top Ax$ and A is the matrix associated with the quadratic form Ψ.

By what has been studied above, let $A = P^{-1}\Lambda P$, with Λ diagonal (matrix of eigenvalues). A is symmetric (since Φ is symmetric), then P is orthonormal and $A = P^\top AP$. Therefore, $\Psi(x) = x^\top P^\top APx$. Let $x' = Px$, then

$$\Psi(x') = x'^\top Ax' = \sum_i \lambda_i x_i^2$$

[7]This calls for **matrix derivation** formulae which can be found in [3]

A straightforward application of this is the study of quadratic functions such as parabola or ellipses. This typically allows to map an equation of the form:

$$F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$$

onto an equation of the form

$$G(x, y) = a'x^2 + b'y^2$$

Hence, this shows the diagonalisation of a quadratic equation is simply a rotation to match the principal axis of the quadratic function studied.

References

[1] F. R. Gantmacher and C. Sarthou. *Théorie des matrices - Tome 1 : théorie générale. Tome 2 : questions spéciales et applications.* Editions Jacques Gabay, 1990.

[2] G. H. Golub and C. F. van Loan. *Matrix computations.* John Hopkins, 1996.

[3] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, 1991.

[4] P. Lascaux and R. Théodor. *Analyse numérique matricielle appliquée à l'art de l'ingénieur. 2 : Méthodes itératives.* Masson, second edition, 1994.

[5] P. Lascaux and R. Théodor. *Analyse numérique matricielle appliquée à l'art de l'ingénieur. 1 : Méthodes directes.* Masson, second edition, 1998.

[6] W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery. *Numerical Recipes in C.* Cambridge University Press, second edition, 1992.

[7] G. Strang. *Linear algebra and its applications.* Harcourt Brace Jovanovich College Publishers, third edition, 1988.