Linear Algebra Refresher Course
August 17 – 27, 2009

Linear Algebra Primer from a Numerical Point of View

Notations:

- $\forall$ means "for all"
- $\exists$ means "there exist(s)"
- $\Longleftrightarrow$ means equivalent
- "iff" is short for "if and only if"
- $i = 1 : n$ stands for $i = 1, 2, \ldots, n$.

1. Vectors and Matrices

Definition 1.1. $v \in \mathbb{R}^n$ is a column vector with entries $v_i \in \mathbb{R}$, $i = 1 : n$, if and only if

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}. \tag{1}$$

The notation $v = (v_i)_{i=1:n}$ will also be used, with the understanding that it denotes a column vector.

Note: Unless otherwise specified, any vector will be considered to be a column vector. A row vector is of the form

$$v = (v_1 \; v_2 \; \ldots \; v_n),$$

with entries $v_i \in \mathbb{R}$, $i = 1 : n$.

Definition 1.2. An $m \times n$ matrix A with m rows and n columns is a linear operator from $\mathbb{R}^n$ to $\mathbb{R}^m$, i.e.,

$$A : \mathbb{R}^n \to \mathbb{R}^m.$$

We will not use the entry by entry notation of matrix A as $A = (A(j,k))_{j=1:m,k=1:n}$. Rather, we will use the column form for A, i.e.,

$$A = (a_1 \mid a_2 \mid \ldots \mid a_n), \tag{2}$$

where a_i is the i-th column vector of A, $i = 1 : n$.

In some instances, we will also use the row form for the matrix A, i.e.,

$$A = \begin{pmatrix} r_1 \\ - - - - \\ r_2 \\ - - - - \\ \vdots \\ - - - - \\ r_m \end{pmatrix} \tag{3}$$

be the row form of matrix A.

Matrix–vector multiplication:
If A is an $m \times n$ matrix given by the column form (2) and v is a column vector of size n given by (1), then

$$Av \;=\; \sum_{i=1}^{n} v_i a_i. \tag{4}$$

In other words, the result of the multiplication of the column vector v by the matrix A is a linear combination of the columns of A with coefficients the entries of vector v.

If A is an $m \times n$ matrix given by the row form (3) and $w = (w_1\ w_2\ \dots\ w_m)$ is a row vector of size m, then

$$wA \;=\; \sum_{j=1}^{m} w_j r_j. \tag{5}$$

In other words, the result of the multiplication of the matrix A at the left by the row vector w is a linear combination of the rows of A with coefficients the entries of vector w.

Matrix–matrix multiplication:
If A is an $m \times n$ matrix and B is an $n \times p$ matrix given by

$$A \;=\; (a_1 \mid a_2 \mid \dots \mid a_n) \quad \text{and} \quad B \;=\; (b_1 \mid b_2 \mid \dots \mid b_p)\,,$$

then AB is an $m \times p$ matrix given by

$$AB \;=\; (Ab_1 \mid Ab_2 \mid \dots \mid Ab_p)\,. \tag{6}$$

The result of multiplying the matrices A and B is a matrix whose columns are the corresponding columns of B multiplied by the matrix A.

Definition 1.3. A linear combination of the vectors $w_1, w_2, \dots, w_n$ is a sum of these vectors multiplied by real coefficients denoted, e.g., by $\alpha_i \in \mathbb{R}$, $i = 1 : n$, i.e.,

$$\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n. \tag{7}$$

Lemma 1.4. *Any matrix-vector product Av is a linear combination of the columns of A.*

Proof. The result follows immediately from (4) and (7). □

Definition 1.5. The transpose matrix of A is denoted by A^t and has entries

$$A^t(j,k) \;=\; A(k,j),\ \forall\ 1 \leq\ j,\ k\ \leq n. \tag{8}$$

If the matrix A is written in column form as $A = (a_1 \mid a_2 \mid \dots \mid a_n)$, where a_i^t, $i = 1 : n$, are row vectors, then its transpose A^t can be written (in row form) as

$$A^t \;=\; \begin{pmatrix} a_1^t \\ ---- \\ a_2^t \\ ---- \\ \vdots \\ ---- \\ a_n^t \end{pmatrix}.$$

The following properties follow immediately from (8):

$$(A^t)^t \;=\; A; \tag{9}$$

$$(A+B)^t \;=\; A^t + B^t. \tag{10}$$

Lemma 1.6.

$$(Av)^t \;=\; v^t A^t$$

Proof. Let $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$ and $v = (v_i)_{i=1:n}$. Then $Av = \sum_{i=1}^n v_i a_i$ and

$$(Av)^t \;=\; \left(\sum_{i=1}^n v_i a_i\right)^t \;=\; \sum_{i=1}^n (v_i a_i)^t \;=\; \sum_{i=1}^n v_i a_i^t. \tag{11}$$

From (5) it follows that

$$v^t A^t \;=\; (v_1\ v_2\ \ldots\ v_n) \begin{pmatrix} a_1^t \\ - - - - \\ a_2^t \\ - - - - \\ \vdots \\ - - - - \\ a_n^t \end{pmatrix} \;=\; \sum_{i=1}^n v_i a_i^t. \tag{12}$$

The desired result, i.e., $(Av)^t = v^t A^t$, follows from (11) and (12). □

Lemma 1.7. *The transpose of the product of two matrices is NOT the product of the transposes of the two matrices, i.e.,*

$$(AB)^t \;\neq\; A^t B^t.$$

Instead, the following rule holds:

$$(AB)^t \;=\; B^t A^t.$$

Note: As mentioned above, we think of a matrix as a collection of column vectors. Almost all the linear algebra proofs involving the individual entries of a matrix can be given using column vectors arguments in a more elegant and compact fashion.

Proof. Let $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$ be an $m \times n$ matrix and let $B = (b_1 \mid b_2 \mid \ldots \mid b_p)$ be an $n \times p$ matrix. Then, $AB = (Ab_1 \mid Ab_2 \mid \ldots \mid Ab_p)$. Using Lemma 1.6 repeatedly, we find that

$$(AB)^t \;=\; \begin{pmatrix} (Ab_1)^t \\ - - - - \\ (Ab_2)^t \\ - - - - \\ \vdots \\ - - - - \\ (Ab_n)^t \end{pmatrix} \;=\; \begin{pmatrix} b_1^t\ A^t \\ - - - - \\ b_2^t\ A^t \\ - - - - \\ \vdots \\ - - - - \\ b_n^t\ A^t \end{pmatrix} \;=\; \begin{pmatrix} b_1^t \\ - - - - \\ b_2^t \\ - - - - \\ \vdots \\ - - - - \\ b_n^t \end{pmatrix} A^t \;=\; B^t\ A^t.$$

□

Definition 1.8. A matrix is a square matrix if it has the same number of rows and columns.

The identity matrix, denoted by I, is a square matrix with entries equal to 1 on the main diagonal and equal to 0 everywhere else, i.e.,

$$I \;=\; \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Note: If the identity matrix is of size $n \times n$, it is also denoted by I_n. We will not use this notation here, but use instead the notation I for identity matrices of any size.

The k-th column of the identity matrix is denoted by e_k, i.e.,

$$e_k \;=\; \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{13}$$

where the entry equal to 1 is on position "k".

Therefore, the identity matrix I is written in column form as

$$I \;=\; (e_1 \mid e_2 \mid \ldots \mid e_n)\,.$$

Lemma 1.9. *Let $A = col(a_k)_{k=1:n}$ be an $m \times n$ matrix. If e_k is the k-th column of the $n \times n$ identity matrix, then*

$$Ae_k \;=\; a_k,\ \forall\ k = 1:n. \tag{14}$$

Let $A = row(r_j)_{j=1:m}$ be an $m \times n$ matrix. If e_j is the j-th column of the $m \times m$ identity matrix, then

$$e_j^t A \;=\; r_j,\ \forall\ j = 1:m. \tag{15}$$

Proof. If $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$, it is easy to see that

$$Ae_k \;=\; \sum_{i=1}^{n} e_k(i)a_i \;=\; 0\cdot a_1 \;+\; \ldots \;+\; 0\cdot a_{k-1} \;+\; 1\cdot a_k \;+\; 0\cdot a_{k+1} \;+\; \ldots \;+\; 0\cdot a_n \;=\; a_k.$$

Assume A is written in the row form (3), with row vectors r_j, $j = 1:m$. Then

$$A^t \;=\; \left(r_1^t \mid r_2^t \mid \ldots \mid r_n^t\right). \tag{16}$$

Using Lemma 1.6, (14) and (16), we find that

$$e_j^t A \;=\; (A^t e_j)^t \;=\; (r_j^t)^t \;=\; r_j,$$

which is the same as (15).

□

Lemma 1.10. *Matrix multiplication by the identity matrix I does not change the matrix, i.e., for any matrix A,*

$$IA \;=\; AI \;=\; A.$$

Proof. Let $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$. From (14) we find that $Ae_k = a_k$ for all $k = 1:n$. Then

$$AI \;=\; (Ae_1 \mid Ae_2 \mid \ldots \mid Ae_n) \;=\; (a_1 \mid a_2 \mid \ldots \mid a_n) \;=\; A.$$

Note that, for any $1 \le k \le n$,

$$Ia_k \;=\; \sum_{i=1}^{n} a_k(i)e_i \;=\; \begin{pmatrix} a_k(1) \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_k(2) \\ \vdots \\ 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_k(n) \end{pmatrix} = \begin{pmatrix} a_k(1) \\ a_k(2) \\ \vdots \\ a_k(n) \end{pmatrix} \;=\; a_k.$$

Therefore,

$$IA \;=\; (Ia_1 \mid Ia_2 \mid \ldots \mid Ia_n) \;=\; (a_1 \mid a_2 \mid \ldots \mid a_n) \;=\; A.$$

□

1.1. **Nonsingular Matrices.** Nonsingular matrices are those square matrices A for which any linear system of the form $Ax = b$ has a unique solution x. Identifying whether a matrix is nonsingular and solving the associated linear system is a fundamental problem in numerical linear algebra. In this section, we introduce the concept of nonsingular matrices and other related topics.

Definition 1.11. The range of an $m \times n$ matrix A is denoted by Range(A) and contains all the vectors obtained from matrix–vector multiplications involving A, i.e.,

$$\text{Range}(A) \;=\; \{Av, \quad \text{where} \quad v \in \mathbb{R}^n\}.$$

Definition 1.12. The space W is called the space generated by the vectors $w_1, w_2, \ldots, w_n$, and is denoted by $W \;= < w_1, w_2, \ldots, w_n >$, if any vector $w \in W$ can be written as a linear combination of the vectors $(w_i)_{i=1:n}$, i.e.,

$$W \;= < w_1, w_2, \ldots, w_n > = \left\{ \sum_{i=1}^{n} \alpha_i w_i, \quad \text{where} \quad \alpha_i \in \mathbb{R},\ i = 1:n \right\}.$$

Lemma 1.13. *The range of a matrix A is equal to the space generated by the column vectors of A, i.e.,*

$$\textit{Range}(A) \;= < a_1, a_2, \ldots, a_n >,$$

where $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$.

Proof. Let $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$ and let $v = (v_i)_{i=1:n} \in \mathbb{R}^n$ be an arbitrary vector. Recall from (4) that

$$Av \;=\; \sum_{i=1}^{n} v_i a_i \;\in < a_1, a_2, \ldots, a_n > .$$

Therefore, from Definition 1.11, we conclude that

$$\text{Range}(A) \;\subset < a_1, a_2, \ldots, a_n > . \tag{17}$$

By definition, for any $w \in< a_1, a_2, \ldots, a_n >$, there exist constants $\alpha_i \in \mathbb{R}$, $i = 1 : n$, such that $w = \sum_{i=1}^{n} \alpha_i a_i$. Then

$$w \;=\; \sum_{i=1}^{n} \alpha_i a_i \;=\; (a_1 \mid \ldots \mid a_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \;=\; Av,$$

where $v \;=\; \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$. Thus,

$$< a_1, a_2, \ldots, a_n > \subset \text{ Range}(A). \tag{18}$$

From (17) and (18), we conclude that Range(A) $= < a_1, a_2, \ldots, a_n >$. □

Definition 1.14. The nullspace of an $m \times n$ matrix A is defined as the set of vectors in $\mathbb{R}^n$ that give 0 if multiplied by the matrix A, i.e.,

$$\text{Null}(A) \;=\; \text{Ker}(A) \;=\; \{v \in \mathbb{R}^n \quad \text{such that} \quad Av = 0\}.$$

The nullspace of a matrix A is also called the kernel of the matrix A and is denoted by Ker(A).

Definition 1.15. The vectors $w_1, w_2, \ldots, w_p$ are called linearly independent if and only if there are no coefficients $\alpha_i \in \mathbb{R}$, $i = 1 : p$, such that

$$\sum_{i=1}^{p} \alpha_i w_i \;=\; 0,$$

except for the case where all the coefficients are zero, i.e., $\alpha_i = 0$, for all $i = 1 : p$.

Definition 1.16. The column (row) rank of a matrix A is equal to the maximal number of columns (rows) of A which are linearly independent.

Lemma 1.17. *If A is a square matrix, then the column rank of A is equal to the row rank of A.*

Definition 1.18. The square matrix A is nonsingular (invertible) if and only if there exists another matrix, denoted by A^{-1}, such that

$$A\,A^{-1} \;=\; A^{-1}\,A \;=\; I. \tag{19}$$

The matrix A^{-1} is called the inverse matrix of A.

Definition 1.19. By definition, the matrix A is called singular if and only if A is not nonsingular.

Lemma 1.20. *The inverse of the inverse of a nonsingular matrix is equal to the matrix itself, i.e.,*

$$(A^{-1})^{-1} \;=\; A. \tag{20}$$

Proof. From definition 1.18 and (19), the matrix A satisfies the definition of the inverse of the matrix A^{-1}, which is what is expressed mathematically in formula (20). □

Theorem 1.21. *Each of the following conditions can be regarded as an equivalent definitions for a nonsingular $n \times n$ matrix A:*

(21)

$$A \text{ nonsingular} \iff rank(A) = n \iff Range(A) = \mathbb{R}^n \iff Null(A) = \{0\} \iff det(A) \neq 0.$$

Similarly, the following conditions are equivalent definitions for a singular matrix A of size n:

$$A \text{ singular} \iff Null(A) \neq \{0\} \iff \exists\, v \in \mathbb{R}^n,\ v \neq 0,\ \text{such that } Av = 0 \iff det(A) = 0. \tag{22}$$

Proof. The proofs of all these results are of little interest for our purposes and will be omitted here. They can be found in any Linear Algebra textbook. □

Lemma 1.22. *The inverse matrix of a nonsingular matrix is unique.*

Proof. Let B_1 and B_2 be two inverse matrices of a nonsingular matrix A. Then, by definition,

$$AB_1 = B_1A = I \quad \text{and} \quad AB_2 = B_2A = I.$$

Multiply $I = AB_1$ to the left by B_2 and use the fact that $B_2A = I$ to obtain

$$B_2 \;=\; B_2I \;=\; B_2(AB_1) \;=\; (B_2A)B_1 \;=\; IB_1 \;=\; B_1.$$

□

Theorem 1.23. *Let A be a square matrix. If B is a matrix such that*

$$AB \;=\; I,$$

then A is nonsingular and B is the inverse matrix of A; therefore, we also have that

$$BA \;=\; I.$$

Similarly, if $BA = I$, then A is nonsingular, B is the inverse matrix of A, and $AB = I$.

Proof. From Lemma 1.26 and (27), we find that $\det(A)\,\det(B) = 1$ and therefore both $\det(A) \neq 0$ and $\det(B) \neq 0$. From (**??**), we conclude that both A and B are nonsingular matrices. Let A^{-1} be the inverse of A. Multiplying $AB = I$ to the left by A^{-1} we find that

$$A^{-1} \;=\; A^{-1}\,(AB) \;=\; B.$$

We conclude that B is the inverse of A. □

Lemma 1.24. *The product AB of two square matrices A and B of the same size is nonsingular if and only if both A and B are nonsingular matrices.*

Proof. "A and B are nonsingular $\Rightarrow$ AB is nonsingular"

If A and B are nonsingular, it is easy to check that the matrix $B^{-1}A^{-1}$ satisfies the definition of the inverse matrix of AB; see also the proof of Lemma 1.25 below.

"AB is nonsingular $\Rightarrow$ A and B are nonsingular"

Assume that AB is nonsingular. If B is singular, then, from (22), we find that there exists $v \neq 0$. such that $Bv = 0$ Thus, $ABv = 0$ and therefore Null$(AB) \neq \{0\}$, which contradicts the fact that AB is nonsingular. Therefore B must be nonsingular.

We showed that, if AB is nonsingular, that B is also nonsingular. Assume that A is nonetheless singular. Again from Theorem 1.21, we find that there exists $w \neq 0$ such that $Aw = 0$. Since B is nonsingular, Range$(B) = \mathbb{R}^n$. Thus, there exists $v \in \mathbb{R}^n$ such that $Bv = w$; note that $v \neq 0$, since $w = Bv \neq 0$. We find that $ABv = Aw = 0$, with $v \neq 0$, which means that Null$(AB) \neq \{0\}$. This contradicts the fact that AB is nonsingular and therefore A must also be nonsingular. □

Lemma 1.25. *Let A and B be nonsingular matrices. Then the product AB is a nonsingular matrix. However, the inverse of the product of two matrices is NOT the product of the inverses, i.e.,*

$$(AB)^{-1} \neq A^{-1}B^{-1}.$$

Instead, as was the case for transposes (see Lemma 1.7), the following holds true:

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Proof. To show that AB is nonsingular, it is enough to check that the matrix $B^{-1}A^{-1}$ satisfies the definition (19) of an inverse matrix, i.e.,

$$\begin{aligned} (B^{-1}A^{-1})\, AB &= I; \\ AB\, (B^{-1}A^{-1}) &= I. \end{aligned}$$

These results follow immediately from the fact that matrix multiplication is associative and

$$\begin{aligned} A^{-1}A &= AA^{-1} = I; \\ B^{-1}B &= BB^{-1} = I. \end{aligned}$$

□

1.2. **Lower Triangular and Upper Triangular Matrices.** There are several special families of square matrices which are important for practical applications:

Symmetric Matrices:

$$A \text{ symmetric} \iff A = A^t \iff A(i,j) = A(j,i),\ \forall\ 1 \leq i,j \leq n$$

Diagonal Matrices:

$$A \text{ diagonal} \iff A(i,j) = 0, \text{ if } i \neq j;$$

Lower Triangular Matrices:

$$A \text{ lower triangular} \iff A(i,j) = 0, \text{ if } i < j;$$

Upper Triangular Matrices:

$$A \text{ upper triangular} \iff A(i,j) = 0, \text{ if } i > j;$$

Banded Matrices:

$$A \text{ banded of band } m \quad \Longleftrightarrow \quad A(i,j) = 0, \text{ if } |i-j| \geq m.$$

Notation: The diagonal matrix

$$D \;=\; \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

can be written in column form as

$$D \;=\; (d_1 e_1 \mid d_2 e_2 \mid \dots \mid d_n e_n)\,, \tag{23}$$

where e_k is the k-th column of the identity matrix I, for $k = 1:n$, or, more briefly, as

$$D = \text{diag}(d_1, d_2, \dots, d_n).$$

Elementary Properties:

Any diagonal matrix is symmetric.

Any diagonal matrix is both upper triangular and lower triangular. In fact, this is an equivalent definition for a diagonal matrix, i.e., a diagonal matrix is a matrix that is both upper triangular and lower triangular.

The transpose of a lower triangular matrix is upper triangular. The transpose of an upper triangular matrix is lower triangular.

Until now, little was said about a concept which is widely taught in a Linear Algebra class: the determinant of a matrix. It was used only once, as one of the necessary and sufficient conditions for a matrix A to be nonsingular or singular, i.e., $\det(A) \neq 0$ or $\det(A) = 0$; cf. (**??**) and (**??**). This is because the main use of the determinant of a matrix in numerical linear algebra would have been as an indication of whether a matrix in nonsingular or not. However, figuring out whether a matrix is singular is usually done as a bi-product of another algorithm called LU decomposition.

If we need to compute the determinant of a matrix, this is never done using the linear algebra definition, since that would require about $n \cdot n! \approx \frac{n^{n+1}}{e^n}$ operations. Rather, it is computed as a bi-product of the LU decomposition, which requires $O(n^3)$ operations.

For numerical linear algebra purposes, we only need a few properties of the determinant which are listed below.

Lemma 1.26.

$$det(AB) \;=\; det(A)\; det(B).$$

Definition 1.27. The determinant of a 2×2 matrix

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

is, by definition,

$$\det(A) \;=\; ad \;-\; bc.$$

Definition 1.28. The determinant of a diagonal matrix D is equal to the product of all its entries on the main diagonal, i.e.,

$$\det(D) \;=\; \prod_{i=1}^{n} D(i,i). \tag{24}$$

The determinant of a lower triangular matrix L is equal to the product of all its entries on the main diagonal, i.e.,

$$\det(L) \;=\; \prod_{i=1}^{n} L(i,i). \tag{25}$$

The determinant of an upper triangular matrix U is equal to the product of all its entries on the main diagonal, i.e.,

$$\det(U) \;=\; \prod_{i=1}^{n} U(i,i). \tag{26}$$

Note that, if I is the identity matrix, then

$$\det(I) \;=\; 1. \tag{27}$$

Lemma 1.29. *A diagonal matrix D is nonsingular if and only if all its entries on the main diagonal are nonzero, i.e., if and only if*

$$D(i,i) \;\neq\; 0,\ \forall\ i = 1:n.$$

A lower triangular matrix L is nonsingular if and only if all its entries on the main diagonal are nonzero, i.e., if and only if

$$L(i,i) \;\neq\; 0,\ \forall\ i = 1:n.$$

An upper triangular matrix U is nonsingular if and only if all its entries on the main diagonal are nonzero, i.e., if and only if

$$U(i,i) \;\neq\; 0,\ \forall\ i = 1:n.$$

Proof. These results follow immediately from the definition of a nonsingular matrix as a matrix with nonzero determinant, see (**??**), and from the formulas (24–26) for the determinant of diagonal, upper, and lower triangular matrices. □

Lemma 1.30. *Let A be an $n \times n$ matrix, and let $D = diag(d_1, d_2, \ldots, d_n)$ be a diagonal matrix. If*

$$A \;=\; (a_1 \mid a_2 \mid \ \ldots\ \mid a_n)$$

is the column form of A and if

$$A \;=\; \begin{pmatrix} r_1 \\ - - - - \\ r_2 \\ - - - - \\ \vdots \\ - - - - \\ r_n \end{pmatrix}$$

is the row form of matrix A, then

$$A\,D \;=\; (d_1 a_1 \mid d_2 a_2 \mid \ \ldots\ \mid d_n a_n)\,;$$

$$D\,A \;=\; \begin{pmatrix} d_1 r_1 \\ - - - - \\ d_2 r_2 \\ - - - - \\ \vdots \\ - - - - \\ d_n r_n \end{pmatrix}.$$

Proof. Recall from (23) that $D = (d_1e_1 \mid d_2e_2 \mid \ldots \mid d_ne_n)$. From (6), we find that

$$A\ D = (d_1(Ae_1) \mid d_2(Ae_2) \mid \ldots \mid d_n(Ae_n))$$
$$= (d_1a_1 \mid d_2a_2 \mid \ldots \mid d_na_n),$$

since $Ae_k = a_k$, for all $k = 1 : n$; cf. (14).

NOT CLEAR HOW TO WRITE THIS UP

□

Lemma 1.31. *The product of two diagonal matrices is diagonal.*
The product of two lower triangular matrices is lower triangular.
The product of two upper triangular matrices is upper triangular.

Proof. The proof for diagonal matrices follows from a simple computation.

We give the proof for lower triangular matrices in detail, using column vector arguments.

Let $L_1 = (c_1 \mid c_2 \mid \ldots \mid c_n)$ and $L_2 = (d_1 \mid d_2 \mid \ldots \mid d_n)$ be lower triangular matrices. The fact that L_1 is a lower triangular matrix is equivalent to saying that the first $k-1$ entries of the k-th column c_k of L_1 are equal to 0, i.e., for all $k = 2 : n$,

$$c_k(j) = 0,\ \forall\ j \leq k-1. \tag{28}$$

A similar necessary and sufficient condition also holds for matrix L_2, i.e., $\forall\ k = 2 : n$,

$$d_k(j) = 0,\ \forall\ j \leq k-1. \tag{29}$$

Since $L_1L_2 = (L_1d_1 \mid L_1d_2 \mid \ldots \mid L_1d_n)$, the k-th column of L_1L_2 is L_1d_k. From (29), we know that $d_k(i) = 0$, $\forall\ i \leq k-1$, and therefore

$$L_1d_k = \sum_{i=1}^{n} d_k(i)\ c_i = \sum_{i=k}^{n} d_k(i)\ c_i \tag{30}$$

Note that all column vectors c_i, $i = k : n$, have the first $k-1$ entries equal to 0; cf. (28). Therefore, any linear combination of the vectors c_k, c_{k+1}, …, c_n has the same property, and, from (30), we conclude that L_1d_k, the k-th column of L_1L_2, has the first $k-1$ entries equal to 0. Thus, L_1L_2 is a lower triangular matrix.

The proof for upper triangular matrices follows step by step the proof for lower triangular matrices. □

Note that a similar result does not hold for symmetric matrices, i.e., the product of two symmetric matrices is not symmetric. Let A and B be symmetric matrices. If AB were symmetric, then $(AB)^t = AB$. From Lemma 1.7, we find that

$$(AB)^t = B^tA^t = BA,$$

since A and B are symmetric. But, in general, $AB \neq BA$, and therefore, $(AB)^t \neq AB$.

Lemma 1.32. *If a lower triangular matrix is nonsingular, then its inverse is also lower triangular.*
If an upper triangular matrix is nonsingular, then its inverse is also upper triangular.

Proof. The proofs for lower and upper triangular matrices are similar. We only give here the proof for upper triangular matrices.

Let $U = (u_1 \mid u_2 \mid \ldots \mid u_n)$ be a nonsingular upper triangular matrix and let $B = (b_1 \mid b_2 \mid \ldots \mid b_n)$ be the inverse matrix of U, i.e.,

$$BU = UB = I.$$

Recall that $BU = (Bu_1 \mid Bu_2 \mid \ldots \mid Bu_n)$ and $I = (e_1 \mid e_2 \mid \ldots \mid e_n)$. Therefore,

$$Bu_k = e_k,\ \forall\ k = 1 : n.$$

For $k = 1$, we find that $Bu_1 = e_1$. Since U is upper triangular, we know that $u_1(j) = 0$, $\forall\ j > 1$. Then

$$e_1 \ = \ Bu_1 \ = \ \sum_{j=1}^{n} u_1(j)b_j \ = \ u_1(1)b_1$$

and therefore

$$b_1 \ = \ \frac{1}{u_1(1)}\ e_1 \ = \ \begin{pmatrix} \frac{1}{u_1(1)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Note that, $u_1(1) \neq 0$ since U is nonsingular; cf. Lemma 1.29.

For $k = 2$, we find that $Bu_2 = e_2$. Since U is upper triangular, we know that $u_2(j) = 0$, $\forall\ j > 2$. Then

$$e_2 \ = \ Bu_2 \ = \ \sum_{j=1}^{n} u_2(j)b_j \ = \ u_2(1)b_1 \ + \ u_2(2)b_2.$$

Solving for b_2, and using the fact that $u_2(2) \neq 0$, cf. Lemma 1.29, we find that

$$b_2 \ = \ \frac{1}{u_2(2)}\ (e_2 - u_2(1)b_1) \ = \ \begin{pmatrix} -\frac{u_2(1)}{u_2(2)}\ \frac{1}{u_1(1)} \\ \frac{1}{u_2(2)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Working one step forward at a time on the equality $Bu_k = e_k$, similar computations will lead to the conclusion that, for any $k = 1 : n$,

$$b_k(j) \ = \ 0,\ \forall\ j > k.$$

This is equivalent to saying that B is an upper triangular matrix.

Note that this proof is essentially a proof by induction, if all details are filled in. □

1.3. **Solving Linear Systems – The Relevance of Triangular Matrices.** Lower and upper triangular matrices are particularly important from a numerical point of view. One of the main problems in numerical linear algebra is solving linear systems:

Find a solution x to the problem $Ax = b$.

If the matrix A is either upper triangular or lower triangular, solving the linear system $Ax = b$ is straightforward:

Assume that $A = L$ is a nonsingular lower triangular matrix, i.e., $L(i, i) \neq 0$, $\forall\ i = 1 : n$.
The linear system $Lx = b$ is solved as follows: first compute $x_1 = b_1/L(1, 1)$. Use this value in the second equation of the linear system to obtain $x_2 = (b_2 - L(2, 1)x_1)/L(2, 2)$. Keep moving forward: in the k-th equation, the only variables involved are $x_1, \ldots, x_k$. The values of $x_1, \ldots, x_{k-1}$ have already been found at the previous steps. Therefore, we can solve for x_k in the k-th equation. Computing x_k involves division by $L(k, k)$, which is nonzero, since L is nonsingular; cf. Lemma 1.29.
The general formula for computing x_k in terms of $x_1, \ldots, x_{k-1}$ is

$$x_k \ = \ \frac{b_k - \sum_{i=1}^{k-1} L(k, i)x_i}{L(k, k)}.$$

This method is called *Forward Substitution*, since we begin by computing x_1 and we move forward computing one variable at a time, until x_n is computed.

Assume that $A = U$ is a nonsingular upper triangular matrix, i.e., $U(i,i) \neq 0$, $\forall\ i = 1 : n$.
The linear system $Ux = b$ is solved as follows: compute $x_n = b_n/U(n,n)$ using the n-th equation. Use this value in the $(n-1)$-th equation to obtain $x_{n-1} = (b_{n-1} - U(n-1,n)x_n)/U(n-1,n-1)$. Keep moving backward: in the k-th equation, the only variables involved are $x_k, \ldots, x_n$. The values of $x_{k+1}, \ldots, x_n$ have already been found at the previous steps. Therefore, we can solve for x_k in the k-th equation. Computing x_k involves division by $U(k,k)$, which is nonzero, since U is nonsingular; cf. Lemma 1.29.
The general formula for computing x_k in terms of $x_{k+1}, \ldots, x_n$ is

$$x_k \ = \ \frac{b_k - \sum_{i=k+1}^{n} U(k,i)x_i}{U(k,k)}.$$

This method is called *Backward Substitution*, since we begin by computing x_n and we move backward computing one variable at a time, until x_1 is computed.

For a nonsingular matrix A that is not upper, nor lower triangular, we can use the LU algorithm to solve the linear system $Ax = b$ can be solved without explicitely computing A^{-1}, by only using forward and backward substitution, provided that we can find a lower triangular matrix L and an upper triangular matrix U such that $A = LU$. A numerical algorithm that does just this called the LU decomposition exists for any nonsingular matrices (row pivoting also required...).

So, assume that $A = LU$, where L is lower triangular and U is upper triangular. Then, solving

$$Ax \ = \ b$$

is equivalent to solving

$$L\,Ux \ = \ b,$$

which is the same as solving

$$Ly \ = \ b$$

for y, and then solving

$$Ux \ = \ y$$

for x. Note that $Ly = b$ is solved by forward substitution, since L is a lower triangular matrix, and $Ux = y$ is solved by backward substitution, since U is an upper triangular matrix.

2. Permutation Matrices

Definition 2.1. A matrix P is called a permutation matrix if and only if P is obtained from the identity matrix I by interchanging (permuting) the columns of I.

Definition 2.2. An elementary permutation matrix is a permutation matrix obtained from the identity matrix by permuting exactly two columns of the identity matrix. The elementary permutation matrix obtained from the identity matrix I by permuting the columns e_i and e_j is denoted by $P_{i,j}$.

Lemma 2.3. *The matrix $P_{i,j}$ is symmetric and*

$$P_{i,j}^2 \;=\; I.$$

Proof. It is easy to see that all the entries of $P_{i,j}$ are equal to zero, except for

$$\begin{aligned} P_{i,j}(k,k) &= 1,\ \forall\ k \neq i,j; \\ P_{i,j}(i,j) &= 1; \\ P_{i,j}(j,i) &= 1. \end{aligned}$$

Then, by definition, the matrix $P_{i,j}$ is symmetric, since $P_{i,j}(k_1,k_2) = P_{i,j}(k_2,k_1)$ for any $1 \leq k_1,k_2 \leq n$.

To show that $P_{i,j}^2 = I$, recall that $I = (e_1 \mid e_2 \mid \ldots \mid e_n)$. Since $P_{i,j}$ is obtained from I by permuting the columns e_i and e_j, we find that

$$P_{i,j} \;=\; (e_1 \mid \ldots \mid e_{i-1} \mid e_j \mid e_{i+1} \mid \ldots \mid e_{j-1} \mid e_i \mid e_{j+1} \mid \ldots \mid e_n). \tag{31}$$

Also, recall from (14), that, if $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$, then $Ae_k = a_k$. Moreover, $P_{i,j}e_j$ is equal to the j-th column of $P_{i,j}$, which is e_i, and $P_{i,j}e_i$ is equal to the i-th column of $P_{i,j}$, which is e_j. In other words, $P_{i,j}e_j = e_i$ and $P_{i,j}e_i = e_j$. Therefore,

$$\begin{aligned} P_{i,j}^2 &= (P_{i,j}e_1 \mid \ldots \mid P_{i,j}e_{i-1} \mid P_{i,j}e_j \mid P_{i,j}e_{i+1} \mid \ldots \mid P_{i,j}e_{j-1} \mid P_{i,j}e_i \mid P_{i,j}e_{j+1} \mid \ldots \mid P_{i,j}e_n) \\ &= (e_1 \mid \ldots \mid e_{i-1} \mid e_i \mid e_{i+1} \mid \ldots \mid e_{j-1} \mid e_j \mid e_{j+1} \mid \ldots \mid e_n) \\ &= I. \end{aligned}$$

□

Lemma 2.4. *Let $P_{i,j}$ be the permutation matrix obtained from I by interchanging e_i and e_j, and let A be an arbitrary square matrix of size n. Then*
(i) $AP_{i,j}$ permutes the columns i and j of A;
(ii) $P_{i,j}A$ permutes the rows i and j of A.

Proof. Recall from (31) that

$$P_{i,j} \;=\; (e_1 \mid \ldots \mid e_{i-1} \mid e_j \mid e_{i+1} \mid \ldots \mid e_{j-1} \mid e_i \mid e_{j+1} \mid \ldots \mid e_n),$$

where e_k, $k = 1:n$, are the columns of the identity matrix, and, from (14), that $Ae_k = a_k$, $\forall\ k = 1:n$, where $A = (a_1 \mid a_2 \mid \ldots \mid a_n)$. Then,

$$\begin{aligned} AP_{i,j} &= (Ae_1 \mid \ldots \mid Ae_{i-1} \mid Ae_j \mid Ae_{i+1} \mid \ldots \mid Ae_{j-1} \mid Ae_i \mid Ae_{j+1} \mid \ldots \mid Ae_n) \\ &= (a_1 \mid \ldots \mid a_{i-1} \mid a_j \mid a_{i+1} \mid \ldots \mid a_{j-1} \mid a_i \mid a_{j+1} \mid \ldots \mid a_n), \end{aligned}$$

which is exactly the matrix A with columns i and j permuted.

Let

$$A \;=\; \begin{pmatrix} r_1 \\ - - - - \\ r_2 \\ - - - - \\ \vdots \\ - - - - \\ r_n \end{pmatrix}$$

be the row form of matrix A.

Showing that $P_{i,j}$ permutes the rows i and j of A is equivalent to

$$P_{i,j}A = \begin{pmatrix} r_1 \\ - - - \\ \vdots \\ - - - \\ r_{i-1} \\ - - - \\ r_j \\ - - - \\ r_{i+1} \\ - - - \\ \vdots \\ - - - \\ r_{j-1} \\ - - - \\ r_i \\ - - - \\ r_{j+1} \\ - - - \\ \vdots \\ - - - \\ r_n \end{pmatrix} \iff (P_{i,j}A)^t = (r_1^t|\dots|r_{i-1}^t \mid r_j^t \mid r_{i+1}^t|\dots|r_{j-1}^t \mid r_i^t \mid r_{j+1}^t|\dots|r_n^t), \tag{32}$$

We know that $P_{i,j}$ is symmetric, cf. Lemma 2.3. Then, from Lemma 1.7, we find that

$$(P_{i,j}A)^t = A^t P_{i,j}^t = A^t P_{i,j}. \tag{33}$$

We can write A^t in column form as $A^t = (r_1^t \mid r_2^t \mid \dots \mid r_n^t)$. We showed in Lemma 2.4 that multiplying a matrix to the right by the elementary permutation matrix $P_{i,j}$ permutes the columns i and j of the matrix. Therefore, using (33), it follows that

$$(P_{i,j}A)^t = A^t P_{i,j} = (r_1^t \mid \dots \mid r_{i-1}^t \mid r_j^t \mid r_{i+1}^t \mid \dots \mid r_{j-1}^t \mid r_i^t \mid r_{j+1}^t \mid \dots \mid r_n^t),$$

which, according to (32), is what we wanted to prove. □

Lemma 2.5. *Any permutation matrix is a product of elementary permutation matrices.*

Proof. This result follows from the fact that any permutation of n numbers can be written as a product of permutations of two of the n numbers. Using Lemma 2.4, it follows that any permutation matrix is a product of the elementary permutation matrices corresponding to the permutations of two of the n numbers. □

Lemma 2.6. *The product of two permutation matrices is a permutation matrix.*

Proof. This result follows immediately from Lemma 2.5. □

3. Numerical Linear Algebra vs. Classical Linear Algebra Approaches

Until now, we only defined the determinant of a matrix for several special families of matrices. We are actually not going to define the determinant of an arbitrary matrix properly, as it is not a useful tool in numerical linear algebra.

For numerical purposes, the inverse of a matrix is rarely computed, and, if it is, it is never computed using the classical linear algebra formula involving the factor $\frac{1}{\det(A)}$ and the matrix of the minors of A. The reason is that such an algorithm would require $O(n\ n!)$ operations, which is a huge number. From Simpson's rule, we know that $n \cdot n!$ is on the order of

$$O\left(n\ \frac{n^n}{e^n}\ \sqrt{2\pi n}\right).$$

For example, for $n = 50$ this number is approximately 10^{64}.

An explanation for why A^{-1} rarely needs to be computed is the following: a fundamental problem in numerical linear algebra is to solve the linear system

$$Ax\ =\ b,$$

i.e., to compute the vector x given the matrix A and the vector b. The linear algebra approach to solving $Ax = b$ is to say that, if A is nonsingular, then $x = A^{-1}b$. This linear system will NEVER be solved numerically by computing A^{-1} and then obtaining x from the matrix-vector multiplication $x = A^{-1}b$. Instead, a numerical algorithm called the LU decomposition will be used. It turns out that, using this algorithm, the number of operations required to find the solution x of $Ax = b$ is just

$$\frac{2}{3}n^3\ +\ O(n^2).$$

The rank of a matrix is also of lesser importance in numerical linear algebra. When solving a linear equation $Ax = b$, the important issue is whether this equation is solvable or not. This is equivalent, for a square matrix A, to deciding whether A is nonsingular (in which case the system $Ax = b$ has a unique solution x), or whether A is singular (in which case the system does not have solution unless $b \in \text{Range}(A)$).

If A is singular, the rank of A would tell us the dimension of the solution space of $Ax = b$, in case a solution would exist,i.e., if $b \in \text{Range}(A)$. This, however, is of little practical relevance.

We also note an interesting fact: from a probabilistic perspective, it can be said that the set of singular matrices is of measure 0. That is because if a singular matrix, with zero determinant has its entries perturbed by even a small amount, say 10^{-6}, then its determinant is almost surely nonzero, and therefore the perturbed matrix will be nonsingular.

4. Eigenvalues and Eigenvectors

Definition 4.1. The (real or complex) number λ is called an eigenvalue of the matrix A if and only if

$$\exists\ v \neq 0 \quad \text{such that} \quad Av \ = \ \lambda v.$$

The vector v is called an eigenvector corresponding to λ.

Remark: If v is an eigenvector corresponding to the eigenvalue λ of A, then so is cv, for any fixed constant c:

$$A\ (cv) \ = \ c\ Av \ = \ c\ \lambda v \ = \ \lambda\ (cv).$$

However, we do not consider cv to be a different eigenvector than v. We count as different only linearly independent eigenvectors.

Note that it is also possible for one eigenvalue to have more than one linearly independent eigenvectors; see below for a precise discussion on this issue.

Example: For the diagonal matrix

$$D \ = \ \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & d_n \end{pmatrix},$$

every diagonal entry d_i is an eigenvalue with corresponding eigenvector e_i, the i-th column of the identity matrix I, i.e.,

$$De_i \ = \ d_i e_i,\ \forall\ i = 1 : n.$$

It is easy to see that $(d_i)_{i=1:n}$ are the only eigenvalues of D, and that e_i is the only eigenvector corresponding to d_i. Thus, any diagonal matrix of size n has n eigenvalues and n eigenvectors.

Lemma 4.2. *λ is an eigenvalue of the matrix A if and only if λ is a root of the following polynomial:*

$$P_A(t) \ = \ det(tI - A),$$

where I is the identity matrix., i.e., if and only if

$$det(\lambda I - A) \ = \ 0.$$

The polynomial $P_A(t)$ is called the characteristic polynomial of A.

Proof. "λ is an eigenvalue of $A \Rightarrow \det(\lambda I - A) = 0$"
If λ is an eigenvalue of A, let $v \neq 0$ be the corresponding eigenvector, i.e., $Av = \lambda v$. Then

$$(\lambda I - A)v = 0 \iff v \in \text{Null}(\lambda I - A) \iff \text{Null}(\lambda I - A) \neq \{0\}.$$

From (22), it follows that the matrix $\lambda I - A$ is singular, and thus that $\det(\lambda I - A) = 0$.

"$\det(\lambda I - A) = 0 \Rightarrow \lambda$ is an eigenvalue of A"
If $\det(\lambda I - A) = 0$, it follows from (22) that the matrix $\lambda I - A$ is singular, and thus that $\text{Null}(\lambda I - A) \neq \{0\}$. Let $v \neq 0$, with $v \in \text{Null}(\lambda I - A)$. Then $(\lambda I - A)v = 0$, and therefore $Av = \lambda v$. Since $v \neq 0$, we conclude, by definition, that λ is an eigenvalue of A. □

Definition 4.3. If λ is a root of multiplicity m_λ of the characteristic polynomial $P_A(t)$ corresponding to matrix A, then m_λ is also called the multiplicity of the eigenvalue λ of A.

Example: The identity matrix I (of size n) has eigenvalue 1 with multiplicity n.

Lemma 4.4. *Let A be an $n \times n$ matrix with entries real numbers. Then the matrix A has at most n eigenvalues, and some of these eigenvalues may be complex numbers.*
More precisely, if $\lambda(A)$ denotes the set of all the eigenvalues of A, then the number of the eigenvalues of A, counted with their multiplicities, is exactly n, i.e.,

$$\sum_{\lambda \in \lambda(A)} m_\lambda \;=\; n.$$

Proof. If A is an $n \times n$ matrix, then its characteristic polynomial $P_A(t)$ has degree n. From Lemma 4.2, we know that all the roots of $P_A(t)$ are the eigenvalues of A. Any polynomial of degree n with real coefficients has at most n roots, and some could be complex numbers. Thus, the matrix A has at most n eigenvalues.

By the Definition 4.3 of the multiplicity of an eigenvalue, and since the sum of the multiplicities of the roots of a polynomial of degree n is equal to n, we find that the number of the eigenvalues of A, counted with their multiplicities, is n. □

By definition, for any eigenvalue there exists at least one corresponding eigenvector. If an eigenvalue λ has multiplicity m_λ, then there could exist at most m_λ linearly independent eigenvectors corresponding to λ. However, it might also happen that there are less than m_λ eigenvectors corresponding to λ.

Example: The matrix

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

has eigenvalue $\lambda = 3$ with multiplicity 2, i.e., $\lambda_1 = \lambda_2 = 3$, but only one eigenvector corresponding to the eigenvalue $\lambda = 3$, i.e.,

$$v_1 \;=\; \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Summary: General properties of eigenvalues and eigenvectors

- Any $n \times n$ matrix A has exactly n eigenvalues, if the eigenvalues are counted with their multiplicities; these eigenvalues are not necessarily real numbers, they might be complex numbers;
- A has at most n linearly independent eigenvectors, but may have less than n linearly independent eigenvectors;
- denote by λ an eigenvalue of A with multiplicity m_λ; then λ has at least one eigenvector, and at most m_λ linearly independent eigenvectors, but possibly less than m_λ linearly independent eigenvectors.

Definition 4.5. The largest (in absolute value) eigenvalue of A is denoted by $\lambda_{max}(A)$. In other words, if $\lambda(A)$ denotes the set of all the eigenvalues of A, then

$$\lambda_{max}(A) \;=\; \max_{\lambda \in \lambda(A)} |\lambda|. \tag{34}$$

Note that $\lambda_{max}(A)$ is also called the spectral radius of A and is also denoted by $\rho(A)$.

Definition 4.6. The smallest (in absolute value) eigenvalue of A is denoted by $\lambda_{min}(A)$, i.e.,

$$\lambda_{min}(A) \;=\; \min_{\lambda \in \lambda(A)} |\lambda|.$$

Lemma 4.7. *The matrix A is singular if and only if A has an eigenvalue equal to 0. If v_0 is a corresponding non–zero eigenvector, then we can also write that A is singular if and only if*

$$\exists\, v_0 \neq 0 \quad \textit{such that} \quad A v_0 \;=\; 0.$$

Proof. From (21), we find that

$$A \text{ singular} \iff \text{Null}(A) \neq \{0\} \iff \exists\, v_0 \neq 0 \text{ s.t. } Av_0 = 0 \iff \lambda = 0 \text{ eigenvalue of } A$$

□

Lemma 4.8. *Let A be a nonsingular matrix, and let A^{-1} be the inverse matrix of A. If (λ, v) are an eigenvalue and the corresponding eigenvector for A, then $\left(\frac{1}{\lambda}, v\right)$ are an eigenvalue and the corresponding eigenvector for A^{-1}.*

Proof. If $v \neq 0$ is the eigenvector corresponding to the eigenvalue λ of A, then $Av = \lambda v$. Multiplying to the left by A^{-1}, we find that

$$v \;=\; A^{-1}\,(Av) \;=\; A^{-1}\,(\lambda v) \;=\; \lambda\,(A^{-1}v)$$

and conclude that

$$A^{-1}v \;=\; \frac{1}{\lambda}v.$$

Since v $neq0$, it follows that v is an eigenvector of A^{-1} corresponding to the eigenvalue $\frac{1}{\lambda}$. □

Lemma 4.9. *Let A be a nonsingular matrix, and let A^{-1} be the inverse matrix of A. Then,*

$$\lambda_{max}(A^{-1}) \;=\; \frac{1}{\lambda_{min}(A)} \tag{35}$$

$$\lambda_{min}(A^{-1}) \;=\; \frac{1}{\lambda_{max}(A)} \tag{36}$$

Proof. Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of A with corresponding eigenvectors $v_1, v_2, \ldots, v_n$, and assume that

$$\lambda_{max}(A) \;=\; |\lambda_1| \;\geq\; |\lambda_2| \;\geq\; \ldots \;\geq\; |\lambda_n| \;=\; \lambda_{min}(A) \;>\; 0.$$

From Lemma 4.8, it follows that the eigenvalues of A^{-1} are

$$\frac{1}{\lambda_1} \;\geq\; \frac{1}{\lambda_2} \;\geq\; \ldots \;\geq\; \frac{1}{\lambda_n},$$

and therefore, by definition,

$$\lambda_{max}(A^{-1}) \;=\; \frac{1}{|\lambda_n|} \;=\; \frac{1}{\lambda_{min}(A)};$$

$$\lambda_{min}(A^{-1}) \;=\; \frac{1}{|\lambda_1|} \;=\; \frac{1}{\lambda_{max}(A)}.$$

□

Lemma 4.10. *Assume that the $n \times n$ matrix A has n different eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, and let $v_1, v_2, \ldots, v_n$ be the corresponding eigenvectors. Then these eigenvectors are linearly independent.*

A general proof of this result requires more advanced knowledge of linear algebra, such as the Van der Monde matrix, which are of no further use to us. We will only prove Lemma 4.10 for the case when the matrix A is nonsingular and no two eigenvalues of A are equal (in absolute value) to each other.

Proof. We will prove the result under the following assumption:

$$|\lambda_1| \;>\; |\lambda_2| \;>\; \ldots \;>\; |\lambda_n| \;>\; 0. \tag{37}$$

We give a proof by contradiction. Assume that the vectors $\{v_i\}_{i=1:n}$ are linearly dependent, i.e., there exists the constants $\{\alpha_i\}_{i=1:n}$ such that

$$\alpha_1 v_1 \;+\; \alpha_2 v_2 \;+\; \ldots \;+\; \alpha_n v_n \;=\; 0. \tag{38}$$

Assume, without any loss of generality, that $\alpha_1 \neq 0$. Multiply (38) by A^k. Note that

$$A^k v_i = \lambda^k v_i,\ \forall\ i = 1:n,\ \forall\ k \geq 1.$$

Then, (38) becomes

$$\alpha_1\lambda_1^k v_1 \ + \ \alpha_2\lambda_2^k v_2 \ + \ \ldots \ + \ \alpha_n\lambda_n^k v_n \ = \ 0. \tag{39}$$

Dividing (39) by λ_1^k, we obtain:

$$\alpha_1 v_1 \ + \ \alpha_2 \left(\frac{\lambda_2}{\lambda_1}\right)^k v_2 \ + \ \ldots \ + \ \alpha_n \left(\frac{\lambda_n}{\lambda_1}\right)^k v_n \ = \ 0. \tag{40}$$

Let $k \to \infty$ in (40). From (37), we find that

$$\lim_{k\to\infty} \left(\frac{\lambda_i}{\lambda_1}\right)^k \ = \ 0, \ \forall \ 1 < i \leq n. \tag{41}$$

From (40) and (41), we find that, as $k \to \infty$,

$$\alpha_1 v_1 \ = \ 0.$$

Since we assumed that $\alpha_1 \neq 0$, cf. (37), we conclude that $v_1 = 0$. This contradicts the fact that v_1 is an eigenvector, since any eigenvector is, by definition, nonzero; cf. Definition 4.1.

Therefore, the eigenvectors $\{v_i\}_{i=1:n}$ must be linearly independent. □

Note: A similar argument will be used to prove the convergence of the Power Method algorithm for finding the largest eigenvalue (i.e., the spectral radius) of a matrix; see Section8.

Definition 4.11. A matrix A has a diagonal form if and only if there exists a nonsingular matrix V and a diagonal matrix Λ such that

$$A \ = \ V\Lambda V^{-1}.$$

If A has a diagonal form, then A is also called diagonalizable.

Theorem 4.12. *An $n \times n$ matrix A has a diagonal form if and only if A has n linear independent eigenvectors.*

More precisely, assume that A has n eigenvectors denoted by v_1, v_2, ..., v_n, and let λ_1, λ_2, ..., λ_n be the corresponding eigenvalues. Let V be the matrix with columns v_1, v_2, ..., v_n, i.e.,

$$V \ = \ (v_1 \mid v_2 \mid \ \ldots \ \mid v_n),$$

and let

$$\Lambda = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$$

be the diagonal matrix with entries the eigenvalues of A.

Then, the matrix V is nonsingular and the matrix A can be written in a diagonal form as follows:

$$A \ = \ V \ \Lambda \ V^{-1}. \tag{42}$$

Proof. "A has a diagonal form $\Rightarrow$ A has n linear independent eigenvectors"

If the matrix A has a diagonal form, then, by definition, there exists a nonsingular matrix V and a diagonal matrix Λ such that $A = V\Lambda V^{-1}$. Let $V = (v_1 \mid v_2 \mid \ \ldots \ \mid v_n)$ and $\Lambda = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Then

$$AV \ = \ (V\Lambda V^{-1})V \ = \ V\Lambda. \tag{43}$$

Recall that

$$AV \ = \ (Av_1 \mid Av_2 \mid \ \ldots \ \mid Av_n). \tag{44}$$

Since $\Lambda = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is a diagonal matrix, it follows from Lemma 1.30 that

$$V\Lambda \ = \ (\lambda_1 v_1 \mid \lambda_2 v_2 \mid \ \ldots \ \mid \lambda_n v_n), \tag{45}$$

From (43), (44), and (45), we find that $Av_i = \lambda_i v_i$, $\forall \ i = 1 : n$. Since V is a nonsingular matrix, it follows that $v_i \neq 0$, $\forall \ i = 1 : n$, and the vectors $\{v_i\}_{i=1:n}$ are linearly independent. Thus, $\{\lambda_i\}_{i=1:n}$ are eigenvalues of A with corresponding eigenvectors v_i, $i = 1 : n$, respectively, which are linearly independent. We conclude that A has n linear independent eigenvectors.

"A has n linear independent eigenvectors $\Rightarrow$ A has a diagonal form"

Let v_i, $i = 1 : n$ be the linearly independent eigenvectors of A with corresponding eigenvalues λ_i, $i = 1 : n$. Then $Av_i = \lambda_i v_i$, $\forall\ i = 1 : n$. Let $V = (v_1 \mid v_2 \mid \ \dots \ \mid v_n)$ and $\Lambda = \mathrm{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$. Since the vectors v_i, $i = 1 : n$ are linearly independent, the column rank of V is equal to n, and therefore V is nonsingular; cf. (21). Recall from (45) that

$$V\Lambda \ = \ (\lambda_1 v_1 \mid \lambda_2 v_2 \mid \ \dots \ \mid \lambda_n v_n)\,. \tag{46}$$

Also,

$$AV \ = \ (Av_1 \mid Av_2 \mid \ \dots \ \mid Av_n) \ = \ (\lambda_1 v_1 \mid \lambda_2 v_2 \mid \ \dots \ \mid \lambda_n v_n) \tag{47}$$

From (46) and (47), we find that $AV = V\Lambda$. Multiplying by V^{-1} to the right, we conclude that

$$A \ = \ V\Lambda V^{-1},$$

which, by definition, is the diagonal form of A. □

Lemma 4.13. *If the matrix A has diagonal form $A = V\Lambda V^{-1}$, then, for every integer j,*

$$A^j \ = \ V\Lambda^j V^{-1}.$$

Proof. If j is a positive integer, it is easy to see that

$$\begin{aligned} A^j &= \left(V\Lambda V^{-1}\right)^j \\ &= V\Lambda(V^{-1}V)\Lambda(V^{-1}V)\dots\Lambda V^{-1} \\ &= V\Lambda^j V^{-1}. \end{aligned}$$

If j is a negative integer, let $k = -j$. Then k is a positive integer and

$$A^k \ = \ V\Lambda^k V^{-1}$$

and therefore

$$\begin{aligned} A^j &= \left(A^k\right)^{-1} \\ &= \left(V\Lambda^k V^{-1}\right)^{-1} \\ &= (V^{-1})^{-1}(\Lambda^k)^{-1}V^{-1} \\ &= V\Lambda^{-k}V^{-1} \\ &= V\Lambda^j V^{-1}; \end{aligned}$$

here, we used the results of Lemma 1.20 and Lemma 1.25. □

In general, the eigenvalues of a matrix with real entries may be complex numbers. Also, an $n \times n$ matrix may have less than n eigenvectors. The following theorem says that this is not the case for symmetric matrices, which have all eigenvalues real and have a full set of eigenvectors.

Theorem 4.14. *If A is a symmetric matrix of size n, i.e., if $A^t = A$, then:*

- *all the eigenvalues of A are real;*
- *eigenvectors corresponding to different eigenvalues are orthogonal (see Definition **??**);*
- *A has a full set of n linearly independent eigenvectors.*

Lemma 4.15. *If A is a symmetric matrix, then A has a diagonal form.*

Proof. From Theorem 4.14, we know that A has n linearly independent eigenvectors. Then, from Theorem 4.12,we conclude that A has a diagonal form. □

Definition 4.16. The $n \times n$ square matrix A is diagonally dominant if and only if

$$|A(j,j)| \ \geq \sum_{k \neq j, k=1:n} |A(j,k)|, \ \forall \ j = 1:n,$$

i.e., if, for every row, the absolute value of the diagonal entry is greater than the sum of the absolute values of all the other entries on that row.

The matrix A is called *strictly* diagonally dominant if and only if

$$|A(j,j)| \ > \sum_{k \neq j, k=1:n} |A(j,k)|, \ \forall \ j = 1:n.$$

Theorem 4.17. *If the matrix A is symmetric and strictly diagonally dominant, then every eigenvalue of A is positive (strictly greater than 0). Thus, the matrix A is also nonsingular.*

If the matrix A is symmetric and diagonally dominant, then every eigenvalue of A is nonnegative, i.e., greater than or equal 0.

Proof. Thus, the matrix A is nonsingular, since no eigenvalue of A can be equal to 0; see Lemma 4.7. □

5. Inner Product

Definition 5.1. The inner product of two vectors u and v from $\mathbb{R}^n$ is defined as

$$(u, v) \;=\; v^t u.$$

Let

$$v \;=\; \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \quad \text{and} \quad u \;=\; \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.$$

Then, the inner product of u and v can be written explicitely as

$$(u, v) \;=\; v^t u \;=\; u_1 v_1 + u_2 v_2 + \cdots + u_n v_n \;=\; \sum_{i=1}^{n} u_i v_i. \tag{48}$$

Lemma 5.2. *If u and v are vectors with real entries, then*

$$(u, v) \;=\; (v, u).$$

Proof. Note that $v^t u$ is a (real) number, and therefore

$$v^t u \;=\; (v^t u)^t \;=\; u^t v.$$

Then,

$$(u, v) \;=\; v^t u \;=\; u^t v \;=\; (v, u).$$

□

The inner product is a bilinear operator, i.e., it has the following properties:

$$\begin{aligned} (u_1 + u_2, v) &= (u_1, v) + (u_2, v),\ \forall\ u_1, u_2, v \in \mathbb{R}^n \\ (u, v_1 + v_2) &= (u, v_1) + (u, v_2),\ \forall\ u, v_1, v_2 \in \mathbb{R}^n \\ (cu, v) &= c(u, v),\ \forall\ c \in \mathbb{R},\ \forall\ u, v \in \mathbb{R}^n \\ (u, cv) &= c(u, v),\ \forall\ c \in \mathbb{R},\ \forall\ u, v \in \mathbb{R}^n \end{aligned} \tag{49}$$

Definition 5.3. The norm of a vector v is defined as

$$||v||^2 \;=\; (v, v) \;=\; v^t v.$$

If $v = (v_i)_{i=1:n}$, then

$$||v||^2 \;=\; (v, v) \;=\; \sum_{i=1}^{n} v_i^2,$$

or, equivalently,

$$||v|| \;=\; \sqrt{\sum_{i=1}^{n} v_i^2} \;=\; \left(\sum_{i=1}^{n} v_i^2 \right)^{1/2}$$

Lemma 5.4. *(Cauchy–Schwarz Inequality) The inner product of two vectors is bounded from above by the product of the norms of the vectors, i.e.,*

$$(u, v) \;\leq\; ||u||\ ||v||,\ \forall\ u, v \in \mathbb{R}^n. \tag{50}$$

Proof. If $u = (u_i)_{i=1:n}$ and $v = (v_i)_{i=1:n}$, then (50) can be written as

$$\left(\sum_{i=1}^{n} u_i\ v_i \right)^2 \;\leq\; \left(\sum_{i=1}^{n} u_i^2 \right)\ \left(\sum_{i=1}^{n} v_i^2 \right),\ \forall\ u_i, v_i \in \mathbb{R},\ i = 1 : n. \tag{51}$$

For any $\alpha \in \mathbb{R}$ arbitrary constant, it is easy to see that

$$\sum_{i=1}^{n} (u_i + \alpha v_i)^2 \;=\; \left(\sum_{i=1}^{n} u_i^2 \right) \;+\; 2\alpha \left(\sum_{i=1}^{n} u_i\ v_i \right) \;+\; \alpha^2 \left(\sum_{i=1}^{n} v_i^2 \right) \;\geq\; 0,\ \forall\ \alpha \in \mathbb{R}. \tag{52}$$

Note that the left hand side of (52) is a quadratic polynomial of α. The inequality (52) holds true for any real number α if and only if this polynomial has at most one real double root, i.e., if its discriminant is nonpositive:

$$(2\left(\sum_{i=1}^{n} u_i\ v_i\right))^2\ -\ 4\left(\sum_{i=1}^{n} u_i^2\right)\ \left(\sum_{i=1}^{n} v_i^2\right)\ \leq\ 0,$$

which is equivalent to (51). □

6. Orthogonality

Definition 6.1. Two vectors u and v are orthogonal if and only if

$$(u, v) \;=\; v^t u \;=\; 0.$$

Definition 6.2. The matrix $Q = (q_1 \mid q_2 \mid \ldots \mid q_n)$ is an orthogonal matrix if and only if all its column vectors have norm equal to 1 and are pairwise orthogonal, i.e.,

$$(q_i, q_j) \;=\; q_j^t q_i \;=\; 0,\ \forall\ 1 \le i \ne j \le n, \quad \text{and} \quad ||q_i||^2 = q_i^t q_i = 1,\ \forall\ i = 1 : n.$$

Lemma 6.3. *Q is orthogonal if and only if*

$$Q^t Q \;=\; Q Q^t \;=\; I.$$

In other words, Q is orthogonal if and only if Q^t is the inverse of Q.

Proof. "Q orthogonal $\Rightarrow Q^tQ = QQ^t = I$"

Let $Q = (q_1 \mid q_2 \mid \ldots \mid q_n)$. It is easy to see that

$$Q^t \;=\; \begin{pmatrix} q_1^t \\ - - - - \\ q_2^t \\ - - - - \\ \vdots \\ - - - - \\ q_n^t \end{pmatrix},$$

and therefore, for any column q_j of Q, $j = 1 : n$,

$$Q^t q_j \;=\; \begin{pmatrix} q_1^t q_j \\ \vdots \\ q_{j-1}^t q_j \\ q_j^t q_j \\ q_{j+1}^t q_j \\ \vdots \\ q_n^t q_j \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \;=\; e_j,$$

where e_j is the j-th column of the identity matrix I. Thus,

$$Q^t Q \;=\; (Q^t q_1 \mid Q^t q_2 \mid \ldots \mid Q^t q_n) \;=\; (e_1 \mid e_2 \mid \ldots \mid e_n) \;=\; I.$$

If $Q^tQ = I$ and Q is a square matrix, it follows from Theorem 1.23 that Q^t is the inverse of Q and therefore $QQ^t = I$.

"$Q^tQ = QQ^t = I \Rightarrow Q$ orthogonal"

Let $Q = (q_1 \mid q_2 \mid \ldots \mid q_n)$ and $I = (e_1 \mid e_2 \mid \ldots \mid e_n)$. Then

$$Q^t Q = I \quad \Longleftrightarrow \quad (Q^t q_1 \mid Q^t q_2 \mid \ldots \mid Q^t q_n) \;=\; (e_1 \mid e_2 \mid \ldots \mid e_n),$$

and therefore $Q^t q_j = e_j,\ \forall\ j = 1 : n$. Thus,

$$Q^t q_j = e_j,\ \forall\ j = 1 : n \quad \Longleftrightarrow \quad \begin{pmatrix} q_1^t q_j \\ \vdots \\ q_{j-1}^t q_j \\ q_j^t q_j \\ q_{j+1}^t q_j \\ \vdots \\ q_n^t q_j \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \;=\; e_j,\ \forall\ j = 1 : n,$$

and we conclude that $q_i^t q_j = 0$, $\forall i \neq j$, and $q_j^t q_j = ||q_j||^2 = 1$, $\forall 1 \leq j \leq n$, which means, by definition, that Q is an orthogonal matrix. □

Lemma 6.4. *Let Q_1 and Q_2 be $n \times n$ orthogonal matrices. Then $Q_1 Q_2$ is also an orthogonal matrix.*

Proof. Let $Q = Q_1 Q_2$. Since Q_1 and Q_2 are orthogonal matrices, it follows that $Q_1^t Q_1 = Q_2^t Q_2 = I$. Then,

$$\begin{aligned} Q^t Q &= (Q_1 Q_2)^t Q_1 Q_2 = Q_2^t Q_1^t Q_1 Q_2 \\ &= Q_2^t (Q_1^t Q_1) Q_2 = Q_2^t Q_2 \\ &= I. \end{aligned}$$

Using Lemma 6.4, we conclude that the matrix $Q = Q_1 Q_2$ is orthogonal. □ □

Lemma 6.5. *Let A be an $n \times n$ square matrix, and let u and v be column vectors of size n. Then,*

$$(Au, v) = (u, A^t v) \tag{53}$$

and

$$(u, Av) = (A^t u, v). \tag{54}$$

Proof. Using the definition of the inner product, it is easy to see that

$$\begin{aligned} (Au, v) &= v^t Au = (v^t A)u = (A^t v)^t u = (u, A^t v); \\ (u, Av) &= (Av)^t u = v^t A^t u = v^t (A^t u) = (A^t u, v). \end{aligned}$$

Here, we used the fact that $(Bx)^t = x^t B^t$ for any matrix B and vector x such that the matrix–vector multiplication Bx can be performed; cf. Lemma 1.6. □

We can now prove one part of Theorem 4.14:

Corollary 6.6. *If A is a symmetric matrix, then the eigenvectors of A corresponding to different eigenvalues are orthogonal.*

Proof. Let $\lambda_1 \neq \lambda_2$ be eigenvalues of A with corresponding eigenvectors v_1 and v_2, i.e.,

$$Av_1 = \lambda_1 v_1 \quad \text{and} \quad Av_2 = \lambda_2 v_2. \tag{55}$$

Note that $(Av_1, v_2) = (v_1, A^t v_2) = (v_1, Av_2)$, since A is symmetric. Then, from (55), we find that

$$(Av_1, v_2) = \lambda_1 (v_1, v_2) = (v_1, Av_2) = \lambda_2 (v_1, v_2).$$

Thus, $(\lambda_1 - \lambda_2)\,(v_1, v_2) = 0$, and, since $\lambda_1 \neq \lambda_2$, we conclude that $(v_1, v_2) = 0$, i.e., that v_1 and v_2 are orthogonal. □

Corollary 6.7. *If the $n \times n$ symmetric matrix A has n different eigenvalues, than the matrix A had a diagonal form $A = Q \Lambda Q^t$.*

Proof. □

Lemma 6.8. *A matrix–vector multiplication by an orthogonal matrix does not change the norm of the vector. If Q is an orthogonal matrix and v is an arbitrary vector, then*

$$||Qv|| = ||v||. \tag{56}$$

Proof.

$$||Qv||^2 = (Qv, Qv) = (Qv)^t Qv = v^t Q^t Q v = v^t v = ||v||^2.$$

□

Lemma 6.9. *Any eigenvalue of an orthogonal matrix has absolute value equal to 1, and therefore the spectral radius of any orthogonal matrix is equal to 1.*

Proof. Let λ be an eigenvalue of the orthogonal matrix Q, and let $v \neq 0$ be the corresponding eigenvector. Then, $Qv = \lambda v$. From (56), it follows that

$$||v|| \;=\; ||Qv|| \;=\; ||\lambda v|| \;=\; |\lambda| \cdot ||v||.$$

Since $||v|| \neq 0$, it follows that

$$|\lambda| = 1, \;\forall\; \lambda \in \lambda(Q). \tag{57}$$

From the definition (34) of the spectral radius of a matrix, and using (57), we obtain that

$$\lambda_{max}(Q) \;=\; \max_{\lambda \in \lambda(Q)} |\lambda| \;=\; 1.$$

□

Lemma 6.10. *Let $v_1, v_2, \ldots, v_n$ be n vectors in $\mathbb{R}^m$. Then*

$$||\sum_{i=1}^{n} v_i||^2 \;=\; \sum_{i=1}^{n} ||v_i||^2 \;+\; 2 \sum_{1 \leq i < j \leq n} (v_i, v_j). \tag{58}$$

In particular, if the vectors $(q_i)_{i=1:n}$ are pairwise orthogonal, i.e, if $(q_i, q_j) = 0$ for any $i \neq j$, then

$$||\sum_{i=1}^{n} q_i||^2 \;=\; \sum_{i=1}^{n} ||q_i||^2. \tag{59}$$

Proof. It is easy to see that

$$\begin{aligned}
||\sum_{i=1}^{n} v_i||^2 \;&=\; \left(\sum_{i=1}^{n} v_i,\; \sum_{i=1}^{n} v_i \right) \\
&=\; \sum_{1 \leq i,j \leq n} (v_i, v_j) \\
&=\; \sum_{i=1}^{n} (v_i, v_i) \;+\; \sum_{1 \leq i \neq j \leq n} (v_i, v_j) + (v_j, v_i) \\
&=\; \sum_{i=1}^{n} ||v_i||^2 \;+\; 2 \sum_{1 \leq i < j \leq n} (v_i, v_j),
\end{aligned}$$

since $(v_i, v_j) = (v_j, v_i)$, $\forall\; i \neq j$, cf. Lemma 5.2.

Formula (59) corresponding to orthogonal vectors follows immediately from (58). □

Alternative proof of Lemma 6.8 using the result of Lemma 6.10:
Let $v = (v_i)_{i=1}^n$, and let $Q = (q_1 \mid q_2 \mid \ldots \mid q_n)$. Then

$$Qv \;=\; \sum_{i=1}^{n} v_i q_i,$$

and, from (58), we find that

$$\begin{aligned}
||Qv||^2 \;&=\; \sum_{i=1}^{n} ||v_i q_i||^2 \;+\; 2 \sum_{1 \leq i < j \leq n} (v_i q_i, v_j q_j) \\
&=\; \sum_{i=1}^{n} v_i^2 ||q_i||^2 \;+\; 2 \sum_{1 \leq i < j \leq n} v_i v_j \; (q_i, q_j) \\
&=\; \sum_{i=1}^{n} v_i^2 \\
&=\; ||v||^2.
\end{aligned}$$

We used the facts that $||q_i|| = 1$, $\forall\ i = 1 : n$, and that $(q_i, q_j) = 0$, $\forall\ 1 \leq i < j \leq n$, since $(q_i)_{i=1:n}$ are columns of the orthogonal matrix Q. $\square$

Theorem 6.11. *If A is a symmetric matrix, then there exists an orthogonal matrix Q the columns of which are the eigenvectors of A, such that*

$$A \ = \ Q\Lambda Q^t, \tag{60}$$

where Λ is a diagonal matrix with entries on the main diagonal real numbers that are the eigenvalues of A.

The proof of Theorem 6.11 is more subtle, and beyond our scope. However, this is an important result. Since the transpose of an orthogonal matrix is also the inverse of the orthogonal matrix, i.e., $Q^t = Q^{-1}$, we conclude that (60) can also be written as

$$A \ = \ Q\Lambda Q^{-1},$$

which is the diagonal form of A.

In other words, a corollary of Theorem 6.11 is that any symmetric matrix is diagonalizable and has a full set of eigenvectors. Moreover, its eigenvectors, which are the columns of the orthogonal matrix Q, are pairwise orthogonal. These results have already been stated, without proof, in Theorem 4.14.

7. Vector and Matrix Norms

Definition 7.1. A *vector norm* on $\mathbb{R}^n$, denoted by $||\cdot||$, is an operator (that is, a function) $||\cdot|| : \mathbb{R}^n \to [0,\infty)$ with the following properties:

$$\begin{aligned} ||x|| &> 0, \ \forall\ x \neq 0 \\ ||x|| &= 0, \text{ if and only if } x = 0 \\ ||cx|| &= |c|\ ||x||, \ \forall\ c \in \mathbb{R},\ x \in \mathbb{R}^n \end{aligned}$$

Lemma 7.2. *Any vector norm satisfies the triangle inequality, i.e.,*

$$||u+v|| \ \leq ||u|| + ||v||, \ \forall\ u, v \in \mathbb{R}^n.$$

Definition 7.3. Two norms on $\mathbb{R}^n$, $||\cdot||_{first}$ and $||\cdot||_{second}$, are called equivalent norms if and only if two constants C_1 and C_2 exist such that

$$C_1||v||_{first} \ \leq \ ||v||_{second} \ \leq \ C_2||v||_{first}, \ \forall\ v \in \mathbb{R}^n.$$

Theorem 7.4. *Any two norms on $\mathbb{R}^n$ are equivalent. More generally, any two norms on a finite dimensional space are equivalent.*

Definition 7.5. A *matrix norm*, denoted by $||\cdot||$, is an operator $||\cdot|| : \mathbb{R}^{n\times n} \to [0,\infty)$ with the following properties:

$$\begin{aligned} ||A|| &> 0, \ \forall\ A \neq 0 \\ ||A|| &= 0, \text{ if and only if } A = 0 \\ ||cA|| &= |c|\ ||A||, \ \forall\ c \in \mathbb{R},\ A \in \mathbb{R}^n \end{aligned}$$

Examples of Vector Norms:

- the 1–norm:
$$||v||_1 \ = \ \sum_{i=1}^{n} |v_i|;$$
- the 2–norm:
$$||v||_2 \ = \ \left(\sum_{i=1}^{n} |v_i|^2 \right)^{1/2};$$
- the ∞–norm (the infinity norm):
$$||v||_\infty \ = \ \max_{i=1:n} |v_i|.$$
- the p–norm, for $1 < p < \infty$:
$$||v||_p \ = \ \left(\sum_{i=1}^{n} |v_i|^p \right)^{1/p};$$

Note that the norm we used until now, $||v||^2 = (v,v) = \sum v_i^2$, was called above the 2–norm.

Lemma 7.6. *The following inequality norms on $\mathbb{R}^n$ hold and are sharp:*

$$||v||_\infty \ \leq \ ||v||_2 \ \leq \ \sqrt{n}||v||_\infty, \ \forall\ v \in \mathbb{R}^n.$$
$$||v||_\infty \ \leq \ ||v||_1 \ \leq \ n||v||_\infty, \ \forall\ v \in \mathbb{R}^n.$$
$$||v||_2 \ \leq \ ||v||_1 \ \leq \ \sqrt{n}||v||_2, \ \forall\ v \in \mathbb{R}^n.$$

Definition 7.7. The matrix norm induced by the vector norm $||\cdot||$ is defined as:

$$||A|| \;=\; \sup_{w\neq 0} \frac{||Aw||}{||w||}. \tag{61}$$

The following result, although straightforward, will be used very often:

Lemma 7.8. *Any matrix norm induced by a vector norm has the following property:*

$$||Av|| \;\leq\; ||A||\;||v||,\;\forall\; v\in\mathbb{R}^n. \tag{62}$$

Proof. By the definition of the supremum, for any $v\neq 0$,

$$||A|| \;=\; \sup_{w\neq 0} \frac{||Aw||}{||w||} \;\geq\; \frac{||Av||}{||v||}$$

and therefore, $||A||\;||v|| \;\geq\; ||Av||$, $\forall\; v\in\mathbb{R}^n$, $v\neq 0$.

If $v=0$, both sides of the inequality (62) are equal to 0. □

We will only work with matrix norms induced by vector norms. If not otherwise specified, any matrix norm form now on is assumed to be induced by a vector norm.

The most common matrix norms are those induced by the 1–norm, 2–norm, and inf–norm:

- the 1–norm of A is equal to the largest value of the column sums of the absolute values of the entries of A, i.e.,
$$||A||_1 \;=\; \max_{k=1:n} \sum_{j=1}^{n} |A(j,k)|;$$
- the 2–norm of A is equal to the square root of the largest value $\lambda_{max}(A^tA)$ of the eigenvalues of the (symmetric) matrix A^tA, i.e.,
$$||A||_2 \;=\; \sqrt{\lambda_{max}(A^tA)}; \tag{63}$$
- the infinity norm of A is equal to the largest value of the row sums of the absolute values of the entries of A, i.e.,
$$||A||_\infty \;=\; \max_{j=1:n} \sum_{k=1}^{n} |A(j,k)|.$$

We are only going to prove formula (63) for the induced 2-norm of a matrix. The proofs of the other two formulas, although interesting in themselves, are only relevant for linear algebra, and not for numerical linear algebra purposes. We first need the following result about symmetric matrices:

Lemma 7.9. *If A is a symmetric matrix, then*

$$||A||_2 \;=\; \lambda_{max}(A) \;=\; \max_{\lambda\in\lambda(A)} |\lambda|$$

Proof. By definition, see (61), and using the fact that $A^t=A$, we find that

$$||A||_2^2 \;=\; \sup_{v\neq 0} \frac{||Av||_2^2}{||v||_2^2} \;=\; \sup_{v\neq 0} \frac{(Av,Av)}{||v||_2^2} \;=\; \sup_{v\neq 0} \frac{v^tA^tAv}{||v||_2^2} \;=\; \sup_{v\neq 0} \frac{v^tA^2v}{||v||_2^2}. \tag{64}$$

From Theorem 6.11, it follows that A can be written as $A=Q\Lambda Q^t$, where Λ is a diagonal matrix with entries on the main diagonal equal to the eigenvalues of A and Q is the matrix whose columns are the eigenvectors of A. Then,

$$A^2 \;=\; (Q\Lambda Q^t)^2 \;=\; Q\Lambda Q^tQ\Lambda Q^t \;=\; Q\Lambda^2Q^t, \tag{65}$$

since $Q^tQ = I$ as Q is orthogonal. From (64) and (65), we find that

$$||A||_2^2 \;=\; \sup_{v\neq 0}\frac{v^tA^2v}{||v||_2^2} \;=\; \sup_{v\neq 0}\frac{v^tQ\Lambda^2Q^tv}{||v||_2^2} \;=\; \sup_{v\neq 0}\frac{(Q^tv)^t\Lambda^2Q^tv}{||v||_2^2}. \tag{66}$$

Let $w = Q^tv$. Then $||w||_2 = ||Q^tv||_2 = ||v||_2$; cf. Lemma 6.8. Therefore, formula (66) can be written as

$$||A||_2^2 \;=\; \sup_{w\neq 0}\frac{w^t\Lambda^2w}{||w||_2^2}. \tag{67}$$

Let $\lambda_1, \lambda_2, \ldots, \lambda_n$, not necessarily different, be the eigenvalues of A, which are all real numbers since A is a symmetric matrix; cf. Theorem 4.14. Assume, without any loss of generality, that

$$\lambda_{max}(A) \;=\; |\lambda_1| \;\geq\; |\lambda_2| \;\geq\; \ldots \;\geq\; |\lambda_n|$$

Let $w = (w_i)_{i=1:n}$. Then

$$w^t\Lambda^2w = (w_1\ w_2\ \ldots\ w_n)\begin{pmatrix}\lambda_1^2 & 0 & \ldots & 0\\ 0 & \lambda_2^2 & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & \lambda_n^2\end{pmatrix}\begin{pmatrix}w_1\\ w_2\\ \vdots\\ w_n\end{pmatrix} = (w_1\ w_2\ \ldots\ w_n)\begin{pmatrix}\lambda_1^2w_1\\ \lambda_2^2w_2\\ \vdots\\ \lambda_n^2w_n\end{pmatrix} = \sum_{i=1}^n\lambda_i^2w_i^2$$

and

$$||w||_2^2 \;=\; \sum_{i=1}^n w_i^2.$$

Since for all $i = 1:n$, $\lambda_i \leq \lambda_{max}(A)$, it follows that

$$w^t\Lambda^2w \;=\; \sum_{i=1}^n\lambda_i^2w_i^2 \;\leq\; \lambda_{max}^2(A)\sum_{i=1}^n w_i^2 \;=\; \lambda_{max}^2(A)||w||_2^2, \tag{68}$$

which holds for any vector $w \in \mathbb{R}^n$. Therefore, from (67) and (68), we find that

$$||A||_2^2 \;\leq\; \lambda_{max}^2(A), \quad \text{i.e.,} \quad ||A||_2 \;\leq\; \lambda_{max}(A). \tag{69}$$

Now, recall from (64) that

$$||A||_2^2 \;=\; \sup_{v\neq 0}\frac{v^tA^2v}{||v||_2^2}. \tag{70}$$

Let $v = v_1$ in (64), where v_1 is the eigenvector corresponding to λ_1. Then,

$$v^tA^2v \;=\; v_1^tA^2v_1 \;=\; v_1^tA\,(Av_1) \;=\; v_1^tA\,(\lambda_1v_1) \;=\; \lambda_1v_1^t\,(Av_1) \;=\; \lambda_1^2v_1^tv_1 \;=\; \lambda_1^2||v_1||_2^2. \tag{71}$$

From (70) and (71) it follows that

$$||A||_2^2 \;=\; \sup_{v\neq 0}\frac{v^tA^2v}{||v||_2^2} \;\geq\; \frac{v_1^tA^2v_1}{||v_1||_2^2} \;=\; \frac{\lambda_1^2||v_1||_2^2}{||v_1||_2^2} \;=\; \lambda_1^2,$$

and therefore

$$||A||_2 \;\geq\; |\lambda_1| \;=\; \lambda_{max}(A). \tag{72}$$

From (69) and (72), we conclude that, if A is symmetric, then

$$||A||_2 \;=\; \lambda_{max}(A).$$

□

We can now prove the result for a general matrix A:

Lemma 7.10. *For an arbitrary matrix A, the following result holds:*

$$||A||_2 \;=\; \sqrt{\lambda_{max}(A^tA)}.$$

Proof. In the proof of Lemma 7.9, we implicitly showed that, for any symmetric matrix M,

$$\sup_{v\neq 0} \frac{v^t M v}{||v||_2^2} \;=\; \lambda_{max}(M). \tag{73}$$

Once again, by definition,

$$||A||_2^2 \;=\; \sup_{v\neq 0} \frac{||Av||_2^2}{||v||_2^2} \;=\; \sup_{v\neq 0} \frac{(Av, Av)}{||v||_2^2} \;=\; \sup_{v\neq 0} \frac{v^t A^t A v}{||v||_2^2} \;=\; \lambda_{max}(A^t A).$$

The last equality follows from (73) since $A^t A$ is a symmetric matrix. We conclude that

$$||A||_2 \;=\; \sqrt{\lambda_{max}(A^t A)}.$$

□

Definition 7.11. The condition number of the matrix A is defined as

$$cond(A) \;=\; ||A||_2 \; ||A^{-1}||_2.$$

Note: If the matrix A is singular, the fact that A^{-1} does not exist is equivalent to saying that $||A^{-1}||_2$ is infinite, and therefore that $cond(A)$ is infinite. Actually, this is an equivalent way of saying that A is a nonsingular matrix:

$$A \text{ nonsingular} \quad \Longleftrightarrow \quad cond(A) \neq \infty.$$

The matrix A is called *well–conditioned* if its condition number is small. There is no well defined number to quantify this statement, but a general rule of thumb would be that $cond(A) \leq 100$ means that A is well–conditioned.

The matrix A is called *ill–conditioned* if its condition number is large. For example, if $cond(A) \geq 1000$, then the matrix A can most probably be considered ill-conditioned.

Lemma 7.12. *For an induced matrix norm,*

$$||AB|| \;\leq\; ||A||\; ||B||.$$

Proof. Using Lemma 7.8 and definition (61), we find that

$$||AB|| \;=\; \sup_{v\neq 0} \frac{||ABv||}{||v||} \;\leq\; \sup_{v\neq 0} \frac{||A||\; ||Bv||}{||v||} \;=\; ||A||\; \sup_{v\neq 0} \frac{||Bv||}{||v||} \;=\; ||A||\; ||B||.$$

□

Lemma 7.13.

$$cond(A) \;\geq\; 1.$$

Proof. Clearly, $||I|| = 1$, and recall that $I = AA^{-1}$. From Lemma 7.12, we find that

$$1 \;=\; ||I|| \;=\; ||AA^{-1}|| \;\leq\; ||A||\; ||A^{-1}|| \;=\; cond(A).$$

□

Lemma 7.14. *If Q is an $n \times n$ orthogonal matrix, then, for any $n \times n$ matrix A,*

$$||QA||_2 \;=\; ||A||_2.$$

This result is not necessarily true for other norms.

Proof. Since Q is orthogonal, we know that $Q^t Q = I$. Then, from (63), it follows that

$$||QA||_2 \;=\; \sqrt{\lambda_{max}((QA)^t QA)} \;=\; \sqrt{\lambda_{max}(A^t Q^t QA)} \;=\; \sqrt{\lambda_{max}(A^t A)} \;=\; ||A||_2.$$

□

Theorem 7.15. *If A is a symmetric matrix, then*

$$||A||_2 \;=\; \lambda_{max}(A) \;=\; \max_{\lambda\in\lambda(A)} |\lambda| \tag{74}$$

$$||A^{-1}||_2 \;=\; \frac{1}{\lambda_{min}(A)} \;=\; \frac{1}{\min_{\lambda\in\lambda(A)} |\lambda|} \tag{75}$$

$$cond(A) \;=\; \frac{\lambda_{max}(A)}{\lambda_{min}(A)} \tag{76}$$

Proof. We already showed that, for a symmetric matrix A, $||A||_2 = \lambda_{max}(A)$; cf. Lemma 7.9.

Since A is symmetric, it follows that A^{-1} is also a symmetric matrix. Recall from (35) of Lemma 4.9 that

$$\lambda_{max}(A^{-1}) \;=\; \frac{1}{\lambda_{min}(A)}$$

From Lemma 7.9 we conclude that

$$||A^{-1}||_2 \;=\; \lambda_{max}(A^{-1}) \;=\; \frac{1}{\lambda_{min}(A)}.$$

From the definition of the condition number, we obtain that

$$cond(A) \;=\; ||A||_2\;||A^{-1}||_2 \;=\; \frac{\lambda_{max}(A)}{\lambda_{min}(A)}.$$

□

8. The Power Method

Generally speaking, the largest and smallest (in absolute value) eigenvalues of a matrix, i.e., $\lambda_{max}(A)$ and $\lambda_{min}(A)$, are the most important ones to know. One reason, for example, is that the condition number of a symmetric matrix is equal to the ratio of the largest and smallest eigenvalues, i.e.,

$$cond(A) \;=\; \frac{\lambda_{max}(A)}{\lambda_{min}(A)};$$

cf. (76).

While other numerical methods, e.g., the QR method, exist for computing all the eigenvalues of a matrix – and therefore also the largest and smallest eigenvalues of the matrix, the Power Method only finds $\lambda_{max}(A)$, and can be easily adapt to obtain $\lambda_{min}(A)$.

Pseudocode for the Power Method

Input: matrix `A`; tolerance `tol`; initial guess vector `w_0`, arbitrary
Output: `lambda_max_A` and corresponding eigenvector `evector_max`

```
w_new = w_0; w_old = w_new - 1;
while norm(w_new - w_old) > tol
     w_old = w_new;
     w_int = A w_new;
     w_new = w_int / norm(w_int);
end
lambda_max_A = norm(A w_new);
evector_max = w_new;
```

To compute $\lambda_{min}(A)$, recall from Lemma 4.7 that, if the matrix A is singular, then $\lambda_{min}(A) = 0$.

Assume that A is nonsingular. Recall from Lemma 4.9 that $\lambda_{max}(A^{-1}) = \frac{1}{\lambda_{min}(A)}$. Therefore, to find the smallest eigenvalue $\lambda_{min}(A)$ of A, it is enough to apply the Power Method to the matrix A^{-1} in order to find $\lambda_{max}(A^{-1})$.

There is one slightly subtle step to deal with: computing

$$\text{w\_int} \;=\; A^{-1}\ \text{w\_new},$$

corresponding to w_int = A w_new from the Pseudocode above. It is important to note that we never compute the matrix A^{-1} in order to do this. Instead, we use a solver for the linear system corresponding to matrix A. Let lin_solve be an algorithm with input the matrix A and the vector b whose output is the vector x, solution to the linear system $Ax = b$, which we denote by $x = \text{lin\_solve}(A, b)$. Then,

$$\text{w\_int} \;=\; \text{lin\_solve}(A,\ \text{w\_new}).$$

Pseudocode for computing the smallest eigenvalue of a matrix using the Power Method

Input: nonsingular matrix `A`; tolerance `tol`; initial guess vector `w_0`, arbitrary
Output: `lambda_max_A` and corresponding eigenvector `evector_max`

```
w_new = w_0; w_old = w_new - 1;
while norm(w_new - w_old) > tol
     w_old = w_new;
     w_int = lin_solve(A,w_new);
```

```
    w_new = w_int/norm(w_int);
end
lambda_max_A = 1/norm(lin_solve(A,w_new));
evector_max = w_new;
```

We now address the question of why does the output of the Power Method algorithm is indeed (approximately) equal to $\lambda_{max}(A)$ and a corresponding eigenvector?

First of all, we denote by w_k the vector w_new obtained after k steps of the Power Method algorithm. It is easy to see that

$$w_1 \;=\; \frac{Aw_0}{||Aw_0||}$$

and

$$w_2 \;=\; \frac{Aw_1}{||Aw_1||} \;=\; \frac{A^2w_0}{||Aw_1||\;||Aw_0||} \tag{77}$$

Note that $||w_2||$ = 1,m by definition, since

$$w_2 \;=\; \left|\left|\frac{Aw_1}{||Aw_1||}\right|\right| \;=\; \frac{1}{||Aw_1||}\;\cdot\;||Aw_1|| \;=\; 1.$$

Also, from (77), we see that w_2 is equal to the vector A^2w_0 multiplied by a positive constant c (which, incidentally, but without a direct relevance to our discussion, is equal to $c = \frac{1}{||Aw_1||\;||Aw_0||}$). In other words, we can write

$$w_2 \;=\; c\;A^2w_0, \quad \text{with} \quad ||w_2|| \;=\; 1.$$

Then, we find that

$$1 \;=\; ||w_2|| \;=\; ||c\;A^2w_0|| \;=\; c\;||A^2w_0|| \iff c \;=\; \frac{1}{A^2w_0}.$$

We conclude that w_2, can also be written as

$$w_2 \;=\; \frac{A^2w_0}{A^2w_0}. \tag{78}$$

The form (78) for w_2 is more useful than form (77), since it can be generalized, by induction, to

$$w_k \;=\; \frac{A^kw_0}{||A^kw_0||},\;\forall\; k \geq 1. \tag{79}$$

To see this, assume as induction hypothesis that $w_k = \frac{A^kw_0}{||A^kw_0||}$. Then

$$w_{k+1} \;=\; \frac{Aw_k}{||Aw_k||} \;=\; \frac{A^{k+1}w_0}{||Aw_k||\;||A^kw_0||} \;=\; c\;A^{k+1}w_0,$$

where $c > 0$ is chosen such that $||w_{k+1}|| = 1$, i.e., with $c = \frac{1}{||A^{k+1}w_0||}$.

For simplicity, let us assume that the matrix A, of size $n \times n$, has n different eigenvalues and that

$$\lambda_{max}(A) \;=\; \lambda_1 \;>\; |\lambda_2| \;\geq\; \ldots \;\geq\; |\lambda_n|,$$

where $\{\lambda_i\}_{i=1:n}$ are the eigenvalues of A with corresponding eigenvectors $(v_i)_{i=1:n}$. From Lemma 4.10, it follows that the vectors $(v_i)_{i=1:n}$ are linearly independent. Then, any vector in $\mathbb{R}^n$ can be written as a linear combination of the vectors $(v_i)_{i=1:n}$. In particular, there exist $(\alpha_i)_{i=1:n}$ such that

$$w_0 \;=\; \sum_{i=1}^{n} \alpha_i v_i.$$

For any positive integer k, recall that $A^k v_i = \lambda_i^k v_i$, $\forall i = 1 : n$. Therefore,

$$A^k w_0 \;=\; A^k \;(\sum_{i=1}^{n} \alpha_i v_i) \;=\; \sum_{i=1}^{n} \alpha_i A^k v_i \;=\; \sum_{i=1}^{n} \alpha_i \lambda_i^k v_i$$

From (79) it follows that

$$\begin{aligned}
w_k &= \frac{A^k w_0}{||A^k w_0||} \\
&= \frac{\sum_{i=1}^{n} \alpha_i \lambda_i^k v_i}{||\sum_{i=1}^{n} \alpha_i \lambda_i^k v_i||} \\
&= \frac{\lambda_1^k \;\sum_{i=1}^{n} \alpha_i \;\left(\frac{\lambda_i}{\lambda_1}\right)^k \; v_i}{\lambda_1^k \;||\sum_{i=1}^{n} \alpha_i \;\left(\frac{\lambda_i}{\lambda_1}\right)^k \; v_i||} \\
&= \frac{\alpha_1 v_1 \;+\; \alpha_2 \;\left(\frac{\lambda_2}{\lambda_1}\right)^k v_2 \;+\; \ldots \;+\; +\, \alpha_n \;\left(\frac{\lambda_n}{\lambda_1}\right)^k v_n}{||\alpha_1 v_1 \;+\; \alpha_2 \;\left(\frac{\lambda_2}{\lambda_1}\right)^k v_2 \;+\; \ldots \;+\; +\, \alpha_n \;\left(\frac{\lambda_n}{\lambda_1}\right)^k v_n||}
\end{aligned}$$

As $k \to \infty$, $\left(\frac{\lambda_i}{\lambda_1}\right)^k \;\to\; 0$, since $|\lambda_i| < \lambda_1$, $\forall\; i \geq 2$. Then,

$$\lim_{k\to\infty} w_k \;=\; \frac{\alpha_1 v_1}{||\alpha_1 v_1||} \;=\; \frac{\alpha_1}{|\alpha_1|} \;\cdot\; \frac{v_1}{||v_1||} \;=\; c\; v_1,$$

where $c = \frac{\alpha_1}{|\alpha_1|}\frac{1}{||v_1||}$. Thus, when convergence is achieved (in the sense that two consecutive iterates are close to each other, i.e., $||w_{k+1} - w_k|| \leq tol$) the value of w_k is a constant multiple of the eigenvector corresponding to the largest eigenvalue of A. In other words, w_k is approximately equal to the eigenvector of A corresponding to $\lambda_1 = \lambda_{max}(A)$, i.e.,

$$Aw_k \;=\; \lambda_1 w_k \;=\; \lambda_{max} w_k.$$

Since $||w_k|| = 1$, we conclude that

$$||Aw_k|| \;=\; \lambda_{max}||w_k|| \;=\; \lambda_{max},$$

which is the output of the Power Method algorithm.

9. Quadratic Forms

Lemma 9.1. *Let $A = (A(j,k))_{j,k=1:n}$ be a square matrix of size n, and let $x = (x_i)_{i=1:n}$ and $y = (y_i)_{i=1:n}$ be two column vectors of size n. Then*

$$y^t A x \;=\; \sum_{1\le j,k\le n} A(j,k) x_k y_j. \tag{80}$$

Proof. Let $A \;=\; \mathrm{col}\,(a_k)_{k=1:n}$ be the column form of A. Then,

$$Ax \;=\; \sum_{k=1:n} x_k a_k. \tag{81}$$

Since $a_k = (A(j,k))_{j=1:n}$, we find that

$$y^t a_k \;=\; \sum_{j=1}^{n} y_j A(j,k). \tag{82}$$

From (81) and (82) it follows that

$$\begin{aligned} y^t A x \;&=\; y^t \left(\sum_{k=1}^{n} x_k a_k \right) \;=\; \sum_{k=1}^{n} x_k (y^t a_k) \\ &=\; \sum_{k=1}^{n} x_k \left(\sum_{j=1}^{n} y_j A(j,k) \right) \\ &=\; \sum_{1\le j,k\le n} A(j,k) x_k y_j. \quad \square \end{aligned}$$

□

Definition 9.2. Let $A = (A(j,k))_{j,k=1:n}$ be a square matrix of size n. The quadratic form $q_A : \mathbb{R}^n \to \mathbb{R}$ associated with the matrix A is defined as

$$q_A(x) \;=\; x^t A x, \tag{83}$$

or, equivalently,

$$q_A(x) \;=\; \sum_{1\le j,k\le n} A(j,k) x_j x_k; \tag{84}$$

cf. (80) for $y = x$.

It is important to note that quadratic forms associated to different matrices can be the same.

Lemma 9.3. *Let A and B be square matrices of size n, and let q_A and q_B be the quadratic forms associated to A and B, respectively. Then*

$$q_A = q_B \quad\Longleftrightarrow\quad A + A^t = B + B^t. \tag{85}$$

Proof.

$$q_A(x) = q_B(x),\ \forall\ x \in \mathbb{R}^n$$

□

Lemma 9.4. *For any square matrix A of size n there exists a unique $n \times n$ symmetric matrix M such that*

$$q_A(x) = q_M(x),\ \forall\ x \in \mathbb{R}^n.$$

Proof. □

Lemma 9.5. *Let A be a square matrix of size n. Then*

$$D\left(q_A(x)\right) \;=\; D\left(x^t A x\right) \;=\; (A + A^t)x.$$

In particular, if A is a symmetric matrix, then

$$D\left(x^t A x\right) \;=\; 2Ax.$$

Proof. □

9.1. **Covariance and Correlation Matrices.**

Definition 9.6. The covariance matrix Σ_X of the random variables $(X_i)_{i=1:n}$ is the $n \times n$ matrix given by

$$\Sigma_X(j,k) \ = \ \text{cov}(X_j, X_k), \ \forall \ 1 \leq j,k \leq n,$$

where $\text{cov}(X_j, X_k)$ denotes the covariance of X_j and X_k.

The covariance matrix Σ_X is symmetric, since

$$\Sigma_X(j,k) \ = \ \text{cov}(X_j, X_k) \ = \ \text{cov}(X_k, X_j) \ = \ \Sigma_X(k,j), \ \forall \ 1 \leq j,k \leq n.$$

Also,

$$\Sigma_X(i,i) \ = \ \text{var}(X_i), \ \forall \ i = 1:n,$$

since, by definition, $\text{cov}(X_i, X_i) = \text{var}(X_i)$, for all $i = 1:n$.

Definition 9.7. The correlation matrix Ω_X of the random variables $(X_i)_{i=1:n}$ is the $n \times n$ matrix given by

$$\Omega_X(j,k) \ = \ \text{corr}(X_j, X_k), \ \forall \ 1 \leq j,k \leq n,$$

where $\text{corr}(X_j, X_k)$ denotes the correlation of X_j and X_k.

The correlation matrix Ω_X is symmetric, since

$$\Omega_X(j,k) \ = \ \text{corr}(X_j, X_k) \ = \ \text{corr}(X_k, X_j) \ = \ \Omega_X(k,j), \ \forall \ 1 \leq j,k \leq n.$$

Also,

$$\Omega_X(i,i) \ = \ 1, \ \forall \ i = 1:n,$$

since, $\text{corr}(X_i, X_i) = 1$, for all $i = 1:n$.

Lemma 9.8. *Let Σ_X and Ω_X be the covariance and the correlation matrix of the random variables $(X_i)_{i=1:n}$. Let σ_i be the standard deviation of X_i, for $i = 1:n$, and denote the diagonal matrix whose main diagonal entries are equal to σ_i by D_σ, i.e.,*

$$D_\sigma \ = \ diag(\sigma_i)_{i=1:n}.$$

Then,

$$\Sigma_X \ = \ D_\sigma \Omega_X D_\sigma. \tag{86}$$

Proof. □

Lemma 9.9. *Let $(X_i)_{i=1:n}$ be n random variables with covariance matrix Σ_X. Let $C = (c_i)_{i=1:n}$ be a column vector of size n. Then,*

$$var\left(\sum_{i=1}^{n} c_i X_i\right) \ = \ C^t \Sigma_X C. \tag{87}$$

Proof. □

Corollary 9.10. *Let Σ_X and Ω_X be the covariance and the correlation matrix of the random variables $(X_i)_{i=1:n}$.*

(i) The matrices Σ_X and Ω_X are symmetric semi-positive definite;

(ii) If the random variables $(X_i)_{i=1:n}$ are linearly independent, then Σ_X is a symmetric positive definite matrix.

Proof. □

Lemma 9.11. *Let Σ_X be the covariance matrix of n random variables $(X_i)_{i=1:n}$. Let $C^{(1)} = (c_i^{(1)})_{i=1:n}$ and $C^{(2)} = (c_i^{(2)})_{i=1:n}$ be two column vectors of size n. Then,*

$$cov\left(\sum_{i=1}^{n} c_i^{(1)} X_i, \sum_{i=1}^{n} c_i^{(2)} X_i\right) \ = \ (C^{(1)})^t \Sigma_X C^{(2)}. \tag{88}$$

Proof. □

Theorem 9.12. ***(Linear Transformation Property.)*** *Let $(X_i)_{i=1:n}$ be n random variables, and denote by Σ_X the covariance matrix of $(X_i)_{i=1:n}$. Let $(Y_i)_{i=1:n}$ be the random variables given by*

$$Y \;=\; M\;X,$$

where M is an $n \times n$ matrix, and denote by Σ_Y the covariance matrix of $(Y_i)_{i=1:n}$.

Then,

$$\Sigma_Y \;=\; M\Sigma_X M^t. \tag{89}$$

Proof. □

Definition 9.13.

Lemma 9.14.

Proof. □

Theorem 9.15.

Proof. □

9.2. **Symmetric Positive Definite Matrices.**

Definition 9.16. An $n \times n$ matrix A is symmetric positive definite (spd) if and only if the matrix A is symmetric and

$$x^t Ax \ > \ 0, \ \forall \ x \in \mathbb{R}^n, \ x \neq 0.$$

The matrix A is symmetric positive semidefinite if and only if the matrix A is symmetric and

$$x^t Ax \ \geq \ 0, \ \forall \ x \in \mathbb{R}^n.$$

There are several equivalent ways of defining an spd matrix – the most important being that all its eigenvalues are positive.

Theorem 9.17. *A matrix is symmetric positive definite if and only if the matrix is symmetric and all the eigenvalues of the matrix are strictly greater than zero, i.e.,*

$$A spd \quad \iff \quad A = A^t \text{ and } \lambda > 0, \ \forall \ \lambda \in \lambda(A).$$

A matrix is symmetric positive semidefinite if and only if the matrix is symmetric and all the eigenvalues of the matrix are greater than or equal to zero.

Proof. "A spd $\Rightarrow$ $A = A^t$ and the eigenvalues of A are positive"

If A is spd, then A is symmetric, i.e., $A = A^t$. Therefore, all the eigenvalues of A are real.

We give a proof by contradiction: assume that there exists an eigenvalue λ of A such that $\lambda \leq 0$. Let v be the corresponding eigenvector, i.e., $v \neq 0$ and $Av = \lambda v$. Then

$$v^t Av \ = \ v^t \lambda v \ = \ \lambda v^t v \ = \ \lambda ||v||^2 \ \leq \ 0,$$

which contradicts the fact that A is spd.

"$A = A^t$ and the eigenvalues of A are positive $\Rightarrow$ A spd"

All we have to prove is that $x^t Ax > 0$, if $x \neq 0$. Since A is symmetric, all the eigenvalues of A, denoted by $\lambda_1, \ \lambda_2, \ \ldots, \ \lambda_n$, are positive, and there exists an orthogonal matrix Q (the columns of Q are the eigenvectors of A) such that

$$A \ = \ Q \Lambda Q^t,$$

where Λ is the diagonal matrix with entries $\lambda_1, \ \lambda_2, \ \ldots, \ \lambda_n$; cf. Theorem 6.11. Then

$$x^t Ax \ = \ x^t Q \Lambda Q^t x \ = \ (Q^t x)^t \Lambda (Q^t x) \ = \ y^t \Lambda y,$$

where $y = Q^t x$. If $y = (y_i)_{i=1:n}$, then

$$x^t Ax \ = \ y^t \Lambda y \ = \ \sum_{i=1}^{n} \lambda_i y_i^2 \ \geq \ 0,$$

since all the eigenvalues of A are positive, i.e., $\lambda_i > 0, \ \forall \ i = 1 : n$. Note that

$$x^t Ax = 0 \iff y_i = 0, \ \forall \ i = 1 : n \iff y = 0 \iff Q^t x = 0 \iff x = 0,$$

since Q is orthogonal and $x = QQ^t x = 0$.

Thus $x^t Ax > 0$ if $x \neq 0$ and therefore A is spd. $\square$ $\square$

Theorem 9.18. *NEEDED??? A spd $\iff$ $B^t AB$ is spd for every nonsingular matrix B; A spd $\iff$ $\exists$ U upper triangular, nonsingular and with positive entries on the main diagonal, such that $A = U^t U$.*

Proof. "$B^t AB$ is spd for every nonsingular matrix B $\Rightarrow$ A spd"

Let $B = I$, the identity matrix. Then $B^t AB = A$ is spd.

"A spd $\Rightarrow$ $B^t AB$ is spd for every nonsingular matrix B"

Let B nonsingular and $M = B^tAB$. We first show that M symmetric, i.e., $M^t = M$. From Lemma 1.6 we find that

$$M^t \;=\; (B^tAB)^t \;=\; B^tA^t(B^t)^t \;=\; B^tAB \;=\; M.$$

We also need to prove that $x^tMx \geq 0$. Let $x \in \mathbb{R}^n$ arbitrary, and let $y = Bx$. Then $y^tAy \geq 0$, since A is spd, and therefore

$$y^tAy \;=\; (Bx)^tABx \;=\; x^tB^tABx \;=\; x^tMx \;\geq\; 0,\ \forall\ x \in \mathbb{R}^n.$$

Also, since A is spd, $x^tMx = 0 \iff y^tAy = 0 \iff y = 0$. Then $y = Bx = 0$, and, since B is nonsingular, $x = B^{-1}Bx = 0$.

This completes the proof of the fact that $M = B^tAB$ is spd.

Proof of (3): this is called the Cholesky decomposition of A and will be discussed in great algorithmic and theoretical detail in the Numerical Linear Algebra class. □

Theorem 9.19. *A symmetric, strictly diagonally dominant matrix with positive entries on the main diagonal is symmetric positive definite.*

A symmetric, diagonally dominant matrix with positive entries on the main diagonal is symmetric positive semidefinite.

Proof. Recall from Theorem 4.17 that the eigenvalues of every symmetric, strictly diagonally dominant matrix are strictly greater than 0, while the eigenvalues of every symmetric, diagonally dominant matrix are greater than or equal 0.

Then, the following results follows from Theorem 9.17: □

10. The Relevance of the Condition Number

Assume that we want to solve the linear system $Ax = b$ numerically and we have an algorithm to do it. (We will learn about, and implement some, efficient algorithms for solving $Ax = b$, e.g., LU and Cholesky algorithms, in the Numerical Linear Algebra class.) The first thing to note is that when you input A and b in your code, a roundoff error is most likely generated right away: the entries of A and b are stored in floating point format as $\widetilde{A}$ and $\widetilde{b}$, and the error factors δA and δb are introduced, i.e.,

$$\begin{aligned} A \quad \text{is stored as } \widetilde{A} &= A + \delta A \\ b \quad \text{is stored as } \widetilde{b} &= b + \delta b. \end{aligned}$$

This error is called the roundoff error, and its order is, for most vectors and matrices, the smallest possible, i.e., on the order of ϵ_m (epsilon machine, approximately equal to 10^{-16} for double precision machines), i.e.,

$$\frac{||\delta A||}{||A||} = O(\epsilon_m) \tag{90}$$

$$\frac{||\delta b||}{||b||} = O(\epsilon_m) \tag{91}$$

Even if the linear system $Ax = b$ were solved exactly, the fact that A and b are not represented exactly would generate an approximate value for x as the output of a numerical code. Let us denote that approximate value by $\widetilde{x} = x + \delta x$. Note that, in general, the method employed to solve $Ax = b$ generates another error itself. What we want is to find out what is the order of the relative error, i.e., $||\delta x||/||x||$, in terms of the epsilon machine (ϵ_m). Ideally, for an optimal algorithm, the relative error should be on the order of the epsilon machine, i.e.,

$$\frac{||\delta x||}{||x||} = O(e_m).$$

Recall that $\widetilde{x} = x + \delta x$ is the output of the algorithm used to solve $Ax = b$. Taking the roundoff errors for A and b into account, we find that $\widetilde{x}$ satisfies an equation of the form $\widetilde{A}\widetilde{x} = \widetilde{b}$, which can be written as

$$(A + \delta A)(x + \delta x) = Ax + (\delta A)x + A(\delta x) + \delta A\ \delta x = b + \delta b.$$

The term $\delta A\ \delta x$ can be neglected, since it is much smaller than the rest of the terms. Also, note that $Ax = b$, since x denotes the exact solution of the linear system. Therefore, we find that

$$(\delta A)x + A(\delta x) \approx \delta b.$$

By solving for δx we obtain

$$\delta x \approx -A^{-1}(\delta A)x + A^{-1}\delta b.$$

By taking the norms in the formula above and using Lemma 7.8 repeatedly, we find that

$$||\delta x|| \leq ||A^{-1}||\ ||\delta A||\ ||x|| + ||A^{-1}||\ ||\delta b||.$$

Dividing by $||x||$ and highlighting the error terms of order ϵ_m, i.e., $||\delta A||/||A||$ and $||\delta b||/||b||$, we obtain

$$\begin{aligned} \frac{||\delta x||}{||x||} &\leq ||A^{-1}||\ ||A||\ \frac{||\delta A||}{||A||} + \frac{1}{||x||}||A^{-1}||\ ||b||\ \frac{||\delta b||}{||b||} \\ &= cond(A)\ \frac{||\delta A||}{||A||} + ||A^{-1}||\frac{||b||}{||x||}\ \frac{||\delta b||}{||b||}. \end{aligned} \tag{92}$$

Recall that $b = Ax$. From Lemma 7.8, we find that $||b|| = ||Ab|| \leq ||A||\ ||x||$, and therefore

$$||A^{-1}||\frac{||b||}{||x||} \leq ||A^{-1}||\ ||A|| = cond(A). \tag{93}$$

From (92) and (93), we conclude that

$$\frac{||\delta x||}{||x||} \;\leq\; cond(A)\;\frac{||\delta A||}{||A||} \;+\; cond(A)\;\frac{||\delta b||}{||b||} \;=\; cond(A)O(\epsilon_m),$$

since the roundoff error for both A and b was assumed to be of order ϵ_m; cf. (90) and (91).

In other words, the relative error for the solution of the linear system $Ax = b$ depends linearly on the condition number of the matrix A. This shows that, as a general rule, it is desirable to work with well–conditioned matrices with small condition number rather than with ill–conditioned matrices.

11. One Period Market Models

Consider a market with m securities. Let S_{1t_0}, S_{2t_0}, ..., S_{mt_0} be the spot prices of the securities at time t_0, and denote by S_{t_0} the price vector of the securities at time t_0, i.e.,

$$S_{t_0} \;=\; \begin{pmatrix} S_{1t_0} \\ S_{2t_0} \\ \vdots \\ S_{mt_0} \end{pmatrix}.$$

Note that S_{t_0} is an $m \times 1$ column vector.

At time $\tau > t_0$, we assume that there are n possible states of the market, denoted by ω^1, ω^2, ..., ω^n. For $i = 1:n$ and $j = 1:m$, let $S^i_{j\tau}$ be the price at time τ of asset j if state ω^i occurs. Let S^i_τ be the price vector of the m assets if state ω^i occurs, i.e,

$$S^i_\tau \;=\; \begin{pmatrix} S^i_{1\tau} \\ S^i_{2\tau} \\ \vdots \\ S^i_{m\tau} \end{pmatrix},\; i = 1:n, \tag{94}$$

and let $S_{j\tau}$ be the vector of all possible prices of asset j at time τ, i.e,

$$S_{j\tau} \;=\; \left(S^1_{j\tau}\; S^2_{j\tau}\; \ldots\; S^n_{j\tau}\right),\; j = 1:m. \tag{95}$$

Note that S^i_τ is an $m \times 1$ column vector, and $S_{j\tau}$ is an $1 \times n$ row vector, for $i = 1:n$ and for $j = 1:m$, respectively.

The payoff matrix M_τ is the $m \times n$ matrix made of all possible prices of the assets at time τ, with the j-th row of matrix M_τ corresponding to the prices of asset j, $j = 1:m$, and the i-th column of matrix M_τ corresponding to the asset prices in state ω^i, $i = 1:n$, i.e.,

$$M_\tau \;=\; \left(S^1_\tau \mid S^2_\tau \mid \ldots \mid S^n_\tau\right) \;=\; \begin{pmatrix} S_{1\tau} \\ ---- \\ S_{2\tau} \\ ---- \\ \vdots \\ ---- \\ S_{m\tau} \end{pmatrix}.$$

The m securities are non–redundant if their price vectors at time τ are linearly independent. Otherwise, the payoff of one of the securities would be replicable by using the other $m-1$ securities, which would render the security redundant. We note that no redundant securities exist in a one period market model if and only if the payoff matrix M_τ is full row rank, i.e., that

$$\text{row rank}(M_\tau) \;=\; m.$$

Consider a portfolio made of the m securities, consisting of Θ_j units of asset j at time t_0. Let $\Theta = (\Theta_j)_{j=1:m}$ be the $m \times 1$ positions vector. The value V_{t_0} of the portfolio at time t_0 is

$$V_{t_0} \;=\; \sum_{j=1}^{m} \Theta_j S_{jt_0},$$

which can be written in matrix form as

$$V_{t_0} \;=\; \Theta^t S_{t_0}.$$

We assume that the asset positions in the portfolio remain unchanged[1] until time τ. Let V_τ the $n \times 1$ row vector of the possible values of the portfolio at time τ, where $V_\tau(i)$ is the value of the

[1]This does not imply, though, that the weights of each asset in the portfolio remain unchanged.

portfolio if state ω^i occurs, $i = 1 : n$. Then

$$V_\tau(i) \;=\; \sum_{j=1}^{m} \Theta_j S^i_{j\tau} \;=\; \Theta^t S^i_\tau$$

and therefore

$$\begin{aligned} V_\tau &= (V_\tau(1)\; V_\tau(2)\; \ldots\; V_\tau(n)) \\ &= \left(\Theta^t S^1_\tau \mid \Theta^t S^2_\tau \mid \ldots \mid \Theta^t S^n_\tau\right) \\ &= \Theta^t \left(S^1_\tau \mid S^2_\tau \mid \ldots \mid S^n_\tau\right) \\ &= \Theta^t M_\tau. \end{aligned}$$

Definition 11.1. A derivative security is called replicable in a market model with m securities and n market states at time $\tau > t_0$ if there exists a portfolio made of the m securities which has the same values at time τ as the derivative security regardless of the state the market is at time τ.

In other words, if s_τ is the price vector at time τ of the replicable derivative security, then there exists a positions vector Θ such that

$$s_\tau \;=\; \Theta^t M_\tau, \tag{96}$$

where M_τ is the payoff matrix at time τ corresponding to the m securities.

Note that, if $\Theta = (\Theta_j)_{j=1:m}$, then

$$\Theta^t M_\tau \;=\; \sum_{j=1}^{m} \Theta_j S_{j\tau}, \tag{97}$$

where $S_{j\tau}$ is the price vector of asset j at time τ; cf. (95).

From (96) and (97) it follows that a derivative security is replicable in a market model with m securities and n market states at time $\tau > t_0$ if and only if the price vector of the derivative security at time τ belongs to the space generated by the price vectors of the m securities at time τ.

To decide if arbitrage opportunities exist in a one period market model, recall the Law of One Price:

Theorem 11.2. *If two portfolios are guaranteed to have the same value at a future time $\tau > t$ regardless of the state of the market at time τ, then they must have the same value at time t.*

If there exists $\tau > t$ such that $V_1(\tau) = V_2(\tau)$ for any state of the market at time τ, then $V_1(t) = V_2(t)$.

The following result can be obtained from Theorem 11.2:

Lemma 11.3. *If the value $V(\tau)$ of a portfolio at time τ in the future is independent of the state of the market at time τ, then*

$$V(t) \;=\; V(\tau)\; e^{-r(\tau - t)}, \tag{98}$$

where $t < \tau$ and r is the risk free rate assumed to be constant between t and τ.

For more details on the Law of One Price and on deriving Lemma 11.3 from Theorem 11.2, see section 1.8 of ???.

Lemma 11.4. *Let s_τ be the price vector at time τ of a derivative security which is replicable in a market model with m securities and n market states at time $\tau > t_0$, and let Θ be the positions vector of the m securities in the portfolio which replicates the security. Then, the no–arbitrage price s_{t_0} at time t_0 of the replicable security is*

$$s_{t_0} \;=\; \Theta^t S_{t_0}, \tag{99}$$

where $S_{t_0} = (S_{jt_0})_{j=1:m}$ is the price vector of the m securities at time t_0.

Proof. Recall that $s_\tau = \Theta^t M_\tau$; cf. (96). Then, from the Law of One Price (Theorem 11.2), it follows that, for no–arbitrage, the value s_{t_0} at time t_0 of the replicable derivative security must be the same as the value of the replicating portfolio at time t_0, which is $\Theta^t S_{t_0}$. □

11.1. **Arbitrage–free markets.** Arbitrage opportunities arise when investment strategies that generate profit with no risk exist. For a one period market model with m securities and n market states, such arbitrage opportunities occur in either one of the two following instances:

(I). If there exists a portfolio with value 0 at time t_0 (i.e., with no set–up cost at time t_0) and with nonnegative values in every state of the market at time τ (and with at least one value strictly greater than 0); in other words, if there exists an $m \times 1$ positions vector Θ and a state k, $1 \leq k \leq n$, such that

$$V_{t_0} = \Theta^t S_{t_0} = 0 \quad \text{and} \quad V_\tau(i) = \Theta^t S_\tau^i \geq 0, \ \forall \ i = 1 : n, \quad \Theta^t S_\tau^k > 0. \tag{100}$$

(II). If there exists a portfolio with negative value at time t_0 (i.e., with negative set–up cost and therefore generating a positive cash flow at time t_0) and with nonnegative values in every state of the market at time τ; in other words, if there exists an $m \times 1$ positions vector Θ such that

$$V_\tau(i) = V_{t_0} = \Theta^t S_{t_0} < 0 \quad \text{and} \quad \Theta^t S_\tau^i \geq 0, \ \forall \ i = 1 : n. \tag{101}$$

The following result gives necessary and sufficient conditions for a one period market model to be arbitrage–free:

Theorem 11.5. *A one period market model with m securities and n market states is arbitrage–free if and only if there exist positive numbers (also called state prices[2]) $Q^i > 0$, $i = 1 : n$, such that*

$$S_{t_0} \ = \ M_\tau Q, \tag{102}$$

where $Q = (Q^i)_{i=1:n}$, S_{t_0} is the price vector of the m securities at time t_0, and M_τ is the payoff matrix at time τ.

The proof of this theorem involves the Fundamental Theorem of Linear Programming, which, loosely speaking, states that if a set of linear inequalities implies another set of linear inequalities, then it does so trivially, i.e., by linear combinations. The strength of the result of Theorem 11.5 is given by the fact that the entries of the vector Q from (102) are strictly positive.

While the proof of Theorem 11.5 is beyond our scope here, we will establish the sufficiency of condition (102) for a non–arbitrage market model to be arbitrage–free.

Assume that there exists a vector $Q = (Q^i)_{i=1:n}$ such that $Q^i > 0$, $i = 1 : n$, and $S_{t_0} = M_\tau Q$.

An arbitrage of type (I) occurs if there exists an $m \times 1$ positions vector Θ and a state k, $1 \leq k \leq n$, such that $\Theta^t S_{t_0} = 0$, $\Theta^t S_\tau^k > 0$ and $\Theta^t S_\tau^i \geq 0$ for all $i = 1 : n$; cf. (100). Then,

$$\Theta^t S_{t_0} \ = \ \Theta^t M_\tau Q \ = \ \left(\Theta^t S_\tau^1 \ \Theta^t S_\tau^2 \ \ldots \ \Theta^t S_\tau^n\right) Q \ = \ \sum_{i=1:n} Q^i \Theta^t S_\tau^i. \tag{103}$$

Note that $\Theta^t S_\tau^k > 0$. Since $Q^i > 0$ and $\Theta^t S_\tau^i \geq 0$ for all $i = 1 : n$, it follows from (103) that

$$\Theta^t S_{t_0} \ = \ \sum_{i=1:n} Q^i \Theta^t S_\tau^i \ \geq \ Q^k \Theta^t S_\tau^k \ > \ 0.$$

This contradicts the assumption $\Theta^t S_{t_0} = 0$ from the no–arbitrage condition.

An arbitrage of type (II) occurs if there exists an $m \times 1$ positions vector Θ such that $\Theta^t S_{t_0} < 0$ and $\Theta^t S_\tau^i \geq 0$ for all $i = 1 : n$; cf. (101). However, since $S_{t_0} = M_\tau Q$ and $\Theta^t S_\tau^i \geq 0$ for all $i = 1 : n$, we find that

$$\Theta^t S_{t_0} \ = \ \Theta^t M_\tau Q \ = \ \sum_{i=1:n} Q^i \Theta^t S_\tau^i \ = \ 0,$$

which contradicts the assumption that $\Theta^t S_{t_0} < 0$.

---

[2]See section 11.3 for an explanation of this nomenclature.

Lemma 11.6. *Consider an arbitrage–free one period market model with m securities and n market states, and let $Q^i > 0$, $i = 1 : n$, denote the state prices. Let s_τ be the $1 \times n$ price vector at time τ of a replicable security. Then, the value s_{t_0} at time t_0 of the replicable security can be obtained as*

$$s_{t_0} \;=\; s_\tau Q, \tag{104}$$

where $Q = (Q^i)_{i=1:n}$.

Proof. If the derivative security is replicable, then there exists a portfolio made of the m securities which has the same values at time τ as the derivative security regardless of the state the market is at time τ. Let Θ be the $m \times 1$ positions vector of the replicating portfolio. Then,

$$s_\tau \;=\; \Theta^t M_\tau, \tag{105}$$

where M_τ is the payoff matrix of the m securities at time τ; cf. (96).

Since there are no arbitrage opportunities, it follows from Lemma 11.4 that the replicable security and the replicating portfolio have the same value at time t_0, i.e.,

$$s_{t_0} \;=\; \Theta^t S_{t_0}, \tag{106}$$

where $S_{t_0} = (S_{jt_0})_{j=1:m}$ is the price vector of the m securities at time t_0; cf. (99).

Since the market is arbitrage–free, it follows from Theorem 11.5 that a vector $Q = (Q^i)_{i=1:n}$ with positive entries $Q^i > 0$, $i = 1 : n$, such that

$$S_{t_0} \;=\; M_\tau Q; \tag{107}$$

cf. (102). From (105), (106) and (107), we conclude that

$$s_{t_0} \;=\; \Theta^t S_{t_0} \;=\; \Theta^t M_\tau Q \;=\; s_\tau Q,$$

which is what we wanted to show; cf. (104). □

11.2. **Complete markets and risk–neutral pricing.**

Definition 11.7. A one period market model with m securities and n market states is complete if and only if any cash flow at time τ can be replicated using a portfolio made of the m securities. In other words, for any $1 \times n$ payoff vector C_τ there exists an $m \times 1$ positions vector Θ such that

$$C_\tau \;=\; \Theta^t M_\tau. \tag{108}$$

Theorem 11.8. *A one period market model with m securities and n market states is complete if and only if the market contains n non–redundant securities, i.e., if and only if the row rank of the payoff matrix M_τ is equal to n, the number of possible states at time τ.*

A consequence of Theorem 11.8 is that a complete market must contain at least as many securities as possible states in the future, i.e., that $m \geq n$, which is a natural requirement.

Proof. From (108) it follows that a market is complete if and only if the linear system

$$C_\tau \;=\; \Theta^t M_\tau \tag{109}$$

has a solution $\Theta \in \mathbb{R}^{m\times 1}$ for any vector $C_\tau \in \mathbb{R}^{1\times n}$. Note that

$$\left\{\Theta^t M_\tau \mid \Theta \in \mathbb{R}^{m\times 1}\right\} \;=\; \left\{\sum_{j=1}^{m} \Theta_j S_{j\tau} \mid \Theta_j \in \mathbb{R}\right\},$$

where $S_{j\tau}$ is the price vector of asset j at time τ, $j = 1 : m$.

Then, the system (109) has a solution for any $C_\tau \in \mathbb{R}^{1\times n}$ if and only if

$$\mathbb{R}^{1\times n} \;=\; \left\{\sum_{j=1}^{m} \Theta_j S_{j\tau} \mid \Theta_j \in \mathbb{R}\right\},$$

which happens if there are exactly n linearly independent vectors among the price vectors $S_{j\tau}$, $j = 1 : m$, of the m securities (and therefore if there exist exactly n non–redundant securities). □

If a market is both complete and arbitrage–free, it follows from Lemma 11.6 that the value V_{t_0} at time t_0 of a derivative security with payoff vector $V_\tau = (V_\tau(i))_{i=1:n}$ at time τ can be computed as

$$V_{t_0} \;=\; V_\tau Q, \;=\; \sum_{i=1}^{n} V_\tau(i) Q^i, \tag{110}$$

where $Q = (Q^i)_{i=1:n}$ is the vector of state prices; cf. (104).

Recall that $Q^i > 0$ for all $i = 1 : n$. We can then normalize each state price Q^i to obtained a discrete probability function $p_{RN}(i)$ associated to each state ω^i of the market at time τ as follows:

$$p_{RN}(i) \;=\; \frac{Q^i}{\sum_{k=1}^{n} Q^k}, \;\forall\; i = 1 : n. \tag{111}$$

It is easy to see that $p_{RN}(i) > 0$ for all $i = 1 : n$, and that

$$\sum_{i=1}^{n} p_{RN}(i) \;=\; 1.$$

These probabilities are called the risk–neutral probabilities associated with each state of the market at time τ, and are independent of the actual probabilities of each state occurring.

Often, one of the assets in the one period market model is cash (or, equivalently, a zero coupon with maturity τ). Assume that asset 1 is USD 1 cash at time t_0. Assume that the risk free rate is constant equal to r between time t_0 and τ. Then,

$$S_{1t_0} = 1 \quad \text{and} \quad S^i_{1\tau} = e^{r(\tau - t_0)}, \;\forall\; i = 1 : n.$$

From the first row of the no–arbitrage condition (102), i.e., from $S_{t_0} = M_\tau Q$, we find that

$$S_{1t_0} \;=\; \sum_{i=1}^{n} S^i_{1\tau} Q^i,$$

which can be written as

$$1 \;=\; \sum_{i=1}^{n} e^{r(\tau - t_0)} Q^i.$$

Therefore,

$$\sum_{i=1}^{n} Q^i = e^{-r(\tau - t_0)} \tag{112}$$

From (110), (111), and (112), we find that

$$\begin{aligned} V_{t_0} \;&=\; \sum_{i=1}^{n} V_\tau(i) Q^i \\ &=\; \left(\sum_{k=1}^{n} Q^k \right) \sum_{i=1}^{n} p_{RN}(i) V_\tau(i) \\ &=\; e^{-r(\tau - t_0)} E_{RN}\left[V_\tau(i) \right], \end{aligned}$$

where $E_{RN}\left[V_\tau(i)\right] = \sum_{i=1}^{n} p_{RN}(i) V_\tau(i)$ is the expected value in the risk–neutral distribution p_{RN} of the payoff V_τ of the derivative security.

The following result was therefore established:

Theorem 11.9. *Consider a complete and arbitrage–free one period market model with m securities and n market states at time $\tau > t_0$. Assume one of the assets is cash, and define the risk–neutral probability p_{RN} associated to each state of the market at time τ by*

$$p_{RN}(i) \;=\; e^{r(\tau - t_0)} Q^i, \;\forall\; i = 1 : n,$$

where r is the constant risk–free interest rate. Then, the value V_{t_0} at time t_0 of a derivative security is the discounted risk–neutral expected value of its payoff V_τ at time τ, i.e.,

$$V_{t_0} \;=\; e^{-r(\tau-t_0)}E_{RN}\left[V_\tau(i)\right] \;=\; e^{-r(\tau-t_0)}\sum_{i=1}^{n} p_{RN}(i)V_\tau(i). \tag{113}$$

11.3. **State prices.** We are now in a position to explain why the values $Q^i > 0$, $i = 1 : n$, which appeared in the condition (102) for a one period market model to be arbitrage–free are called state prices.

Consider a derivative security which pays \$1 if state k occurs at time τ and 0 otherwise. (This is essentially an insurance contract that pays off if state k occurs, and is worthless otherwise.) In other words, if $C_{k\tau}$ is the $n \times 1$ price vector of this insurance contract at time τ, then

$$C_{k\tau}(i) = 0,\ \forall\ 1 \le i \ne k \le n \quad \text{and} \quad C_{k\tau}(k) = 1.$$

Let C_{kt_0} be the value of this insurance contract at time t_0.

If the market is complete and arbitrage–free, it follows from (110) that the value of the insurance contract is

$$C_{kt_0} \;=\; \sum_{i=1}^{n} C_{k\tau}(i)Q^k \;=\; Q^k.$$

We conclude that, for any $k = 1 : n$, Q^k is the price of the insurance contract paying \$1 if state k occurs, which can also be regarded as the price at time t_0 of state k occuring at time τ.