

The Moore–Penrose Pseudoinverse: A Tutorial Review of the Theory

João Carlos Alves Barata · Mahir Saleh Hussein

Received: 27 October 2011 / Published online: 16 December 2011
© Sociedade Brasileira de Física 2011

Abstract In the last decades, the Moore–Penrose pseudoinverse has found a wide range of applications in many areas of science and became a useful tool for physicists dealing, for instance, with optimization problems, with data analysis, with the solution of linear integral equations, etc. The existence of such applications alone should attract the interest of students and researchers in the Moore–Penrose pseudoinverse and in related subjects, such as the singular value decomposition theorem for matrices. In this note, we present a tutorial review of the theory of the Moore–Penrose pseudoinverse. We present the first definitions and some motivations, and after obtaining some basic results, we center our discussion on the spectral theorem and present an algorithmically simple expression for the computation of the Moore–Penrose pseudoinverse of a given matrix. We do not claim originality of the results. We rather intend to present a complete and self-contained tutorial review, useful for those more devoted to applications, for those more theoretically oriented, and for those who already have some working knowledge of the subject.

Keywords Moore–Penrose pseudoinverse · Singular values decomposition

J. C. A. Barata (✉) · M. S. Hussein
Instituto de Física, Universidade de São Paulo, C.P. 66318,
05314-970 São Paulo, São Paulo, Brazil
e-mail: jbarata@fma.if.usp.br

M. S. Hussein
e-mail: hussein@if.usp.br

1 Introduction, Motivation, and Notation

In this paper, we present a self-contained review of some of the basic results on the so-called Moore–Penrose pseudoinverse of matrices, a concept that generalizes the usual notion of inverse of a square matrix, but that is also applicable to singular square matrices or even to non-square matrices. This notion is particularly useful in dealing with certain linear least squares problems, as we shall discuss in Section 6, i.e., problems where one searches for an optimal approximation for solutions of linear equations like $Ax = y$, where A is a given $m \times n$ matrix, y is a given column vector with m components, and the unknown x , a column vector with n components, is the searched solution. In many situations, a solution is non-existing or non-unique, but one asks for a vector x such that the norm of the difference $Ax - y$ is the smallest possible (in terms of least squares).

Let us be a little more specific. Let $A \in \text{Mat}(\mathbb{C}, m, n)$ (the set of all complex $m \times n$ matrices) and $y \in \mathbb{C}^m$ be given and consider the problem of finding $x \in \mathbb{C}^n$ satisfying the linear equation

$$Ax = y. \quad (1)$$

If $m = n$ and A has an inverse, the (unique) solution is, evidently, $x = A^{-1}y$. In other cases the solution may not exist or may not be unique. We can, however, consider the alternative problem of finding the set of all vectors $x' \in \mathbb{C}^n$ such that the Euclidean norm $\|Ax' - y\|$ reaches its least possible value. This set is called the *minimizing set* of the linear problem (1). Such vectors $x' \in \mathbb{C}^n$ would be the best approximants for the solution of (1) in terms of the Euclidean norm, i.e., in terms of “least squares.” As we will show in Theorem 6.1,

the Moore–Penrose pseudoinverse provides this set of vectors x' that minimize $\|Ax' - y\|$: It is the set

$$\{A^+y + (\mathbb{1}_n - A^+A)z, z \in \mathbb{C}^n\}, \tag{2}$$

where $A^+ \in \text{Mat}(\mathbb{C}, n, m)$ denotes the Moore–Penrose pseudoinverse of A . An important question for applications is to find a general and algorithmically simple way to compute A^+ . The most common approach uses the singular values decomposition and is described in “Appendix 2.” Using the spectral theorem and Tikhonov’s regularization method, we show that A^+ can be computed by the algorithmically simpler formula

$$A^+ = \sum_{\substack{b=1 \\ \beta_b \neq 0}}^s \frac{1}{\beta_b} \left(\prod_{\substack{l=1 \\ l \neq b}}^s (\beta_b - \beta_l)^{-1} \right) \times \left[\prod_{\substack{l=1 \\ l \neq b}}^s (A^*A - \beta_l \mathbb{1}_n) \right] A^*, \tag{3}$$

where A^* denotes the adjoint matrix of A and $\beta_k, k = 1, \dots, s$, are the distinct eigenvalues of A^*A . See Theorem 5.1 for a more detailed statement. One of the aims of this paper is to present a proof of (3) by combining the spectral theorem with the a regularization procedure due to Tikhonov [1, 2].

1.1 Some Applications of the Moore–Penrose Pseudoinverse

Problems involving the determination of the minimizing set of (1) are always present when the number of unknowns exceeds the number of values provided by measurements. Such situations occur in many areas of Applied Mathematics, Physics, and Engineering, ranging from imaging methods, such as magnetic resonance imaging (MRI) [3–5], functional MRI [6, 7], positron emission tomography [8, 9], and magnetic source imaging [10–12] to seismic inversion problems [13, 14].

The Moore–Penrose pseudoinverse and/or the singular values decomposition (SVD) of matrices (discussed in “Appendix 2”) are also employed in data analysis, as in the treatment of electroencephalographic source localization [15] and in the so-called principal component analysis. Applications of this last method to astronomical data analysis can be found in [16–19], and applications to gene expression analysis can be found in [20, 21]. Image compression algorithms using SVD are known at least since [22], and digital image restoration using the Moore–Penrose pseudoinverse has been studied in [23, 24].

Problems involving the determination of the minimizing set of (1) also occur, for instance, in certain numerical algorithms for finding solutions of linear Fredholm integral equations of the first kind:

$$\int_a^b k(x, y)u(y) dy = f(x),$$

where $-\infty < a < b < \infty$ and where k and f are given functions. See Section 4 for a further discussion of this issue. For an introductory account on integral equations, rich in examples and historical remarks, see [25].

Even this short list of applications should convince a student of Physics or Applied Mathematics of the relevance of the Moore–Penrose pseudoinverse and related subjects, and our main objective is to provide a self-contained introduction to the required theory.

1.2 Organization

In Section 2, we present the definition of the Moore–Penrose pseudoinverse and obtain its basic properties. In Section 3, we further develop the theory of the Moore–Penrose pseudoinverses. In Section 4, we describe Tikhonov’s regularization method for the computation of Moore–Penrose pseudoinverses and present a first proof of existence. Section 5 collects the previous results and derives expression (3), based on the spectral theorem, for the computation of Moore–Penrose pseudoinverses. This expression is algorithmically simpler than the usual method based on the singular values decomposition (described in “Appendix 2”). In Section 6, we show the relevance of the Moore–Penrose pseudoinverse for the solution of linear least squares problems, its main motivation. In “Appendix 1,” we present a self-contained review of the results on linear algebra and Hilbert space theory, not all of them elementary, that we need in the main part of this paper. In “Appendix 2,” we approach the existence problem of the Moore–Penrose pseudoinverse by using the usual singular values decomposition method.

1.3 Notation and Preliminary Definitions

In the following, we fix the notation utilized throughout the paper. We denote \mathbb{C}^n the vector space of all n -tuples of complex numbers: $\mathbb{C}^n := \left\{ \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \right\}$, with $z_k \in \mathbb{C}$ for all $k = 1, \dots, n$. We denote the usual scalar

product in \mathbb{C}^n by $\langle \cdot, \cdot \rangle_{\mathbb{C}}$ or simply by $\langle \cdot, \cdot \rangle$, where for $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \in \mathbb{C}^n$ and $w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{C}^n$, we have

$$\langle z, w \rangle_{\mathbb{C}} \equiv \langle z, w \rangle := \sum_{k=1}^n \overline{z_k} w_k.$$

Note that this scalar product is linear in the second argument and anti-linear in the first, in accordance with the convention adopted in Physics. Two vectors u and $v \in \mathbb{C}^n$ are said to be orthogonal according to the scalar product $\langle \cdot, \cdot \rangle$ if $\langle u, v \rangle = 0$. If $W \subset \mathbb{C}^n$ is a subspace of \mathbb{C}^n , we denote by W^\perp the subspace of \mathbb{C}^n composed by all vectors orthogonal to all vectors of W . The usual norm of a vector $z \in \mathbb{C}^n$ will be denoted by $\|z\|_{\mathbb{C}}$ or simply by $\|z\|$ and is defined by $\|z\|_{\mathbb{C}} \equiv \|z\| = \sqrt{\langle z, z \rangle}$. It is well known that \mathbb{C}^n is a Hilbert space with respect to the usual scalar product.

The set of all complex $m \times n$ matrices (m rows and n columns) will be denoted by $\text{Mat}(\mathbb{C}, m, n)$. The set of all square $n \times n$ matrices with complex entries will be denoted by $\text{Mat}(\mathbb{C}, n)$.

The identity matrix will be denoted by $\mathbb{1}$. Given $A \in \text{Mat}(\mathbb{C}, m, n)$, we denote by A^T the element of $\text{Mat}(\mathbb{C}, n, m)$ whose matrix elements are $(A^T)_{ij} = A_{ji}$ for all $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$. The matrix A^T is said to be the transpose of A . It is evident that $(A^T)^T = A$ and that $(AB)^T = B^T A^T$ for all $A \in \text{Mat}(\mathbb{C}, m, n)$ and $B \in \text{Mat}(\mathbb{C}, n, p)$.

If $A \in \text{Mat}(\mathbb{C}, m, n)$, then its adjoint $A^* \in \text{Mat}(\mathbb{C}, n, m)$ is defined as the matrix whose matrix elements $(A^*)_{ij}$ are given by $\overline{A_{ji}}$ for all $0 \leq i \leq n$ and $0 \leq j \leq m$.

Given a set $\alpha_1, \dots, \alpha_n$ of complex numbers, we denote by $\text{diag}(\alpha_1, \dots, \alpha_n) \in \text{Mat}(\mathbb{C}, n)$ the diagonal matrix whose k -th diagonal entry is α_k :

$$(\text{diag}(\alpha_1, \dots, \alpha_n))_{ij} = \begin{cases} \alpha_i, & \text{for } i = j, \\ 0, & \text{for } i \neq j. \end{cases}$$

The spectrum of a square matrix $A \in \text{Mat}(\mathbb{C}, n)$ coincides with the set of its eigenvalues (see the definitions in “Appendix 1”) and will be denoted by $\sigma(A)$.

We denote by $\mathbb{0}_{a,b} \in \text{Mat}(\mathbb{C}, a, b)$ the $a \times b$ matrix whose matrix elements are all zero. We denote by $\mathbb{1}_l \in \text{Mat}(\mathbb{C}, l)$ the $l \times l$ identity matrix. If no danger of confusion is present, we will simplify the notation and write $\mathbb{0}$ and $\mathbb{1}$ instead of $\mathbb{0}_{a,b}$ and $\mathbb{1}_l$, respectively. We will also employ the following

definitions: for $m, n \in \mathbb{N}$, let $I_{m, m+n} \in \text{Mat}(\mathbb{C}, m, m+n)$ and $J_{m+n, n} \in \text{Mat}(\mathbb{C}, m+n, n)$ be given by

$$I_{m, m+n} := (\mathbb{1}_m \ \mathbb{0}_{m, n}) \quad \text{and} \quad J_{m+n, n} := \begin{pmatrix} \mathbb{1}_n \\ \mathbb{0}_{m, n} \end{pmatrix}. \tag{4}$$

The corresponding transpose matrices are

$$\begin{aligned} (I_{m, m+n})^T &:= \begin{pmatrix} \mathbb{1}_m \\ \mathbb{0}_{n, m} \end{pmatrix} = J_{m+n, m} \quad \text{and} \\ (J_{m+n, n})^T &:= (\mathbb{1}_n \ \mathbb{0}_{n, m}) = I_{n, m+n}. \end{aligned} \tag{5}$$

The following useful identities will be used below:

$$I_{m, m+n} (I_{m, m+n})^T = I_{m, m+n} J_{m+n, m} = \mathbb{1}_m, \tag{6}$$

$$(J_{m+n, n})^T J_{m+n, n} = I_{n, m+n} J_{m+n, n} = \mathbb{1}_n, \tag{7}$$

For each $A \in \text{Mat}(\mathbb{C}, m, n)$, we can associate a square matrix $A' \in \text{Mat}(\mathbb{C}, m+n)$ given by

$$\begin{aligned} A' &:= (I_{m, m+n})^T A (J_{m+n, n})^T \\ &= J_{m+n, m} A I_{n, m+n} = \begin{pmatrix} A & \mathbb{0}_{m, m} \\ \mathbb{0}_{n, n} & \mathbb{0}_{n, m} \end{pmatrix}. \end{aligned} \tag{8}$$

As one easily checks, we get from (6)–(7) the useful relation

$$A = I_{m, m+n} A' J_{m+n, n}. \tag{9}$$

The canonical basis of vectors in \mathbb{C}^n is

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \tag{10}$$

Let x^1, \dots, x^n be vectors, represented in the canonical basis as

$$x^a = \begin{pmatrix} x_1^a \\ \vdots \\ x_n^a \end{pmatrix}.$$

We will denote by $\llbracket x^1, \dots, x^n \rrbracket$ the $n \times n$ matrix constructed in such a way that its a -th column is the vector x^a , that means,

$$\llbracket x^1, \dots, x^n \rrbracket = \begin{pmatrix} x_1^1 & \dots & x_1^n \\ \vdots & \ddots & \vdots \\ x_n^1 & \dots & x_n^n \end{pmatrix}. \tag{11}$$

It is obvious that $\mathbb{1} = \left[\mathbf{e}_1, \dots, \mathbf{e}_n \right]$. With this notation, we write

$$B \left[x^1, \dots, x^n \right] = \left[Bx^1, \dots, Bx^n \right], \tag{12}$$

for any $B \in \text{Mat}(\mathbb{C}, m, n)$, as one easily checks. Moreover, if D is a diagonal matrix $D = \text{diag}(d_1, \dots, d_n)$, then

$$\left[x^1, \dots, x^n \right] D = \left[d_1 x^1, \dots, d_n x^n \right]. \tag{13}$$

If v_1, \dots, v_k are elements of a complex vector space V , we denote by $[v_1, \dots, v_k]$ the subspace generated v_1, \dots, v_k , i.e., the collection of all linear combinations of the v_1, \dots, v_k : $[v_1, \dots, v_k] := \left\{ \alpha_1 v_1 + \dots + \alpha_k v_k, \alpha_1, \dots, \alpha_k \in \mathbb{C} \right\}$. More definitions and general results can be found in “Appendix 1.”

2 The Moore–Penrose Pseudoinverse: Definition and First Properties

In this section, we define the notion of a Moore–Penrose pseudoinverse and study its uniqueness. The question of the existence of the Moore–Penrose pseudoinverse of a given matrix is analyzed in other sections.

2.1 Generalized Inverses, or Pseudoinverses

Let $m, n \in \mathbb{N}$ and let $A \in \text{Mat}(\mathbb{C}, m, n)$ be a $m \times n$ matrix (not necessarily a square matrix). A matrix $B \in \text{Mat}(\mathbb{C}, n, m)$ is said to be a *generalized inverse*, or a *pseudoinverse*, of A if it satisfies the following conditions:

1. $ABA = A$,
2. $BAB = B$.

If $A \in \text{Mat}(\mathbb{C}, n)$ is a non-singular square matrix, its inverse A^{-1} satisfies trivially the defining properties of the generalized inverse above. We will prove later that every matrix $A \in \text{Mat}(\mathbb{C}, m, n)$ has at least one generalized inverse, namely the Moore–Penrose pseudoinverse. The general definition above is not enough to guarantee uniqueness of the generalized inverse of any matrix $A \in \text{Mat}(\mathbb{C}, m, n)$.

The definition above is too wide to be useful, and it is convenient to narrow it in order to deal with certain specific problems. In what follows, we will discuss the specific case of the Moore–Penrose pseudoinverse and its application to optimization of linear least squares problems.

2.2 Defining the Moore–Penrose Pseudoinverse

Let $m, n \in \mathbb{N}$ and let $A \in \text{Mat}(\mathbb{C}, m, n)$. A matrix $A^+ \in \text{Mat}(\mathbb{C}, n, m)$ is said to be a *Moore–Penrose pseudoinverse* of A if it satisfies the following conditions:

1. $AA^+A = A$,
2. $A^+AA^+ = A^+$,
3. $AA^+ \in \text{Mat}(\mathbb{C}, m)$ and $A^+A \in \text{Mat}(\mathbb{C}, n)$ are self-adjoint.

It is easy to see again that if $A \in \text{Mat}(\mathbb{C}, n)$ is non-singular, then its inverse satisfies all defining properties of a Moore–Penrose pseudoinverse.

The notion of Moore–Penrose pseudoinverse was introduced by E. H. Moore [26] in 1920 and rediscovered by R. Penrose [27, 28] in 1955. The Moore–Penrose pseudoinverse is a useful concept in dealing with optimization problems, as the determination of a “least squares” solution of linear systems. We will treat such problems later (see Theorem 6.1), after dealing with the question of uniqueness and existence of the Moore–Penrose pseudoinverse.

2.3 The Uniqueness of the Moore–Penrose Pseudoinverse

We will first show the uniqueness of the Moore–Penrose pseudoinverse of a given matrix $A \in \text{Mat}(\mathbb{C}, m, n)$, assuming its existence. Let $A^+ \in \text{Mat}(\mathbb{C}, n, m)$ be a Moore–Penrose pseudoinverse of $A \in \text{Mat}(\mathbb{C}, m, n)$ and let $B \in \text{Mat}(\mathbb{C}, n, m)$ be another Moore–Penrose pseudoinverse of A , i.e., such that $ABA = A$, $BAB = B$ with AB and BA self-adjoint. Let $M_1 := AB - AA^+ = A(B - A^+) \in \text{Mat}(\mathbb{C}, m)$. By the hypothesis, M_1 is self-adjoint (since it is the difference of two self-adjoint matrices) and $(M_1)^2 = (AB - AA^+)A(B - A^+) = (ABA - AA^+A)(B - A^+) = (A - A)(B - A^+) = 0$. Since M_1 is self-adjoint, the fact that $(M_1)^2 = 0$ implies that $M_1 = 0$, since for all $x \in \mathbb{C}^m$ one has $\|M_1 x\|^2 = \langle M_1 x, M_1 x \rangle = \langle x, (M_1)^2 x \rangle = 0$, implying $M_1 = 0$. This showed that $AB = AA^+$. Following the same steps, we can prove that $BA = A^+A$ (consider the self-adjoint matrix $M_2 := BA - A^+A \in \text{Mat}(\mathbb{C}, n)$ and proceed as above). Now, all this implies that $A^+ = A^+AA^+ = A^+(AA^+) = A^+AB = (A^+A)B = BAB = B$, thus establishing uniqueness.

As we have already commented, if $A \in \text{Mat}(\mathbb{C}, n)$ is a non-singular square matrix, its inverse A^{-1} trivially satisfies the defining conditions of the Moore–Penrose pseudoinverse, and therefore, we have in this case $A^+ = A^{-1}$ as the unique Moore–Penrose pseudoinverse of A . It is also evident from the definition that

for $\mathbb{0}_{mn}$, the $m \times n$ identically zero matrix, one has $(\mathbb{0}_{mn})^+ = \mathbb{0}_{nm}$.

2.4 Existence of the Moore–Penrose Pseudoinverse

We will present two proofs of the existence of the Moore–Penrose pseudoinverse A^+ for an arbitrary matrix $A \in \text{Mat}(\mathbb{C}, m, n)$. Both proofs produce algorithms for the explicit computation of A^+ . The first one will be presented in Section 4 (Theorems 4.3 and 5.1) and will follow from results presented below. Expressions (39) and (40) furnish explicit expressions for the computation of A^+ in terms of A , A^* and the eigenvalues of AA^* or A^*A (i.e., the singular values of A).

The second existence proof will be presented in “Appendix 2” and relies on the singular values decomposition presented in Theorem A.16. For this proof, the preliminary results presented below are not required. This second proof is the one more frequently found in the literature, but we believe that expressions (39) and (40) provide an algorithmically simpler way for the determination of the Moore–Penrose pseudoinverse of a given matrix.

2.5 Computing the Moore–Penrose Pseudoinverse in Some Special Cases

If $A \in \text{Mat}(\mathbb{C}, m, 1)$, $A = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}$, a non-zero column vector, then one can easily verify that $A^+ = \frac{1}{\|A\|^2} A^* = \frac{1}{\|A\|^2} (\bar{a}_1, \dots, \bar{a}_m)$, where $\|A\| = \sqrt{|a_1|^2 + \dots + |a_m|^2}$. In particular, if $z \in \mathbb{C}$, then $(z)^+ = \begin{cases} 0, & z = 0 \\ \frac{1}{z}, & z \neq 0 \end{cases}$, by taking z as an element of $\text{Mat}(\mathbb{C}, 1, 1)$.

This can be further generalized. If $A \in \text{Mat}(\mathbb{C}, m, n)$ and $(AA^*)^{-1}$ exist, then

$$A^+ = A^*(AA^*)^{-1}, \tag{14}$$

because we can readily verify that the right-hand side satisfies the defining conditions of A^+ . Analogously, if $(A^*A)^{-1}$ exists, one has

$$A^+ = (A^*A)^{-1}A^*. \tag{15}$$

For instance, for $A = \begin{pmatrix} 2 & 0 & i \\ 0 & i & 1 \end{pmatrix}$, one can check that AA^* is invertible, but A^*A is not, and we have $A^+ = A^*(AA^*)^{-1} = \frac{1}{9} \begin{pmatrix} 4 & -2i \\ 1 & -5i \\ -i & 4 \end{pmatrix}$. Similarly, for $A = \begin{pmatrix} 1 & 2 \\ 0 & i \\ 0 & 3 \end{pmatrix}$, AA^* is singular, but A^*A is invertible and we have $A^+ = (A^*A)^{-1}A^* = \frac{1}{10} \begin{pmatrix} 10 & 2i & -6 \\ 0 & -i & 3 \end{pmatrix}$.

The relations (14) and (15) are significant because they will provide an important hint to find the Moore–Penrose pseudoinverse of a general matrix, as we will

discuss later. In Proposition 3.2, we will show that one has in general $A^+ = A^*(AA^*)^+ = (A^*A)^+A^*$, and in Theorem 4.3, we will discuss what can be done in the cases when A^*A or AA^* are not invertible.

3 Further Properties of the Moore–Penrose Pseudoinverse

The following properties of the Moore–Penrose pseudoinverse follow immediately from its definition and from uniqueness. The proofs are elementary and left to the reader: For any $A \in \text{Mat}(\mathbb{C}, m, n)$, one has

1. $(A^+)^+ = A$,
2. $(A^+)^T = (A^T)^+$, $\overline{A^+} = (\overline{A})^+$ and, consequently $(A^+)^* = (A^*)^+$,
3. $(zA)^+ = z^{-1}A^+$ for all $z \in \mathbb{C}, z \neq 0$.

It is, however, important to remark that for $A \in \text{Mat}(\mathbb{C}, m, n)$ and $B \in \text{Mat}(\mathbb{C}, n, p)$, the Moore–Penrose pseudoinverse $(AB)^+$ is not always equal to B^+A^+ , in contrast to what happens with the usual inverse in the case $m = n = p$. A relevant exception will be found in Proposition 3.2.

The next proposition lists some important properties that will be used below.

Proposition 3.1 *The Moore–Penrose pseudoinverse satisfies the following relations:*

$$A^+ = A^+(A^+)^*A^*, \tag{16}$$

$$A = AA^*(A^+)^*, \tag{17}$$

$$A^* = A^*AA^+, \tag{18}$$

$$A^+ = A^*(A^+)^*A^+, \tag{19}$$

$$A = (A^+)^*A^*A, \tag{20}$$

$$A^* = A^+AA^*, \tag{21}$$

valid for all $A \in \text{Mat}(\mathbb{C}, m, n)$.

For us, the most relevant of the relations above is relation (18), since we will make use of it in the proof of Proposition 6.1 when deal with optimization of least squares problems.

Proof of Proposition 3.1 Since AA^+ is self-adjoint, one has $AA^+ = (AA^+)^* = (A^+)^*A^*$. Multiplying to the left by A^+ , we get $A^+ = A^+(A^+)^*A^*$, proving (16). Replacing $A \rightarrow A^+$ and using the fact that $A = (A^+)^+$, one gets from (16) $A = AA^*(A^+)^*$, which is relation

(17). Replacing $A \rightarrow A^*$ and using the fact that $(A^*)^+ = (A^+)^*$, we get from (17) that $A^* = A^*AA^+$, which is relation (18).

Relations (19)–(21) can be obtained analogously from the fact that A^+A is also self-adjoint, but they follow more easily by replacing $A \rightarrow A^*$ in (16)–(18) and by taking the adjoint of the resulting expressions. \square

From Proposition 3.1, other interesting results can be obtained, some of which are listed in the following proposition:

Proposition 3.2 *For all $A \in \text{Mat}(\mathbb{C}, m, n)$, one has*

$$(AA^*)^+ = (A^*)^+A^+. \tag{22}$$

From this we get

$$A^+ = A^*(AA^*)^+ = (A^*A)^+A^*, \tag{23}$$

also valid for all $A \in \text{Mat}(\mathbb{C}, m, n)$.

Expression (23) generalizes (14) and (15) and can be employed to compute A^+ provided $(AA^*)^+$ or $(A^*A)^+$ were previously known.

Proof of Proposition 3.2 Let $B = (A^*)^+A^+$. One has

$$\begin{aligned} AA^* &\stackrel{(17)}{=} AA^*(A^+)^*A^* \stackrel{(21)}{=} AA^*(A^+)^*A^+AA^* \\ &= (AA^*)B(AA^*), \end{aligned}$$

where we use that $(A^*)^+ = (A^+)^*$. One also has

$$\begin{aligned} B &= (A^*)^+A^+ \stackrel{(16)}{=} (A^+)^*A^+AA^+ \\ &\stackrel{(19)}{=} (A^+)^*A^+AA^*(A^+)^*A^+ = B(AA^*)B. \end{aligned}$$

Notice that

$$(AA^*)B = (AA^*(A^+)^*)A^+ \stackrel{(18)}{=} AA^+$$

which is self-adjoint, by definition. Analogously,

$$B(AA^*) = (A^+)^*(A^+AA^*) \stackrel{(20)}{=} (A^*)^+A^*,$$

which is also self-adjoint. The facts exposed in the lines above prove that B is the Moore–Penrose pseudoinverse of AA^* , establishing (22). Replacing $A \rightarrow A^*$ in (22), one also gets

$$(A^*A)^+ = A^+(A^*)^+. \tag{24}$$

Notice now that

$$A^*(AA^*)^+ \stackrel{(22)}{=} A^*(A^*)^+A^+ \stackrel{(19)}{=} A^+$$

and that

$$(A^*A)^+A^* \stackrel{(24)}{=} A^+(A^*)^+A^* \stackrel{(16)}{=} A^+,$$

establishing (23). \square

3.1 The Kernel and the Range of a Matrix and the Moore–Penrose Pseudoinverse

The kernel and the range (or image) of a matrix $A \in \text{Mat}(\mathbb{C}, m, n)$ are defined by $\text{Ker}(A) := \{u \in \mathbb{C}^n \mid Au = 0\}$ and $\text{Ran}(A) := \{Au, u \in \mathbb{C}^n\}$, respectively. It is evident that $\text{Ker}(A)$ is a linear subspace of \mathbb{C}^n and that $\text{Ran}(A)$ is a linear subspace of \mathbb{C}^m .

The following proposition will be used below, but is interesting by itself.

Proposition 3.3 *Let $A \in \text{Mat}(\mathbb{C}, m, n)$ and let us define $P_1 := \mathbb{1}_n - A^+A \in \text{Mat}(\mathbb{C}, n)$ and $P_2 := \mathbb{1}_m - AA^+ \in \text{Mat}(\mathbb{C}, m)$. Then, the following claims are valid:*

1. P_1 and P_2 are orthogonal projectors, that means, they satisfy $(P_k)^2 = P_k$ and $P_k^* = P_k, k = 1, 2$.
2. $\text{Ker}(A) = \text{Ran}(P_1), \text{Ran}(A) = \text{Ker}(P_2), \text{Ker}(A^+) = \text{Ran}(P_2)$ and $\text{Ran}(A^+) = \text{Ker}(P_1)$.
3. $\text{Ran}(A) = \text{Ker}(A^+)^{\perp}$ and $\text{Ran}(A^+) = \text{Ker}(A)^{\perp}$.
4. $\text{Ker}(A) \oplus \text{Ran}(A^+) = \mathbb{C}^n$ and $\text{Ker}(A^+) \oplus \text{Ran}(A) = \mathbb{C}^m$, both being direct sums of orthogonal subspaces.

Proof Since AA^+ and A^+A are self-adjoint, so are P_1 and P_2 . One also has $(P_1)^2 = \mathbb{1} - 2A^+A + A^+AA^+A = \mathbb{1} - 2A^+A + A^+A = \mathbb{1} - A^+A = P_1$ and analogously for P_2 . This proved item 1.

Let $x \in \text{Ker}(A)$. Since $\text{Ran}(P_1)$ is a closed linear subspace of \mathbb{C}^n , the “Best Approximant Theorem,” Theorem A.1, and the Orthogonal Decomposition Theorem, Theorem A.3, guarantee the existence of a unique $z_0 \in \text{Ran}(P_1)$ such that $\|x - z_0\| = \min\{\|x - z\|, z \in \text{Ran}(P_1)\}$. Moreover, $x - z_0$ is orthogonal to $\text{Ran}(P_1)$. Hence, there exists at least one $y_0 \in \mathbb{C}^m$ such that $x - P_1y_0$ is orthogonal to every element of the form P_1y , i.e., $\langle x - P_1y_0, P_1y \rangle = 0$ for all $y \in \mathbb{C}^m$, what implies $\langle P_1(x - P_1y_0), y \rangle = 0$ for all $y \in \mathbb{C}^m$ what, in turn, implies $P_1(x - P_1y_0) = 0$. This, however, says that $P_1x = P_1y_0$. Since $x \in \text{Ker}(A)$, one has $P_1x = x$ (by the definition of P_1). We therefore proved that if $x \in \text{Ker}(A)$, then $x \in \text{Ran}(P_1)$, establishing that $\text{Ker}(A) \subset \text{Ran}(P_1)$. On the other hand, the fact that $AP_1 = A(\mathbb{1} - A^+A) = A - A = 0$ implies $\text{Ran}(P_1) \subset \text{Ker}(A)$, establishing that $\text{Ran}(P_1) = \text{Ker}(A)$.

If $z \in \text{Ker}(P_1)$, then $z = A^+Az$, proving that $z \in \text{Ran}(A^+)$. This establishes that $\text{Ker}(P_1) \subset \text{Ran}(A^+)$. On the other hand, if $u \in \text{Ran}(A^+)$, then there exists

$v \in \mathbb{C}^m$ such that $u = A^+v$. Therefore, $P_1u = (\mathbb{1}_n - A^+A)A^+v = (A^+ - A^+AA^+)v = 0$, proving that $u \in \text{Ker}(P_1)$ and that $\text{Ran}(A^+) \subset \text{Ker}(P_1)$. This establishes that $\text{Ker}(P_1) = \text{Ran}(A^+)$.

P_2 is obtained from P_1 by the substitution $A \rightarrow A^+$ (recalling that $(A^+)^+ = A$). Hence, the results above imply that $\text{Ran}(P_2) = \text{Ker}(A^+)$ and that $\text{Ker}(P_2) = \text{Ran}(A)$. This proves item 2.

If $M \in \text{Mat}(\mathbb{C}, p)$ (with $p \in \mathbb{N}$, arbitrary) is self-adjoint, then $\langle y, Mx \rangle = \langle My, x \rangle$ for all $x, y \in \mathbb{C}^p$. This relation makes evident that $\text{Ker}(M) = \text{Ran}(M)^\perp$. Therefore, item 3 follows from item 2 by taking $M = P_1$ and $M = P_2$. Item 4 is evident from item 3. \square

4 Tikhonov’s Regularization and Existence Theorem for the Moore–Penrose Pseudoinverse

In (14) and (15), we saw that if $(AA^*)^{-1}$ exists, then $A^+ = A^*(AA^*)^{-1}$, and that if $(A^*A)^{-1}$ exists, then $A^+ = (A^*A)^{-1}A^*$. If those inverses do not exist, there is an alternative procedure to obtain A^+ . We know from Proposition A.4 that even if $(AA^*)^{-1}$ does not exist, the matrix $AA^* + \mu\mathbb{1}$ will be invertible for all non-vanishing $\mu \in \mathbb{C}$ with $|\mu|$ small enough. Hence, we could conjecture that the expressions $A^*(AA^* + \mu\mathbb{1})^{-1}$ and $(A^*A + \mu\mathbb{1})^{-1}A^*$ are well-defined for $\mu \neq 0$ and $|\mu|$ small enough and converge to A^+ when the limit $\mu \rightarrow 0$ is taken. As will now show, this conjecture is correct.

The provisional replacement of the singular matrices AA^* or A^*A by the non-singular ones $AA^* + \mu\mathbb{1}$ or $A^*A + \mu\mathbb{1}$ (with $\mu \neq 0$ and $|\mu|$ “small”) is a regularization procedure known as *Tikhonov’s regularization*. This procedure was introduced by Tikhonov in [1] (see also [2] and, for historical remarks, [25]) in his search for uniform approximations for the solutions of Fredholm’s equation of the first kind

$$\int_a^b k(x, y)u(y) dy = f(x), \tag{25}$$

where $-\infty < a < b < \infty$ and where k and f are given functions satisfying adequate smoothness conditions. In operator form, (25) becomes $Ku = f$ and K is well-known to be a compact operator (see, e.g., [29]) if k is a continuous function. By using the method of finite differences or by using expansions in terms of orthogonal functions, the inverse problem (25) can be replaced by an approximating inverse matrix problem $Ax = y$, like (1). By applying A^* to the left, one gets $A^*Ax = A^*y$. Since the inverse of A^*A may not exist, one first considers a solution x_μ of the *regularized equa-*

tion $(A^*A + \mu\mathbb{1})x_\mu = A^*y$, with some adequate $\mu \in \mathbb{C}$, and asks whether the limit $\lim_{|\mu| \rightarrow 0} (A^*A + \mu\mathbb{1})^{-1}A^*y$ can be taken. As we will see, the limit exists and is given precisely by A^+y . In Tikhonov’s case, the regularized equation $(A^*A + \mu\mathbb{1})x_\mu = A^*y$ can be obtained from a related Fredholm’s equation of the *second* kind, namely $K^*Ku_\mu + \mu u_\mu = K^*f$, for which the existence of solutions, i.e., the existence of the inverse $(K^*K + \mu\mathbb{1})^{-1}$, is granted by Fredholm’s alternative theorem (see, e.g., [29]) for all μ in the resolvent set of K^*K and, therefore, for all $\mu > 0$ (since K^*K is a positive compact operator)¹. It is then a technical matter to show that the limit $\lim_{\substack{\mu \rightarrow 0 \\ \mu > 0}} u_\mu$ exists and provides a uniform approximation to a solution of (25).

Tikhonov, however, does not point to the relation of his ideas to the theory of the Moore–Penrose inverse. This will be described in what follows. Our first result, presented in the next two lemmas, establishes that the limits $\lim_{\mu \rightarrow 0} A^*(AA^* + \mu\mathbb{1}_m)^{-1}$ and $\lim_{\mu \rightarrow 0} (A^*A + \mu\mathbb{1}_n)^{-1}A^*$, described above, indeed exist and are equal.

Lemma 4.1 *Let $A \in \text{Mat}(\mathbb{C}, m, n)$ and let $\mu \in \mathbb{C}$ be such that $AA^* + \mu\mathbb{1}_m$ and $A^*A + \mu\mathbb{1}_n$ are non-singular (that means $\mu \notin \sigma(AA^*) \cup \sigma(A^*A)$, a finite set). Then, $A^*(AA^* + \mu\mathbb{1}_m)^{-1} = (A^*A + \mu\mathbb{1}_n)^{-1}A^*$.*

Recall that, by Proposition A.7, $\sigma(AA^*)$ and $\sigma(A^*A)$ differ at most by the element 0.

Proof of Lemma 4.1 Let $B_\mu := A^*(AA^* + \mu\mathbb{1}_m)^{-1}$ and $C_\mu := (A^*A + \mu\mathbb{1}_n)^{-1}A^*$. We have

$$\begin{aligned} A^*AB_\mu &= A^*[AA^*](AA^* + \mu\mathbb{1}_m)^{-1} \\ &= A^*[AA^* + \mu\mathbb{1}_m - \mu\mathbb{1}_m](AA^* + \mu\mathbb{1}_m)^{-1} \\ &= A^*(\mathbb{1}_m - \mu(AA^* + \mu\mathbb{1}_m)^{-1}) = A^* - \mu B_\mu. \end{aligned}$$

Therefore, $(A^*A + \mu\mathbb{1}_n)B_\mu = A^*$, what implies $B_\mu = (A^*A + \mu\mathbb{1}_n)^{-1}A^* = C_\mu$. \square

Lemma 4.2 *For all $A \in \text{Mat}(\mathbb{C}, m, n)$ the limits $\lim_{\mu \rightarrow 0} A^*(AA^* + \mu\mathbb{1}_m)^{-1}$ and $\lim_{\mu \rightarrow 0} (A^*A + \mu\mathbb{1}_n)^{-1}A^*$ exist and are equal (by Lemma 4.1), defining an element of $\text{Mat}(\mathbb{C}, n, m)$.*

¹Tikhonov’s argument in [1] is actually more complicated, since he does not consider the regularized equation $(K^*K + \mu\mathbb{1})u_\mu = K^*f$, but a more general version where the identity operator $\mathbb{1}$ is replaced by a Sturm–Liouville operator.

Proof Notice first that A is an identically zero matrix iff AA^* or A^*A are zero matrices. In fact, if, for instance, $A^*A = 0$, then for any vector x one has $0 = \langle x, A^*Ax \rangle = \langle Ax, Ax \rangle = \|Ax\|^2$, proving that $A = 0$. Hence, we will assume that AA^* and A^*A are non-zero matrices.

The matrix $AA^* \in \text{Mat}(\mathbb{C}, m)$ is evidently self-adjoint. Let $\alpha_1, \dots, \alpha_r$ be its *distinct* eigenvalues. By the spectral theorem for self-adjoint matrices (see Theorems A.9 and A.13), we may write

$$AA^* = \sum_{a=1}^r \alpha_a E_a, \tag{26}$$

where E_a are the spectral projectors of AA^* and satisfy $E_a E_b = \delta_{ab} E_a$, $E_a^* = E_a$, and $\sum_{a=1}^r E_a = \mathbb{1}_m$. Therefore,

$$AA^* + \mu \mathbb{1}_m = \sum_{a=1}^r (\alpha_a + \mu) E_a$$

and, hence, for $\mu \notin \{\alpha_1, \dots, \alpha_r\}$, one has, by (50),

$$\begin{aligned} (AA^* + \mu \mathbb{1}_m)^{-1} &= \sum_{a=1}^r \frac{1}{\alpha_a + \mu} E_a \quad \text{and} \\ A^*(AA^* + \mu \mathbb{1}_m)^{-1} &= \sum_{a=1}^r \frac{1}{\alpha_a + \mu} A^* E_a. \end{aligned} \tag{27}$$

There are now two cases to be considered: (1) zero is not an eigenvalue of AA^* and (2) zero is eigenvalue of AA^* .

In case 1, it is clear from (27) that the limit $\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1}$ exists and

$$\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1} = \sum_{a=1}^r \frac{1}{\alpha_a} A^* E_a. \tag{28}$$

In case 2, let us have, say, $\alpha_1 = 0$. The corresponding spectral projector E_1 projects on the kernel of AA^* : $\text{Ker}(AA^*) := \{u \in \mathbb{C}^n \mid AA^*u = 0\}$. If $x \in \text{Ker}(AA^*)$, then $A^*x = 0$ because $0 = \langle x, AA^*x \rangle = \langle A^*x, A^*x \rangle = \|A^*x\|^2$. Therefore,

$$A^*E_1 = 0 \tag{29}$$

and, hence, we may write,

$$A^*(AA^* + \mu \mathbb{1}_m)^{-1} = \sum_{a=2}^r \frac{1}{\alpha_a + \mu} A^* E_a,$$

from which we get

$$\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1} = \sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a. \tag{30}$$

This proves that $\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1}$ always exists. By Lemma 4.1, the limit $\lim_{\mu \rightarrow 0} (A^*A + \mu \mathbb{1}_n)^{-1} A^*$ also exists and coincides with $\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1}$. \square

The main consequence is the following theorem, which contains a general proof for the existence of the Moore–Penrose pseudoinverse:

Theorem 4.3 (Tikhonov’s Regularization) *For all $A \in \text{Mat}(\mathbb{C}, m, n)$ one has*

$$A^+ = \lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1} \tag{31}$$

and

$$A^+ = \lim_{\mu \rightarrow 0} (A^*A + \mu \mathbb{1}_n)^{-1} A^*. \tag{32}$$

Proof The statements to be proven are evident if $A = \mathbb{0}_{mn}$ because, as we already saw, $(\mathbb{0}_{mn})^+ = \mathbb{0}_{nm}$. Hence, we will assume that A is a non-zero matrix. This is equivalent (by the comments found in the proof of Lemma 4.2) to assume that AA^* and A^*A are non-zero matrices.

By Lemmas 4.1 and 4.2, it is enough to prove (31). There are two cases to be considered: (1) zero is not an eigenvalue of AA^* and (2) zero is an eigenvalue of AA^* . In case (1), we saw in (28) that

$$\lim_{\mu \rightarrow 0} A^*(AA^* + \mu \mathbb{1}_m)^{-1} = \sum_{a=1}^r \frac{1}{\alpha_a} A^* E_a =: B.$$

Notice now that

$$\begin{aligned} AB &= \sum_{a=1}^r \frac{1}{\alpha_a} AA^* E_a = \sum_{a=1}^r \frac{1}{\alpha_a} \left(\sum_{b=1}^r \alpha_b E_b \right) E_a \\ &= \sum_{a=1}^r \sum_{b=1}^r \frac{1}{\alpha_a} \alpha_b \delta_{ab} E_a = \sum_{a=1}^r E_a = \mathbb{1}_m, \end{aligned} \tag{33}$$

which is self-adjoint and that

$$BA = \sum_{a=1}^r \frac{1}{\alpha_a} A^* E_a A, \tag{34}$$

which is also self-adjoint because $\alpha_a \in \mathbb{R}$ for all a and because $(A^* E_a A)^* = A^* E_a A$ for all a , since $E_a^* = E_a$.

From (33), it follows that $ABA = A$. From (34), it follows that

$$BAB = \left(\sum_{a=1}^r \frac{1}{\alpha_a} A^* E_a A \right) \left(\sum_{b=1}^r \frac{1}{\alpha_b} A^* E_b \right) = \sum_{a=1}^r \sum_{b=1}^r \frac{1}{\alpha_a \alpha_b} A^* E_a (A A^*) E_b .$$

Now, by the spectral decomposition (26) for AA^* , it follows that $(AA^*)E_b = \alpha_b E_b$. Therefore,

$$BAB = \sum_{a=1}^r \sum_{b=1}^r \frac{1}{\alpha_a} A^* E_a E_b = \left(\sum_{a=1}^r \frac{1}{\alpha_a} A^* E_a \right) \underbrace{\left(\sum_{b=1}^r E_b \right)}_{\mathbb{1}_m} = B .$$

This proves that $A = A^+$ when 0 is not an eigenvalue of AA^* .

Let us now consider the case when AA^* has a zero eigenvalue, say, α_1 . As we saw in (30),

$$\lim_{\mu \rightarrow 0} A^* (AA^* + \mu \mathbb{1}_m)^{-1} = \sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a =: B .$$

Using the fact that $(AA^*)E_a = \alpha_a E_a$ (what follows from the spectral decomposition (26) for AA^*), we get

$$AB = \sum_{a=2}^r \frac{1}{\alpha_a} AA^* E_a = \sum_{a=2}^r \frac{1}{\alpha_a} \alpha_a E_a = \sum_{a=2}^r E_a = \mathbb{1}_m - E_1, \tag{35}$$

which is self-adjoint, since E_1 is self-adjoint. We also have

$$BA = \sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a A, \tag{36}$$

which is also self-adjoint.

From (35), it follows that $ABA = A - E_1 A$. Notice now that $(E_1 A)^* = A^* E_1 = 0$, by (29). This establishes

that $E_1 A = 0$ and that $ABA = A$. From (36), it follows that

$$BAB = \left(\sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a A \right) \left(\sum_{b=2}^r \frac{1}{\alpha_b} A^* E_b \right) = \sum_{a=2}^r \sum_{b=2}^r \frac{1}{\alpha_a \alpha_b} A^* E_a (A A^*) E_b .$$

Using again $(AA^*)E_b = \alpha_b E_b$, we get

$$BAB = \sum_{a=2}^r \sum_{b=2}^r \frac{1}{\alpha_a} A^* E_a E_b = \left(\sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a \right) \underbrace{\left(\sum_{b=2}^r E_b \right)}_{\mathbb{1}_m - E_1} = B - \sum_{a=2}^r \frac{1}{\alpha_a} A^* E_a E_1 = B,$$

since $E_a E_1 = 0$ for $a \neq 1$. This shows that $BAB = B$. Hence, we established that $A = A^+$ also in the case when AA^* has a zero eigenvalue, completing the proof of (31). \square

5 The Moore–Penrose Pseudoinverse and the Spectral Theorem

The proof of Theorem 4.3 also establishes the following facts:

Theorem 5.1 *Let $A \in \text{Mat}(\mathbb{C}, m, n)$ be a non-zero matrix and let $AA^* = \sum_{a=1}^r \alpha_a E_a$ be the spectral representation of AA^* , where $\{\alpha_1, \dots, \alpha_r\} \subset \mathbb{R}$ is the set of distinct eigenvalues of AA^* and E_a are the corresponding self-adjoint spectral projections. Then, we have*

$$A^+ = \sum_{\substack{a=1 \\ \alpha_a \neq 0}}^r \frac{1}{\alpha_a} A^* E_a . \tag{37}$$

Analogously, let $A^* A = \sum_{b=1}^s \beta_b F_b$ be the spectral representation of $A^* A$, where $\{\beta_1, \dots, \beta_s\} \subset \mathbb{R}$ is the set of distinct eigenvalues of $A^* A$ and F_b the corresponding self-adjoint spectral projections. Then, we also have

$$A^+ = \sum_{\substack{b=1 \\ \beta_b \neq 0}}^s \frac{1}{\beta_b} F_b A^* . \tag{38}$$

Is it worth mentioning that, by Proposition A.7, the sets of non-zero eigenvalues of AA^* and of $A^* A$ coincide: $\{\alpha_1, \dots, \alpha_r\} \setminus \{0\} = \{\beta_1, \dots, \beta_s\} \setminus \{0\}$.

From (37) and (38) it follows that for a non-zero matrix A , we have

$$A^+ = \sum_{\substack{a=1 \\ \alpha_a \neq 0}}^r \frac{1}{\alpha_a} \left(\prod_{\substack{l=1 \\ l \neq a}}^r (\alpha_a - \alpha_l)^{-1} \right) \times A^* \left[\prod_{\substack{l=1 \\ l \neq a}}^r (AA^* - \alpha_l \mathbb{1}_m) \right], \tag{39}$$

$$A^+ = \sum_{\substack{b=1 \\ \beta_b \neq 0}}^s \frac{1}{\beta_b} \left(\prod_{\substack{l=1 \\ l \neq b}}^s (\beta_b - \beta_l)^{-1} \right) \times \left[\prod_{\substack{l=1 \\ l \neq b}}^s (A^*A - \beta_l \mathbb{1}_n) \right] A^*. \tag{40}$$

Expression (39) or (40) provides a general algorithm for the computation of the Moore–Penrose pseudoinverse for any non-zero matrix A . Its implementation requires only the determination of the eigenvalues of AA^* or of A^*A and the computation of polynomials on AA^* or A^*A .

Proof of Theorem 5.1 Equation (37) was established in the proof of Theorem 4.3 (see (28) and (30)). Relation (38) can be proven analogously, but it also follows easier (see (37)), by replacing $A \rightarrow A^*$ and taking the adjoint of the resulting expression. Relations (39) and (40) follow from Proposition A.11, particularly from the explicit formula for the spectral projector given in (52). \square

6 The Moore–Penrose Pseudoinverse and Least Squares

Let us now consider one of the main applications of the Moore–Penrose pseudoinverse, namely to optimization of linear least squares problems. Let $A \in \text{Mat}(\mathbb{C}, m, n)$ and $y \in \mathbb{C}^m$ be given and consider the problem of finding $x \in \mathbb{C}^n$ satisfying the linear equation

$$Ax = y. \tag{41}$$

If $m = n$ and A has an inverse, the (unique) solution is, evidently, $x = A^{-1}y$. In the other cases, the solution may not exist or may not be unique. We can, however, consider the alternative problem of finding the set of all vectors $x' \in \mathbb{C}^n$ such that the Euclidean norm $\|Ax' - y\|$ reaches its least possible value. This set is called the

minimizing set of the linear problem (41). Such vectors $x' \in \mathbb{C}^n$ would be the best approximants for the solution of (41) in terms of the Euclidean norm, i.e., in terms of “least squares.” As we will show, the Moore–Penrose pseudoinverse provides this set of vectors x' that minimize $\|Ax' - y\|$. The main result is condensed in the following theorem:

Theorem 6.1 *Let $A \in \text{Mat}(\mathbb{C}, m, n)$ and $y \in \mathbb{C}^m$ be given. Then, the set of all vectors of \mathbb{C}^n for which the map $\mathbb{C}^n \ni x \mapsto \|Ax - y\| \in [0, \infty)$ assumes a minimum coincides with the set*

$$A^+y + \text{Ker}(A) = \left\{ A^+y + (\mathbb{1}_n - A^+A)z, z \in \mathbb{C}^n \right\}. \tag{42}$$

By Proposition 3.3, we also have $A^+y + \text{Ker}(A) = A^+y + \text{Ran}(A^+)^\perp$.

Theorem 6.1 says that the minimizing set of the linear problem (41) consists of all vectors obtained by adding to the vector A^+y an element of the kernel of A , i.e., of all vectors obtained adding to A^+y a vector annihilated by A . Notice that for the elements x' of the minimizing set of the linear problem (41), one has $\|Ax' - y\| = \|(AA^+ - \mathbb{1}_m)y\| = \|P_2y\|$, which vanishes if and only if $y \in \text{Ker}(P_2) = \text{Ran}(A)$ (by Proposition 3.3), a rather obvious fact.

Proof of Theorem 6.1 The image of A , $\text{Ran}(A)$, is a closed linear subspace of \mathbb{C}^m . The best approximant theorem and the orthogonal decomposition theorem guarantee the existence of a *unique* $y_0 \in \text{Ran}(A)$ such that $\|y_0 - y\|$ is minimal and that this y_0 is such that $y_0 - y$ is orthogonal to $\text{Ran}(A)$.

Hence, there exists at least one $x_0 \in \mathbb{C}^n$ such that $\|Ax_0 - y\|$ is minimal. Such x_0 is not necessarily unique, and as one easily sees, $x_1 \in \mathbb{C}^n$ has the same properties if and only if $x_0 - x_1 \in \text{Ker}(A)$ (since $Ax_0 = y_0$ and $Ax_1 = y_0$, by the uniqueness of y_0). As we already observed, $Ax_0 - y$ is orthogonal to $\text{Ran}(A)$, i.e., $\langle (Ax_0 - y), Au \rangle = 0$ for all $u \in \mathbb{C}^n$. This means that $\langle (A^*Ax_0 - A^*y), u \rangle = 0$ for all $u \in \mathbb{C}^n$ and, therefore, x_0 satisfies

$$A^*Ax_0 = A^*y. \tag{43}$$

Now, relation (18) shows us that $x_0 = A^+y$ satisfies (43) because $A^*AA^+y \stackrel{(18)}{=} A^*y$. Therefore, we conclude that the set of all $x \in \mathbb{C}^n$ satisfying the condition of $\|Ax - y\|$ being minimal is composed by all vectors of the form $A^+y + x_1$ with $x_1 \in \text{Ker}(A)$. By Proposition 3.3, x_1

is of the form $x_1 = (\mathbb{1}_n - A^+ A)z$ for some $z \in \mathbb{C}^n$, completing the proof. \square

Acknowledgments We are specially grateful to Prof. Nestor Caticha for providing us with some references on applications of the Moore–Penrose pseudoinverse and of the singular values decomposition. This work was supported in part by the Brazilian Agencies CNPq and FAPESP.

Appendix 1: A Brief Review of Hilbert Space Theory and Linear Algebra

In this appendix, we collect the more important definitions and results on linear algebra and Hilbert space theory that we used in the main part of this paper. For the benefit of the reader, especially of students, we provide all results with proofs.

Hilbert Spaces: Basic Definitions

A scalar product in a complex vector space \mathcal{V} is a function $\mathcal{V} \times \mathcal{V} \rightarrow \mathbb{C}$, denoted here by $\langle \cdot, \cdot \rangle$, such that the following conditions are satisfied: (1) For all $u \in \mathcal{V}$, one has $\langle u, u \rangle \geq 0$ and $\langle u, u \rangle = 0$ if and only if $u = 0$; (2) for all $u, v_1, v_2 \in \mathcal{V}$ and all $\alpha_1, \alpha_2 \in \mathbb{C}$, one has $\langle u, (\alpha_1 v_1 + \alpha_2 v_2) \rangle = \alpha_1 \langle u, v_1 \rangle + \alpha_2 \langle u, v_2 \rangle$ and $\langle (\alpha_1 v_1 + \alpha_2 v_2), u \rangle = \overline{\alpha_1} \langle v_1, u \rangle + \overline{\alpha_2} \langle v_2, u \rangle$; and (3) $\overline{\langle u, v \rangle} = \langle v, u \rangle$ for all $u, v \in \mathcal{V}$.

The norm associated to the scalar product $\langle \cdot, \cdot \rangle$ is defined by $\|u\| := \sqrt{\langle u, u \rangle}$, for all $u \in \mathcal{V}$. As one easily verifies using the defining properties of a scalar product, this norm satisfies the so-called *parallelogram identity*: For all $a, b \in \mathcal{V}$, one has

$$\|a + b\|^2 + \|a - b\|^2 = 2\|a\|^2 + 2\|b\|^2. \tag{44}$$

We say that a sequence $\{v_n \in \mathcal{V}, n \in \mathbb{N}\}$ of vectors in \mathcal{V} converges to an element $v \in \mathcal{V}$ if for all $\epsilon > 0$ there exists a $N(\epsilon) \in \mathbb{N}$ such that $\|v_n - v\| \leq \epsilon$ for all $n \geq N(\epsilon)$. In this case, we write $v = \lim_{n \rightarrow \infty} v_n$. A sequence $\{v_n \in \mathcal{V}, n \in \mathbb{N}\}$ of vectors in \mathcal{V} is said to be a *Cauchy sequence* if for all $\epsilon > 0$ there exists a $N(\epsilon) \in \mathbb{N}$ such that $\|v_n - v_m\| \leq \epsilon$ for all $n, m \in \mathbb{N}$ such that $n \geq N(\epsilon)$ and $m \geq N(\epsilon)$. A complex vector space \mathcal{V} is said to be a *Hilbert space* if it has a scalar product and if it is *complete*, i.e., if all Cauchy sequences in \mathcal{V} converge to an element of \mathcal{V} .

The Best Approximant Theorem

A subset A of a Hilbert space \mathcal{H} is said to be *convex* if for all $u, v \in A$ and all $\mu \in [0, 1]$ one has $\mu u + (1 - \mu)v \in A$. A subset A of a Hilbert space \mathcal{H} is said to be *closed* if every sequence $\{u_n \in A, n \in \mathbb{N}\}$ of elements

of A that converges in \mathcal{H} converges to an element of A . The following theorem is of fundamental importance in the theory of Hilbert spaces.

Theorem A.1 (Best Approximant Theorem) *Let A be a convex and closed subset of a Hilbert space \mathcal{H} . Then, for all $x \in \mathcal{H}$ there exists a unique $y \in A$ such that $\|x - y\|$ equals the smallest possible distance between x and A , that means, $\|x - y\| = \inf_{y' \in A} \|x - y'\|$.*

Proof Let $D \geq 0$ be defined by $D = \inf_{y' \in A} \|x - y'\|$. For each $n \in \mathbb{N}$, let us choose a vector $y_n \in A$ with the property that $\|x - y_n\|^2 < D^2 + \frac{1}{n}$. Such a choice is always possible, by the definition of the infimum of a set of real numbers bounded from below.

Let us now prove that the sequence $y_n, n \in \mathbb{N}$ is a Cauchy sequence in \mathcal{H} . Let us take $a = x - y_n$ and $b = x - y_m$ in the parallelogram identity (44). Then, $\|2x - (y_m + y_n)\|^2 + \|y_m - y_n\|^2 = 2\|x - y_n\|^2 + 2\|x - y_m\|^2$. This can be written as $\|y_m - y_n\|^2 = 2\|x - y_n\|^2 + 2\|x - y_m\|^2 - 4\|x - (y_m + y_n)/2\|^2$. Now, using the fact that $\|x - y_n\|^2 < D^2 + \frac{1}{n}$ for each $n \in \mathbb{N}$, we get

$$\|y_m - y_n\|^2 \leq 4D^2 + 2\left(\frac{1}{n} + \frac{1}{m}\right) - 4\|x - (y_m + y_n)/2\|^2.$$

Now $(y_m + y_n)/2 \in A$, since the left-hand side is a convex linear combination of elements of the convex set A . Hence, by the definition of D , $\|x - (y_m + y_n)/2\|^2 \geq D^2$. Therefore, we have

$$\begin{aligned} \|y_m - y_n\|^2 &\leq 4D^2 + 2\left(\frac{1}{n} + \frac{1}{m}\right) - 4D^2 \\ &= 2\left(\frac{1}{n} + \frac{1}{m}\right). \end{aligned}$$

The right-hand side can be made arbitrarily small, by taking both m and n large enough, proving that $\{y_n\}_{n \in \mathbb{N}}$ is a Cauchy sequence. Since A is a closed subspace of the complete space \mathcal{H} , the sequence $\{y_n\}_{n \in \mathbb{N}}$ converges to $y \in A$.

Now we prove that $\|x - y\| = D$. In fact, for all $n \in \mathbb{N}$, one has

$$\begin{aligned} \|x - y\| &= \|(x - y_n) - (y - y_n)\| \\ &\leq \|x - y_n\| + \|y - y_n\| \\ &< \sqrt{D^2 + \frac{1}{n}} + \|y - y_n\|. \end{aligned}$$

Taking $n \rightarrow \infty$ and using the fact that y_n converges to y , we conclude that $\|x - y\| \leq D$. On the other hand, $\|x - y\| \geq D$ by the definition of D and we must have $\|x - y\| = D$.

At last, it remains to prove the uniqueness of y . Assume that there is another $y' \in A$ such that $\|x - y'\| = D$. Using again the parallelogram identity (44), but now with $a = x - y$ and $b = x - y'$, we get

$$\begin{aligned} & \|2x - (y + y')\|^2 + \|y - y'\|^2 \\ &= 2\|x - y\|^2 + 2\|x - y'\|^2 = 4D^2, \end{aligned}$$

which means that

$$\begin{aligned} \|y - y'\|^2 &= 4D^2 - \|2x - (y + y')\|^2 \\ &= 4D^2 - 4\|x - (y + y')/2\|^2. \end{aligned}$$

Since $(y + y')/2 \in A$ (for A being convex), it follows that $\|x - (y + y')/2\|^2 \geq D^2$ and, hence, $\|y - y'\|^2 \leq 0$, proving that $y = y'$. \square

Orthogonal Complements

If E is a subset of a Hilbert space \mathcal{H} , we define its *orthogonal complement* E^\perp as the set of vectors in \mathcal{H} orthogonal to all vectors in E : $E^\perp = \{y \in \mathcal{H} \mid \langle y, x \rangle = 0 \text{ for all } x \in E\}$. The following proposition is of fundamental importance:

Proposition A.2 *The orthogonal complement E^\perp of a subset E of a Hilbert space \mathcal{H} is a closed linear subspace of \mathcal{H} .*

Proof If $x, y \in E^\perp$, then, for any $\alpha, \beta \in \mathbb{C}$, one has $\langle \alpha x + \beta y, z \rangle = \overline{\alpha} \langle x, z \rangle + \overline{\beta} \langle y, z \rangle = 0$ for any $z \in E$, showing that $\alpha x + \beta y \in E^\perp$. Hence, E^\perp is a linear subspace of \mathcal{H} . If x_n is a sequence in E^\perp converging to $x \in \mathcal{H}$, then, for all $z \in E$, one has $\langle x, z \rangle = \left\langle \lim_{n \rightarrow \infty} x_n, z \right\rangle = \lim_{n \rightarrow \infty} \langle x_n, z \rangle = 0$, since $\langle x_n, z \rangle = 0$ for all n . Hence, $x \in E^\perp$, showing that E^\perp is closed. Above, in the first equality, we used the continuity of the scalar product. \square

The Orthogonal Decomposition Theorem

Theorem A.3 (Orthogonal Decomposition Theorem) *Let \mathcal{M} be a closed and linear (and therefore convex) subspace of a Hilbert space \mathcal{H} . Then every $x \in \mathcal{H}$ can be written in a unique way in the form $x = y + z$, with*

$y \in \mathcal{M}$ and $z \in \mathcal{M}^\perp$. The vector y is such that $\|x - y\| = \inf_{y' \in \mathcal{M}} \|x - y'\|$, i.e., is the best approximant of x in \mathcal{M} .

Proof Let x be an arbitrary element of \mathcal{H} . Since \mathcal{M} is convex and closed, let us evoke Theorem 6.2 and choose y as the (unique) element of \mathcal{M} such that $\|x - y\| = \inf_{y' \in \mathcal{M}} \|x - y'\|$. Defining $z := x - y$, all we have to do is to show that $z \in \mathcal{M}^\perp$ and to show uniqueness of y and z . Let us first prove that $z \in \mathcal{M}^\perp$. By the definition of y , one has $\|x - y\| \leq \|x - y - \lambda y'\|^2$ for all $\lambda \in \mathbb{C}$ and all $y' \in \mathcal{M}$. By the definition of z , it follows that $\|z\|^2 \leq \|z - \lambda y'\|^2$ for all $\lambda \in \mathbb{C}$. Writing the right-hand side as $\langle z - \lambda y', z - \lambda y' \rangle$, we get $\|z\|^2 \leq \|z\|^2 - 2\text{Re}(\lambda \langle z, y' \rangle) + |\lambda|^2 \|y'\|^2$. Hence,

$$2\text{Re}(\lambda \langle z, y' \rangle) \leq |\lambda|^2 \|y'\|^2. \tag{45}$$

Now, write $\langle z, y' \rangle = |\langle z, y' \rangle| e^{i\alpha}$, for some $\alpha \in \mathbb{R}$. Since (45) holds for all $\lambda \in \mathbb{C}$, we can pick λ in the form $\lambda = t e^{-i\alpha}$, $t > 0$, and (45) becomes $2t |\langle z, y' \rangle| \leq t^2 \|y'\|^2$. Hence, $|\langle z, y' \rangle| \leq \frac{t}{2} \|y'\|^2$, for all $t > 0$. But this is only possible if the left-hand side vanishes: $|\langle z, y' \rangle| = 0$. Since y' is an arbitrary element of \mathcal{M} , this shows that $z \in \mathcal{M}^\perp$.

To prove uniqueness, assume that $x = y' + z'$ with $y' \in \mathcal{M}$ and $z' \in \mathcal{M}^\perp$. We would have $y - y' = z' - z$. But $y - y' \in \mathcal{M}$ and $z' - z \in \mathcal{M}^\perp$. Hence, both belong to $\mathcal{M} \cap \mathcal{M}^\perp = \{0\}$, showing that $y - y' = z' - z = 0$. \square

The Spectrum of a Matrix

The *spectrum* of a matrix $A \in \text{Mat}(\mathbb{C}, n)$, denoted by $\sigma(A)$, is the set of all $\lambda \in \mathbb{C}$ for which the matrix $\lambda \mathbb{1} - A$ has no inverse.

The *characteristic polynomial* of a matrix $A \in \text{Mat}(\mathbb{C}, n)$ is defined by $p_A(z) := \det(z\mathbb{1} - A)$. It is clearly a polynomial of degree n on z . It follows readily from these definitions that $\sigma(A)$ coincides with the roots of p_A . The elements of $\sigma(A)$ are said to be the *eigenvalues* of A . If λ is an eigenvalue of A , the matrix $A - \lambda \mathbb{1}$ has no inverse, and therefore, there exists at least one non-vanishing vector $v \in \mathbb{C}^n$ such that $(A - \lambda \mathbb{1})v = 0$, that means, such that $Av = \lambda v$. Such a vector is said to be an *eigenvector* of A with eigenvalue λ . The set of all eigenvectors associated to a given eigenvalues (plus the null vector) is a linear subspace of \mathbb{C}^n , as one easily sees.

The multiplicity of a root λ of the characteristic polynomial of a matrix $A \in \text{Mat}(\mathbb{C}, n)$ is called the *algebraic multiplicity* of the eigenvalue λ . The dimension of the subspace generated by the eigenvectors associated

to the eigenvalues λ is called the *geometric multiplicity* of the eigenvalue λ . The *algebraic multiplicity* of an eigenvalue is always larger than or equal to its *geometric multiplicity*.

The Neighborhood of Singular Matrices

Proposition A.4 *Let $A \in \text{Mat}(\mathbb{C}, n)$ be arbitrary and let $B \in \text{Mat}(\mathbb{C}, n)$ be a non-singular matrix. Then, there exist constants M_1 and M_2 (depending on A and B) with $0 < M_1 \leq M_2$ such that $A + \mu B$ is invertible for all $\mu \in \mathbb{C}$ with $0 < |\mu| < M_1$ and for all $\mu \in \mathbb{C}$ with $|\mu| > M_2$.*

Proof Since B has an inverse, we may write $A + \mu B = (\mu \mathbb{1} + AB^{-1})B$. Hence, $A + \mu B$ has an inverse if and only if $\mu \mathbb{1} + AB^{-1}$ is non-singular.

Let $C \equiv -AB^{-1}$ and let $\{\lambda_1, \dots, \lambda_n\} \subset \mathbb{C}$ be the n not necessarily distinct roots of the characteristic polynomial p_C of C . If all roots vanish, we take $M_1 = M_2 > 0$, arbitrary. Otherwise, let us define $M_1 := \min\{|\lambda_k|, \lambda_k \neq 0\}$ and $M_2 := \max\{|\lambda_k|, k = 1, \dots, n\}$. Then, the sets $\{\mu \in \mathbb{C} \mid 0 < |\mu| < M_1\}$ and $\{\mu \in \mathbb{C} \mid |\mu| > M_2\}$ do not contain roots of p_C , and therefore, for μ in these sets, the matrix $\mu \mathbb{1} - C = \mu \mathbb{1} + AB^{-1}$ is non-singular. \square

Similar Matrices

Two matrices $A \in \text{Mat}(\mathbb{C}, n)$ and $B \in \text{Mat}(\mathbb{C}, n)$ are said to be similar if there is a non-singular matrix $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1}AP = B$. One has the following elementary fact:

Proposition A.5 *Let A and $B \in \text{Mat}(\mathbb{C}, n)$ be two similar matrices. Then their characteristic polynomials coincide, $p_A = p_B$, and therefore, their spectra also coincide, $\sigma(A) = \sigma(B)$, as well as the geometric multiplicities of their eigenvalues*

Proof Let $P \in \text{Mat}(\mathbb{C}, n)$ be such that $P^{-1}AP = B$. Then, $p_A(z) = \det(z\mathbb{1} - A) = \det(P^{-1}(z\mathbb{1} - A)P) = \det(z\mathbb{1} - P^{-1}AP) = \det(z\mathbb{1} - B) = p_B(z)$, for all $z \in \mathbb{C}$. \square

The Spectrum of Products of Matrices

The next proposition contains a non-evident consequence of Propositions A.4 and A.5.

Proposition A.6 *Let $A, B \in \text{Mat}(\mathbb{C}, n)$. Then, the characteristic polynomials of the matrices AB and BA coincide: $p_{AB} = p_{BA}$. Therefore, their spectra also co-*

incide, $\sigma(AB) = \sigma(BA)$, as well as the geometric multiplicities of their eigenvalues.

Proof If A or B (or both) are non-singular, then AB and BA are similar. In fact, in the first case, we can write $AB = A(BA)A^{-1}$ and in the second one has $AB = B^{-1}(BA)B$. In both cases, the claim follows from Proposition A.5. Let us now consider the case where neither A nor B are invertible. We know from Proposition A.4 that there exists $M > 0$ such that $A + \mu \mathbb{1}$ is non-singular for all $\mu \in \mathbb{C}$ with $0 < |\mu| < M$. Hence, for such values of μ , we have by the argument above that $p_{(A+\mu\mathbb{1})B} = p_{B(A+\mu\mathbb{1})}$. Now the coefficient of the polynomials $p_{(A+\mu\mathbb{1})B}$ and $p_{B(A+\mu\mathbb{1})}$ are polynomials in μ and, therefore, are continuous. Hence, the equality $p_{(A+\mu\mathbb{1})B} = p_{B(A+\mu\mathbb{1})}$ remains valid by taking the limit $\mu \rightarrow 0$, leading to $p_{AB} = p_{BA}$. \square

Proposition A.6 can be extended to products of non-square matrices:

Proposition A.7 *Let $A \in \text{Mat}(\mathbb{C}, m, n)$ and $B \in \text{Mat}(\mathbb{C}, n, m)$. Clearly, $AB \in \text{Mat}(\mathbb{C}, m)$ and $BA \in \text{Mat}(\mathbb{C}, n)$. Then, one has $x^n p_{AB}(x) = x^m p_{BA}(x)$. Therefore, $\sigma(AB) \setminus \{0\} = \sigma(BA) \setminus \{0\}$, i.e., the set of non-zero eigenvalues of AB coincide with the set of non-zero eigenvalues of BA .*

Proof Consider the two $(m+n) \times (m+n)$ matrices defined by

$$A' := \begin{pmatrix} A & \mathbb{0}_{m,m} \\ \mathbb{0}_{n,n} & \mathbb{0}_{n,m} \end{pmatrix} \quad \text{and} \quad B' := \begin{pmatrix} B & \mathbb{0}_{n,n} \\ \mathbb{0}_{m,m} & \mathbb{0}_{m,n} \end{pmatrix}.$$

See (8). It is easy to see that

$$A'B' = \begin{pmatrix} AB & \mathbb{0}_{m,n} \\ \mathbb{0}_{n,m} & \mathbb{0}_{n,n} \end{pmatrix} \quad \text{and that} \quad B'A' = \begin{pmatrix} BA & \mathbb{0}_{n,m} \\ \mathbb{0}_{m,n} & \mathbb{0}_{m,m} \end{pmatrix}.$$

From this, it is now easy to see that $p_{A'B'}(x) = x^n p_{AB}(x)$ and that $p_{B'A'}(x) = x^m p_{BA}(x)$. By Proposition A.6, one has $p_{A'B'}(x) = p_{B'A'}(x)$, completing the proof. \square

Diagonalizable Matrices

A matrix $A \in \text{Mat}(\mathbb{C}, n)$ is said to be *diagonalizable* if it is similar to a diagonal matrix. Hence, $A \in \text{Mat}(\mathbb{C}, n)$ is diagonalizable if there exists a non-singular matrix $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1}AP$ is diagonal. The next theorem gives a necessary and sufficient condition for a matrix to be diagonalizable:

Theorem A.8 *A matrix $A \in \text{Mat}(\mathbb{C}, n)$ is diagonalizable if and only if it has n linearly independent*

eigenvectors, i.e., if the subspace generated by its eigenvectors is n -dimensional.

Proof Let us assume that A has n linearly independent eigenvectors $\{v^1, \dots, v^n\}$, whose eigenvalues are $\{d_1, \dots, d_n\}$, respectively. Let $P \in \text{Mat}(\mathbb{C}, n)$ be defined by $P = \llbracket v^1, \dots, v^n \rrbracket$. By (12), one has

$$AP = \llbracket Av^1, \dots, Av^n \rrbracket = \llbracket d_1v^1, \dots, d_nv^n \rrbracket$$

and by (13), one has $\llbracket d_1v^1, \dots, d_nv^n \rrbracket = PD$. Therefore, $AP = PD$. Since the columns of P are linearly independent, P is non-singular and one has $P^{-1}AP = D$, showing that A is diagonalizable.

Let us now assume that A is diagonalizable and that there is a non-singular $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1}AP = D = \text{diag}(d_1, \dots, d_n)$. It is evident that the vectors of the canonical base (10) are eigenvectors of D , with $D\mathbf{e}_a = d_a\mathbf{e}_a$. Therefore, $v_a = P\mathbf{e}_a$ are eigenvectors of A , since $Av_a = AP\mathbf{e}_a = PD\mathbf{e}_a = P(d_a\mathbf{e}_a) = d_aP\mathbf{e}_a = d_av_a$. To show that these vectors v_a are linearly independent, assume that there are complex numbers $\alpha_1, \dots, \alpha_n$ such that $\alpha_1v_1 + \dots + \alpha_nv_n = 0$. Multiplying by P^{-1} from the left, we get $\alpha_1\mathbf{e}_1 + \dots + \alpha_n\mathbf{e}_n = 0$, implying $\alpha_1 = \dots = \alpha_n = 0$, since the elements \mathbf{e}_a of the canonical basis are linearly independent. \square

The spectral theorem is one of the fundamental results of functional analysis, and its version for bounded and unbounded self-adjoint operators in Hilbert spaces is of fundamental importance for the so-called probabilistic interpretation of quantum mechanics. Here we prove its simplest version for square matrices.

Theorem A.9 (Spectral Theorem for Matrices) *A matrix $A \in \text{Mat}(\mathbb{C}, n)$ is diagonalizable if and only if there exist $r \in \mathbb{N}$, $1 \leq r \leq n$, scalars $\alpha_1, \dots, \alpha_r \in \mathbb{C}$, and non-zero distinct projectors $E_1, \dots, E_r \in \text{Mat}(\mathbb{C}, n)$ such that*

$$A = \sum_{a=1}^r \alpha_a E_a, \tag{46}$$

and

$$\mathbb{1} = \sum_{a=1}^r E_a, \tag{47}$$

with $E_i E_j = \delta_{i,j} E_j$. The numbers $\alpha_1, \dots, \alpha_r$ are the distinct eigenvalues of A .

The projectors E_a in (46) are called the *spectral projectors* of A . The decomposition (46) is called *spectral decomposition* of A . In Proposition A.11, we will show

how the spectral projections E_a can be expressed in terms of polynomials in A . In Proposition A.12, we establish the uniqueness of the spectral decomposition of a diagonalizable matrix.

Proof of Theorem A.9 If $A \in \text{Mat}(\mathbb{C}, n)$ is diagonalizable, there exists $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1}AP = D = \text{diag}(\lambda_1, \dots, \lambda_n)$, where $\lambda_1, \dots, \lambda_n$ are the eigenvalues of A . Let us denote by $\{\alpha_1, \dots, \alpha_r\}$, $1 \leq r \leq n$, the set of all *distinct* eigenvalues of A .

One can clearly write $D = \sum_{a=1}^r \alpha_a K_a$, where $K_a \in \text{Mat}(\mathbb{C}, n)$ are diagonal matrices having 0 or 1 as diagonal elements, so that

$$(K_a)_{ij} = \begin{cases} 1, & \text{if } i = j \text{ and } (D)_{ii} = \alpha_a, \\ 0, & \text{if } i = j \text{ and } (D)_{ii} \neq \alpha_a, \\ 0, & \text{if } i \neq j. \end{cases}$$

Hence, $(K_a)_{ij} = 1$ if $i = j$ and $(D)_{ii} = \alpha_a$ and $(K_a)_{ij} = 0$ otherwise. It is trivial to see that

$$\sum_{a=1}^r K_a = \mathbb{1} \tag{48}$$

and that

$$K_a K_b = \delta_{a,b} K_a. \tag{49}$$

Since $A = PDP^{-1}$, one has $A = \sum_{a=1}^r \alpha_a E_a$, where $E_a := PK_a P^{-1}$. It is easy to prove from (48) that $\mathbb{1} = \sum_{a=1}^r E_a$ and it is easy to prove from (49) that $E_i E_j = \delta_{i,j} E_j$.

Reciprocally, let us now assume that A has a representation like (46), with the E_a 's having the above-mentioned properties. Let us first notice that for any vector x and for $k \in \{1, \dots, r\}$, one has by (46)

$$A E_k x = \sum_{j=1}^r \alpha_j E_j E_k x = \alpha_k E_k x.$$

Hence, $E_k x$ is either zero or is an eigenvalue of A . Therefore, the subspace \mathcal{S} generated by all vectors $\{E_k x, x \in \mathbb{C}^n, k = 1, \dots, r\}$ is a subspace of the space \mathcal{A} generated by all eigenvectors of A . However, from (47), one has, for all $x \in \mathbb{C}^n$, $x = \mathbb{1}x = \sum_{k=1}^r E_k x$, and this reveals that $\mathbb{C}^n = \mathcal{S} \subset \mathcal{A}$. Hence, $\mathcal{A} = \mathbb{C}^n$, and by Theorem A.8, A is diagonalizable. \square

The spectral theorem has the following corollary, known as the *functional calculus*:

Theorem A.10 (Functional Calculus) *Let $A \in \text{Mat}(\mathbb{C}, n)$ be diagonalizable and let $A = \sum_{a=1}^r \alpha_a E_a$*

be its spectral decomposition. Then, for any polynomial p , one has $p(A) = \sum_{a=1}^r p(\alpha_a) E_a$.

Proof By the properties of the spectral projectors E_a , one sees easily that $A^2 = \sum_{a,b=1}^r \alpha_a \alpha_b E_a E_b = \sum_{a,b=1}^r \alpha_a \alpha_b \delta_{a,b} E_a = \sum_{a=1}^r (\alpha_a)^2 E_a$. It is then easy to prove by induction that $A^m = \sum_{a=1}^r (\alpha_a)^m E_a$, for all $m \in \mathbb{N}_0$ (by adopting the convention that $A^0 = \mathbb{1}$, the case $m = 0$ is simply (47)). From this, the rest of the proof is elementary. \square

One can also easily show that for a non-singular diagonalizable matrix $A \in \text{Mat}(\mathbb{C}, n)$, one has

$$A^{-1} = \sum_{a=1}^r \frac{1}{\alpha_a} E_a. \tag{50}$$

Getting the Spectral Projections

One of the most useful consequences of the functional calculus is an explicit formula for the spectral projections of a diagonalizable matrix A in terms of a polynomial on A .

Proposition A.11 *Let $A \in \text{Mat}(\mathbb{C}, n)$ be non-zero and diagonalizable and let $A = \alpha_1 E_1 + \dots + \alpha_r E_r$ be its spectral decomposition. Let the polynomials $p_j, j = 1, \dots, r$, be defined by*

$$p_j(x) := \prod_{\substack{l=1 \\ l \neq j}}^r \left(\frac{x - \alpha_l}{\alpha_j - \alpha_l} \right). \tag{51}$$

Then,

$$E_j = p_j(A) = \left(\prod_{\substack{k=1 \\ k \neq j}}^r \frac{1}{\alpha_j - \alpha_k} \right) \prod_{\substack{l=1 \\ l \neq j}}^r (A - \alpha_l \mathbb{1}) \tag{52}$$

for all $j = 1, \dots, r$.

Proof By the definition of the polynomials p_j , it is evident that $p_j(\alpha_k) = \delta_{j,k}$. Hence, by Theorem A.10, $p_j(A) = \sum_{k=1}^r p_j(\alpha_k) E_k = E_j$. \square

Uniqueness of the Spectral Decomposition

Proposition A.12 *The spectral decomposition of a diagonalizable matrix $A \in \text{Mat}(\mathbb{C}, n)$ is unique.*

Proof Let $A = \sum_{k=1}^r \alpha_k E_k$ be the spectral decomposition of A as described in Theorem A.9, where $\alpha_k, k = 1, \dots, r$, with $1 \leq r \leq n$ are the distinct eigenvalues of A , Let $A = \sum_{k=1}^s \beta_k F_k$ be a second representation of A , where the β_k 's are distinct and where the F_k 's are non-vanishing and satisfy $F_j F_l = \delta_{j,l} F_l$ and $\mathbb{1} = \sum_{k=1}^s F_k$. For a vector $x \neq 0$, it holds $x = \sum_{k=1}^s F_k x$, so that not all vectors $F_k x$ vanish. Let $F_{k_0} x \neq 0$. One has $A F_{k_0} x = \sum_{k=1}^s \beta_k F_k F_{k_0} x = \beta_{k_0} F_{k_0} x$. This shows that β_{k_0} is one of the eigenvalues of A and, hence, $\{\beta_1, \dots, \beta_s\} \subset \{\alpha_1, \dots, \alpha_r\}$ and we must have $s \leq r$. Let us order both sets such that $\beta_k = \alpha_k$ for all $1 \leq k \leq s$. Hence,

$$A = \sum_{k=1}^r \alpha_k E_k = \sum_{k=1}^s \alpha_k F_k. \tag{53}$$

Now, consider the polynomials $p_j, j = 1, \dots, r$, defined in (51), for which $p_j(\alpha_j) = 1$ and $p_j(\alpha_k) = 0$ for all $k \neq j$. By the functional calculus, it follows from (53) that, for $1 \leq j \leq s$,

$$p_j(A) = \underbrace{\sum_{k=1}^r p_j(\alpha_k) E_k}_{=E_j} = \underbrace{\sum_{k=1}^s p_j(\alpha_k) F_k}_{=F_j}, \quad \therefore E_j = F_j.$$

(The equality $p_j(A) = \sum_{k=1}^s p_j(\alpha_k) F_k$ follows from the fact that the E_k 's and the F_k 's satisfy the same algebraic relations and, hence, the functional calculus also holds for the representation of A in terms of the F_k 's). Since $\mathbb{1} = \sum_{k=1}^r E_k = \sum_{k=1}^s E_k$ and $E_j = F_j$ for all $1 \leq j \leq s$, one has $\sum_{k=s+1}^r E_k = 0$. Hence, multiplying by E_l , with $s+1 \leq l \leq r$, it follows that $E_l = 0$ for all $s+1 \leq l \leq r$. This is only possible if $r = s$, since the E_k 's are non-vanishing. This completes the proof. \square

Self-Adjointness and Diagonalizability

Let $A \in \text{Mat}(\mathbb{C}, m, n)$. The adjoint matrix $A^* \in \text{Mat}(\mathbb{C}, n, m)$ is defined as the unique matrix for which the equality

$$\langle u, Av \rangle = \langle A^*u, v \rangle$$

holds for all $u \in \mathbb{C}^m$ and all $v \in \mathbb{C}^n$. If A_{ij} are the matrix elements of A in the canonical basis, it is an easy exercise to show that $(A^*)_{ij} = \overline{A_{ji}}$, where the bar denotes complex conjugation. It is trivial to prove that the

following properties hold: 1. $(\alpha_1 A_1 + \alpha_2 A_2)^* = \overline{\alpha_1} A_1^* + \overline{\alpha_2} A_2^*$ for all $A_1, A_2 \in \text{Mat}(\mathbb{C}, m, n)$ and all $\alpha_1, \alpha_2 \in \mathbb{C}$; 2. $(AB)^* = B^*A^*$ for all $A \in \text{Mat}(\mathbb{C}, m, n)$ and $B \in \text{Mat}(\mathbb{C}, p, m)$; 3. $A^{**} \equiv (A^*)^* = A$ for all $A \in \text{Mat}(\mathbb{C}, m, n)$.

A square matrix $A \in \text{Mat}(\mathbb{C}, n)$ is said to be *self-adjoint* if $A = A^*$. A square matrix $U \in \text{Mat}(\mathbb{C}, n)$ is said to be *unitary* if $U^{-1} = U^*$. Self-adjoint matrices have real eigenvalues. In fact, if A is self-adjoint, $\lambda \in \sigma(A)$, and $v \in \mathbb{C}^n$ is a normalized (i.e., $\|v\| = 1$) eigenvector of A with eigenvalue λ , then $\lambda = \lambda(v, v) = \langle v, \lambda v \rangle = \langle v, Av \rangle = \langle Av, v \rangle = \langle \lambda v, v \rangle = \overline{\lambda} \langle v, v \rangle = \overline{\lambda}$, showing that $\lambda \in \mathbb{R}$.

Projectors and Orthogonal Projectors

A matrix $E \in \text{Mat}(\mathbb{C}, n)$ is said to be a *projector* if $E^2 = E$, and it is said to be a *orthogonal projector* if it is a self-adjoint projector: $E^2 = E$ and $E^* = E$. An important example of an orthogonal projector is the following. Let $v \in \mathbb{C}^n$ be such that $\|v\| = 1$ and define,

$$P_v u := \langle v, u \rangle v, \tag{54}$$

for each $u \in \mathbb{C}^n$. In the canonical basis, the matrix elements of P_v are given by $(P_v)_{ij} = \overline{v_j} v_i$, where the v_k 's are the components of v . One has,

$$P_v^2 u = \langle v, u \rangle P_v v = \langle v, u \rangle \langle v, v \rangle v = \langle v, u \rangle v = P_v u,$$

proving that $P_v^2 = P_v$. On the other hand, for any $a, b \in \mathbb{C}^n$, we get

$$\begin{aligned} \langle a, P_v b \rangle &= \langle a, \langle v, b \rangle v \rangle = \langle v, b \rangle \langle a, v \rangle \\ &= \overline{\langle a, v \rangle} \langle v, b \rangle = \langle \langle v, a \rangle v, b \rangle = \langle P_v a, b \rangle, \end{aligned}$$

showing that $P_v^* = P_v$. Another relevant fact is that if v_1 and v_2 are orthogonal unit vectors, i.e., $\langle v_i, v_j \rangle = \delta_{ij}$, then $P_{v_1} P_{v_2} = P_{v_2} P_{v_1} = 0$. In fact, for any $a \in \mathbb{C}^n$, one has

$$\begin{aligned} P_{v_1}(P_{v_2} a) &= P_{v_1}(\langle v_2, a \rangle v_2) = \langle v_2, a \rangle P_{v_1} v_2 \\ &= \langle v_2, a \rangle \langle v_1, v_2 \rangle v_1 = 0. \end{aligned}$$

This shows that $P_{v_1} P_{v_2} = 0$ and, since both are self-adjoint, one has also $P_{v_2} P_{v_1} = 0$.

Spectral Theorem for Self-Adjoint Matrices

The following theorem establishes a fundamental fact about self-adjoint matrices.

Theorem A.13 (Spectral Theorem for Self-Adjoint Matrices) *If $A \in \text{Mat}(\mathbb{C}, n)$ is self-adjoint, one can find an orthonormal set $\{v_1, \dots, v_n\}$ of eigenvectors of A*

with real eigenvalues $\lambda_1, \dots, \lambda_n$, respectively, and one has the spectral representation

$$A = \lambda_1 P_{v_1} + \dots + \lambda_n P_{v_n}, \tag{55}$$

where $P_{v_k} u := \langle v_k, u \rangle v_k$ satisfy $P_{v_k}^* = P_{v_k}$ and $P_{v_j} P_{v_k} = \delta_{jk} P_{v_k}$ and one has $\sum_{k=1}^n P_{v_k} = \mathbb{1}$.

Therefore, if $A \in \text{Mat}(\mathbb{C}, n)$ is a self-adjoint matrix, it is diagonalizable. Moreover, there is a unitary $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1} A P = \text{diag}(\lambda_1, \dots, \lambda_n)$.

Proof Let $\lambda_1 \in \mathbb{R}$ be an eigenvalue of A and let v_1 be a corresponding eigenvector. Let us choose $\|v_1\| = 1$. Define $A_1 \in \text{Mat}(\mathbb{C}, n)$ by $A_1 := A - \lambda_1 P_{v_1}$. Since both A and P_{v_1} are self-adjoint, so is A_1 , since λ_1 is real.

It is easy to check that $A_1 v_1 = 0$. Moreover, $[v_1]^\perp$, the subspace orthogonal to v_1 , is invariant under the action of A_1 . In fact, for $w \in [v_1]^\perp$, one has $\langle A_1 w, v_1 \rangle = \langle w, A_1 v_1 \rangle = 0$, showing that $A_1 w \in [v_1]^\perp$.

It is therefore obvious that the restriction of A_1 to $[v_1]^\perp$ is also a self-adjoint operator. Let $v_2 \in [v_1]^\perp$ be an eigenvector of this self-adjoint restriction with eigenvalues λ_2 and choose $\|v_2\| = 1$. Define

$$A_2 := A_1 - \lambda_2 P_{v_2} = A - \lambda_1 P_{v_1} - \lambda_2 P_{v_2}.$$

Since λ_2 is real, A_2 is self-adjoint. Moreover, A_2 annihilates the vectors in the subspace $[v_1, v_2]$ and keeps $[v_1, v_2]^\perp$ invariant. In fact, $A_2 v_1 = A v_1 - \lambda_1 P_{v_1} v_1 - \lambda_2 P_{v_2} v_1 = \lambda_1 v_1 - \lambda_1 v_1 - \lambda_2 \langle v_2, v_1 \rangle v_2 = 0$. Analogously, $A_2 v_2 = A v_2 - \lambda_1 P_{v_1} v_2 - \lambda_2 P_{v_2} v_2 = \lambda_2 v_2 - \lambda_2 v_2 = 0$. Finally, for any $\alpha, \beta \in \mathbb{C}$ and $w \in [v_1, v_2]^\perp$, one has $\langle A_2 w, (\alpha v_1 + \beta v_2) \rangle = \langle w, A_2(\alpha v_1 + \beta v_2) \rangle = 0$, showing that $[v_1, v_2]^\perp$ is invariant by the action of A_2 .

Proceeding inductively, we find a set of vectors $\{v_1, \dots, v_n\}$, with $\|v_k\| = 1$ and with $v_a \in [v_1, \dots, v_{a-1}]^\perp$ for $2 \leq a \leq n$, and a set of real numbers $\{\lambda_1, \dots, \lambda_n\}$ such that $A_n = A - \lambda_1 P_{v_1} - \dots - \lambda_n P_{v_n}$ annihilates the subspace $[v_1, \dots, v_n]$. But, since $\{v_1, \dots, v_n\}$ is an orthonormal set, one must have $[v_1, \dots, v_n] = \mathbb{C}^n$, and therefore, we must have $A_n = 0$, meaning that

$$A = \lambda_1 P_{v_1} + \dots + \lambda_n P_{v_n}. \tag{56}$$

One has $P_{v_k} P_{v_l} = \delta_{k,l} P_{v_k}$, since $\langle v_k, v_l \rangle = \delta_{kl}$. Moreover, since $\{v_1, \dots, v_n\}$ is a basis in \mathbb{C}^n , one has

$$x = \alpha_1 v_1 + \dots + \alpha_n v_n \tag{57}$$

for all $x \in \mathbb{C}^n$. By taking the scalar product with v_k , one gets that $\alpha_k = \langle v_k, x \rangle$ and, hence,

$$\begin{aligned} x &= \langle v_1, x \rangle v_1 + \dots + \langle v_n, x \rangle v_n \\ &= P_{v_1} x + \dots + P_{v_n} x = (P_{v_1} + \dots + P_{v_n}) x. \end{aligned}$$

Since x was an arbitrary element of \mathbb{C}^n , we established that $P_{v_1} + \dots + P_{v_n} = \mathbb{1}$.

It follows from (56) that $Av_a = \lambda_a v_a$. Hence, each v_k is an eigenvector of A with eigenvalue λ_k . By Theorem A.8, A is diagonalizable: There is $P \in \text{Mat}(\mathbb{C}, n)$ such that $P^{-1}AP = \text{diag}(\lambda_1, \dots, \lambda_n)$. As we saw in the proof of Theorem A.8, we can choose $P = \begin{bmatrix} v^1, & \dots, & v^n \end{bmatrix}$. This is, however, a unitary matrix, since, as one easily checks,

$$P^*P = \begin{pmatrix} \langle v_1, v_1 \rangle & \dots & \langle v_1, v_n \rangle \\ \vdots & \ddots & \vdots \\ \langle v_n, v_1 \rangle & \dots & \langle v_n, v_n \rangle \end{pmatrix} = \mathbb{1},$$

because $\langle v_a, v_b \rangle = \delta_{a,b}$. □

The Polar Decomposition Theorem for Square Matrices

It is well known that every complex number z can be written in the so-called *polar form* $z = |z|e^{i\theta}$, where $|z| \geq 0$ and $\theta \in [-\pi, \pi)$, with $|z| := \sqrt{\bar{z}z}$ and $e^{i\theta} := z|z|^{-1}$. There is an analogous claim for square matrices $A \in \text{Mat}(\mathbb{C}, n)$. This is the content of the so-called Polar Decomposition Theorem, Theorem A.14, below. Let us make some preliminary remarks.

Let $A \in \text{Mat}(\mathbb{C}, n)$ and consider A^*A . One has $(A^*A)^* = A^*A^{**} = A^*A$, and hence, A^*A is self-adjoint. By Theorem A.13, we can find an orthonormal set $\{v_k, k = 1, \dots, n\}$ of eigenvectors of A^*A , with eigenvalues $d_k, k = 1, \dots, n$, respectively, with the matrix

$$P := \begin{bmatrix} v_1, & \dots, & v_n \end{bmatrix} \tag{58}$$

being unitary and such that $P^*(A^*A)P = D := \text{diag}(d_1, \dots, d_n)$. One has $d_k \geq 0$ since $d_k \|v_k\|^2 = d_k \langle v_k, v_k \rangle = \langle v_k, Av_k \rangle = \langle Av_k, Av_k \rangle = \|Av_k\|^2$ and, hence, $d_k = \|Av_k\|^2 / \|v_k\|^2 \geq 0$.

Define $D^{1/2} := \text{diag}(\sqrt{d_1}, \dots, \sqrt{d_n})$. One has $(D^{1/2})^2 = D$. Moreover, $(D^{1/2})^* = D^{1/2}$, since every $\sqrt{d_k}$ is real. The non-negative numbers $\sqrt{d_1}, \dots, \sqrt{d_n}$ are called the *singular values* of A .

Define the matrix $\sqrt{A^*A} \in \text{Mat}(\mathbb{C}, n)$ by

$$\sqrt{A^*A} := PD^{1/2}P^*. \tag{59}$$

The matrix $\sqrt{A^*A}$ is self-adjoint, since $(\sqrt{A^*A})^* = (PD^{1/2}P^*)^* = PD^{1/2}P^* = \sqrt{A^*A}$. Notice that

$(\sqrt{A^*A})^2 = P(D^{1/2})^2P^* = PDP^* = A^*A$. From this, it follows that

$$\begin{aligned} \left(\det(\sqrt{A^*A})\right)^2 &= \det\left(\left(\sqrt{A^*A}\right)^2\right) \\ &= \det(A^*A) = \det(A^*)\det(A) \\ &= \overline{\det(A)}\det(A) = |\det(A)|^2. \end{aligned}$$

Hence, $\det(\sqrt{A^*A}) = |\det(A)|$ and, therefore, $\sqrt{A^*A}$ is invertible if and only if A is invertible.

We will denote $\sqrt{A^*A}$ by $|A|$, following the analogy suggested by the complex numbers. Now we can formulate the polar decomposition theorem for matrices:

Theorem A.14 (Polar Decomposition Theorem) *If $A \in \text{Mat}(\mathbb{C}, n)$, there is a unitary matrix $U \in \text{Mat}(\mathbb{C}, n)$ such that*

$$A = U\sqrt{A^*A}. \tag{60}$$

If A is non-singular, then U is unique. The representation (60) is called the polar representation of A .

Proof As above, let $d_k, k = 1, \dots, n$ be the eigenvalues of A^*A and let $v_k, k = 1, \dots, n$ be a corresponding orthonormal set of eigenvectors: $A^*Av_k = d_kv_k$ and $\langle v_k, v_l \rangle = \delta_{kl}$ (see Theorem A.13).

Since $d_k \geq 0$ we order them in a way that $d_k > 0$ for all $k = 1, \dots, r$ and $d_k = 0$ for all $k = r + 1, \dots, n$. Hence,

$$Av_k = 0 \text{ for all } k = r + 1, \dots, n, \tag{61}$$

because $A^*Av_k = 0$ implies $0 = \langle v_k, A^*Av_k \rangle = \langle Av_k, Av_k \rangle = \|Av_k\|^2$.

For $k = 1, \dots, r$, let w_k be the vectors defined by

$$w_k := \frac{1}{\sqrt{d_k}}Av_k, \quad k = 1, \dots, r. \tag{62}$$

It is easy to see that

$$\begin{aligned} \langle w_k, w_l \rangle &= \frac{1}{\sqrt{d_k d_l}} \langle Av_k, Av_l \rangle = \frac{1}{\sqrt{d_k d_l}} \langle A^*Av_k, v_l \rangle \\ &= \frac{d_k}{\sqrt{d_k d_l}} \langle v_k, v_l \rangle = \frac{d_k}{\sqrt{d_k d_l}} \delta_{kl} = \delta_{kl}, \end{aligned}$$

for all $k, l = 1, \dots, r$. Hence, $\{w_k, k = 1, \dots, r\}$ is an orthonormal set. We can add to this set an additional orthonormal set $\{w_k, k = r + 1, \dots, n\}$ in the orthogonal complement of the set generated by $\{w_k, k = 1, \dots, r\}$ and get a new orthonormal set $\{w_k, k = 1, \dots, n\}$ as a basis for \mathbb{C}^n .

Let $P \in \text{Mat}(\mathbb{C}, n)$ be defined as in (58) and let Q and U be elements of $\text{Mat}(\mathbb{C}, n)$ defined by

$$Q := \begin{bmatrix} w_1, & \dots, & w_n \end{bmatrix}, \quad U := QP^*.$$

Since $\{v_k, k = 1, \dots, n\}$ and $\{w_k, k = 1, \dots, n\}$ are orthonormal sets, one easily sees that P and Q are unitary and, therefore, U is also unitary.

It is easy to show that $AP = QD^{1/2}$, where $D^{1/2} := \text{diag}(\sqrt{d_1}, \dots, \sqrt{d_n})$. In fact,

$$\begin{aligned} AP &\stackrel{(58)}{=} A \begin{bmatrix} v_1, & \dots, & v_n \end{bmatrix} \stackrel{(12)}{=} \begin{bmatrix} Av_1, & \dots, & Av_n \end{bmatrix} \\ &\stackrel{(61)}{=} \begin{bmatrix} Av_1, & \dots, & Av_r, & 0, & \dots, & 0 \end{bmatrix} \\ &\stackrel{(62)}{=} \begin{bmatrix} \sqrt{d_1}w_1, & \dots, & \sqrt{d_r}w_r, & 0, & \dots, & 0 \end{bmatrix} \\ &\stackrel{(13)}{=} \begin{bmatrix} w_1, & \dots, & w_n \end{bmatrix} D^{1/2} = QD^{1/2}. \end{aligned}$$

Now, since $AP = QD^{1/2}$, it follows that $A = QD^{1/2}P^* = UPD^{1/2}P^* \stackrel{(59)}{=} U\sqrt{A^*A}$, as we wanted to show.

To show that U is uniquely determined if A is invertible, assume that there exists U' such that $A = U\sqrt{A^*A} = U'\sqrt{A^*A}$. We noticed above that $\sqrt{A^*A}$ is invertible if and only if A is invertible. Hence, if A is invertible, the equality $U\sqrt{A^*A} = U'\sqrt{A^*A}$ implies $U = U'$. If A is not invertible, the arbitrariness of U lies in the choice of the orthonormal set $\{w_k, k = r + 1, \dots, n\}$. \square

The following corollary is elementary:

Theorem A.15 *Let $A \in \text{Mat}(\mathbb{C}, n)$. Then, there exists a unitary matrix $V \in \text{Mat}(\mathbb{C}, n)$ such that*

$$A = \sqrt{AA^*}V. \tag{63}$$

If A is non-singular, then V is unique.

Proof For the matrix A^* , relation (60) says that $A^* = U_0\sqrt{(A^*)^*A^*} = U_0\sqrt{AA^*}$ for some unitary U_0 . Since $\sqrt{AA^*}$ is self-adjoint, one has $A = \sqrt{AA^*}U_0^*$. Identifying $V \equiv U_0^*$, we get what we wanted. \square

The polar decomposition theorem can be generalized to bounded or closed unbounded operators acting on Hilbert spaces and even to C^* -algebras. See, e.g., [29] and [30].

Singular Values Decomposition

The polar decomposition theorem, Theorem A.14, has a corollary of particular interest.

Theorem A.16 (Singular Values Decomposition Theorem) *Let $A \in \text{Mat}(\mathbb{C}, n)$. Then, there exist unitary matrices V and $W \in \text{Mat}(\mathbb{C}, n)$ such that*

$$A = VSW^*, \tag{64}$$

*where $S \in \text{Mat}(\mathbb{C}, n)$ is a diagonal matrix whose diagonal elements are the singular values of A , i.e., the eigenvalues of $\sqrt{A^*A}$.*

Proof The claim follows immediately from (60) and from (59) by taking $V = UP$, $W = P$, and $S = D^{1/2}$. \square

Theorem A.16 can be generalized to rectangular matrices. In what follows, $m, n \in \mathbb{N}$ and we will use definitions (4), (8), and relation (9) that allow to injectively map rectangular matrices into certain square matrices.

Theorem A.17 (Singular Values Decomposition Theorem. General Form) *Let $A \in \text{Mat}(\mathbb{C}, m, n)$. Then, there exist unitary matrices V and $W \in \text{Mat}(\mathbb{C}, m + n)$ such that*

$$A = I_{m, m+n}VSW^*J_{m+n, n}, \tag{65}$$

*where $S \in \text{Mat}(\mathbb{C}, m + n)$ is a diagonal matrix whose diagonal elements are the singular values of A' (defined in (8)), i.e., are the eigenvalues of $\sqrt{(A')^*A'}$.*

Proof The matrix $A' \in \text{Mat}(\mathbb{C}, m + n)$ is a square matrix, and by Theorem A.16, it can be written in terms of a singular value decomposition $A' = VSW^*$ with V and $W \in \text{Mat}(\mathbb{C}, m + n)$, both unitary, and $S \in \text{Mat}(\mathbb{C}, m + n)$ being a diagonal matrix whose diagonal elements are the singular values of A' . Therefore, (65) follows from (9). \square

Appendix 2: Singular Values Decomposition and Existence of the Moore–Penrose Pseudoinverse

We will now present a second proof of the existence of the Moore–Penrose pseudoinverse of a general matrix $A \in \text{Mat}(\mathbb{C}, m, n)$ making use of Theorem A.16. We first consider square matrices and later consider general rectangular matrices.

The Moore–Penrose Pseudoinverse of Square Matrices

Let us first consider square diagonal matrices. If $D \in \text{Mat}(\mathbb{C}, n)$ is a diagonal matrix, its Moore–Penrose pseudoinverse is given by $D^+ \in \text{Mat}(\mathbb{C}, n)$, where, for $i = 1, \dots, n$, one has

$$(D^+)_{ii} = \begin{cases} (D_{ii})^{-1}, & \text{if } D_{ii} \neq 0, \\ 0, & \text{if } D_{ii} = 0. \end{cases}$$

It is elementary to check that $DD^+D = D$, $D^+DD^+ = D^+$ and that DD^+ and D^+D are self-adjoint. Actually, $DD^+ = D^+D$, a diagonal matrix whose diagonal elements are either 0 or 1:

$$(DD^+)_{ii} = (D^+D)_{ii} = \begin{cases} 1, & \text{if } D_{ii} \neq 0, \\ 0, & \text{if } D_{ii} = 0. \end{cases}$$

Now, let $A \in \text{Mat}(\mathbb{C}, n)$ and let $A = VSW^*$ be its singular values decomposition (Theorem A.16). We claim that its Moore–Penrose pseudoinverse A^+ is given by

$$A^+ = WS^+V^*. \tag{66}$$

In fact, $AA^+A = (VSW^*)(WS^+V^*)(VSW^*) = VSS^+SW^+ = VSW^* = A$ and

$$\begin{aligned} A^+AA^+ &= (WS^+V^*)(VSW^*)(WS^+V^*) \\ &= WS^+SS^+V^* = WS^+V^* = A^+. \end{aligned}$$

Moreover, $AA^+ = (VSW^*)(WS^+V^*) = V(SS^+)V^*$ is self-adjoint, since SS^+ is a diagonal matrix with diagonal elements 0 or 1. Analogously, $A^+A = (WS^+V^*)(VSW^*) = W(S^+S)W^*$ is self-adjoint.

The Moore–Penrose Pseudoinverse of Rectangular Matrices

Consider now $A \in \text{Mat}(\mathbb{C}, m, n)$ and let $A' \in \text{Mat}(\mathbb{C}, m+n)$ be the $(m+n) \times (m+n)$ defined in (8). Since A' is a square matrix, it has, by the comments above, a unique Moore–Penrose pseudoinverse $(A')^+$ satisfying

1. $A'(A')^+A' = A'$,
2. $(A')^+A'(A')^+ = (A')^+$,
3. $A'(A')^+$ and $(A')^+A'$ are self-adjoint.

In what follows, we will show that $A^+ \in \text{Mat}(\mathbb{C}, n, m)$ is given by

$$A^+ := I_{n, m+n}(A')^+J_{m+n, m}, \tag{67}$$

with the definitions (4) and (5), i.e.,

$$A^+ = I_{n, m+n}(J_{m+n, m}AI_{n, m+n})^+J_{m+n, m}. \tag{68}$$

The starting point is the existence of the Moore–Penrose pseudoinverse of the square matrix A' . Relation $A'(A')^+A' = A'$ means, using definition (8), that $J_{m+n, m}A'[I_{n, m+n}(A')^+J_{m+n, m}]AI_{n, m+n} = J_{m+n, m}AI_{n, m+n}$ and from (6) and (7) it follows, by multiplying to the left by $I_{m, m+n}$ and to the right by $J_{m+n, n}$, that $AA^+A = A$, one of the relations we wanted to prove.

Relation $(A')^+A'(A')^+ = (A')^+$ means, using definition (8), that $(A')^+J_{m+n, m}AI_{n, m+n}(A')^+ = (A')^+$. Multiplying to the left by $I_{n, m+n}$ and to the right by $J_{m+n, m}$, this establishes that $A^+AA^+ = A^+$.

Since $A'(A')^+$ is self-adjoint, it follows from the definition (8) that $J_{m+n, m}AI_{n, m+n}(A')^+$ is self-adjoint, i.e.,

$$J_{m+n, m}AI_{n, m+n}(A')^+ = (AI_{n, m+n}(A')^+)^* I_{m, m+n}.$$

Therefore, multiplying to left by $I_{m, m+n}$ and to the right by $J_{m+n, m}$, it follows from (6) that

$$\begin{aligned} AI_{n, m+n}(A')^+J_{m+n, m} &= I_{m, m+n}(AI_{n, m+n}(A')^+)^* \\ &= (AI_{n, m+n}(A')^+J_{m+n, m})^*, \end{aligned}$$

proving that AA^+ is self-adjoint

Finally, since $(A')^+A'$ is self-adjoint, it follows from definition (8) that $(A')^+J_{m+n, m}AI_{n, m+n}$ is self-adjoint, i.e.,

$$(A')^+J_{m+n, m}AI_{n, m+n} = J_{m+n, n}((A')^+J_{m+n, m}A)^*.$$

Hence, multiplying to the left by $I_{n, m+n}$ and to the right by $J_{m+n, n}$, it follows from (7) that

$$\begin{aligned} I_{n, m+n}(A')^+J_{m+n, m}A &= ((A')^+J_{m+n, m}A)^* J_{m+n, n} \\ &= (I_{n, m+n}(A')^+J_{m+n, m}A)^*, \end{aligned}$$

establishing that A^+A is self-adjoint. This proves that A^+ given in (67) is the Moore–Penrose pseudoinverse of A .

References

1. A.N. Tikhonov, Solution of incorrectly formulated problems and the regularization method, *Sov. Math., Dokl.* **4**, 1035–1038 (1963). English translation of *Dokl. Akad. Nauk USSR* **151**, 501–504 (1963)
2. A.N. Tikhonov, V.A. Arsenin, *Solution of Ill-Posed Problems* (Winston, Washington, DC, 1977)
3. D.K. Sodickson, C.A. McKenzie, A generalized approach to parallel magnetic resonance imaging, *Med. Phys.* **28**, 1629 (2001). doi:10.1118/1.1386778

4. R. Van De Walle, H.H. Barrett, K.J. Myers, M.I. Aitbach, B. Desplanques, A. F. Gmitro, J. Cornelis, I. Lemahieu, Reconstruction of MR images from data acquired on a general nonregular grid by pseudoinverse calculation, *IEEE Trans. Med. Imag.* **19** 1160–1167 (2000). doi:[10.1109/42.897806](https://doi.org/10.1109/42.897806)
5. H. Ammari, *An Introduction to Mathematics of Emerging Biomedical Imaging. Mathématiques et Applications*, vol. 62 (Springer, New York, 2008). ISBN 978-3-540-79552-0
6. G. Lohmann, K. Müller, V. Bosch, H. Mentzel, S. Hessler, L. Chen, S. Zysset, D.Y. von Cramon. Lipsia—a new software system for the evaluation of functional magnetic resonance images of the human brain, *Comput. Med. Imaging Graph.* **25**, 449–457 (2001). doi:[10.1016/S0895-6111\(01\)00008-8](https://doi.org/10.1016/S0895-6111(01)00008-8)
7. X. Li, D. Coyle, L. Maguire, T.M. McGinnity, D.R. Watson, H. Benali, A least angle regression method for fMRI activation detection in phase-encoded experimental designs, *NeuroImage* **52**, 1390–1400 (2010). doi:[10.1016/j.neuroimage.2010.05.017](https://doi.org/10.1016/j.neuroimage.2010.05.017)
8. V. Stefanescu, D.A. Stoichescu, C. Faye, A. Florescu, Modeling and simulation of cylindrical PET 2D using direct inversion method, in *16th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2010* (IEEE, Piscataway, 2010), pp. 107–112. doi:[10.1109/SIITME.2010.5653649](https://doi.org/10.1109/SIITME.2010.5653649)
9. M. Bertero, P. Boccacci, *Introduction to Inverse Problems in Imaging* (Taylor & Francis, Bristol, 1998). ISBN: 978-0750304351
10. J.-Z. Wang, S.J. Williamson, L. Kaufman, Magnetic source imaging based on the minimum-norm least-squares inverse, *Brain Topogr.* **5**(4), 365–371 (1993). doi:[10.1007/BF01128692](https://doi.org/10.1007/BF01128692)
11. N.G. Gençer, S.J. Williamson, Magnetic source images of human brain functions, *Behav. Res. Meth.* **29**(1), 78–83 (1997). doi:[10.3758/BF03200570](https://doi.org/10.3758/BF03200570)
12. J.-Z. Wang, S.J. Williamson, L. Kaufman, Spatio-temporal model of neural activity of the human brain based on the MNLS inverse, in *Biomagnetism: Fundamental Research and Clinical Applications. Studies in Applied Electromagnetics and Mechanics, Vol. 7. International Conference on Biomagnetism 1995 (University of Vienna)*, ed. by C. Baumgartner, L. Deecke, G. Stroink, S.J. Williamson (Elsevier, Amsterdam, 1995). ISBN: 978-9051992335
13. M.T. Page, S. Custódio, R.J. Archuleta, J.M. Carlson, Constraining earthquake source inversions with GPS data I: Resolution based removal of artifacts, *J. Geophys. Res.* **114**, B01314 (2009). doi:[10.1029/2007JB005449](https://doi.org/10.1029/2007JB005449)
14. S. Atzori, A. Antonioli, Optimal fault resolution in geodetic inversion of coseismic data, *Geophys. J. Int.* **185**, 529–538 (2011). doi:[10.1111/j.1365-246X.2011.04955.x](https://doi.org/10.1111/j.1365-246X.2011.04955.x)
15. R.D. Pascual-Marqui, Standardized low resolution brain electromagnetic tomography (sLORETA): technical details, *Methods Find. Exp. Clin. Pharmacol.* **24D**, 5–12 (2002)
16. C. Hennig, N. Christlieb, Validating visual clusters in large datasets: fixed point clusters of spectral features, *Comput. Stat. Data Anal.* **40**, 723–739 (2002). doi:[10.1016/S0167-9473\(02\)00077-4](https://doi.org/10.1016/S0167-9473(02)00077-4)
17. L. Bedini, D. Herranz, E. Salerno, C. Baccigalupi, E.E. Kuruoğlu, A. Tonazzini, Separation of correlated astrophysical sources using multiple-lag data covariance matrices, *EURASIP J. Appl. Signal Process.* **15**, 2400–2412 (2005)
18. T.V. Ricci, J.E. Steiner, R.B. Menezes, NGC 7097: the active galactic nucleus and its mirror, revealed by principal component analysis tomography, *Astrophys. J.* **734**, L10 (2011). doi:[10.1088/2041-8205/734/L10](https://doi.org/10.1088/2041-8205/734/L10)
19. J.E. Steiner, R.B. Menezes, T.V. Ricci, A.S. Oliveira, PCA tomography: how to extract information from data cubes, in *Monthly Notices of the Royal Astronomical Society*, vol. 395 (2009), p. 64
20. M.E. Wall, A. Rechtsteiner, L.M. Rocha, Singular values decomposition and principal component analysis, in *A Practical Approach to Microarray Data Analysis*, ed. by D.P. Berrar, W. Dubitzky, M. Granzow (Kluwer, Norwell, 2003), pp. 91–109. LANL LA-UR-02-4001
21. O. Troyanskaya, M. Cantor, G. Sherlock, P. Brown, T. Hastie, R. Tibshirani, D. Botstein, R.B. Altman, Missing value estimation methods for DNA microarrays, *Bioinformatics* **17**(6), 520–525 (2001)
22. H. Andrews, C. Patterson III, Singular values decomposition (SVD) image coding, *IEEE Trans. Commun.* **24**(4), 425–432 (1976)
23. S. Chountasis, V.N. Katsikis, D. Pappas, Applications of the Moore–Penrose inverse in digital image restoration. *Math. Probl. Eng.* **2009**, Article ID 170724, 12 pp. (2009). doi:[10.1155/2009/170724](https://doi.org/10.1155/2009/170724)
24. S. Chountasis, V.N. Katsikis, D. Pappas, Digital image reconstruction in the spectral domain utilizing the Moore–Penrose inverse. *Math. Probl. Eng.* **2010**, Article ID 750352, 14 pp. (2010). doi:[10.1155/2010/750352](https://doi.org/10.1155/2010/750352)
25. C.W. Groetsch, Integral equations of the first kind, inverse problems and regularization: a crash course, *J. Phys.: Conf. Ser.* **73**, 012001 (2007). doi:[10.1088/1742-6596/73/1/012001](https://doi.org/10.1088/1742-6596/73/1/012001)
26. E.H. Moore, On the reciprocal of the general algebraic matrix. *Bull. Am. Math. Soc.* **26**, 394–395 (1920)
27. R. Penrose, A generalized inverse for matrices, *Proc. Camb. Philos. Soc.* **51**, 406–413 (1955)
28. R. Penrose, On best approximate solution of linear matrix equations, *Proc. Camb. Philos. Soc.* **52**, 17–19 (1956)
29. M. Reed, B. Simon, *Methods of Modern Mathematical Physics. Vol. 1: Functional Analysis* (Academic, New York, 1972–1979)
30. O. Bratteli, D.W. Robinson, *Operator Algebras and Quantum Statistical Mechanics I* (Springer, New York, 1979)