Linear Algebra for Computer Scientists

Lecture Notes
Part II

A. S. Bandeira and R. Weismantel
ETH Zürich

Last update on November 1, 2024

“Read me” for Part II

These lecture notes serve as **a continuation**[1] **of Part I**, taught by Prof. Bernd Gärtner, available at `https://ti.inf.ethz.ch/ew/courses/LA23/notes_part_I.pdf`. Please read the Preface there. Please note there may be some changes in notation. Furthermore, we will try to stay close to the notation in [Str23], but there also be some differences.

[Str23] Gilbert Strang. Introduction to Linear Algebra. Wellesley - Cambridge Press, 6th ed., 2023.

The **course page** has relevant information for the course: `https://ti.inf.ethz.ch/ew/courses/LA23`.

There are countless excellent Linear Algebra books with the material covered in this course. For Part II we will roughly continue to follow, in structure and content, [Str23], with some small deviations. I will try to keep the numbering of Chapters/Sections and Sections/Subsections consistent with [Str23] (as far as the deviations allow). See Appendix A for some important preliminaries and some remarks on notation.

Throughout the notes, and the lectures, we will try to motivate some of the material with **Guiding Question**s. For students who would like to explore the topic further, I will include some **Exploratory Challenge**s and **Further Reading**, these often will include difficult problems or topics. I will also take some opportunities to share some active **Research Question**s related to the topics we covered (we are still discovering new phenomena in Linear Algebra today and for many years to come!).

After deriving a result, we will often do some **Sanity Check**s, and some things we will leave as a **Challenge**: these should be accessible and of difficulty comparable to homework questions, a $\star$ indicates a harder problem (but still within the scope). On the other hand, **Exploratory Challenges** are generally outside the scope of the course or of substantial higher difficulty.

Linear Algebra is a beautiful topic, connecting Algebra with Geometry[2], and has countless applications making it a key component of almost all quantitative pursuits. We sincerely hope you will enjoy the course as much as we enjoy teaching this beautiful subject!

[1] If you are reading these notes and did not follow Part I, please read Appendix A.

[2] and Analysis, as you will likely see later in your academic life. For example, when Joseph Fourier invented Fourier Series to develop a theory of heat transfer he was essentially finding good orthonormal bases for functions.

We believe the Questions, Sanity Checks, Challenges, etc are very useful to learn the material, but **when you want to review the material**, or do a last read before the exam, you can focus on the Definitions, Propositions, Theorems, etc (and **focus less on the blue parts**).

As your mathematical level matures over the semester, the notes will have less illustrations and more definitions and mathematical statements. Our recommendation is to read the notes with pen & paper next to you and to draw the picture yourself, this "translation" you will be doing — from mathematical statement to picture — will help you greatly in the learning of Mathematics!

There are also countless high-quality videos and other content online about Linear Algebra, for example there is also an excellent series of videos by Gil Strang filmed ∼15 years ago: `https://www.youtube.com/playlist?list=PLE7DDD91010BC51F8`.

Strang actually retired just a few months ago, at almost 90 years of age! You can see his last lecture online: `https://www.youtube.com/watch?v=lUUte2o2Sn8`

Moreover, there are many excellent animations online giving lots of great intuition on several Linear Algebra topics and phenomena. While it is a great idea to take advantage of this, I would recommend first trying yourself to develop an intuition of the concept/phenomenon (e.g. by drawing a picture) and using these tools only after — use them to improve your intuition, not to create it!

As these Lecture Notes are being continuously updated, and sometimes the discussion in lectures leads us into proving an extra result, or suggests a remark, etc, I will try to add then and not change the numbering of things downstream, I do this by numbering them with $+1000$.

After each lecture, we post the handwritten notes from lecture on the course website `https://ti.inf.ethz.ch/ew/courses/LA23/index.html`. My suggestion would be to use the Lecture Notes to review the material, not the handwritten notes (which are mainly meant to support my oral exposition).

CONTENTS

"Read me" for Part II 2

5. Orthogonality 5

5.1. Orthogonality of vectors and subspaces 5

5.2. Projections 9

5.3. Least Squares Approximation 13

5.4. Orthonormal Bases and Gram Schmidt 17

5.5. The Pseudoinverse, also known as Moore–Penrose Inverse 23

5.6. Projections of sets and the Farkas lemma 27

6. The determinant 32

7. Eigenvalues and Eigenvectors 41

7.0. Complex Numbers 42

7.1. Introduction to Eigenvalues and Eigenvectors 45

7.2. Diagonalizing a Matrix and Change of Basis of a Linear Transformation 56

7.3. Symmetric Matrices and the Spectral Theorem 59

8. Singular Value Decomposition; and some open questions in Linear Algebra 65

8.1. The Singular Value Decomposition 65

8.2. Vector and Matrix Norms 69

8.3. Some Mathematical Open Problems 70

Acknowledgements 72

Appendix A. Some Important Preliminaries and Remarks on Notation 72

Appendix B. A "Simple proof" of the Fundamental Theorem of Algebra 73

73

5. Orthogonality

5.1. Orthogonality of vectors and subspaces.

Guiding Question 1. Our task is to explore orthogonality as a geometric and algebraic tool in order to be able to decompose a space into subspaces. Among many results our knowledge will then put us in position to understand how to solve systems of linear equations.

Let us begin by introducing orthogonality.

Definition 5.1.1. *Two vectors $v, w \in \mathrm{R}^n$ are called orthogonal if $v^T w = \sum_{i=1}^n v_i w_i = 0$. Two subspaces V and W are orthogonal if for all $v \in V$ and $w \in W$, the vectors v and w are orthogonal.*

In order to check whether two subspaces V and W are orthogonal it is enough to verify it for the vectors forming a basis of V and W, respectively.

Lemma 5.1.2. *Let $v_1, \dots, v_k$ be a basis of subspace V. Let $w_1, \dots, w_l$ be a basis of subspace W. V and W are orthogonal if and only if v_i and w_j are orthogonal for all $i \in \{1, \dots, k\}$ and $j \in \{1, \dots, l\}$.*

Proof. Let us begin by proving the statement from left to right: Suppose V and W are orthogonal. Since $v_i \in V$ for all $i \in \{1, \dots, k\}$ and $w_j \in W$ for all $j \in \{1, \dots, l\}$, we have that $v_i^T w_j = 0$ for all $i \in \{1, \dots, k\}$ and $j \in \{1, \dots, l\}$.

For the converse direction, assume that $v_i^T w_j = 0$ for all $i \in \{1, \dots, k\}$ and $j \in \{1, \dots, l\}$. Let $v \in V$ and $w \in W$. Then, there exist real multipliers such that

$$v = \sum_{i=1}^{k} \lambda_i v_i \text{ and } w = \sum_{j=1}^{l} \mu_j v_j.$$

Then

$$v^T w = \sum_{i=1}^{k} \lambda_i v_i^T w = \sum_{i=1}^{k} \sum_{j=1}^{l} \mu_j \lambda_i v_i^T w_j = 0.$$

□

Lemma 5.1.3. *Let V and W be two orthogonal subspaces of R^n. Let $v_1, \dots, v_k$ be a basis of subspace V. Let $w_1, \dots, w_l$ be a basis of subspace W. The set of vectors $\{v_1, \dots, v_k, w_1, \dots, w_l\}$ are linearly independent.*

Proof. Consider the linear combination

$$\sum_{i=1}^{k} \lambda_i v_i + \sum_{j=1}^{l} \mu_j w_j = 0.$$

We want to show that $\lambda_i = 0$ for all $i \in \{1,\dots,k\}$ and $\mu_j = 0$ for all $j \in \{1,\dots,l\}$. Let $v = \sum_{i=1}^{k} \lambda_i v_i$. The linear combination is equivalent to $v = -\sum_{j=1}^{l} \mu_j w_j$. We obtain $v^T v = -\sum_{j=1}^{l} \mu_j v^T w_j = 0$. Hence, $v = 0$. This implies that $\lambda_i = 0$ for all $i \in \{1,\dots,k\}$ since $v_1,\dots,v_k$ is a basis of V. The same argument can be applied to show that $w = \sum_{j=1}^{l} \mu_j w_j$ must equal the all-zero vector and hence, $\mu_j = 0$ for all $j \in \{1,\dots,l\}$. This is the result. □

Lemma 5.1.3 allows us to derive an important fact about orthogonal subspaces. Namely we can take bases of the two subspaces V and W and their union gives a basis for the subspace

$$\{\lambda v + \mu w \mid \lambda, \mu \in \mathrm{R},\ v \in V,\ w \in W\}.$$

Corollary 5.1.4. *Let V and W be orthogonal subspaces. Then $V \cap W = \{0\}$. Moreover, if* $\dim(V) = k$ *and* $\dim(W) = l$*, then* $\dim(\{\lambda v + \mu w \mid \lambda, \mu \in \mathrm{R},\ v \in V,\ w \in W\}) = k + l \leq n$.

5.1.1. *The orthogonal complement of a subspace.*

So far we have explored general subspaces V and W that are orthogonal. Next consider a subspace V. Then there is a special orthogonal subspace attached to V.

Definition 5.1.5. *Let V be a subspace of* R^n. *We define the orthogonal complement of V as*

$$V^{\perp} = \{w \in \mathrm{R}^n \mid w^T v = 0 \textit{ for all } v \in V\}.$$

Challenge 2. Prove that $V^{\perp}$ is a subspace of R^n.

This concept of orthogonal subspaces allows us to decompose the space. Let us first see an important example of how this idea can be used.

Theorem 5.1.6. *Let $A \in \mathrm{R}^{m \times n}$ be a matrix.*

$$N(A) = C(A^T)^{\perp} = R(A)^{\perp}.$$

Proof. Let us show that $N(A) \subseteq C(A^T)^{\perp}$.

Let $x \in N(A)$. Take any $b \in R(A)$. By definition, $b = A^T y$ for some $y \in \mathrm{R}^m$. Then $b^T x = y^T Ax = 0$. Hence, $x \in C(A^T)$.

Conversely, we want to show that $C(A^T)^\perp \subseteq N(A)$. To this end let $x \in C(A^T)^\perp$. Then $b^T x = 0$ for all $b \in C(A^T)$. Take $y := Ax \in \mathrm{R}^m$ Then $b := A^T y \in C(A^T)$ and hence, $x^T b = 0$. We obtain

$$0 = x^T b = x^T A^T y = x^T A^T Ax = \|Ax\|^2.$$

This implies that $Ax = 0$, i.e., $x \in N(A)$. □

From the lecture in Chapter 3.5 we know already that if $r = \dim(R(A))$, then $n - r = \dim(N(A)$. This fact together with Theorem 5.1.6 allows us to prove a decomposition theorem of the space R^n.

Theorem 5.1.7. *Let V, W be orthogonal subspaces of* R^n.

The following statements are equivalent.

(i) $W = V^\perp$.
(ii) $\dim(V) + \dim(W) = n$.
(iii) *Every $u \in \mathrm{R}^n$ can be written as $u = v + w$ with unique vectors $v \in V$, $w \in W$.*

Proof. Let $v_1, \dots, v_k$ be a basis of V and $w_1, \dots, w_l$ a basis of W. From Lemma 5.1.2 V and W are orthogonal if and only if $v_i^T w_j = 0$ for all $i \in \{1, \dots, k\}$ and $j \in \{1, \dots, l\}$.

(i) implies (ii): Define $A \in \mathrm{R}^{k \times n}$ to be the matrix with row vectors $v_1, \dots, v_k$. Then $V = R(A) = C(A^T)$. Moreover, $W = V^\perp = N(A)$ from Theorem 5.1.6. From our remark before $\dim(V) = k$ and hence, $\dim(W) = n - k$.

(ii) implies (iii): From Lemma 5.1.3 the vectors in the set $\{v_1, \dots, v_k, w_1, \dots, w_l\}$ are linearly independent. Since by assumption $l = n - k$, this set is a basis of R^n. Hence, every vector $u \in \mathrm{R}^n$ has a unique representation in form of

$$u = \sum_{i=1}^{k} \lambda_i v_i + \sum_{j=1}^{l} \mu_j w_j, \text{ where } \lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_l \in \mathrm{R}.$$

Define the unique vectors $v := \sum_{i=1}^{k} \lambda_i v_i$, $w := \sum_{j=1}^{l} \mu_j w_j$. This gives the statement.

(iii) implies (i): We need to show that $W = V^\perp$. Note that $W \subseteq V^\perp$ since W is orthogonal to V. To show the reverse inclusion, take any vector $u \in V^\perp \subseteq \mathrm{R}^n$ Hence, from our assumption in (iii) we know that $u = v + w$ where $v \in V$ and $w \in W$. Then

$$0 = u^T v = v^T v + v^T w = v^T v = \|v\|^2.$$

Hence, $v = 0$ and it follows that $u = w \in W$. □

Indeed Theorem 5.1.7 allows us to decompose the space R^n according to a given subspace $V \subseteq \mathrm{R}^n$. We write

$$\mathrm{R}^n = V + V^{\perp} = \{v + w \mid v \in V,\ w \in V^{\perp}\}.$$

This decomposition is symmetric in the sense that we can also take the subspace $V^{\perp}$ and then write

$$\mathrm{R}^n = V^{\perp} + (V^{\perp})^{\perp} = V^{\perp} + V.$$

This follows from the following observation.

Lemma 5.1.8. *Let V be a subspace of R^n. Then $V = (V^{\perp})^{\perp}$.*

Proof. Let $v_1, \dots, v_k$ be a basis of V and $w_1, \dots, w_l$ a basis of $V^{\perp}$. It follows that $l = n - k$. From Lemma 5.1.2 we conclude that $v_i^T w_j = 0$ for all indices i and j. Then by definition

$$(V^{\perp})^{\perp} = \{x \in \mathrm{R}^n \mid x^T w_j = 0 \text{ for all } j = 1, \dots, n-k\}.$$

Since $v_i^T w_j = 0$ for all $j = 1, \dots, n-k$ we obtain that $V \subseteq (V^{\perp})^{\perp}$. From Theorem 5.1.7 we obtain that $\dim((V^{\perp})^{\perp}) = n - (n-k) = k$. Since $\{v_1, \dots, v_k\} \subseteq V \subseteq (V^{\perp})^{\perp}$ are linearly independent, they form a basis of $(V^{\perp})^{\perp}$. Hence $V = (V^{\perp})^{\perp}$. □

This lemma in combination with Theorem 5.1.6 allows us to conclude that for a matrix A we have that $C(A^T) = N(A)^{\perp}$.

Corollary 5.1.9. *Let $A \in \mathrm{R}^{m \times n}$. $N(A) = C(A^T)^{\perp}$ and $C(A^T) = N(A)^{\perp}$.*

5.1.2. *The set of all solutions to a system of linear equations.*

The machinery developed in the previous chapters allows us to understand the set of solutions to a system of linear equations over the reals. To make it precise, let $A \in \mathrm{R}^{m \times n}$. There are two important subspaces associated with A:

$$N(A) = \{x \in \mathrm{R}^n \mid Ax = 0\} \text{ and } R(A) = C(A^T) = \{x \in \mathrm{R}^n \mid \exists y \in \mathrm{R}^m \text{ such that } x = A^T y\}.$$

We have learned that $N(A)$ is the orthogonal complement of $R(A)$. Vice versa, $R(A)$ is the orthogonal complement of $N(A)$. Hence all of R^n can be written as the sum of two elements: one is from $N(A)$ and the other one from $R(A)$. In other words:

$$\forall x \in \mathrm{R}^n \text{ there exist } x_0 \in N(A) \text{ and } x_1 \in R(A) \text{ such that } x = x_0 + x_1 \text{ and } x_1^T x_0 = 0.$$

We summarize below how the set of all solutions to a system of equations is described.

Theorem 5.1.10.

$$\{x \in \mathrm{R}^n \mid Ax = b\} = x_1 + N(A) \textit{ where } x_1 \in R(A) \textit{ such that } Ax_1 = b.$$

There is one final link between the nullspace of a matrix A and the nullspace of the matrix $A^T A$ that we will need in our analysis of projections later on.

Lemma 5.1.11. *Let* $A \in \mathrm{R}^{m \times n}$. *Then* $N(A) = N(A^T A)$ *and* $C(A^T) = C(A^T A)$.

Proof. If $x \in \mathrm{N}(A)$ then $Ax = 0$ and so $A^\top Ax = 0$, thus $x \in \mathrm{N}(A^\top A)$. The other implication is more interesting.

If $x \in \mathrm{N}(A^\top A)$ then $A^\top Ax = 0$. This implies that $x^\top A^\top Ax = x^\top 0 = 0$. But $x^\top A^\top Ax = (Ax)^\top (Ax) = \|Ax\|^2$ so Ax must be a vector with norm 0 which implies that $Ax = 0$ and so $x \in \mathrm{N}(A)$.

For the second statement we utilize Corollary 5.1.9. We have

$$C(A^T) = N(A)^\perp = N(A^T A)^\perp = C((A^T A)^T) = C(A^T A).$$

□

5.2. **Projections.**

Guiding Question 3. If we have a system of linear equations that has no solution, how do we find the "solution" that has the smallest error? This question is central in countless applications[3].

[3] as you will see later on, it is in a sense what Machine Learning is all about.

Before diving into systems of equations, we will study Projections of vectors in a subspace.

Definition 5.2.1 (Projection of a vector onto a subspace)**.** *The projection of a vector $b \in \mathbb{R}^m$ on a subspace S (of $\mathbb{R}^m$) is the point in S that is closest to b. In other words*

$$\operatorname{proj}_S(b) = \operatorname*{argmin}_{p \in S} \|b - p\|. \tag{1}$$

Sanity Check 4. This is only a proper definition if the minimum exists and is unique. Can you show it exists and is unique? (perhaps at the end of the lecture?)

Let us build us some intuition by starting with one-dimensional subspaces.

5.2.1. *The one-dimensional case.*

Let S be the subspace corresponding to the line that goes through the vector $a \in R^m \setminus \{0\}$, i.e. $S = \{\lambda a \mid \lambda \in R\} = C(a)$. By drawing a two dimensional example one can see that the projection p is the vector in the subspace S such that the "error vector" $e = b - p$ is perpendicular to a (i.e. $b - p \perp a$). This geometric intuition turns out to be correct. We will verify it algebraically.

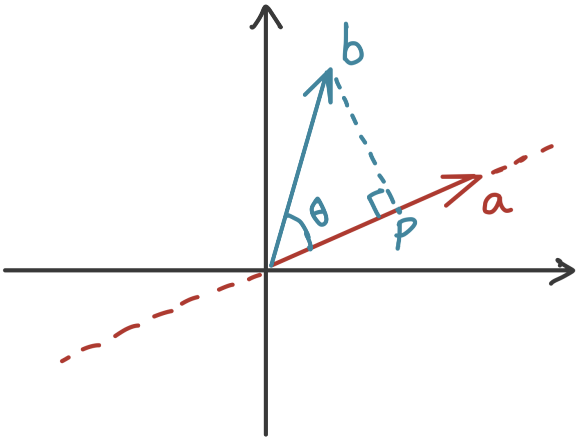


FIGURE 1. Projection on a line.

Lemma 5.2.2. *Let $a \in R^m \setminus \{0\}$. The projection of $b \in R^m$ on $S = \{\lambda a \mid \lambda \in R\} = C(a)$ is given by*

$$\operatorname{proj}_S(b) = \frac{aa^T}{a^T a} b.$$

Proof. Let $p \in S$, $p = \lambda a$ for $\lambda \in \mathrm{R}$. Then

$$\|b-p\|^2 = (b-p)^T(b-p) = b^Tb - 2b^Tp + p^Tp = \|b\|^2 - 2\lambda b^Ta + \lambda^2\|a\|^2 = g(\lambda).$$

g is a convex, quadratic function in one variable λ. Hence, the minimizer is obtained at the point λ^* where the derivative vanishes. We obtain

$$g'(\lambda) = -2b^Ta + 2\lambda\|a\|^2 = 0 \iff \lambda^* = \frac{b^Ta}{a^Ta}.$$

Hence, we have shown that

$$\mathrm{proj}_S(b) = \lambda^* a = a\frac{b^Ta}{a^Ta} = a\frac{a^Tb}{a^Ta} = \frac{aa^T}{a^Ta}b.$$

□ □

Let us next verify that our initial geometric understanding is indeed correct: the projection p should be the vector in the subspace S such that the "error vector" $e = b - p$ is perpendicular to a, i.e.,

$$(b - \mathrm{proj}_S(b)) \perp \mathrm{proj}_S(b).$$

Indeed by substituting what we just computed we obtain

$$(b - \frac{aa^T}{a^Ta}b)^T\frac{aa^T}{a^Ta}b = \frac{b^Taa^Tb}{a^Ta} - b^T\frac{aa^T}{a^Ta}\frac{aa^T}{a^Ta}b = \frac{(a^Tb)^2}{a^Ta} - \frac{b^Taa^Tb}{a^Ta} = 0.$$

The projection of a vector that is already a multiple of a should be the identity operation. This is indeed true. Check that this is the case!

5.2.2. *The general case.*

For general subspaces the idea is precisely the same as with dimension one. Let S be a subspace in R^m with dimension n. Let $a_1, \ldots, a_n$ be a basis of S, meaning that

$$S = \text{ span}(a_1, \ldots, a_n) = C(A) = \{A\lambda \mid \lambda \in \mathrm{R}^n\}, \text{ where}$$

A is the matrix with column vectors $a_1, \ldots, a_n$.

Lemma 5.2.3. *The projection of a vector $b \in \mathrm{R}^m$ to the subspace $S = C(A)$ can be written as*

$$\mathrm{proj}_S(b) = A\hat{x}, \textit{ where } \hat{x} \textit{ satisfies the normal equations } A^TA\hat{x} = A^Tb.$$

Proof. Let $b \in \mathrm{R}^m$. The vector b can be written as $b = p + e$ where $p \in S$ and $e \in S^\perp$, i.e., $p^T e = 0$. Now consider another point $p' \in S$. Then $p - p' \in S$ and hence, $e^T(p - p') = 0$. This gives

$$\|p' - b\|^2 = \|p' - p + p - b\|^2 = \|p' - p - e\|^2 = \|p' - p\|^2 + \|e\|^2 \geq \|e\|^2 = \|p - b\|^2.$$

Hence, we have shown that $\mathrm{proj}_S(b) = p = A\hat{x} \in S$ where $b = p + e$ with $e \in S^\perp$. This shows us that

$$(b - \mathrm{proj}_S(b)) \perp a_i \text{ for all } i = 1, \ldots, n \iff a_i^T(b - \mathrm{proj}_S(b)) = 0 \text{ for all } i = 1, \ldots, n.$$

This is equivalent to saying that

$$A^T(b - \mathrm{proj}_S(b)) = 0 \iff A^T(b - A\hat{x}) = 0 \iff A^T A\hat{x} = A^T b.$$

□ □

If we can show that $A^\top A$ is invertible then we would have $p = A\hat{x} = A\left(A^\top A\right)^{-1} A^\top b$. Let's make a detour to show that it is indeed invertible.

Lemma 5.2.4. *$A^\top A$ is invertible if and only if A has linearly independent columns.*

Proof. This follows essentially from Lemma 5.1.11 where we proved that $A^\top A$ and A have the same nullspace. This is enough because, since $A^\top A$ is a square matrix it is invertible if and only if its nullspace only has the 0 vector, and A has linearly independent columns if and only if its nullspace only has the 0 vector.[4] □

Corollary 5.2.5. *If A has linearly independent columns then $A^\top A$ is a square matrix, it is invertible and symmetric.*[5]

Now back to deriving a formula for projections: Since the columns of A are a basis they are linearly independent and so $A^\top A$ is indeed invertible. We just proved the following.

Theorem 5.2.6. *Let S be a subspace in $\mathbb{R}^m$ and A a matrix whose columns are a basis of S. The projection of $b \in \mathbb{R}^m$ to S is given by*

$$\mathrm{proj}_S(b) = Pb,$$

[4] We usually call a nullspace with only the zero vector, a trivial nullspace.

where $P = A\left(A^\top A\right)^{-1} A^\top$ *is the projection matrix.*

The matrix $P = A\left(A^\top A\right)^{-1} A^\top$ is known as a Projection Matrix, it maps a vector b to its projection Pb on a subspace S. For the case of lines, P was given by $P = \frac{aa^\top}{a^\top a} = a\frac{1}{a^\top a}a^\top$.

Caution! 5. The matrix A (and $A^\top$) are not necessarily square, and so they don't have inverses. The expression $A\left(A^\top A\right)^{-1} A^\top$ **cannot** be simplified by expanding $\left(A^\top A\right)^{-1}$ (which would yield $I = P$, this would only make sense if S was all of $\mathbb{R}^m$ and note that, unsurprisingly, this would correspond exactly to the case when A is invertible).

Let us summarize a few facts about the projection matrix P. P can be viewed as a mapping: for a given vector b its projection is given by $\text{proj}_S(b) = Pb$.

Remark 5.2.7.

- *If* $b \in \mathrm{R}^m$, *then* $\text{proj}_S(\text{proj}_s(b)) = \text{proj}_S(b)$ *by definition. This requires us to have that* $PPb = Pb$, *i.e., we should have* $P^2 = P$. *Indeed*
$$P^2 = \left(A\left(A^\top A\right)^{-1} A^\top\right)^2 = A\left(A^\top A\right)^{-1} A^\top A\left(A^\top A\right)^{-1} A^\top = A\left(A^\top A\right)^{-1} A^\top = P.$$
- *Let* $S^\perp$ *be the orthogonal complement of* S *and* P *the projection matrix onto the subspace* S, *i.e.,* $\text{proj}_S(b) = Pb$. *Then* $I - P$ *is the projection matrix that maps* $b \in \mathrm{R}^m$ *to* $\text{proj}_{S^\perp}(b)$. *This follows since* $b = e + \text{proj}_S(b) = e + Pb$ *where* $e \in S^\perp$. *Hence,*
$$(I-P)b = b - Pb = e = \text{proj}_{S^\perp}(b).$$
- *Note that – as it should be – we have that* $(I-P)^2 = I - 2P + P^2 = I - P$.

5.3. **Least Squares Approximation.**

We go back to the guiding question of what to do when we want to "solve" a linear system that does not have an exact solution. More precisely let us suppose we have a linear system

$$Ax = b,$$

for which no solution x exists (for example, with too many equations, which would happen if $A \in \mathbb{R}^{m\times n}$ and $m > n$). A natural approach is to try to find x for which Ax is as close as possible to b

$$\min_{\hat{x}\in\mathbb{R}^n} \|A\hat{x} - b\|^2. \tag{2}$$

Further Remark 6. This seemingly simple observation is key to countless technologies. Measurement systems often have errors and so it is impossible to find the target object/signal x that satisfies them all exactly, and we look for the one that satisfies them the best possible. In Data Science and Learning Theory we often want to find a predictor that best describes a set of *training data*, but usually no predictor described the data exactly, so we look for the best possible, etc etc. We'll see a couple of applications later.

We can solve this problem using the ideas we developed above. What we are looking for is a vector $\hat{x}$ for which the error $e = b - A\hat{x}$ is as small as possible. Since the set of possible vectors $y = A\hat{x}$ is exactly $\mathrm{C}(A)$, $A\hat{x}$ is precisely the projection of b on $\mathrm{C}(A)$. As we saw in the Section above, this means that

$$A^\top(b - A\hat{x}) = 0.$$

These are known as the *normal equations* and can be rewritten as

$$A^\top A\hat{x} = A^\top b. \tag{3}$$

Recall that we had shown in Lemma 5.1.11 that for any matrix A, $\mathrm{C}(A^\top) = \mathrm{C}(A^\top A)$. Hence, the system (3) always has a solution.

We also know that if A has linearly independent columns, then $A^\top A$ is invertible and so we can write $\hat{x} = (A^\top A)^{-1}A^\top b$. We will address the case in which A has dependent columns shortly.

Fact 5.3.1. *A minimizer of* (2) *is also a solution of* (3). *When A has independent columns the unique minimizer $\hat{x}$ of* (2) *is given by*

$$\hat{x} = (A^\top A)^{-1}A^\top b \tag{4}$$

5.3.1. *Linear Regression — fitting a line to data points.*

One of the most common tasks in data analysis is linear regression, to fit a line through data points. Let us consider data points

$$(t_1, b_1), (t_2, b_2), \ldots, (t_m, b_m),$$

perhaps representing some attribute b over time t. If the relation between t and b is (at least partly) explained by a linear relationship then it makes sense to search for constants $\alpha_0 \in \mathbb{R}$ and $\alpha_1 \in \mathbb{R}$ such that

$$b_k \approx \alpha_0 + \alpha_1 t_k.$$

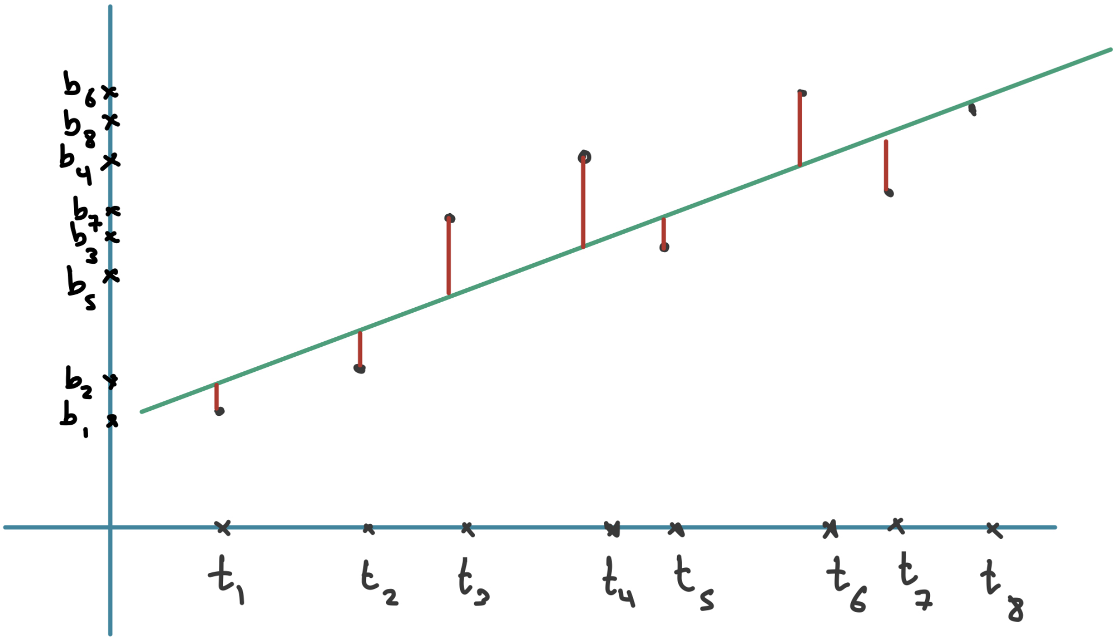


FIGURE 2. Fitting a line to points

See Figure 2. In particular, it is natural to search for α_0 and α_1 that minimize the sum of squares of the errors ("least squares"),

$$\min_{\alpha_0,\alpha_1} \sum_{k=1}^{m} (b_k - [\alpha_0 + \alpha_1 t_k])^2 .$$

In matrix-vector notation

$$\min_{\alpha_0,\alpha_1} \left\| b - A \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \right\|^2 , \tag{5}$$

where

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-1} \\ b_m \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} 1 & t_1 \\ 1 & t_2 \\ \vdots & \vdots \\ 1 & t_{m-1} \\ 1 & t_m \end{bmatrix} .$$

We can assume w.l.o.g. that A has independent columns, see Lemma 5.3.2. Hence, the solution to (5) is given by

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = (A^\top A)^{-1} A^\top b = \begin{bmatrix} m & \sum_{k=1}^m t_k \\ \sum_{k=1}^m t_k & \sum_{k=1}^m t_k^2 \end{bmatrix}^{-1} \begin{bmatrix} \sum_{k=1}^m b_k \\ \sum_{k=1}^m t_k b_k \end{bmatrix}$$

Lemma 5.3.2. *The columns of the $m \times 2$ matrix A defined before are linearly dependent if and only if $t_i = t_j$ for all $i \neq j$.*

Proof. Suppose that there are two indices $i \neq j$ such that $t_i \neq t_j$. Let $\mathbf{1}$ be the all ones-vector in R^m and t the vector with components $t_1, \ldots, t_m$. Consider the system in variables λ, μ

$$\lambda \mathbf{1} + \mu t = 0.$$

Since $t_i \neq t_j$ we can subtract row j from row i to obtain

$$\lambda 0 + \mu(t_i - t_j) = 0 \iff \mu = 0 \text{ since } t_i - t_j \neq 0.$$

This implies that $\lambda = 0$ and hence A has full column rank.

Conversely, if $t_i = t_j$ for all i and j, then $t = t_1\mathbf{1}$. Then the two columns of A are linearly dependent. □

Remark 5.3.3. *If the columns of A are pairwise orthogonal, then $A^\top A$ is a diagonal matrix, which is easy to invert. In this example, the columns of A being orthogonal corresponds to $\sum_{k=1}^m t_k = 0$. We could simply do a change of variables to a new time $t_k^{new} = t_k - \frac{1}{m}\sum_{i=1}^m t_i$ to achieve this. If indeed $\sum_{k=1}^m t_k = 0$ then the equation above could be easily simplified:*

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} m & 0 \\ 0 & \sum_{k=1}^m t_k^2 \end{bmatrix}^{-1} \begin{bmatrix} \sum_{k=1}^m b_k \\ \sum_{k=1}^m t_k b_k \end{bmatrix} = \begin{bmatrix} \frac{1}{m} & 0 \\ 0 & \frac{1}{\sum_{k=1}^m t_k^2} \end{bmatrix} \begin{bmatrix} \sum_{k=1}^m b_k \\ \sum_{k=1}^m t_k b_k \end{bmatrix}$$
$$= \begin{bmatrix} \frac{1}{m}\sum_{k=1}^m b_k \\ \left(\sum_{k=1}^m t_k b_k\right) / \left(\sum_{k=1}^m t_k^2\right) \end{bmatrix},$$

this is an instance where having orthogonal vectors is beneficial. In this next Section we will see how to build orthonormal basis for subspaces, and some of the many benefits they have.

Challenge 7. Try to work out the actual change of variables that makes the t_k's add up to zero and derive a formula for fitting a line to points without the assumption in Remark 5.3.3

Example 5.3.4 (Fitting a Parabola)**.** *We can use Linear Algebra to do fits of many other curves (or functions), not just lines. If we believe the relationship between t_k and b_k is quadratic we could attempt to fit a Parabola:*

$$b_k \approx \alpha_0 + \alpha_1 t_k + \alpha_2 t_k^2.$$

While this isn't a linear function in t_k, this is still a linear function on the coefficients α_0, α_1, and α_2, and this is what is important. Similarly as with linear regression, it is natural to attempt to *minimze*

$$\min_{\alpha_0,\alpha_1,\alpha_2} \left\| b - A \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} \right\|^2, \tag{6}$$

where

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-1} \\ b_m \end{bmatrix} \quad \textit{and} \quad A = \begin{bmatrix} 1 & t_1 & t_1^2 \\ 1 & t_2 & t_2^2 \\ \vdots & \vdots & \\ 1 & t_{m-1} & t_{m-1}^2 \\ 1 & t_m & t_m^2 \end{bmatrix},$$

and we can use the technology we developed in this section to solve this problem as well.

Challenge 8. Try to work out the example of fitting a parabola further. What is $A^\top A$? When is $A^\top A$ diagonal?

Further Reading 9. There is a whole (beautiful) area of Mathematics related to studying so-called *Orthogonal Polynomials*. The basic idea can be already hinted at from these examples: In the example of the parabola we wrote a function of t as a linear combination of the polynomials 1, t, and t^2. But we could have picked other polynomials, we could have e.g. written something like $b \approx \alpha_0' + \alpha_1'(t - 2023) + \alpha_2(t^2 + t)$, and a particularly good choice (that would depend on the distribution of the points t_k) might have resulted in a diagonal matrix $A^\top A$... *search "orthogonal polynomials" online to learn more.*

Further Reading 10. A lot of Machine Learning includes Linear Regression as a key component. The idea is to create, find, or *learn* features of the data points. Given n data points $t_1, \dots t_n$ (which now can be perhaps pixel images, rather than just time points) we might want to do classification (for example, in the case of images, maybe we want a function that is large when the picture has a dog in it and small when it has a cat in it). It is hard to imagine that this can be done with a linear fit, but if we build good feature vectors $\varphi(t_k) \in \mathbb{R}^p$ for very large p then the function can depend on all coordinates of $\varphi(t_k)$ (the p features) and this is incredible powerful. There are several ways to construct features, a bit over a decade ago they were sometimes handmade, now they are often learned (this is in a sense what Deep Learning does). Another important way to build (or compute with) features are the so-called Kernel Methods.

5.4. **Orthonormal Bases and Gram Schmidt.**

When we think of (or draw) a basis of a subspace, we tend to think of (or draw) vectors that are orthogonal (have an angle of 90°) and that have the same length (length 1). Indeed, these bases have many advantages, this section is about these bases, some of their advantages, and how to find them.

Definition 5.4.1 (Orthonormal vectors)**.** *Vectors $q_1,\dots,q_n \in \mathbb{R}^m$ are orthonormal if they are orthogonal and have norm 1. In other words, for all $i,j \in \{1,\dots,n\}$*

$$q_i^T q_j = \delta_{ij},$$

where δ_{ij} is the Kronecker delta

$$\delta_{ij} = \begin{cases} 0 & \textit{if } i \neq j \\ 1 & \textit{if } i = j. \end{cases} \tag{7}$$

If Q is the matrix whose columns are the vectors q_i's, then the condition that the vectors are orthonormal can be rewritten as $Q^\top Q = I$.

Caution! 11. Q may not be a square matrix, and so it is not necessarily the case that $QQ^\top = I$.

Example 5.4.2. *A classical example of an orthonormal set of vectors is the canonical basis, $e^1,\dots,e^n \in \mathbb{R}^n$ where e^i is the vector with a 1 in the i-th entry and 0 in all other entries, i.e., $(e^i)_j = \delta_{ij}$.*

When Q is a square matrix then $Q^\top Q = I$ implies also that $QQ^\top = I$ and so $Q^{-1} = Q^\top$. We call such matrices *orthogonal matrices*. This corresponds to the case when the q_i's are an orthonormal basis for all of $\mathbb{R}^n$.

Definition 5.4.3 (Orthogonal Matrix)**.** *A square matrix $Q \in \mathbb{R}^{n\times n}$ is an orthogonal matrix when $Q^\top Q = I$. In this case, $QQ^\top = I$, $Q^{-1} = Q^\top$, and the columns of Q form an orthonormal basis for $\mathbb{R}^n$.*

Example 5.4.4. *The 2×2 matrix Q that corresponds to rotating, counterclockwise, the plane by θ,*

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

is an orthogonal matrix. Indeed,

$$R_\theta^T R_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = I.$$

Example 5.4.5. *Permutation matrices are another example of orthogonal matrices. A permutation is a map*

$$\pi:\ \{1,\dots,n\} \mapsto \{1,\dots,n\} \textit{ such that } \pi(i) \neq \pi(j) \textit{ for } i \neq j.$$

The permutation matrix $A \in \mathrm{R}^{n\times n}$ associated with π has entries $A_{ij} = 1$ if $\pi(i) = j$ and $A_{ij} = 0$, otherwise. From this definition one can derive that A^T is the permutation matrix associated with the permutation σ defined as $\sigma(j) = i$ for $\pi(i) = j$. Hence, $A^TA = I$, i.e., A is an orthogonal matrix.

Challenge 12 ($\star$)**.** Show that for every permutation matrix P there exists a positive integer k such that $P^k = I$.

Proposition 5.4.6. *Orthogonal matrices preserve norm and inner product of vectors. In other words, if $Q \in \mathbb{R}^{n\times n}$ is orthogonal then, for all $x, y \in \mathbb{R}^n$*

$$\|Qx\| = \|x\| \text{ and } (Qx)^\top(Qy) = x^\top y$$

Proof. To show the second inequality note that, for $x, y \in \mathbb{R}^n$ we have that $(Qx)^\top(Qy) = x^\top Q^\top Qy = x^\top Iy = x^\top y$. To show the first equality note that, since for $x \in \mathbb{R}^n$ we have that $\|Qx\| \geq 0$ and $\|x\| \geq 0$, it suffices to show that the squares are equal and indeed $\|Qx\|^2 = (Qx)^\top(Qx) = x^\top x = \|x\|^2$. □

5.4.1. *Projections with Orthonormal Basis.*

One advantage of having access to an orthonormal basis is that projections become much simpler. The reason is easy to explain. When we discussed projections and least squares, many of the expressions we derived included $A^\top A$, but in the case when A has orthonormal columns, these all simplify as $A^\top A = I$. We collect these observations in the following proposition.

Proposition 5.4.7. *Let S be a subspace of $\mathbb{R}^m$ and $q_1,\ldots,q_n$ be an orthonormal basis for S. Let Q be the $m\times n$ matrix whose columns are the q_i's; $Q = \begin{bmatrix} q_1 & , & \cdots & , & q_n \end{bmatrix}$. Then the Projection Matrix that projects to S is given by $QQ^\top$ and the Least Squares solution to $Qx = b$ is given by $\hat{x} = Q^\top b$.*

Remark 5.4.8. *When Q is a square matrix then the projection $QQ^\top$ is simply the identity (corresponding to projecting to the entire ambient space $\mathbb{R}^n$. Even in this seemingly trivial instance, it is useful to look closer at what this operation does: For a vector $x \in \mathbb{R}^n$ it gives*

$$x = q_1\left(q_1^\top x\right) + q_2\left(q_2^\top x\right) + \cdots + q_n\left(q_n^\top x\right).$$

It is writing x as a linear combination of the orthonormal basis $\{q_i\}_{i=1}^n$ (as we will see later this is sometimes referred to as a change of basis*).*[6]

5.4.2. *Gram-Schmidt Process.*

By now we have given some evidence that orthonormal bases are useful. Fortunately, there is a relatively simple process to construct orthonormal bases, that will also suggest a new matrix factorization.

The idea is simple: If we have 2 linearly independent vectors a_1 and a_2 which span a subspace S, it is straightforward to transform them into an orthonormal basis of S: we first normalize a_1: $q_1 = \frac{a_1}{\|a_1\|}$, then subtract from a_2 a multiple of q_1 so that it becomes orthogonal to q_1, followed by a normalization step:

$$q_2 = \frac{a_2 - (a_2^\top q_1)q_1}{\|a_2 - (a_2^\top q_1)q_1\|}.$$

Let us check that indeed these vectors are orthonormal: By construction they have unit norm, and

$$q_1^\top q_2 = q_1^\top \frac{a_2 - (a_2^\top q_1)q_1}{\|a_2 - (a_2^\top q_1)q_1\|} = \frac{q_1^\top a_2 - (a_2^\top q_1)q_1^\top q_1}{\|a_2 - (a_2^\top q_1)q_1\|} = \frac{0}{\|a_2 - (a_2^\top q_1)q_1\|} = 0.$$

Note that the denominator is not zero because a_1 and a_2 are linearly independent; and that, since q_1 has unit norm, $(a_2^\top q_1)q_1 = \mathrm{proj}_{\mathrm{Span}(q_1)}(a_2)$.

For more vectors, the idea is to apply this process recursively, by removing from a vector a_{k+1} the projection of it on the subspace spanned by the k vectors before it. More formally:

Algorithm 5.4.9. *[Gram-Schmidt Process] Given n linearly independent vectors $a_1, \ldots, a_n$ that span a subspace S, the Gram-Schmidt process constructs $q_1, \ldots q_n$ in the following way:*

- $q_1 = \frac{a_1}{\|a_1\|}$.
- *For $k = 2, \ldots, n$ set*
  $q'_k = a_k - \sum_{i=1}^{k-1} (a_k^\top q_i) q_i$
  $q_k = \frac{q'_k}{\|q'_k\|}$.

Theorem 5.4.10 (Correctness of Gram-Schmidt)**.** *Given n linearly independent vectors $a_1, \ldots, a_n$, the Gram-Schmidt process returns an orthonormal basis for the span of $a_1, \ldots, a_n$.*

[6] There are countless instances in which doing this operation is beneficial, for example one of the most important algorithms, the *Fast Fourier Transform*, is an instance of this operation.

Proof. Let S_k be the subspace spanned by $a_1,\dots,a_k$. Then $S = S_n$. We will show, by induction, that $q_1,\dots,q_k$ are an orthonormal basis for S_k. It is enough to show that they are orthonormal and are in S_k since orthonormality implies linearly independence and S_k has dimension k.

For the base case, note that $\|q_1\| = 1$ and q_1 is a multiple of a_1 and so $q_1 \in S_1$.

Now we assume the hypothesis for $i = 1,\dots k-1$ and prove it for k. By the hypothesis $q_1,\dots,q_{k-1}$ are orthonormal, so we have to show that $\|q_k\| = 1$ and that $q_i^\top q_k = 0$ for all $1 \le i \le k-1$.

- Since a_k is linearly independent from the other original vectors it is not in S_{k-1} and so $q'_k \neq 0$. Thus $\|q_k\| = 1$.
- By construction $a_k \in S_k$ and so $q_k \in S_k$.
- Let $1 \le j \le k-1$. Since $q_1,\dots,q_{k-1}$ are orthonormal, we have
$$q_j^\top \left(a_k - \sum_{i=1}^{k-1} (a_k^\top q_i) q_i \right) = q_j^\top a_k - \sum_{i=1}^{k-1} (a_k^\top q_i) q_j^\top q_i = q_j^\top a_k - (a_k^\top q_j) = 0,$$
and $q_j^\top q_k = \frac{1}{\|q'_k\|} q_j^\top q'_k = 0$.

□

Challenge 13. Try to do the Gram-Schmidt process for the columns of

$$\begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 4 & 5 & 6 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & 9 \end{bmatrix}.$$

Is it the case that the Gram-Schmidt process of the columns of an upper triangular matrix (with non-zero diagonal elements) is always a subset of the canonical basis? Can you come up with an example of a set of vectors for which Gram-Schmidt does not output elements of the canonical basis?

Gram-Schmidt actually provides us with a new matrix factorization. Let A be an $m \times n$ matrix with linearly independent columns $a_1,\dots,a_n$ and Q the $m \times n$ matrix whose columns are $q_1,\dots,q_n$ as outputted by Algorithm 5.4.9. Let $R = Q^\top A$, since each q_k is orthogonal to every a_i for $i < k$ we have that R is upper triangular. Q is not necessarily a square matrix, and so not necessarily invertible. But $QQ^\top$ is the projection on the span of the q_i's and thus also on the a_i's, this means that $QQ^\top A = A$ and so we have that $QR = QQ^\top A = A$. We call $A = QR$ the QR decomposition.

Definition 5.4.11 (QR decomposition)**.** *Let A be an $m \times n$ matrix with linearly independent columns. The QR decomposition is given by*

$$A = QR,$$

where Q is an $m \times n$ matrix with orthonormal columns (they are the output of Gram Schmidt, Algorithm 5.4.9, on the columns of A) and R is an upper triangular matrix given by $R = Q^\top A$.

It requires us to show that indeed this is a proper definition. We need to convince ourselves that R is upper triangluar.

Lemma 5.4.12. *The matrix R defined in Definition 5.4.11 is upper triangular and invertible. Moreover, $QQ^T A = A$ and hence, $A = QR$ is well defined.*

Proof. $q_k^T q_i = 0$ for all $i = 1, \dots k-1$. Since $q_1, \dots, q_{k-1}$ and $a_1, \dots, a_{k-1}$ span the same subspace S_{k-1} we have that $q_k^T a_i = 0$ for all $i = 1, \dots, k-1$. Hence $R = Q^T A$ is upper triangular. Moreover, QQ^T is the projection onto the subspace $C(Q) = C(A)$. Hence, for every index i,

$$\text{proj}_{S_n}(a_i) = a_i = QQ^T a_i.$$

This is equivalent to $QQ^T A = QR = A$. Finally, $N(A) = \{0\}$ and since $A = QR$, we must have that $N(R) = \{0\}$. Since R is an n by n matrix R is invertible and hence, R^T as well. □

Fact 5.4.13. *The QR decomposition greatly simplifies calculations involving Projections and Least Squares.*

- *Since* $\mathrm{C}(A) = \mathrm{C}(Q)$ *then projections on* $\mathrm{C}(A)$ *can be done with Q which means they are given by* $\text{proj}_{\mathrm{C}(A)}(b) = QQ^\top b$.
- *The least squares solution to $Ax = b$ denoted by $\hat{x}$ is defined as a solution of the normal equations (recall* (3)*)*

  $$A^\top A\hat{x} = A^\top b.$$

  Furthermore, $A^\top A = (QR)^\top (QR) = R^\top Q^\top QR = R^\top R$, and so we can write

  $$R^\top R\hat{x} = R^\top Q^\top b. \tag{8}$$

  Since R has independent columns (is full column rank) then $\mathrm{N}(R) = \{0\}$ *and so we can simplify* (8) *to*

  $$R\hat{x} = Q^\top b, \tag{9}$$

which can be efficiently solved by back-substitution since R is a triangular matrix.

5.5. **The Pseudoinverse, also known as Moore–Penrose Inverse.**

The goal of this Section is to construct an analogue to the inverse of a matrix A for matrices that have no inverse. Such an analogue is called a pseudoinverse, or the Moore-Penrose Inverse, and we will denote it by $A^{\dagger}$. It is also commonly denoted by A^{+}.

Guiding Question 14. While not all matrices are A invertible, we saw that we can still aim to find the (or a) vector x such that Ax is as close as possible to a target vector b. Can we develop this idea to define a “pseudoinverse” for any matrix A, a matrix that is, in a sense, closest to being an inverse for A? What should “closest to being an inverse” even mean?

There are (at least) three issues we need to overcome to try to define a *pseudoinverse* for a non-invertible matrix A: (i) For some vectors b there might not be a vector x such that $Ax = b$, (ii) For some vectors b there may be more than one x such that $Ax = b$ and we would have to pick one, and (iii) even if we make such choices, it is not clear that such an operation will correspond to multiplying by a matrix $A^{\dagger}$.

Let $A \in \mathbb{R}^{m\times n}$ be an $m \times n$ matrix. There are a couple of different ways we could try to define a *pseudoinverse* $A^{\dagger}$ for a non-invertible matrix A. Let us start by building on what we discussed in Section 5.3 (Least Squares Approximations), if the columns of A are linearly independent that it would make sense to build $A^{\dagger}$ such that $A^{\dagger}b$ is the Least Squares Solution $\hat{x} = (A^{\top}A)^{-1}A^{\top}b$ (the vector $\hat{x}$ such that $A\hat{x}$ is as close as possible to b), and so for matrices A with independent columns we will define $A^{\dagger} = (A^{\top}A)^{-1}A^{\top}$. This motivates the following definition.

Definition 5.5.1 (Pseudoinverse for matrices of full column rank)**.** *For $A \in \mathbb{R}^{m\times n}$ with* $\operatorname{rank}(A) = n$ *we define the pseudo-inverse $A^{\dagger} \in \mathbb{R}^{n\times m}$ of A as*

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

Proposition 5.5.2. *For $A \in \mathbb{R}^{m\times n}$ with* $\operatorname{rank}(A) = n$*, the pseudoinverse $A^{\dagger}$ is a left inverse of A, meaning that $A^{\dagger}A = I$.*

Proof. Since $\operatorname{rank}(A) = n$, $A^{\top}A$ is invertible. Furthermore, $A^{\dagger}A = (A^{\top}A)^{-1}A^{\top}A = I$. □

Let us know consider the case for which the rows are linearly independent (in other words, $A \in \mathbb{R}^{m\times n}$ is full row rank; or equivalently $\operatorname{rank}(A) = m$). One natural way to define a pseudoinverse is based on the observation that $A^\top$ has full column rank and to define $A^\dagger$ as

$$\left(\left(A^\top\right)^\dagger\right)^\top = \left(\left(\left(A^\top\right)^\top\left(A^\top\right)\right)^{-1}\left(A^\top\right)^\top\right)^\top = \left(\left(AA^\top\right)^{-1}A\right)^\top = A^\top\left(AA^\top\right)^{-1}.$$

Definition 5.5.3 (Pseudoinverse for matrices of full row rank)**.** *For $A \in \mathbb{R}^{m\times n}$ with $\operatorname{rank}(A) = m$ we define the pseudo-inverse $A^\dagger \in \mathbb{R}^{n\times m}$ of A as*

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

Lemma 5.5.4. *For $A \in \mathbb{R}^{m\times n}$ with $\operatorname{rank}(A) = m$, the pseudoinverse $A^\dagger$ is a right inverse of A, meaning that $AA^\dagger = I$.*

Proof. Since $\operatorname{rank}(A) = m$, $AA^\top$ is invertible. Furthermore, $AA^\dagger = AA^\top(AA^\top)^{-1} = I$. □

Let us try to understand what $A^\dagger$ is achieving for full row rank matrices A. Since A is full row rank, for all $b \in \mathbb{R}^m$, there exists $x \in \mathbb{R}^n$ such that $Ax = b$. The issue is that there are potentially many such vectors. A natural strategy in this case is to pick, among all such vectors, the one with smallest norm.[7] In other words to solve

$$\begin{aligned} \min_{x\in\mathbb{R}^n} \quad & \|x\|^2 \\ s.t. \quad & Ax = b, \end{aligned} \tag{10}$$

where s.t. stands for "subject to" or "such that". If x_1 and x_2 are vectors such that $Ax_1 = Ax_2 = b$ then $x_1 - x_2 \in \mathrm{N}(A)$, and conversely, if $Ax = b$ and $y \in \mathrm{N}(A)$ then $A(x + y) = b$. Thus, given one vector x_1 such that $Ax_1 = b$ the set of solutions to $Ax = b$ are all vectors of the form $x_1 + y$ where $y \in \mathrm{N}(A)$. So we would like to find the minimum $\|x_1 + y\|$ among all vectors $y \in \mathrm{N}(A)$. Let us write $x_1 = \left(x_1 - \mathrm{proj}_{\mathrm{N}(A)}(x_1)\right) + \mathrm{proj}_{\mathrm{N}(A)}(x_1)$. Since $y \in \mathrm{N}(A)$ we have that $\left(x_1 - \mathrm{proj}_{\mathrm{N}(A)}(x_1)\right) \perp \left(y + \mathrm{proj}_{\mathrm{N}(A)}(x_1)\right)$ and so, by Pythagoras,

$$\begin{aligned} \|x_1 + y\|^2 &= \left\|\left(x_1 - \mathrm{proj}_{\mathrm{N}(A)}(x_1)\right) + \mathrm{proj}_{\mathrm{N}(A)}(x_1) + y\right\|^2 \\ &= \left\|x_1 - \mathrm{proj}_{\mathrm{N}(A)}(x_1)\right\|^2 + \left\|\mathrm{proj}_{\mathrm{N}(A)}(x_1) + y\right\|^2, \end{aligned}$$

[7] This idea, of picking the smallest (or simplest) solution among many possibilities goes far beyond Linear Algebra and is known as "regularization" in Statistics, Machine Learning, Signal Processing, and Image Processing, etc. It can be viewed as a mathematical version of the famous "Occam's razor" principle in Philosophy.

and so picking $y = -\operatorname{proj}_{\mathrm{N}(A)}(x_1)$ yields the smallest norm solution. Since the vectors orthogonal to $\mathrm{N}(A)$ are precisely the vectors that are in $\mathrm{C}(A^\top)$, i.e., the row space of A. We just proved.

Lemma 5.5.5. *For any matrix A and a vector $b \in C(A)$, the (unique) solution to* (10) *is given by the vector $\hat{x} \in \mathrm{C}(A^\top)$ that satisfies the constraint $A\hat{x} = b$.*

$A^\dagger$ is precisely the matrix that maps b to a point $\hat{x}$ that corresponds to a solution of (10).

Proposition 5.5.6. *For a full row rank matrix A, the (unique) solution to* (10) *is given by the vector $\hat{x} = A^\dagger b$.*

Proof. By using Lemma 5.5.5 we just need to show that $\hat{x} = A^\dagger b$ satisfies $A\hat{x} = b$ and that $\hat{x} = A^\dagger b$ is in $\mathrm{C}(A^\top)$. Both these are easy to verify: $A\hat{x} = AA^\dagger b = AA^\top(AA^\top)^{-1}b = b$ and $\hat{x} = A^\dagger b = A^\top\left((AA^\top)^{-1}b\right)$ and so $\hat{x} \in \mathrm{C}(A^\top)$. □

Our next task is to define $A^\dagger$ for all matrices, not just full rank matrices. The idea is to write A as a product of two matrices, one which is of full column rank and one which is of full row rank. Recall that in Part I of the lecture we achieved this task by introducing the *CR*-decomposition. For $A \in \mathbb{R}^{m\times n}$, with $\operatorname{rank}(A) = r$, the CR decomposition writes $A = CR$ where $C \in \mathbb{R}^{m\times r}$ has the first r linearly independent columns of A and $R \in \mathbb{R}^{r\times n}$ is upper triangular. Note that C has full column rank and R full row rank.

Definition 5.5.7 (Pseudoinverse for all matrices)**.** *For $A \in \mathbb{R}^{m\times n}$ with* $\operatorname{rank}(A) = r$ *and CR decomposition $A = CR$ we define the pseudoinverse $A^\dagger$ as*

$$A^\dagger = R^\dagger C^\dagger,$$

which can be rewritten as

$$A^\dagger = R^\top\left(RR^\top\right)^{-1}\left(C^\top C\right)^{-1}C^\top = R^\top\left(C^\top CRR^\top\right)^{-1}C^\top = R^\top\left(C^\top AR^\top\right)^{-1}C^\top.$$

The following lemma characterizes what the matrix $A^\dagger$ achieves for us.

Lemma 5.5.8. *Given $A \in \mathbb{R}^{m\times n}$ and a vector $b \in \mathbb{R}^n$, the (unique) solution to*

$$\begin{aligned} \min_{x\in\mathbb{R}^n} \quad & \|x\|^2 \\ s.t. \quad & A^\top Ax = A^\top b, \end{aligned} \tag{11}$$

is given by $\hat{x} = A^\dagger b$.

Proof. Let r be the rank of A and $A = CR$ with $C \in \mathbb{R}^{m\times r}$ and $R \in \mathbb{R}^{r\times n}$. Then $\hat{x} = A^\dagger b = R^\top \left(C^\top AR^\top\right)^{-1} C^\top b$. Thus,

$$A^\top A\hat{x} = A^\top AR^\top \left(C^\top AR^\top\right)^{-1} C^\top b = R^\top C^\top AR^\top \left(C^\top AR^\top\right)^{-1} C^\top b = R^\top C^\top b = A^\top b.$$

It remains to show that $\hat{x}$ is the smallest norm solution. To verify this we use Lemma 5.5.5, i.e., we need to verify that $\hat{x} \in \mathrm{C}(A^\top A)$. From Lemma 5.1.11 we conclude that $C(A^TA) = C(A^T)$. Hence it is enough to show that $\hat{x} \in \mathrm{C}(A^\top)$ and since $\mathrm{C}(A^\top) = \mathrm{C}(R^\top)$ we have that $\hat{x} = R^\top \left(C^\top AR^\top\right)^{-1} C^\top b \in \mathrm{C}(R^\top)$ from which the statement follows. □

In this proof, the only property of the matrices CR we used is that $A = CR$ and both C and R are full rank. So we have actually shown that we can compute the pseudoinverse from any full rank factorization, not just specifically the CR decomposition. We write it here as a proposition.

Proposition 5.5.9. *For $A \in \mathbb{R}^{m\times n}$, with $\operatorname{rank}(A) = r$, and let $S \in \mathbb{R}^{m\times r}$ and $T \in \mathbb{R}^{r\times n}$ such that $A = ST$. Then,*

$$A^\dagger = T^\dagger S^\dagger.$$

Remark 5.5.10. *Note that If $A = ST$ and $\operatorname{rank}(A) = r$ then $rank(S) \geq r$ and $\operatorname{rank}(T) \geq r$ and so the matrices ST in Proposition 5.5.9 are indeed full rank (either full column rank or full row rank).*

Let us finally summarize a few important properties about the matrix A and its pseudoinverse $A^\dagger$.

Theorem 5.5.11. *Let $A \in \mathbb{R}^{m\times n}$.*

(1) $AA^\dagger A = A$

(2) $A^\dagger AA^\dagger = A^\dagger$.

(3) $AA^\dagger$ *is symmetric. It is the projection matrix for projection on* $\mathrm{C}(A)$,

(4) $A^{\dagger}A$ *is symmetric. It is the projection matrix for projection on* $\mathrm{C}(A^{\top})$.
(5) $(A^{\top})^{\dagger} = (A^{\dagger})^{\top}$,

Proof. (1) We calculate

$$AA^{\dagger}A = CRR^T(C^TCRR^T)^{-1}C^TCR = CRR^T(RR^T)^{-1}(C^TC)^{-1}C^TCR = CR = A.$$

(3) To see that $AA^{\dagger}$ is symmetric we calculate

$$AA^{\dagger} = CRR^T(RR^T)^{-1}(C^TC)^{-1}C^T = C(C^TC)^{-1}C^T = \left(C(C^TC)^{-1}C^T\right)^T = (AA^{\dagger})^T.$$

Since the column space of A, $C(A)$ and the column space of C coincide and since C is a basis for $C(A)$ Theorem 5.2.6 applies and shows us that $AA^{\dagger} = C(C^TC)^{-1}C^T$ is the projection matrix for projecting onto $C(A)$. □

Challenge 15. Prove Statements (2), (4) and (5) of Theorem 5.5.11.

Proposition 5.5.12. *Let* $A \in \mathbb{R}^{m\times n}$ *be a matrix and recall that* $\mathrm{C}(A)$ *and* $\mathrm{C}(A^{\top})$ *denote respectively its column and row spaces. When* $A : x \to Ax$ *is viewed as a function from* $\mathrm{C}(A^{\top})$ *to* $\mathrm{C}(A)$ *it is a bijection. In other words, for all* $b \in \mathrm{C}(A)$ *there is one and only one* $x \in \mathrm{C}(A^{\top})$ *such that* $Ax = b$.

Challenge 16. Prove Proposition 5.5.12

5.6. **Projections of sets and the Farkas lemma.**

We have so far seen that a single point can be projected to a subspace by solving a least squares problem. Now we want to consider entire sets of points and understand their projections.

Guiding Question 17. Suppose we are given a set of linear inequalities in R^n. How can we certify that the set is nonempty? An answer to this question is absolutely fundamental and has numerous applications in other areas of science.

In order to attack this question we remark that projections are a way to reduce the dimension of the initial question about feasibility of a set in R^n to a question about feasibility of a set in smaller dimension. We will not consider here arbitrary sets, but focus on sets described by linear inequalities whose coefficients are all rational. Let us make this precise

Definition 5.6.1. *Let $A \in \mathrm{Q}^{m \times n}$, $b \in \mathrm{Q}^m$ and $P = \{x \in \mathrm{R}^n \mid Ax \leq b\}$. P is called a polyhedron. Let $S = \{1, \dots, s\}$. The* **projection of P** *on the subspace* R^s *associated with the variables in the subset S is*

$$\mathrm{proj}_S(P) := \{x \in \mathrm{R}^s \mid \exists y \in \mathrm{R}^{n-s} \textit{ such that } (x,y) \in P\}.$$

.

From the definition it is clear that $P \neq \emptyset$ if and only if $\mathrm{proj}_S(P) \neq \emptyset$. The question though is whether the set $\mathrm{proj}_S(P)$ also has a description in the form of a finite system of linear inequalities. If so, then we can indeed reduce the question of whether $P \neq \emptyset$ to a question of the same form in smaller dimension.

Let us build some intuition by analyzing the situation when we project a one-dimensional set of inequalities to dimension 0. Let $a \in \mathrm{Q}^m$, $a_i \neq 0$ for all i and $b \in \mathrm{Q}^m$. We consider $P = \{x \in \mathrm{R} \mid ax \leq b\} \subseteq \mathrm{R}$. We first notice that we can rewrite the constrains in P as follows. Set

$$u := \min\{\frac{b_i}{a_i} \mid a_i > 0\}, \quad l := \max\{\frac{b_i}{a_i} \mid a_i < 0\}.$$

Then

$$P = \{x \in \mathrm{R} \mid x \leq \frac{b_i}{a_i} \text{ if } a_i > 0,\, x \geq \frac{b_i}{a_i} \text{ if } a_i < 0\} = \{x \in \mathrm{R} \mid x \leq u,\, x \geq l\}.$$

Now we are in the position to clarify when $P = \emptyset$.

Proposition 5.6.2.

$$P \neq \emptyset \iff l \leq u \iff 0 \leq u - l \iff 0 \leq y^T b \textit{ for all } y \geq 0 \textit{ such that } y^T a = 0.$$

This idea can be applied in general.

5.6.1. *Elimination of one variable.*

Let $A \in \mathrm{Q}^{m \times n}$, $b \in \mathrm{Q}^m$ and $P = \{x \in \mathrm{R}^n \mid Ax \leq b\}$. In what follows we denote the entries of the matrix A by a_{ij}. Hence, row i gives us an inequality of the form

$$\sum_{j=1}^{n} a_{ij} x_j \leq b_i.$$

Let $\bar{x} = (x_1, \dots, x_{n-1})$ and define the matrix consisting of the first $n-1$ columns by

$$\bar{A} = [A_{\cdot 1} \dots A_{\cdot n-1}].$$

Consider now the algorithm that applies the following steps.

Step 1 Partition the indices $M = \{1,\dots,m\}$ of the rows of the matrix A into three subsets

$$M_0 = \{i \in M \mid a_{i,n} = 0\}, \quad M_+ = \{i \in M \mid a_{i,n} > 0\} \text{ and } M_- = \{i \in M \mid a_{i,n} < 0\}.$$

Step 2

- For every row with index $i \in M_+$ multiply the corresponding constraint by $\frac{1}{a_{in}}$. This gives a new representation of the i-th. row as follows

$$x_n \leq d_i + f_i^T \bar{x} \text{ for } i \in M_+ \text{ where } d_i = \frac{b_i}{a_{in}},\ f_{ij} = -\frac{a_{ij}}{a_{in}}.$$

- Every row with index $k \in M_0$ can be rewritten as

$$0 \leq d_k + f_k^T \bar{x} \text{ for } k \in M_0 \text{ where } d_k = b_k,\ f_{kj} = -a_{kj}.$$

- For every row with index $i \in M_-$ multiply the corresponding constraint by $\frac{1}{a_{in}}$. This gives a new representation of the i-th. row as follows

$$x_n \geq d_i + f_i^T \bar{x} \text{ for } i \in M_- \text{ where } d_i = \frac{b_i}{a_{in}},\ f_{ij} = -\frac{a_{ij}}{a_{in}}.$$

Step 3 Return

$$\begin{aligned} Q = \quad & \Big\{\bar{x} \in \mathrm{R}^{n-1} \mid \quad 0 \leq & d_k + f_k^T \bar{x} \text{ for all } k \in M_0, \\ & d_l + f_l^T \bar{x} \qquad \leq & d_i + f_i^T \bar{x} \text{ for all } l \in M_-,\ i \in M_+ \Big\}. \end{aligned}$$

Theorem 5.6.3. *The set Q returned in Step 3 is a polyhedron. Moreover, $Q = \mathrm{proj}_S(P)$, where $S = \{1,\dots,n-1\}$.*

Proof. Q is a polyhedron, because we can define a matrix $F \in \mathrm{Q}^{k \times n-1}$ and a right hand side vector δ such that

$$Q = \Big\{\bar{x} \in \mathrm{R}^{n-1} \mid F\bar{x} \leq \delta\Big\}.$$

Indeed, $k = |M_0| + |M_-||M_+|$. The rows of F contain all rows of A with index $i \in M_0$ and the corresponding right hand side vector satisfies that $\delta_i = b_i$. The other rows of F are of the form $(f_l - f_i)^T$ for indices $l \in M_-$ and $i \in M_+$. The corresponding right hand side entry of δ is then $\delta_i = d_i - d_l$.

Let us show next that $\mathrm{proj}_S(P) \subseteq Q$. Take any $\bar{x} \in \mathrm{proj}_S(P)$. By definition there exists $z \in \mathrm{R}$ such that $(\bar{x}, z) \in P$. Hence z satisfies the constraints presented in Step 2. In particular, $d_l + f_l^T \bar{x} \leq z \leq d_i + f_i^T \bar{x}$ for all $l \in M_,\ i \in M_+$. This shows that $\bar{x} \in Q$.

To see why $Q \subseteq \text{proj}_S(P)$, take any $\bar{x} \in Q$. It follows that

$$\begin{array}{rcll} 0 & \leq & d_k + f_k^T \bar{x} & \text{for all } k \in M_0, \\ d_l + f_l^T \bar{x} & \leq & d_i + f_i^T \bar{x} & \text{for all } l \in M_-,\ i \in M_+. \end{array}$$

Let $L := \max\{d_l + f_l^T \bar{x} \mid l \in M_-\}$ and $U := \min\{d_i + f_i^T \bar{x} \mid i \in M_+\}$. Take any value $z \in [L,U]$. Then $(\bar{x}, z) \in P$. Hence, $\bar{x} \in \text{proj}_S(P)$. □

Our next task is to use these projections repeatedly.

Lemma 5.6.4. *Let $A \in \mathrm{Q}^{m\times n}$, $b \in \mathrm{Q}^m$ and $P = \{x \in \mathrm{R}^n \mid Ax \leq b\}$. Let $S_1 = \{1,\ldots,n-1\}$ and $S_2 = \{1,\ldots,n-2\}$. Then*

$$\text{proj}_{S_2}(P) = \text{proj}_{S_2}(\text{proj}_{S_1}(P)).$$

Proof. Let $z \in \text{proj}_{S_2}(P)$. Hence, there exist real values (x_{n-1}, x_n) such that $(z, x_{n-1}, x_n) \in P$. In particular, there exists a value x_n such that $(z, x_{n-1}, x_n) \in P$. Hence, $(z, x_{n-1}) \in \text{proj}_{S_1}(P)$ and hence, $z \in \text{proj}_{S_2}(\text{proj}_{S_1}(P)$.

Conversely, take any $z \in \text{proj}_{S_2}(\text{proj}_{S_1}(P))$. By definition, there exists a real value x_{n-1} such that $(z, x_{n-1}) \in \text{proj}_{S_1}(P)$. Hence there also exists a real value x_n such that $(z, x_{n-1}, x_n) \in P$. Hence, $z \in \text{proj}_{S_2}(P)$. □

It is an inductive argument to show the following generalization of Lemma 5.6.4. This is left as an exercise.

Challenge 18. Let $A \in \mathrm{Q}^{m\times n}$, $b \in \mathrm{Q}^m$ and $P = \{x \in \mathrm{R}^n \mid Ax \leq b\}$. Let $S_1 = \{1,\ldots,n-k\}$ and $S_2 = \{1,\ldots,n-j\}$ for indices $1 \leq k < j < n$. Then

$$\text{proj}_{S_2}(P) = \text{proj}_{S_2}(\text{proj}_{S_1}(P)).$$

5.6.2. *A compact algebraic description of projections and the Farkas Lemma.*

In view of Challenge 18 we can start with a polyhedron P in dimension n and eliminate variable by variable. At the end there is no variable left and we simply reduced the question of whether P is empty or not to a logical statement that is either true or false, see Proposition 5.6.2. The question emerges how to describe this elimination process algebraically?

This requires us to set up some terminology.

Definition 5.6.5. *Let $A \in Q^{m\times n}$, $b \in Q^m$ and $P = \{x \in R^n \mid Ax \leq b\}$. For $k \in \{1,\dots,j\}$ let $A^{(j)}$ to be the submatrix of A with column vectors $A_{\cdot k}$. Let $P^{(0)} = P$ and $C^{(0)} = R^m_+$. Define for $i \in \{1,\dots,n\}$*

$$C^{(i)} = \Big\{y \in R^m_+ \mid y^T A_{\cdot k} = 0 \, for\, all\; k = n-i+1,\dots,n\Big\}.$$

$$P^{(i)} = \Big\{\bar{x} \in R^{n-i} \mid y^T A^{(n-i)}\bar{x} \leq y^T b \, for\, all\; y \in C^{(i)}\Big\}.$$

With this notation we can now elegantly describe the projection of a polyhedron.

Theorem 5.6.6. $\text{proj}_{S_{n-i}}(P) = P^{(i)}$.

Proof. We first verify that $\text{proj}_{S_{n-i}}(P) \subseteq P^{(i)}$. Indeed, take any $\bar{x} \in \text{proj}_{S_{n-i}}(P)$. By definition there exists a real vector z of dimension i such that $(\bar{x}, z) \in P$. Hence, $(\bar{x}, z)$ satisfies the following inequalities

$$\sum_{k=1}^{n-i} A_{\cdot k}\bar{x}_k + \sum_{k=n-i+1}^{n} A_{\cdot k}z_k \leq b.$$

This implies that for all $y \in C^{(i)}$ we obtain that

$$\sum_{k=1}^{n-i} y^T A_{\cdot k}\bar{x}_k + \sum_{k=n-i+1}^{n} y^T A_{\cdot k}z_k = \sum_{k=1}^{n-i} y^T A_{\cdot k}\bar{x}_k = y^T A^{(n-i)}\bar{x} \leq y^T b.$$

Hence, $\bar{x} \in P^{(i)}$.

For the converse direction, we apply induction. Let $i = 1$. We have

$$C^{(1)} = \Big\{y \in R^m_+ \mid y^T A_{\cdot n} = 0\Big\} \text{ and } P^{(1)} = \Big\{\bar{x} \in R^{n-1} \mid y^T A^{(n-1)}\bar{x} \leq y^T b \text{ for all } y \in C^{(1)}\Big\}.$$

Our task is to show that $P^{(1)} \subseteq \text{proj}_{S_{n-1}}(P)$. This follows from Theorem 5.6.3. To see this, let e_i be the i-th. unit vector in R^m. Take as y the unit vector e_k for $k \in M_0$. Then $e_k \in C^{(1)}$. Moreover, pick two indices $l \in M_-$ and $i \in M_+$. Then

$$-\frac{1}{a_{ln}}e_l + \frac{1}{a_{in}}e_i \in C^{(1)}.$$

This gives precisely the description of Q in Theorem 3.

This argument can be adapted to show the inductive step. The details are left as an exercise. □

Challenge 19. Prove that $P^{(i)} \subseteq \text{proj}_{S_{n-i}}(P)$.

We are now in the position to prove the famous Farkas Lemma.

Theorem 5.6.7 (The Farkas Lemma)**.** *Let $A \in \mathrm{Q}^{m \times n}$, $b \in \mathrm{Q}^m$. Either there exists a vector $x \in \mathrm{R}^n$ such that $Ax \leq b$ or there exists a vector $y \in \mathrm{R}^m$ such that $y \geq 0, y^T A = 0$ and $y^T b < 0$.*

Proof. We refer to the notation introduced in Definition 5.6.5.

$$C^{(n)} = \{y \in \mathrm{R}^m_+ \mid y^T A_{\cdot j} = 0 \text{ for all } j = 1, \ldots, n\} = \{y \geq 0 \mid y^T A = 0\}.$$

$P^{(n)} = \{0 \leq y^T b \text{ for all } y \in C^{(n)}\}$. We conclude with Proposition 5.6.2 that

$$P \neq \emptyset \iff P^{(1)} \neq \emptyset \iff \ldots \iff P^{(n)} \neq \emptyset \iff \text{for all } y \geq 0 \text{ with } y^T A = 0 \text{ we have } y^T b \geq 0.$$

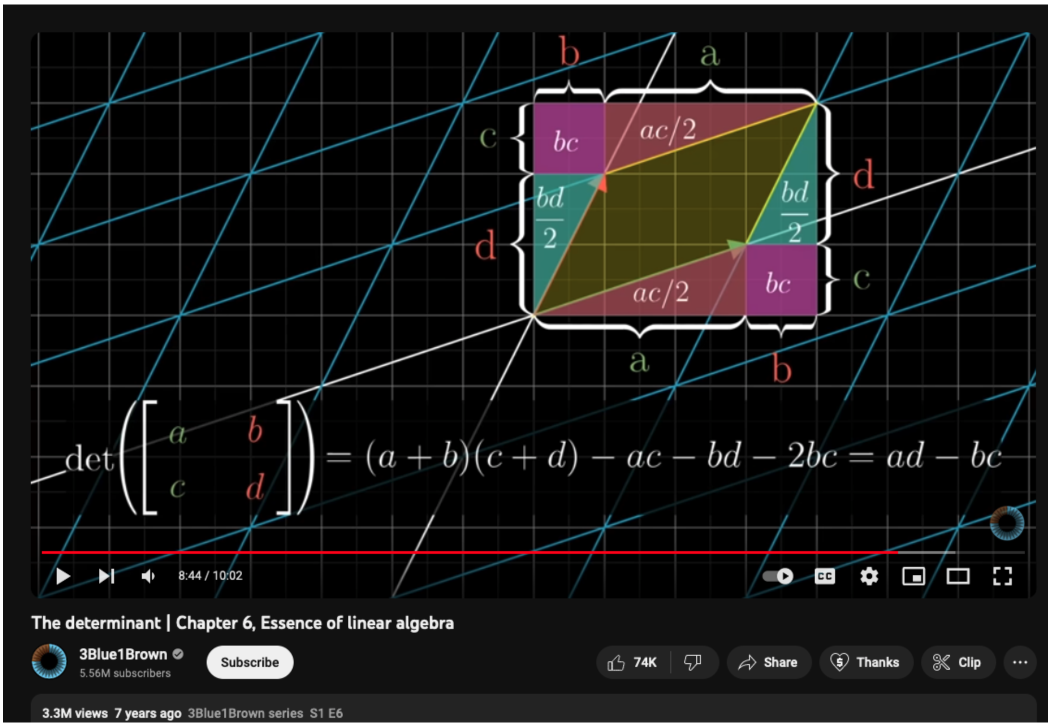
This leads to the following conclusion. Either $P \neq \emptyset$ or $P = \emptyset$. This is equivalent to saying: either there exists a vector $x \in \mathrm{R}^n$ such that $Ax \leq b$ or there exists a vector $y \in \mathrm{R}^m$ such that $y \geq 0$, $y^T A = 0$ and $y^T b < 0$. □

The power of Theorem 5.6.7 is that it allows us to give a nice certificate of when a polyhedron is empty. Indeed, if $P \neq \emptyset$, then we can simply find a point in P that is feasible and convince ourselves that $P \neq \emptyset$. However, when $P = \emptyset$, then it is not clear how to convince someone that this is indeed the case. In the CS lenz we will see several important applications of Theorem 5.6.7.

6. The determinant

We will now introduce the notion of determinant $\det(A)$ of a square matrix A. While this has a somewhat involved definition for $n \times n$ matrices, it is useful to first discuss what the determinant geometrically corresponds to, and to focus on small matrices.

In a nutshell, **the determinant of a matrix is a number that corresponds to how much the associated linear transformation inflates space, it corresponds precisely to the volume (or area, in $\mathbb{R}^2$) of the image of the unit cube (the red square in the pictures above in $\mathbb{R}^2$); with a negative sign when the orientation changes (in the pictures above in $\mathbb{R}^2$, when the order of the colored dots, on the red square, changed).** If we think about the determinant this way, then many of the properties we will list below can be intuitively understood (while it is hard to do so from the formula for the $n \times n$ determinant). For this reason, this section will be somewhat less proof-based, and rather focus on the most relevant properties of the determinant.



b
a
c
bc
ac/2
bd/2
d
bd/2
ac/2
bc
c
a
b
det([a b; c d]) = (a + b)(c + d) − ac − bd − 2bc = ad − bc
8:44 / 10:02
The determinant | Chapter 6, Essence of linear algebra
3Blue1Brown
5.56M subscribers
Subscribe
74K
Share
Thanks
Clip
3.3M views 7 years ago 3Blue1Brown series S1 E6

FIGURE 3. Calculation in 3Blue1Brown's video (see Remark 6.0.1) computing the determinant of a 2×2 matrix as the area of the image of the unit square after a linear transformation (that does not change orientation).

Remark 6.0.1. *Grant Sanderson has a website* `https://www.3blue1brown.com/` *and Youtube channel* `https://www.youtube.com/3blue1brown` *with excellent animation-heavy explanations of topics in Mathematics, including Linear Algebra. I particularly recommend the video on Determinants, it has also 3 dimensional visualizations that are harder to do on a static medium. You can find it here* `https://youtu.be/Ip3X9LOh2dk` *or here* `https://www.3blue1brown.com/lessons/determinant`*. See also Figure 3.*

A calculation of the area of the image of the unit square by left-multiplication by a 2×2 matrix shows (see Figure 3) that

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} := \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc.$$

Before we actually formally define the determinant for general $n \times n$ matrices we will first focus on the special case of 2×2- matrices to derive several important properties of the determinant.

6.0.1. *The 2×2 - case.*

Let us first understand how the determinant changes when we multiply matrices. To this end, let

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \text{ and } W = \begin{bmatrix} x & z \\ y & w \end{bmatrix}.$$

Next we multiply these two matrices and obtain an explicit representation of the coefficients

$$AW = \begin{bmatrix} ax+cy & az+cw \\ bx+dy & bz+dw \end{bmatrix}.$$

Using this representation we obtain the following result.

Lemma 6.0.2. *Let* $A, W \in \mathrm{R}^{2\times 2}$*. Then* $\det(AW) = \det(A)\det(W)$.

Proof.

$$\begin{aligned} det(AW) &= (ax+cy)(bz+dw) - (az+cw)(bx+dy) \\ &= axbz + axdw + cybz + cydw - azbx - azdy - cwbx - cwdy \\ &= axdw + cybz - azdy - cwbx \\ &= ad(xw - zy) + cb(zy - xw) = \det(A)\det(W). \end{aligned}$$

□

This computation allows us to derive a characterization of when a 2 × 2-matrix is invertible.

Lemma 6.0.3. *A matrix* $A \in \mathrm{R}^{2\times 2}$ *is invertible if and only if* $\det(A) \neq 0$.

Proof. Let

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

If A is invertible, then A^{-1} exists and hence, $AA^{-1} = I$ implies together with the previous lemma that $\det(A)\det(A^{-1}) = 1$. Hence, $\det(A) \neq 0$.

Conversely, if $\det(A) \neq 0$, then $a \neq 0$ or $b \neq 0$. Without loss of generality we can assume that $a \neq 0$. Consider now the system of linear equations $AW = I$.

$$\begin{aligned} ax + cy = 1 \quad &\text{implies that} \quad x = \tfrac{1-cy}{a} \\ az + cw = 0 \quad &\text{implies that} \quad z = \tfrac{-cw}{a}. \end{aligned}$$

By substituting these expressions into the other two equations $bx+dy=0$ and $bz+dw=1$ we obtain

$$\frac{b}{a}-\frac{cyb}{a}+dy=0 \iff b+y(ad-bc)=0 \iff y=\frac{-b}{\det(A)}.$$

$$\frac{-bcw}{a}+dw=1 \iff -bcw+adw=a \iff w=\frac{a}{\det(A)}.$$

This then gives us a formula for the parameters z and x in form of

$$z=\frac{-c}{\det(A)} \text{ and } x=\frac{1+\frac{cd}{\det(A)}}{a}=\frac{d}{\det(A)}.$$

These calculations show that A^{-1} exists whenever $\det(A)\neq 0$. □

Notice that our calculations give us an explicit formula for the inverse of matrix A and its determinant:

$$A^{-1}=\frac{1}{\det(A)}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}. \tag{12}$$

6.0.2. *The $n\times n$ - case.*

It turns out that what we have verified in dimension two carries over to general dimensions. It is, however much more involved to verify it algebraically.

We now give the definition of a determinant for $n\times n$ matrices. This requires us to discuss permutations.

Definition 6.0.4 (Sign of a permutation)**.** *Given a permutation $\sigma:\{1,\dots,n\}\to\{1,\dots,n\}$ of n elements, its sign $\operatorname{sgn}(\sigma)$ can be 1 or -1. The sign counts the parity of the number of pairs of elements that are out of order (sometimes called inversions) after applying the permutation. In other words,*

$$\operatorname{sgn}(\sigma)=\begin{cases} 1 & \textit{if} \quad |(i,j)\in\{1,\dots,n\}\times\{1,\dots,n\} \textit{ such that } i<j \textit{ and } \sigma(i)>\sigma(j)| \textit{ is even}, \\ -1 & \textit{if} \quad |(i,j)\in\{1,\dots,n\}\times\{1,\dots,n\} \textit{ such that } i<j \textit{ and } \sigma(i)>\sigma(j)| \textit{ is odd}. \end{cases}$$

Example 6.0.5. *Let $n=4$. Consider the permutation π defined as $\pi(1)=1$, $\pi(2)=3$, $\pi(3)=2$, $\pi(4)=4$. The pairs (i,j) such that $i<j$ are*

$$(1,2),(1,3),(1,4),(2,3),(2,4),(3,4).$$

For all these listed pairs (i,j) we have that $\pi(i)<\pi(j)$ except for the pair $(2,3)$. Hence, $\operatorname{sgn}(\pi)=-1$.

Exploratory Challenge 20. The sign of a permutation has many nice properties. Try to prove a couple of them:

(1) The sign of a permutation is multiplicative, i.e.: for two permutations σ, γ we have that $\text{sgn}(\sigma \circ \gamma) = \text{sgn}(\sigma)\text{sgn}(\gamma)$.

(2) For all $n \geq 2$, exactly half of the permutations have sign 1 and exactly half have sign -1.

The identity has a sign of 1, the sign of a transposition (a permutation that only swaps two elements) is -1 and for two permutations σ, γ we have that $\text{sgn}(\sigma \circ \gamma) = \text{sgn}(\sigma)\text{sgn}(\gamma)$.

We are now in position to introduce the general notion of a determinant of a square matrix.

Definition 6.0.6. *Given a square matrix $A \in \mathbb{R}^{n\times n}$ the determinant* $\det(A)$ *is defined as*

$$\det(A) = \sum_{\sigma\in\Pi_n} \text{sgn}(\sigma)\prod_{i=1}^{n} A_{i,\sigma(i)},$$

where Π_n is the set of all permutations of n elements.

If A is a 1×1 matrix, since there is only one permutation of 1 element (the permutation $\sigma(1) = 1$, which has sign 1). It follows that $\det(A) = A$.

For 2×2 matrices we observe that here are two permutations. Let us call σ_1 the identity permutation (that doesn't move any element, which has sign 1) and σ_2 the permutation that swaps the two elements (which has sign -1). Hence, for a 2×2 matrix A with entries A_{ij} we have

$$\det(A) = \sum_{\sigma\in\Pi_2} \text{sgn}(\sigma)\prod_{i=1}^{2} A_{i,\sigma(i)} = (+1)\prod_{i=1}^{2} A_{i,\sigma_1(i)} + (-1)\prod_{i=1}^{2} A_{i,\sigma_2(i)} = A_{11}A_{22} - A_{12}A_{21}.$$

This corresponds precisely to.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Definition 6.0.6 allows us to derive a few results.

Proposition 6.0.7. *Given a permutation matrix $P \in \mathbb{R}^{n\times n}$ corresponding to a permutation σ, then* $\det(P) = \text{sgn}(\sigma)$. *We sometimes also write* $\text{sgn}(P)$.

Proposition 6.0.8. *Given a triangular (either upper- or lower-) matrix $T \in \mathbb{R}^{n\times n}$ we have*

$$\det(T) = \prod_{k=1}^{n} T_{kk},$$

in particular, $\det(I) = 1$.

Theorem 6.0.9. *Given a matrix* $A \in \mathbb{R}^{n\times n}$ *we have*

$$\det(A^\top) = \det(A).$$

Proof. For a permutation σ let σ^{-1} denote the inverse permutation, i.e.,

$$\sigma(i) = j \iff \sigma^{-1}(j) = i \text{ for all } i, j.$$

From Challenge 20 it follows that $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$. The conclusion $\det(A^\top) = \det(A)$ follows from observing

$$\sum_{\sigma\in\Pi_n} \operatorname{sgn}(\sigma)\prod_{i=1}^{n} A_{i,\sigma(i)} = \sum_{\sigma^{-1}\in\Pi_n} \operatorname{sgn}(\sigma^{-1})\prod_{i=1}^{n} A_{\sigma^{-1}(i),i} = \sum_{\sigma\in\Pi_n} \operatorname{sgn}(\sigma)\prod_{i=1}^{n} A_{\sigma(i),i}.$$

□

The following is a consequence of the propositions above.

Proposition 6.0.10. *If* $Q \in \mathbb{R}^{n\times n}$ *is an orthogonal matrix then*

$$\det(Q) = 1 \quad \textit{or} \quad \det(Q) = -1.$$

Proof. By Propositions 6.0.8 and 6.0.12 we have $1 = \det(I) = \det(Q^\top Q) = \det(Q^\top)\det(Q)$. by Proposition 6.0.9 we have $1 = \det(Q)^2$ and so $\det(Q)$ is 1 or -1. □

Proposition 6.0.11. *A matrix* $A \in \mathbb{R}^{n\times n}$ *is invertible if and only if*

$$\det(A) \neq 0.$$

We can also multiply matrices as we did in the 2 dimensional case and see the effect on their determinants.

Proposition 6.0.12. *Given matrices $A, B \in \mathbb{R}^{n\times n}$ we have*

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

Following the same line of argument we also have

Proposition 6.0.13. *Given a matrix $A \in \mathbb{R}^{n\times n}$ such that $\det(A) \neq 0$, then A is invertible and*

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Example 6.0.14. *For 3×3 matrices there are $3! = 6$ permutations, so there will be 6 terms. For A a 3×3 matrix, we can write its determinant as (where an empty entry corresponds to a zero entry)*

$$\begin{aligned}
\det(A) &= \begin{vmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{vmatrix} \\
&= \begin{vmatrix} A_{11} & & \\ & A_{22} & \\ & & A_{33} \end{vmatrix} + \begin{vmatrix} & A_{12} & \\ A_{21} & & \\ & & A_{33} \end{vmatrix} + \begin{vmatrix} & A_{12} & \\ & & A_{23} \\ A_{31} & & \end{vmatrix} \\
&\quad + \begin{vmatrix} & & A_{13} \\ & A_{22} & \\ A_{31} & & \end{vmatrix} + \begin{vmatrix} & & A_{13} \\ A_{21} & & \\ & A_{32} & \end{vmatrix} + \begin{vmatrix} A_{11} & & \\ & & A_{23} \\ & A_{32} & \end{vmatrix} \\
&= A_{11}A_{22}A_{33} - A_{12}A_{21}A_{33} + A_{12}A_{23}A_{31} - A_{13}A_{22}A_{31} + A_{13}A_{21}A_{32} - A_{11}A_{23}A_{32}.
\end{aligned}$$

There is another convenient way of writing this determinant

$$\begin{vmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{vmatrix} = A_{11}\begin{vmatrix} A_{22} & A_{23} \\ A_{32} & A_{33} \end{vmatrix} - A_{12}\begin{vmatrix} A_{21} & A_{23} \\ A_{31} & A_{33} \end{vmatrix} + A_{13}\begin{vmatrix} A_{21} & A_{22} \\ A_{31} & A_{32} \end{vmatrix}. \tag{13}$$

In general, these terms are called the co-factors of A.

Definition 6.0.15. *Given $A \in \mathbb{R}^{n\times n}$, for each $1 \leq i, j \leq n$ let $\mathscr{A}_{ij}$ denote the $(n-1)\times(n-1)$ matrix obtained by removing row i and column j from A. Then we define the co-factors of A as*

$$C_{ij} = (-1)^{i+j}\det(\mathscr{A}_{ij}).$$

Just as in (13), the determinant can be written in terms of the co-factors.

Proposition 6.0.16. *Let $A \in \mathbb{R}^{n\times n}$, for any $1 \leq i \leq n$,*

$$\det(A) = \sum_{j=1}^{n} A_{ij}C_{ij}.$$

The formula we derived above for the inverse of 2×2 matrices (Equation 12), also has an analogue in n dimensions.

Proposition 6.0.17. *Given $A \in \mathbb{R}^{n\times n}$ with $\det(A) \neq 0$ we have*

$$A^{-1} = \frac{1}{\det(A)} C^{\top},$$

where C is the $n \times n$ matrix with the co-factors of A as entries.

The formula in Proposition 6.0.17 can be rewritten as

$$AC^{\top} = \det(A)I.$$

Remark 6.0.18. *Computationally speaking, this is not a good way to compute the inverse, as it involves computing many determinants.*

Challenge 21. Verify that Proposition 6.0.17 indeed corresponds to the formula we derived for A^{-1} when $n = 2$.

Exploratory Challenge 22. Try to prove Proposition 6.0.17 by showing that $AC^{\top} = \det(A)I$. Perhaps start with $n = 3$. You can also use Cramer's Rule (below) to prove this.

6.0.3. *Cramer's Rule.*

The determinant also allows us to write a formula for the solution of the linear system of the type $Ax = b$ when $A \in \mathbb{R}^{n\times n}$ and $\det(A) \neq 0$. The idea is simple, we will illustrate it here for $n = 3$.

If $\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$, then we have

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \begin{bmatrix} x_1 & 0 & 0 \\ x_2 & 1 & 0 \\ x_3 & 0 & 1 \end{bmatrix} = \begin{bmatrix} b_1 & A_{12} & A_{13} \\ b_2 & A_{22} & A_{23} \\ b_3 & A_{32} & A_{33} \end{bmatrix}.$$

Since the determinant is multiplicative, and the determinant of the second matrix in the expression is x_1, we have

$$\det(A)x_1 = \det(\mathscr{B}_1),$$

where $\mathscr{B}_1$ is the matrix obtained by A by replacing the first column of A with the vector b.

Since we can do this for any of the columns, we have $x_j = \det(\mathscr{B}_j)/\det(A)$. In general

Proposition 6.0.19 (Cramer's Rule). *Let $A \in \mathbb{R}^{n\times n}$ such that $\det(A) \neq 0$ and $b \in \mathbb{R}^n$ then the solution $x \in \mathbb{R}^n$ of $Ax = b$ is given by*

$$x_j = \frac{\det(\mathscr{B}_j)}{\det(A)},$$

where $\mathscr{B}_j$ is the matrix obtained by A by replacing the j-th column of A with the vector b.

Remark 6.0.20. *As with the formula for the inverse: computationally speaking, this is not a good way to solve linear systems, as it involves computing many determinants.*

6.0.4. Several further comments on the determinant.

The definition we used for the determinant of a square matrix involves a formula with $n!$ terms. This formula is computational infeasible for even moderate levels of n (it is faster than exponential! For example, 100! has almost 160 digits!). In practice, the determinant of a matrix A is computed by Gaussian Elimination and the matrix decomposition $PA = LU$ (P permutation and so $\det(P) = \text{sgn}(P)$, U is upper triangular and L is lower triangular with only 1s in the diagonal, and so $\det(L) = 1$) . This gives us the formula

$$\det(A) = \frac{1}{\det(P)}\det(L)\det(U) = \text{sgn}(P)\det(U), \tag{14}$$

and since U is a triangular matrix its determinants can be easily computed by Proposition 6.0.8.

Alternatively, one can also think of Gaussian Elimination as directly computing the determinant via the following two propositions

Proposition 6.0.21. *If A is an $n \times n$ matrix and P is a permutation that swaps two elements, meaning that PA corresponds to swapping two rows of A then* $\det(PA) = -\det(A)$.

Proposition 6.0.22. *The determinant is linear in each row (or each column). In other words, for any $a_0, a_1, a_2 \ldots, a_n \in \mathbb{R}^n$ and $\alpha_0, \alpha_1 \in \mathbb{R}$ we have*

$$\begin{vmatrix} - & \alpha_0 a_0^\top + \alpha_1 a_1^\top & - \\ - & a_2^\top & - \\ & \vdots & \\ - & a_n^\top & - \end{vmatrix} = \alpha_0 \begin{vmatrix} - & a_0^\top & - \\ - & a_2^\top & - \\ & \vdots & \\ - & a_n^\top & - \end{vmatrix} + \alpha_1 \begin{vmatrix} - & a_1^\top & - \\ - & a_2^\top & - \\ & \vdots & \\ - & a_n^\top & - \end{vmatrix},$$

and

$$\begin{vmatrix} | & | & & | \\ \alpha_0 a_0 + \alpha_1 a_1 & a_2 & \cdots & a_n \\ | & | & & | \end{vmatrix} = \alpha_0 \begin{vmatrix} | & | & & | \\ a_0 & a_2 & \cdots & a_n \\ | & | & & | \end{vmatrix} + \alpha_1 \begin{vmatrix} | & | & & | \\ a_1 & a_2 & \cdots & a_n \\ | & | & & | \end{vmatrix}.$$

Exploratory Challenge 23. The more mathematical way of presenting this material is to define a determinant as a function that goes from $n \times n$ matrices to $\mathbb{R}$ with the following properties:

(1) it is linear in each column,
(2) $\det(I) = 1$ and
(3) $\det(A) = 0$ whenever A has two identical columns.

It is then possible to prove that the only function satisfying these three properties is the determinant as we defined it.

7. Eigenvalues and Eigenvectors

We are (almost) ready for one of the most important concepts (if not the most important one) in Linear Algebra, **eigenvalues and eigenvectors**. In a sense, *it has all been building up to this!*

Guiding Strategy 24. Given a square matrix A, as we will see below, an eigenvalue λ and eigenvector v will be, respectively, a scalar and a non-zero vector satisfying $Av = \lambda v$. This means that $(A - \lambda I)v = 0$ and so $(A - \lambda I)$ is not invertible, or equivalently $\det(A - \lambda I) = 0$. We can look for eigenvalues as solutions of $\det(A - \lambda I) = 0$ which is a polynomial[8] in λ but unfortunately, not

[8] This is one of the main reasons we had to cover determinants.

all polynomials have real zeros.[9] For example if $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $\det(A - \lambda I) = 0$ corresponds to $\lambda^2 + 1 = 0$ which only has solutions in $\mathbb{C}$, the Complex Numbers. For this reason we will start this Chapter with a brief introduction to Complex Numbers. It all starts with asking for a number λ such that $\lambda^2 + 1 = 0$.

Further Reading 25. Complex Analysis is a beautiful topic in Mathematics, what we will cover here is just a tiny peak at it, there is a all bookshelf of excellent books in this topic in our library. I have personally taught a course at ETH on Complex Analysis, and since it was during the COVID pandemic I made videos available online, which are still available at `https://www.youtube.com/playlist?list=PLiud-28tsatLRRGqO_Eg_x0S4LVyxuV5p` (In particular, the first lecture covers roughly the content here).

7.0. **Complex Numbers.** If we start with the natural numbers $\mathbb{N}$ and want to solve equations like $x + 10 = 1$, we need negative numbers. This motivates considering the integers $\mathbb{Z}$. Similarly, rational numbers $\mathbb{Q}$ are needed to solve equations like $10x = 1$ and real numbers $\mathbb{R}$ are needed to solve $x^2 = 2$.[10] Similarly, the Complex Numbers are needed to solve equations such as $x^2 + 1 = 0$. It starts with the introduction of an imaginary number $i \in \mathbb{C}$ such that $i^2 = -1$. You can think of i as $\sqrt{-1}$.

The complex numbers are numbers of the form $z = a + ib$ for $a \in \mathbb{R}$ and $b \in \mathbb{R}$. $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$. Keeping in mind that $i^2 = -1$ we can do operations with complex numbers:

- $(a+ib) + (x+iy) = (a+x) + i(b+y)$,
- $(a+ib)(x+iy) = ax + i(ay+bx) + i^2 by = ax + i(ay+bx) - by = (ax-by) + i(ay+bx)$,
- $(a+ib)(a-ib) = a^2 + b^2$,
- $\frac{a+ib}{x+iy} = \frac{(x-iy)(a+ib)}{(x-iy)(x+iy)} = \frac{(ax+by)+i(bx-ay)}{x^2+y^2} = \left(\frac{ax+by}{x^2+y^2}\right) + i\left(\frac{bx-ay}{x^2+y^2}\right)$.

Given $z \in \mathbb{C}$ with $z = a + ib$ we have the following notation

$$\Re(a+ib) := a \quad \text{called the real part of } z = a+ib, \tag{15}$$

$$\Im(a+ib) := b \quad \text{called the imaginary part of } z = a+ib, \tag{16}$$

$$|z| := \sqrt{a^2+b^2} \quad \text{called the modulus of } z = a+ib, \tag{17}$$

$$\overline{a+ib} := a - ib \quad \text{called the complex conjugate of } z = a+ib. \tag{18}$$

[9] A zero of a polynomial P is a point x such that $P(x) = 0$, this is also called a root of the polynomial. In German, it's a "Nullstelle". In fact, a (rather deep) multidimensional version of Theorem 7.0.3, and one of the most important facts in Algebraic Geometry, is called "Hilbert's Nullstellensatz".

[10] If you have never seen the proof that there exists no $x \in \mathbb{Q}$ such that $x^2 = 2$ I highly recommend trying to do it: set $x = a/b$ for $a, b \in \mathbb{Z}$ and try to count how many times 2 divides both a and b and find a contradiction.

Note that for $z_1, z_2 \in \mathbb{C}$, we have $|z|^2 = z\bar{z}$, $z_1 z_2 = z_2 z_1$, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, and $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$.

Fact 7.0.1 (Euler's Formula)**.** *Given $\theta \in \mathbb{R}$, we have*

$$e^{i\theta} = \cos\theta + i\sin\theta. \tag{19}$$

This means, in particular, that $e^{i\pi} = -1$. This is usually written as $e^{i\pi} + 1 = 0$.

Further Reading 26. In order to prove Euler's Formula, we need to first define what we mean by $e^{i\theta}$, this can be done, for example, by the Taylor series of the exponential, but this is outside the scope of this course (see Further Reading 25).

Fact 7.0.2 (Polar Coordinates)**.** *A complex number $z \in \mathbb{C}$ can be written as*

$$z = re^{i\theta}, \tag{20}$$

where $r \geq 0$ is the modulus of z and $\theta \in \mathbb{R}$ (we can restrict to $\theta \in [0, 2\pi[$) is an angle, also called the argument of z.

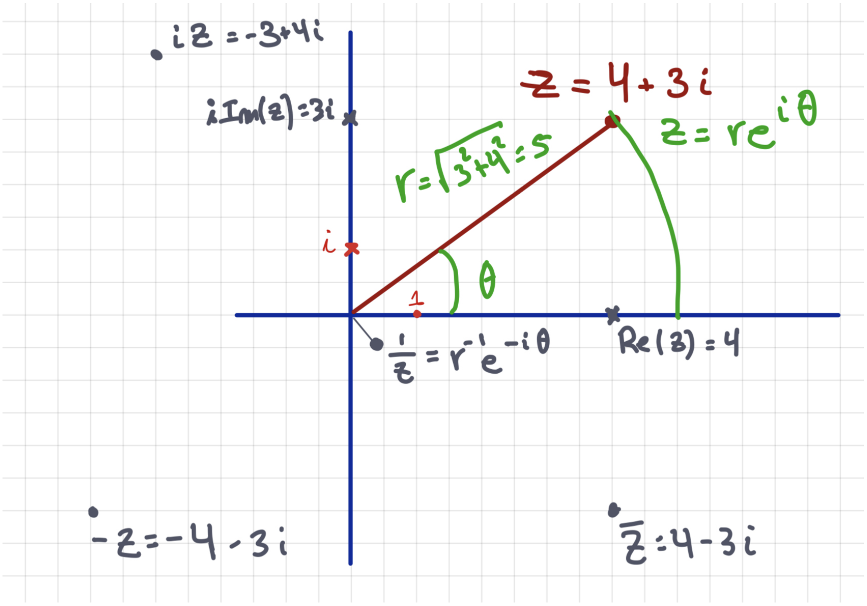


FIGURE 4. A complex number $z = 4 + 3i$ in the Complex plane.

The most important property of Complex Numbers, and what makes them a very natural mathematical object, is that any univariate polynomial equation with complex number coefficients has a (complex) solution, in a certain sense we don't need to extend numbers further, $\mathbb{C}$ is **Algebraically closed**.

Theorem 7.0.3 (Fundamental Theorem of Algebra)**.** *Any degree n non-constant ($n \geq 1$) polynomial $P(z) = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \cdots + \alpha_1 z + \alpha_0$ (with $\alpha_n \neq 0$) has a zero: $\lambda \in \mathbb{C}$ such that $P(\lambda) = 0$.*

Further Reading 27. As the name suggests, Theorem 7.0.3 is a central result in Complex Analysis. Proving it is outside the scope of this course.[11] Complex analysis (which leads to the proof of this theorem) is a beautiful example of interaction between analysis, algebra, and geometry. In a nutshell the idea for the classical proof is that differentiable functions in the complex plane $f : \mathbb{C} \to \mathbb{C}$ are very special and, in a sense, need to behave like polynomials (this is a deep statement that needs a significant amount of background to properly state and prove). If a polynomial $P(z)$ doesn't have a zero then $1/P(z)$ is a differentiable function that cannot behave like a non-constant polynomial because it does not grow sufficiently far away from zero, and so it must be a constant function which means that $P(z)$ had to be constant, so any non-constant polynomial has a zero. For more on Complex Analysis see Further Reading 25.

Further Remark 28. Once we have λ a zero of $P(z)$, we can divide $P(z)$ by $(z - \lambda)$ to get $P(z) = (z - \lambda) P_1(z)$, then use a zero of P_1 to reiterate, and so on. This argument (carried out carefully) gives the following corollary.

Corollary 7.0.4. *Any degree n non-constant ($n \geq 1$) polynomial $P(z) = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \cdots + \alpha_1 z + \alpha_0$ (with $\alpha_n \neq 0$) has n zeros: $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$, perhaps with repetitions, such that*

$$P(z) = \alpha_n (z - \lambda_1)(z - \lambda_2) \cdots (z - \lambda_n). \tag{21}$$

The number of times $\lambda \in \mathbb{C}$ appears in this expansion is called the algebraic multiplicity *of the zero.*

7.0.1. *Complex-valued Matrices and Vectors.*

Analogously to $\mathbb{R}^n$ we also define $\mathbb{C}^n$ as the set of n-dimentional complex valued vectors. We can have complex valued vectors $v \in \mathbb{C}^n$ and matrices $A \in \mathbb{C}^{m \times n}$. The natural operation of "transposing" for complex vectors and matrices is that of "conjugate transpose" or "hermitian transpose" denoted by A^*, or sometimes A^H,

$$A^* = \overline{A}^T. \tag{22}$$

[11] But you can see Appendix B for a relatively elementary proof.

Given $v \in \mathbb{C}^n$ we have

$$\|v\|^2 = v^* v = \overline{v}^T v = \sum_{i=1}^{n} \overline{v_i} v_i = \sum_{i=1}^{n} |v_i|^2.$$

The inner-product (or dot-product) in $\mathbb{C}^n$ is given by $\langle v, w \rangle = w^* v$.

Similarly to the situation in $\mathbb{R}^n$, we say $v_1, \dots, v_k \in \mathbb{C}^n$ are linearly independent if there is no (complex valued) non-zero linear combination giving zero, meaning that if $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$ for $\alpha_1, \dots, \alpha_k \in \mathbb{C}$ we must have $\alpha_1 = \cdots = \alpha_k = 0$. Also, the span of $v_1, \dots, v_k \in \mathbb{C}^n$ is the set of possible linear combinations $\alpha_1 v_1 + \cdots + \alpha_k v_k$ for $\alpha_1, \dots, \alpha_k \in \mathbb{C}$. If $v_1, \dots, v_k$ is a spanning set of a subspace and linearly independent we say it is a basis of that subspace. As with $\mathbb{R}^n$ if we have $v_1, \dots, v_n \in \mathbb{C}^n$ that are either a spanning set of $\mathbb{C}^n$ or linearly independent then they must actually be both (and so are a basis).

Further Reading 29. With these definitions you can already understand the Discrete Fourier Transform (which is the linear transformation corresponding to the DFT matrix, one of the most important complex valued matrices). This is the key object behind signal processing, you can read more about it on the lecture notes of another course I usually teach [BM23]. You can also see a discussion of Fourier Transform, circulant matrices, and signal convolutions in [Str23] (end of Section 6.4).

7.1. **Introduction to Eigenvalues and Eigenvectors.** Even though the theory can be analogously developed for complex valued matrices, we will focus on real valued matrices.

Guiding Example 30. We will use a guiding example to illustrate both some of the power, and some of the properties, of eigenvalues and eigenvectors. In Guiding Example numbers 30 through 36 we will derive a formula for the n-th Ficonacci Number. The Fibonacci numbers are defined by the recurrence:

$$F_0 = 0,\ F_1 = 1, \text{ and, for } n \geq 2,\ F_n = F_{n-1} + F_{n-2}. \tag{23}$$

The recurrence can be rewritten in linear algebraic notation as, for $n \geq 2$,

$$\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix}. \tag{24}$$

Defining

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } g_n = \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}, \tag{25}$$

the recurrence can be rewritten as

$$g_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } g_n = M g_{n-1},$$

meaning that

$$g_n = M^n g_0. \tag{26}$$

Definition 7.1.1. *Given $A \in \mathbb{R}^{n\times n}$, we say $\lambda \in \mathbb{C}$ is an eigenvalue of A and $v \in \mathbb{C}^n \setminus \{0\}$ is an eigenvector of A, associated with with the eigenvalue λ, when the following holds:*

$$Av = \lambda v.$$

We call them an eigenvalue-eigenvector pair. If $\lambda \in \mathbb{R}$ then we will call λ a real eigenvalue, and the associated eigenvalue-eigenvector pair a real eigenvalue-eigenvector pair.

Guiding Example 31. Let us try to find eigenvalues (and later the eigenvectors) of $M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. We are looking for $v \in \mathbb{R}^2 \setminus \{0\}$ and $\lambda \in \mathbb{R}$ such that $Mv = \lambda v$, but this can be rewritten as $(M - \lambda I)v = 0$ and since $v \neq 0$ it means that $M - \lambda I$ is non-invertible (also called singular).[12] This is equivalent to $\det(M - \lambda I) = 0$ and so we can find the eigenvalues λ with this equation:

$$0 = \det(M - \lambda I) = \begin{vmatrix} 1-\lambda & 1 \\ 1 & 0-\lambda \end{vmatrix} = (1-\lambda)(0-\lambda) - 1 = \lambda^2 - \lambda - 1. \tag{27}$$

By the quadratic formula,[13] the solutions to (27) are given by

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \text{ and } \lambda_2 = \frac{1-\sqrt{5}}{2}. \tag{28}$$

Further Reading 32 (Golden Ratio)**.** The number $\varphi = \frac{1+\sqrt{5}}{2}$ is the celebrated Golden Ratio; believed, since the ancient Greeks, to be the ideal aspect ratio for a rectangle.

> *"Some of the greatest mathematical minds of all ages, from Pythagoras and Euclid in ancient Greece, through the medieval Italian mathematician Leonardo of Pisa and the Renaissance astronomer Johannes Kepler, to present-day scientific figures such as Oxford physicist Roger Penrose, have spent endless hours over this simple ratio and its properties. [...] Biologists, artists, musicians, historians, architects, psychologists, and even mystics have pondered and debated the basis of its ubiquity and appeal. In fact, it is probably fair to say that the Golden Ratio has inspired thinkers of all disciplines like no other number in the history of mathematics."*
>
> — The Golden Ratio: The Story of Phi, the World's Most Astonishing Number

[12] Normally, we would have to look for $\lambda \in \mathbb{C}$ and $v \in \mathbb{C}^n$ but in this case the eigenvalues, as we will see, are real.

[13] Recall that the quadratic formula says that the zeros of $ax^2 + b + c$ are given by $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

The following is the original definition which dates back to Euclid around 2300 years ago (they called the number “extreme and mean ratio” back then)

> *“A straight line is said to have been cut in extreme and mean ratio when, as the whole line is to the greater segment, so is the greater to the lesser”*

Guiding Example 33. Now we can try to find the eigenvectors v_1 and v_2 such that $Av_1 = \lambda_1 v_1$ and $Av_2 = \lambda_2 v_2$.

Let us start with v_1. We are looking for a non-zero element of $\mathrm{N}\left(A - \frac{1+\sqrt{5}}{2} I\right)$. In other words

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 - \frac{1+\sqrt{5}}{2} & 1 \\ 1 & -\frac{1+\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} (v_1)_1 \\ (v_1)_2 \end{bmatrix}.$$

This is an under-determined system and we are looking for a non-zero solution, so let us start by setting $(v_1)_2 = 1$. The second equation gives us $(v_1)_1 = \frac{1+\sqrt{5}}{2}$. Indeed $v_1 = \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix}$ is an eigenvector of M associated to the eigenvalue $\lambda_1 = \frac{1+\sqrt{5}}{2}$.

A similar calculation for $\lambda_2 = \frac{1-\sqrt{5}}{2}$ gives that $v_2 = \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix}$. Indeed

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix} = \frac{1+\sqrt{5}}{2} \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix} = \frac{1-\sqrt{5}}{2} \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix} \tag{29}$$

Challenge 34. Carry out the calculations in Guiding Example 33 and confirm that we have indeed found two eigenvectors (check the two equalities in (29)).

Further Remark 35. The v_1 and v_2 we constructed in 33 are not the only possible choices, for example any non-zero scalar multiples of these would have also been a possible choice. Normally one picks a unit-norm representative, but in this case we picked vectors that make the calculations the cleanest.

What we carried out in the example above is very general and we now develop the theory for general matrices.

Let λ and v be an eigenvalue-eigenvector pair of a matrix A. Since $v \neq 0$ and $(A - \lambda I)v = Av - \lambda v = 0$ we have that $\det(A - \lambda I) = 0$. Conversely, if $\det(A - \lambda I) = 0$ for some λ, then there exists $v \in \mathrm{N}(A - \lambda I) \setminus \{0\}$ and so λ is an eigenvalue. This gives a procedure to find eigenvalues and eigenvectors: (i) eigenvalues are the solution of $\det(A - \lambda I) = 0$, which is a polynomial equation, and (ii) an associated eigenvector is a non-zero element of $\mathrm{N}(A - \lambda I)$.

Let us first formulate this for real eigenvalues and eigenvectors.

Proposition 7.1.2. *Let $A \in \mathbb{R}^{n\times n}$. $\lambda \in \mathbb{R}$ is a (real) eigenvalue of A if and only if* $\det(A-\lambda I) = 0$*. A vector v is an eigenvector associated with the eigenvalue λ if (and only if) it is a non-zero element of* $\mathrm{N}(A-\lambda I)$.

A direct inspection of the formula for the determinant (Definition 6.0.6) gives the following.

Proposition 7.1.3. $\det(A-\lambda I)$ *is a polynomial, in λ, of degree n. The coefficient of the λ^n term is $(-1)^n$.*

The Fundamental Theorem of Algebra (Theorem 7.0.3) immediately implies

Theorem 7.1.4. *Every matrix $A \in \mathbb{R}^{n\times n}$ has an eigenvalue (perhaps complex-valued).*

Remark 7.1.5. *For now we will focus on real eigenvalues, and address complex valued ones later on. Essentially all the properties we will describe below also hold for complex valued eigenvalues (just by replacing $\mathbb{R}$ by $\mathbb{C}$ and doing the appropriate adjustments). For example, Proposition 7.1.2 also holds for complex-valued eigenvalues, one just needs to think of* $\mathrm{N}(A-\lambda I)$ *as a subspace of $\mathbb{C}^n$, meaning the vectors $v \in \mathbb{C}^n$ such that $(A-\lambda I)v = 0$.*

Guiding Example 36. Let us return to our guiding example. Notice that v_1 and v_2 are linearly independent, and so they are a basis for $\mathbb{R}^2$. We can write $g_0 = \alpha_1 v_1 + \alpha_2 v_2$.

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = g_0 = \alpha_1 v_1 + \alpha_2 v_2 = \begin{bmatrix} \alpha_1 \frac{1+\sqrt{5}}{2} + \alpha_2 \frac{1-\sqrt{5}}{2} \\ \alpha_1 + \alpha_2 \end{bmatrix} = \begin{bmatrix} (\alpha_1+\alpha_2)\frac{1}{2} + (\alpha_1-\alpha_2)\frac{\sqrt{5}}{2} \\ \alpha_1 + \alpha_2 \end{bmatrix},$$

and so $\alpha_1 = \frac{1}{\sqrt{5}}$ and $\alpha_2 = -\frac{1}{\sqrt{5}}$.

Recall that $g_n = A^n g_0$ and so

$$g_n = A^n \left(\frac{1}{\sqrt{5}} v_1 - \frac{1}{\sqrt{5}} v_2 \right) = \frac{1}{\sqrt{5}} A^n v_1 - \frac{1}{\sqrt{5}} A^n v_2 = \frac{1}{\sqrt{5}} \left(A^n v_1 - A^n v_2 \right).$$

Since $Av_1 = \lambda_1 v_1$ we have that $A^2 v_1 = A(\lambda_1 v_1) = \lambda_1^2 v_1$ and iterating this procedure[14] gives $A^n v_1 = \lambda_1^n v_1$. This means that

$$g_n = \frac{A^n v_1 - A^n v_2}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n v_1 - \left(\frac{1-\sqrt{5}}{2}\right)^n v_2}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n}{\sqrt{5}} \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix} - \frac{\left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix}.$$

Since F_n is the second coordinate of g_n, we derived a closed formula for the n-th terms of the Fibonacci sequence:

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{30}$$

An important property that allowed us to do the calculation above was that applying a power of a matrix to an eigenvector was a simple operation, this is the next proposition.

Proposition 7.1.6. *If λ and v are an eigenvalue-eigenvector pair of a matrix A, then, for $k \geq 1$, λ^k and v are an eigenvalue-eigenvector pair of the matrix A^k.*

Proof. Proof by Induction: The base case $k = 1$ is trivial. For the induction step, since λ^k and v are an eigenvalue-eigenvector pair then $A^k v = A\left(A^{k-1} v\right) = A\left(\lambda^{k-1} v\right) = \lambda^k v$. □

Proposition 7.1.7. *Let A be an invertible matrix. If λ and v are an eigenvalue-eigenvector pair of the matrix A, then, $\frac{1}{\lambda}$ and v are an eigenvalue-eigenvector pair of the matrix A^{-1}.*

Proof. A is invertible and hence, in the statement $\lambda \neq 0$. Since $Av = \lambda v$ we have $A^{-1}(\lambda v) = v$ and so $\lambda A^{-1} v = v$, which (since $\lambda \neq 0$) is equivalent to $A^{-1} v = \frac{1}{\lambda} v$. □

Another important property was that we were able to write a vector as a linear combination of eigenvectors, which was possible because the eigenvectors were linearly independent.

Proposition 7.1.8. *Let $A \in R^{n \times n}$ and let $v_1, \ldots, v_k \in \mathbb{R}^n$ be eigenvectors corresponding to eigenvalues $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$. If $\lambda_1, \ldots, \lambda_k$ are all distinct, the eigenvectors $v_1, \ldots, v_k$ are linearly independent.*

[14] A formal proof would use induction

Proof. We will prove this by contradiction. Assume that $v_1,\dots,v_k$ are linearly dependent. For $i=1,\dots,k$, let d_i denote the dimension of the span of $v_1,\dots,v_i$. Since $v_1\neq 0$ we have $d_1=1$. By the hypothesis $d_k<k$. Let j be the smallest positive integer for which $d_j<j$. Note that, by construction, $d_{j-1}=d_j=j-1$, this means that $v_1,\dots,v_{j-1}$ are linearly independent but that v_j is in the span of $v_1,\dots,v_{j-1}$. We can then write

$$v_j=\alpha_1v_1+\cdots\alpha_{j-1}v_{j-1}. \tag{31}$$

If we multiply by A both sides we get

$$\lambda_jv_j=Av_j=A\left(\alpha_1v_1+\cdots\alpha_{j-1}v_{j-1}\right)=\alpha_1\lambda_1v_1+\cdots\lambda_{j-1}\alpha_{j-1}v_{j-1}.$$

Replacing the v_j in the left hand side with the right hand side of (31) we get

$$\lambda_j\left(\alpha_1v_1+\cdots\alpha_{j-1}v_{j-1}\right)=\alpha_1\lambda_1v_1+\cdots\lambda_{j-1}\alpha_{j-1}v_{j-1},$$

which we can rearrange as

$$\alpha_1\left(\lambda_j-\lambda_1\right)v_1+\alpha_2\left(\lambda_j-\lambda_2\right)v_2+\cdots+\alpha_{j-1}\left(\lambda_j-\lambda_{j-1}\right)v_{j-1}=0. \tag{32}$$

Since $\lambda_j-\lambda_i\neq 0$ for all $i\leq j-1$ and not all α_i's are zero, this is a non-zero linear combination of $v_1,\dots,v_{j-1}$ adding to zero, which would be a contradiction with $d_{j-1}=j-1$. □

A very important consequence of this is that if a matrix has n distinct real eigenvalues then the eigenvectors form a basis for $\mathbb{R}^n$.

Theorem 7.1.9. *Let $A\in\mathbb{R}^{n\times n}$ with n distinct real eigenvalues (meaning that the n zeros of* $\det(A-\lambda I)$*, as described in Corollary 7.0.4, are all distinct) then there is a basis of $\mathbb{R}^n$, $v_1,\dots,v_n$, made up of eigenvectors of A.*

Guiding Example 37. Guiding Example 30 is yet to stop providing us with insight into properties of eigenvalues and eigenvectors! Here are a couple of observations, which although outside of the core scope of this course, have significant impact in several areas:

- Notice that since $|\lambda_2|<|\lambda_1|$, the contribution of $\lambda_2^n\alpha_2v_2$ becomes negligible (when compared to $\lambda_1^n\alpha_1v_1$) as $n\to\infty$. This observation can be used in a clever way: we can approximate the eigenvector v_1 by A^ng_0 and so if we have a fast way to do matrix-vector multiply, we can approximate eigenvalues and eigenvectors. This is often referred to as the *Power Method*. In a CS Lens I plan to show you how Google's celebrated PageRank algorithm is based on the idea of how eigenvectors can be used for ranking (you can also read more about it here [BSS].[15]), calculating the eigenvector using a version of the Power Method is a crucial part of the algorithm.[16]

- The vector g_n gets larger and larger as $n \to \infty$ because $|\lambda_1| > 1$. If both eigenvalues satisfied $|\lambda| < 1$ then $g_n \to 0$ as $n \to \infty$. This illustrates the importance of the largest absolute values of the eigenvalues of a matrix in understanding the long term behaviour of systems of the form $A^n g_0$ for some A. If it represents a dynamical system it is related to stability or instability/chaos, if it represents e.g. the evolution of an economical system over time (or the finances of a company) it can be the difference between growth or ruin.[17]

A few properties of the eigenvalues follow from the fact that, by Corollary 7.0.4,

$$(-1)^n \det(A - zI) = \det(zI - A) = (z-\lambda_1)(z-\lambda_2)\cdots(z-\lambda_n). \tag{33}$$

The polynomial (33) is called the Characteristic Polynomial of the matrix A.[18]

Proposition 7.1.10. *Given $A \in \mathbb{R}^{n\times n}$ the eigenvalues of A are the same as the ones of $A^\top$.*

Proof. This follows from (33), and the fact that, for $\det(A - zI) = \det((A - zI)^\top) = \det(A^\top - zI)$. □

Definition 7.1.11. *Given a matrix $A \in \mathbb{R}^{n\times n}$, the trace of A is defined as*

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} A_{ii}.$$

A link between eigenvalues and the trace o a matrix is given below.

Proposition 7.1.12. *Let $A \in \mathbb{R}^{n\times n}$ and $\lambda_1, \ldots, \lambda_n$ its n eigenvalues as they show up in* (33) *(meaning that a value λ may be repeated, the number of times it shows up is the algebraic*

[15] Take a look also at "Landau on Chess Tournaments and Google's PageRank" by Rainer Sinn and Günter M. Ziegler (`https://arxiv.org/pdf/2210.17300.pdf`).

[16] An important advantage is that if we already have a good approximation of v_1, e.g. the page ranks from last week, we can compute a better approximation of v_1 (of this week's rankings) with very few matrix multiplies, you can read more about it here [BSS] and in the references therein.

[17] Try to modify the Fibonacci recurrence rule so that the new numbers go to zero as $n \to \infty$. Can you pick a recurrence such that they stabilize as $n \to \infty$ (without going to ∞ or 0)? Maybe linear algebra students in 2823 years will be studying your sequence!

[18] There is a converse to this in the sense that any monic polynomial can be written as a characteristic polynomial of a matrix, there is a particularly elegant way to build the matrix, if you are interested in learning more, look-up "companion matrix".

multiplicity of the eigenvalue) then

$$\operatorname{Tr}(A) = \sum_{i=1}^{n} \lambda_i, \tag{34}$$

$$\det(A) = \prod_{i=1}^{n} \lambda_i. \tag{35}$$

Remark 7.1.13. *When calculating eigenvalues, Proposition 7.1.12 is very useful to check computations.*

It is not difficult to verify that one can calculate with the trace-operator.

Lemma 7.1.14. *For matrices $A, B, C \in \mathbb{R}^{n\times n}$ one has*

(i) $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$

(ii) $\operatorname{Tr}(ABC) = \operatorname{Tr}(BCA) = \operatorname{Tr}(CAB)$.

Proof. (i)

$$\operatorname{Tr}(AB) = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}B_{ji} = \sum_{j=1}^{n}\sum_{i=1}^{n} B_{ji}A_{ij} = \operatorname{Tr}(BA).$$

(ii)

$$\operatorname{Tr}(ABC) = \operatorname{Tr}(A(BC)) = \operatorname{Tr}((BC)A) = \operatorname{Tr}(B(CA)) = \operatorname{Tr}(CAB).$$

□

Proof. [of Proposition 7.1.12] Let us consider the characteristic polynomial established in (33).

$$\begin{array}{rcl} (-1)^n \det(A - zI) & = & (z-\lambda_1)(z-\lambda_2)\cdots(z-\lambda_n) \\ & = & z^n + (-\sum_{i=1}^n \lambda_i)z^{n-1} + \sum_{k=1}^{n-2} b_k z^k + (-1)^n \prod_{i=1}^n \lambda_i, \end{array}$$

where $b_k \in \mathbb{C}$.

Set $z = 0$ in the expression above. It gives $(-1)^n \det(A) = (-1)^n \prod_{i=1}^n \lambda_i$ as claimed in (35).

For (34) note that the coefficient of z^{n-1} in the characteristic polynomial (33) is given in the right hand side by $(-\sum_{i=1}^n \lambda_i)$. On the left hand side the coefficient of z^{n-1} can only come from the permutation that takes all diagonal elements in the matrix $zI - A$. Hence it is the coefficient of

z^{n-1} of $\prod_{i=1}^{n}(z - A_{ii})$ which is $-\sum_{i=1}^{n} A_i i = -\operatorname{Tr}(A)$. □

Caution! 38. We write this caution as Remark 7.1.15 below given how important it is (so that it appears in black font).

Remark 7.1.15. *A few important words of caution:*

(1) Even though the eigenvalues of A and $A^\top$ are the same, the eigenvectors are not!

(2) The eigenvalues of $A+B$ are not easily computed from the eigenvalues of A and the ones of B, in particular they are not their sum!

(3) The eigenvalues of AB or BA are not easily computed from the eigenvalues of A and the ones of B, in particular they are not their product![19]

(4) Gaussian Elimination doesn't preserve eigenvalues and eigenvectors. The eigenvalues are not the diagonal elements of the U matrix in the $PA = LU$ factorization.[20]

While we focus on real eigenvalues on this course, let us see an example of a matrix that has no real eigenvalues and only complex valued ones.

Example 7.1.16. *The eigenvalues of the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, corresponding to a 90^o counter-clockwise rotation, are the solutions to $0 = \det(A - \lambda I) = \lambda^2 + 1$, which are $\lambda_1 = i$ and $\lambda_2 = -i$. The eigenvectors are given by $v_1 = \begin{bmatrix} i \\ 1 \end{bmatrix}$ and $v_2 = \begin{bmatrix} -i \\ 1 \end{bmatrix}$.*

Challenge 39. Try to work out an example for another rotation of $\mathbb{R}^2$.

This is a particular case of an orthogonal matrix, whose eigenvalues have a special property.

Proposition 7.1.17. *Let $Q \in \mathbb{R}^{n\times n}$ be an orthogonal matrix.*[21] *If $\lambda \in \mathbb{C}$ is an eigenvalue of Q, then $|\lambda| = 1$.*

[19] Interesting, there is a deep connection between A and B commuting (meaning $AB = BA$) and having the same eigenvectors. This is important in a few fields, in particular in Quantum Physics. If you want to learn more look-up "simultaneously diagonalizable".

[20] How to actually compute eigenvalues efficiently is outside of the scope of this course, it turns out that one can do it using the QR decomposition that we learned here as a subroutine. If you want to learn more look-up "QR algorithm".

Proof. Let $\lambda \in \mathbb{C}$ be an eigenvalue of Q and $v \in \mathbb{C}^n$ an associated eigenvector. Then $Qv = \lambda v$. Since Q is an orthogonal matrix we have $\|v\|^2 = \|Qv\|^2 = \|\lambda v\|^2 = |\lambda|^2\|v\|^2$. Since $v \neq 0$ we have $|\lambda| = 1$. □

Further Fact 40. If $\lambda \in \mathbb{C}$ is an eigenvalue of a matrix A with real entries, then $\overline{\lambda}$ is also an eigenvalue of A. This can be shown by noticing that $\det\left(A - \overline{\lambda}I\right) = \overline{\det(A - \lambda I)}$ (due to the polynomial representation of the determinant in (33), the fact that A has real entries).

7.1.1. *Repeated eigenvalues.*

An important part of the success of the strategy we took in Guiding Example 30 was the fact that we were able to build a basis of $\mathbb{R}^2$ with eigenvectors of the matrix M. In Theorem 7.1.9 we showed that we can always build a basis of $\mathbb{R}^n$ with eigenvectors of an $n \times n$ matrix A if A has n distinct real eigenvalues. One obstacle could be if some of the eigenvalues are not real valued but, even though we have not focused in complex valued eigenvalues, a straightforward adaption of the proof shows that if A has n distinct eigenvalues (not necessarily real) then there is a basis of $\mathbb{C}^n$ made up of eigenvectors of A. However, repeated eigenvalues can (but doesn't have to) pose a real obstacle to building a basis.

Example 7.1.18. *The matrix* $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ *does not have two linearly independent eigenvectors. Indeed,* $\det(A - \lambda I) = \lambda^2$ *which means that* $\lambda = 0$ *is the only eigenvalue and has algebraic multiplicity* 2*. However,* $N(A - 0I) = N(A)$ *only has dimension* 1*, so there is only one eigenvector (and multiples of it). with*

Example 7.1.19. *The zero matrix* $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ *does have two linearly independent eigenvectors. Indeed,* $\det(A - \lambda I) = \lambda^2$ *which means that* $\lambda = 0$ *is the only eigenvalue and has algebraic multiplicity* 2*. But, unlike in Example 7.1.18,* $N(A - 0I) = N(A)$ *has dimension* 2*, so there is a basis made up of two eigenvectors (in fact any two linearly independent vectors will be such a basis).*

Further Remark 41. Notice that in Example 7.1.18, $N\left(A^2\right)$ does have dimension 2. When there exist a positive integer k such that $A^k = 0$ we call A Nilpotent. There is a (rather deep) Theorem that essentially says nilpotency is the only obstacle to getting a complete set of eigenvectors. It roughly says that when there are "missing" eigenvectors they can be found in the Nullspace of powers of $A - \lambda I$, and this gives rise to something called "Jordan Normal Form".

Definition 7.1.20. *If, given a matrix $A \in \mathbb{R}^{n\times n}$, we can build a basis of $\mathbb{R}^n$ with eigenvectors of A we say that A has a complete set of real eigenvectors.*[22]

Theorem 7.1.9 states that a matrix with n distinct eigenvalues always has a complete set of real eigenvectors.

Proposition 7.1.21 (Eigenvalues and Eigenvectors of a Projection Matrix)**.** *Let P be the projection matrix on the subspace $U \subseteq \mathbb{R}^n$. Then P has two eigenvalues,* 0 *and* 1*, and a complete set of real eigenvectors.*

Proof. Let m be the dimension of U. Let $u_1, \ldots, u_m$ be a orthonormal basis of U, and $w_1, \ldots, w_{n-m}$ an orthonormal basis of $U^{\perp}$. It is easy to see that $Pu_k = 1u_k$ for any $1 \le k \le m$ and $Pw_k = 0w_k$ for any $1 \le k \le n-m$, so all n vectors are eigenvectors of P (with eigenvalues either 1 or 0). By construction of $U^{\perp}$, they form an orthonormal basis. □

In general when there is an eigenvalue λ with algebraic multiplicity larger than 1, it can be that $\mathrm{N}(A-\lambda I)$ is of large enough dimension to find enough linearly independent eigenvectors (as it is the case in projection matrices above, but not in the nilpotent example).

Definition 7.1.22. *Given a matrix $A \in \mathbb{R}^{n\times n}$ and an eigenvalue λ of A we call the dimension of $\mathrm{N}(A-\lambda I)$ the geometric multiplicity of λ.*

Further Fact 42. A matrix has a complete set of eigenvectors when the geometric multiplicities are the same as the algebraic multiplicites of all eigenvalues.

Exploratory Challenge 43. Prove Further Fact 42

Example 7.1.23. *For $D \in \mathbb{R}^{n\times n}$ a diagonal matrix, the eigenvalues of D are the diagonal entries of D. The canonical basis $e_1, \ldots, e_n$ is a set of eigenvectors of D.*

Challenge 44. Prove the statement in Example 7.1.23

Further Fact 45. The eigenvalues of an $n \times n$ triangular matrix are the n values in the diagonal. However, triangular matrices may not have a complete set of eigenvectors.

[22] If the matrix A has complex valued eigenvalues and we can instead build a basis of $\mathbb{C}^n$ we say it has a complete set of eigenvectors. Essentially everything we do below can be (straightforwardly) extended to this case but we will focus on real eigenvalues and eigenvectors for ease of exposition.

Challenge 46. Prove this fact. Hint: For the positive part use (33), for the negative part recall Example 7.1.18.

Challenge 47. Let's say a matrix $A \in \mathbb{R}^{n\times n}$ has an LU decomposition (without the need for P in $PA = LU$). Remark 7.1.15 says the eigenvalues of $A \in \mathbb{R}^{n\times n}$ are not the ones of U in the LU decomposition $PA = LU$. The eigenvalues of U are indeed their diagonal entries, and the eigenvalues of L are all 1 (by Further Fact 7.1.1). Why is it the case that the eigenvalues of A are not the diagonal entries of U?

7.2. **Diagonalizing a Matrix and Change of Basis of a Linear Transformation.**

Let us continue dissecting Guiding Example 30. Essentially, what we did was to write g_0 in the basis v_1, v_2 of eigenvectors of M and then exploit the fact that linear transformation given M had a very simple behaviour when written in the basis v_1, v_2 (the coefficients simply were multiplied by the eigenvalues of M). This motivates us to take a detour in briefly studying linear transformations written in different basis, and to discuss "change of bases".

7.2.1. *Change of basis.*

For this detour we will briefly consider $m \times n$ matrices, before returning to square matrices when discussing eigenvalues and eigenvectors.

Let $A^{m\times n}$ be a matrix representing a linear transformation $L : \mathbb{R}^n \to \mathbb{R}^m$ given by $x \in \mathbb{R}^n \to Ax \in \mathbb{R}^m$, with both input and output written in the canonical bases as $x = \sum_{j=1}^n x_j e_j$ and $Ax = \sum_{i=1}^m (Ax)_i e_i$. Recall (Example 5.4.2) that $(e_i)_j = \delta_{ij}$, and that $(Ax)_i$ is the i-th entry of the vector Ax.

Now, let's say we have a basis for $\mathbb{R}^n$ given by $u_1, \dots, u_n$ and one for $\mathbb{R}^m$ given by $v_1, \dots, v_m$ (neither being necessarily the canonical basis) and we want to understand the the linear transformation L written in this basis. Then L takes a vector $x = \sum_{j=1}^n \alpha_j u_j$ and outputs $L(x) = \sum_{j=1}^n \beta_i v_i$. We want to compute the matrix B that takes $\alpha = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$ to $\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}$. In other words, such that $B\alpha = \beta$. Let $U \in \mathbb{R}^{n\times n}$ be the matrix whose columns are the basis elements $u_1, \dots, u_n$ and $V \in \mathbb{R}^{m\times m}$ the matrix whose columns are the basis elements $v_1, \dots, v_m$. Then, $x = U\alpha$ and $L(x) = V\beta$ and so $\beta = V^{-1}AU\alpha$, the matrix B, corresponding to the linear transformation L written in the new bases is $B = V^{-1}AU$. Note that we can do change of basis between any pair of basis, it needs not be from the canonical basis to another basis, in that case the role of U and V would be played by the change of basis matrix (the matrix that maps the coefficients of a vector written in the old basis, to its coefficients when written in the new basis).

$$\begin{aligned} L : \mathbb{R}^n &\to \mathbb{R}^m && \text{linear transformation} \\ L\left(\sum_{j=1}^{n} x_j e_j\right) &= \sum_{i=1}^{n} (Ax)_i e_i && x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \\ L\left(\sum_{j=1}^{n} \alpha_j u_j\right) &= \sum_{i=1}^{n} (B\alpha)_i v_i && \alpha = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \end{aligned} \tag{36}$$

where $B = V^{-1}AU \in \mathbb{R}^{m\times n}$, $U = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix} \in \mathbb{R}^{n\times n}$, $V = \begin{bmatrix} v_1 & \cdots & v_m \end{bmatrix} \in \mathbb{R}^{m\times m}$.

7.2.2. Diagonalizing a Matrix.

Let us focus back on square matrices $A \in \mathbb{R}^{n\times n}$. In particular, let A be a matrix with a complete set of real eigenvectors (in the sense of Definition 7.1.20) and let $v_1, \dots, v_n \in \mathbb{R}^{n\times n}$ be a basis formed with eigenvectors of A. The crucial fact we used in Guiding Example 30 also holds in this general situation: if we write a vector $x \in \mathbb{R}^n$ as $x = \sum_{i=1}^n \alpha_i v_i$ then $Ax = \sum_{i=1}^n \lambda_i \alpha_i v_i$ (and also $A^k x = \sum_{i=1}^n \lambda_i^k \alpha_i v_i$, for $k \geq 1$, where λ_i is the eigenvalue associated with the eigenvector v_i). One way to think about this is that the linear transformation corresponding to the matrix A, when written in the basis V is simply a diagonal matrix/transformation. This is the key idea behind *Matrix Diagonalization*. This is one of the most important facts in Linear Algebra.

Theorem 7.2.1. *Let $A \in \mathbb{R}^{n\times n}$ be a matrix with a complete set of real eigenvectors (in the sense of Definition 7.1.20) and let $v_1, \dots, v_n \in \mathbb{R}^{n\times n}$ be a basis formed with eigenvectors of A and let $\lambda_1, \dots, \lambda_n$ be the associated eigenvalues (λ_i associated to v_i). Let V be the matrix whose columns are the eigenvectors v_i, $V = \begin{bmatrix} v_1 & \cdots & v_m \end{bmatrix} \in \mathbb{R}^{n\times n}$. Then,*

$$A = V\Lambda V^{-1}, \tag{37}$$

where Λ is a diagonal matrix with $\Lambda_{ii} = \lambda_i$ (and $\Lambda_{ij} = 0$ for all $i \neq j$).

Proof. Since $v_1, \dots, v_n$ is a basis, V is an invertible matrix, so it suffices to prove that

$$V^{-1}AV = \Lambda. \tag{38}$$

This can be done by direct calculation: For any $1 \leq j \leq n$, the j-th column of the matrix $V^{-1}AV$ is given by

$$\left(V^{-1}AV\right)_{\cdot j} := \left(V^{-1}AV\right) e_j = V^{-1}Av_j = V^{-1}\lambda_j v_j = \lambda_j V^{-1} v_j = \lambda_j e_j,$$

since $V^{-1}v_j = V^{-1}Ve_j = e_j$. Recall that e_j is the vector in $\mathbb{R}^n$ with a 1 in j-th entry and zero elsewhere. Since for any $1 \leq j \leq n$, $\lambda_j e_j$ is also the j-th column of Λ, we have that $V^{-1}AV = \Lambda$. □

Definition 7.2.2 (Diagonalizable Matrix). *A matrix $A \in \mathbb{R}^{n\times n}$ is called a diagonalizable matrix if there exists an invertible matrix V such that $V^{-1}AV = \Lambda$, where Λ is a diagonal matrix.*

Challenge 48. Most properties of the eigenvalues are very easy to prove by using Theorem 7.2.1 (for the matrices that have a complete set of eigenvectors). Try it!

The eigenvalues of Λ are also $\lambda_1, \ldots, \lambda_n$ (recall Example 7.1.23). More generally, for an invertible matrix S we always have that A and $S^{-1}AS$ have the same eigenvalues.

Definition 7.2.3 (Similar Matrices). [23] *We say that $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times n}$ are similar matrices if there exists an invertible matrix S such that $B = S^{-1}AS$.*

Proposition 7.2.4. *Similar matrices have the same eigenvalues.*

Challenge 49. Try to show Proposition 7.2.4 via (33).

Challenge 50. Try to show that if λ is an eigenvalue of $S^{-1}AS$ (with associated eigenvector v) then it is also an eigenvalue of A and compute the associated eigenvector in terms of v and S. (without using Proposition 7.2.4 or (33).

Remark 7.2.5 (Diagonalizing a matrix and finding a good basis for a linear transformation). *If we have a matrix $A \in \mathbb{R}^{n\times n}$ with a complete set of real eigenvectors then Theorem 7.2.1 tells us that the corresponding linear transformation, when viewed in the bases $v_1, \ldots, v_n$ is simply a diagonal matrix (recall that in this case $B = \Lambda$, see* (36)*). This is a remarkable fact: since most matrices have a full set of eigenvectors (in particular all for which the eigenvalues are all distinct do) this says that all the corresponding linear combinations, regardless of how complicated they might seem, are actually just a diagonal operation when viewed in the basis $v_1, \ldots, v_n$.*

[23] The operation $A \to S^{-1}AS$ is sometimes called conjugation but this is not to be confused with complex conjugation $z \to \bar{z}$, one term comes from “conjugation” in group theory, the other from “conjugation” in complex analysis.

7.3. **Symmetric Matrices and the Spectral Theorem.**

This section is devoted to real symmetric matrices,[24] meaning matrices $A \in \mathbb{R}^{n\times n}$ for which $A^\top = A$ (see Further Remark 54 for a brief discussion of how symmetric matrices appear naturally in several settings). The main goal of this section is to prove the Spectral Theorem.

Theorem 7.3.1 (Spectral Theorem)**.** *Any symmetric[25] matrix $A \in \mathbb{R}^{n\times n}$ has n real eigenvalues and an orthonormal basis made of eigenvectors of A.*

Together with Theorem 7.2.1 this implies the following corollary.

Corollary 7.3.2. *For any symmetric matrix $A \in \mathbb{R}^{n\times n}$ there exists an orthogonal matrix $V \in \mathbb{R}^{n\times n}$ (whose columns are eigenvectors of A) such that*

$$A = V\Lambda V^\top,$$

where $\Lambda \in \mathbb{R}^{n\times n}$ is a diagonal matrix with the eigenvalues of A in its diagonal (and $V^\top V = I$).

Remark 7.3.3 (Eigendecomposition)**.** *The decompositions in Corollary 7.3.2 and Theorem 7.2.1 are called Eigendecompositions.*

The following follows easily from the Spectral Theorem.

Corollary 7.3.4. *The rank of a real symmetric matrix A is the number of non-zero eigenvalues (counting repetitions).*

Remark 7.3.5. *For general $n \times n$ (non-symmetric) matrices, the rank is n minus the dimension of the nullspace, so it is n minus the geometric multiplicity of $\lambda = 0$. Since symmetric matrices always have a complete set of eigenvalues and eigenvectors, the geometric multiplicities are always the same as the algebraic multiplicities.*

[24] The same theory can be developed (by a straightforward adaption) to complex matrices but the property of being symmetric is replaced by being Hermitian, which means that a matrix $A = A^* = \overline{A}^\top$. In both situations we say A is self-adjoint.

Proposition 7.3.6. *Let A be a real $n \times n$ symmetric matrix and let $v_1, \ldots, v_n$ be an orthonormal basis of eigenvectors of A (the columns of the matrix V in Corollary 7.3.2) and $\lambda_1, \ldots, \lambda_n$ the associated eigenvalues. Then*

$$A = \sum_{k=1}^{n} \lambda_i v_i v_i^\top$$

Proof. Follows directly by Corollary 7.3.2. □

We "build up" to the proof of Theorem 7.3.1 with a few propositions.

Proposition 7.3.7. *Let $A \in \mathbb{R}^{n \times n}$ be a symmetric matrix and $\lambda \in \mathbb{C}$ an eigenvalue of A, then $\lambda \in \mathbb{R}$.*

Proof. Let $v \in \mathbb{C}^n$ be an eigenvector associated with the eigenvalue λ. We have $Av = \lambda v$. Recall that, for a matrix (or vector) M, its Hermitian conjugate is given by $M^* = \overline{M}^\top$. Since A is real symmetric we have $A^* = A$. Thus, we have

$$\overline{\lambda} \|v\|^2 = \overline{\lambda} v^* v = (\lambda v)^* v = (Av)^* v = v^* A^* v = v^* A v = v^* \lambda v = \lambda \|v\|^2.$$

Since $v \neq 0$, then $\|v\| \neq 0$ and so $\lambda = \overline{\lambda}$. This implies that $\lambda \in \mathbb{R}$. □

This, together with Theorem 7.1.4, immediately implies the following.

Corollary 7.3.8. *Every symmetric matrix $A \in \mathbb{R}^{n \times n}$ has a real eigenvalue λ.*

Remark 7.3.9. *The fact that two eigenvectors of a real symmetric matrix are orthogonal follows from Theorem 7.3.1 but it is useful to see a simple argument of that (the main difficulty of proving Theorem 7.3.1 is proving that the matrix indeed has a complete set of eigenvectors). Let's say we have $\lambda_1 \neq \lambda_2$ eigenvalues of a real symmetric matrix A and $v_1, v_2 \in \mathbb{R}^n \setminus \{0\}$ corresponding eigenvectors. Then*

$$\lambda_1 v_1^\top v_2 = (Av_1)^\top v_2 = v_1^\top A^\top v_2 = v_1^\top A v_2 = v_1^\top (Av_2) = \lambda_2 v_1^\top v_2,$$

since $\lambda_1 \neq \lambda_2$ we must have that $v_1^\top v_2 = 0$

Further Remark 51. Corollary 7.3.8 is a great example of the usefulness of complex numbers. Even though it is a statement just about real matrices and real eigenvalues we proved it by going through the complex numbers and using results in Complex Analysis. There is an alternative proof without going through the complex numbers but it would need more background, and I find this one more transparent.[26]

Proof. [of Theorem 7.3.1]

Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix. We will prove the following by induction, which for $k = n$ implies the theorem we want to show:

- For any $1 \leq k \leq n$ there are k orthogonal eigenvectors of A.

The base case $k = 1$ follows directly by Corollary 7.3.8 as we can always normalize the eigenvector to have norm 1.

We now assume that the statement is true for k and show it for $k+1$. We will show that if a real symmetric matrix A has k (with $1 \leq k < n$) orthonormal eigenvectors then we can build an extra one, orthogonal to the others (to achieve norm 1 we simply need to normalize it).[27]

Let $v_1, \ldots, v_k$ denote k orthonormal eigenvectors of A and $\lambda_1, \ldots, \lambda_k$ the respective eigenvalues. Let $u_{k+1}, \ldots, u_n$ be an orthonormal basis of the orthogonal complement of the span of $v_1, \ldots, v_k$. Let V_k be the $n \times n$ matrix whose i-th column is v_i if $i \leq k$ and u_i if $i > k$. V_k is an orthogonal

[26] If you would like to see a nice example of how improving knowledge can lead to much simpler and more transparent methods/models, search "Ptolemaic Epicycle Machine".

[27] In a first reading of the proof I recommend taking $k = 1$ in the induction step, as it is simpler while already containing all the relevant ideas.

matrix. Moreover, let us define $B \in \mathbb{R}^{n\times n}$ as $B = V^\top AV$, then:

$$\begin{aligned}
B = V^\top AV \quad &= \begin{bmatrix} — & v_1^\top & — \\ & \vdots & \\ — & v_k^\top & — \\ — & u_{k+1}^\top & — \\ & \vdots & \\ — & u_n^\top & — \end{bmatrix} \begin{bmatrix} | & & | & | & & | \\ Av_1 & \cdots & Av_k & Au_{k+1} & \cdots & Au_n \\ | & & | & | & & | \end{bmatrix} \\
&= \begin{bmatrix} — & v_1^\top & — \\ & \vdots & \\ — & v_k^\top & — \\ — & u_{k+1}^\top & — \\ & \vdots & \\ — & u_n^\top & — \end{bmatrix} \begin{bmatrix} | & & | & | & & | \\ \lambda v_1 & \cdots & \lambda v_k & Au_{k+1} & \cdots & Au_n \\ | & & | & | & & | \end{bmatrix} \\
&= \begin{bmatrix} \Lambda_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & C \end{bmatrix},
\end{aligned}$$

where Λ_k is a diagonal matrix with $\lambda_1, \ldots, \lambda_k$ in the diagonal, $0_{(n-k)\times k}$ and $0_{k\times(n-k)}$ are zero matrices of size respectively $(n-k)\times k$ and $k\times(n-k)$. C is a $(n-k)\times(n-k)$ symmetric matrix.

Since C is a $(n-k)\times(n-k)$ symmetric matrix, Theorem 7.3.8 implies it has a real eigenvalue λ_{k+1} and a real eigenvector $y \in \mathbb{R}^{n-k}$. Let $w \in \mathbb{R}^n$ be the vector with 0 in the first k coordinates and y in the remaining $n-k$, in other words

$$w_i = \begin{cases} 0 & \text{if } \ i \le k \\ y_{i-k} & \text{if } \ i > k. \end{cases}$$

We have

$$Bw = \begin{bmatrix} \Lambda_k & 0_{k\times(n-k)} \\ 0_{(n-k)\times k} & C \end{bmatrix} \begin{bmatrix} 0_{k\times 1} \\ y \end{bmatrix} = \begin{bmatrix} 0_{k\times 1} \\ Cy \end{bmatrix} = \begin{bmatrix} 0_{k\times 1} \\ \lambda_{k+1} y \end{bmatrix} = \lambda_{k+1} w.$$

Let $v_{k+1} := Vw$. Since V is orthogonal we have that $A = VBV^\top$. Thus,

$$Av_{k+1} = VBV^\top v_{k+1} = VBw = V\lambda_{k+1} w = \lambda_{k+1} v_{k+1},$$

so v_{k+1} is an eigenvector of A. To see that it is orthogonal to $v_1, \ldots, v_k$ note that the inner products $v_i^\top v_{k+1}$ for $i \le k$ appear in the first k entries of $V^\top v_{k+1} = w$ and that w has its first k coordinates 0 by construction. By normalizing the vector we can have it have unit norm.

□

Proposition 7.3.10 (Rayleigh Quotient)**.** *Given a symmetric matrix $A \in \mathbb{R}^{n\times n}$ the Rayleigh Quotient, defined for $x \in \mathbb{R}^n \setminus \{0\}$, as*

$$R(x) = \frac{x^\top Ax}{x^\top x}$$

attains its maximum at $R(v_{\max}) = \lambda_{\max}$ and its minimum at $R(v_{\min}) = \lambda_{\min}$ where $\lambda_{\max}$ and $\lambda_{\min}$ are respectively the largest and smallest eigenvalues of A and $v_{\max}$, $v_{\min}$ their associated eigenvectors.

Proof. It is easy to see that $R(v_{\max}) = \lambda_{\max}$ and $R(v_{\min}) = \lambda_{\min}$ so it suffices to show that, for all $x \in \mathbb{R}^n \setminus \{0\}$ we have $\lambda_{\min} \leq R(x) \leq \lambda_{\max}$. Using Proposition 7.3.6 we can write, for $x \in \mathbb{R}^n \setminus \{0\}$,

$$R(x) = \frac{x^\top \left(\sum_{i=1}^n \lambda_i v_i v_i^\top\right) x}{\|x\|^2} = \frac{\sum_{i=1}^n \lambda_i \left(x^\top v_i\right)^2}{\|x\|^2},$$

where $v_1, \ldots, v_n$ form an orthonormal basis of eigenvectors of A and $\lambda_1, \ldots, \lambda_n$ are the associated eigenvalues. Since $\left(x^\top v_i\right)^2 \geq 0$ for all $1 \leq i \leq n$ we have that, for all $1 \leq i \leq n$,

$$\lambda_{\min} \left(x^\top v_i\right)^2 \leq \lambda_i \left(x^\top v_i\right)^2 \leq \lambda_{\max} \left(x^\top v_i\right)^2.$$

Collecting all these inequalities we get

$$\lambda_{\min} \frac{\sum_{i=1}^n \left(x^\top v_i\right)^2}{\|x\|^2} \leq \frac{\sum_{i=1}^n \lambda_i \left(x^\top v_i\right)^2}{\|x\|^2} \leq \lambda_{\max} \frac{\sum_{i=1}^n \left(x^\top v_i\right)^2}{\|x\|^2}.$$

To conclude the proof note that, since the v_i's are orthonormal, the matrix V with the v_i's as columns is orthogonal and $\sum_{i=1}^n \left(x^\top v_i\right)^2 = \|Vx\|^2 = \|x\|^2$ and so $\frac{\sum_{i=1}^n \left(x^\top v_i\right)^2}{\|x\|^2} = 1$. □

Definition 7.3.11 (Positive Definite and Positive Semidefinite matrix)**.** *A symmetric matrix $A \in \mathbb{R}^{n\times n}$ is said to be Positive Semidefinite (PSD) if all its eigenvalues are non-negative. If all the eigenvalues of A are strictly positive then we say A is Positive Definite (PD).*

Exploratory Challenge 52. Even though the eigenvalues of $A + B$ are not easily described by the eigenvalues of A and the ones of B it turns out that if both are PSD (or PD) then so is the sum. Can you show that?

The following follows directly from Proposition 7.3.10.

Proposition 7.3.12. *A symmetric matrix $A \in \mathbb{R}^{n\times n}$ is Positive Semidefinite if and only if $x^\top Ax \geq 0$ for all $x \in \mathbb{R}^n$. Analogously, a symmetric matrix $A \in \mathbb{R}^{n\times n}$ is Positive Definite if and only if $x^\top Ax > 0$ for all $x \in \mathbb{R}^n \setminus \{0\}$.*

Fact 7.3.13. *If two $n \times n$ matrices A and B are PSD (or PD) then their sum is PSD (or PD).*

Challenge 53. Exploratory Challenge 52 looked pretty difficult, but now with Proposition 7.3.12 it is much easier, try to prove Fact 7.3.13.

Definition 7.3.14 (Gram Matrix)**.** *Given n vectors, $v_1,\dots,v_n$ in $\mathbb{R}^m$ we call their Gram Matrix the $n\times n$ matrix of inner products*

$$G_{ij} = v_i^\top v_j.$$

Note that if $V \in \mathbb{R}^{m\times n}$ is the matrix whose columns are the n vectors, then $G = V^\top V$ is the Gram matrix of V.

Remark 7.3.15. *Given a matrix $A \in \mathbb{R}^{m\times n}$, as an abuse of notation, we sometimes also call $AA^\top$ a Gram matrix of A. Notice that, if $a_1,\dots,a_n \in \mathbb{R}^m$ are the columns of A then $AA^\top$ is $m\times m$ and*

$$AA^\top = \sum_{i=1}^{n} a_i a_i^\top. \tag{39}$$

Proposition 7.3.16. *Given a real matrix $A \in \mathbb{R}^{m\times n}$, the non-zero eigenvalues of $A^\top A \in \mathbb{R}^{n\times n}$ are the same as the ones of $AA^\top \in \mathbb{R}^{m\times m}$. Both matrices are symmetric and positive semidefinite.*

Proof. Let r be the rank of A. We know $\operatorname{rank}(A) = \operatorname{rank}(A^\top) = \operatorname{rank}(A^\top A) = \operatorname{rank}(AA^\top)$ (recall Proposition **??** and Challenge **??**). It is straightforward that both $A^\top A$ and $AA^\top$ are symmetric. Let us prove they are positive semidefinite. We have $x^\top A^\top Ax = \|Ax\|^2 \geq 0$ for all x which implies $A^\top A$ is PSD, and the same argument can be used for $AA^\top$.

Now, both $AA^\top$ and $A^\top A$ have a complete set of real eigenvalues and orthogonal eigenvectors. Let $\lambda_1,\dots,\lambda_r$ be the r non-zero eigenvalues of $A^\top A$ and $v_1 \dots, v_r$ be the corresponding eigenvectors. We have, for $1 \leq k \leq r$, $A^\top Av_k = \lambda_k v_k$, multiplying by A both sides we get $AA^\top Av_k = \lambda_k Av_k$ and so λ_k is an eigenvalue of $AA^\top$ with eigenvector Av_k (note that $Av_k \neq 0$). Furthermore, For $j \neq k$ we have $(Av_j)^\top(Av_k) = v_j^\top A^\top Av_k = v_j^\top \lambda_k v_k = \lambda_k v_j^\top v_k = 0$ and so the r eigenvectors of $AA^\top$ built this way are orthogonal, and so $\lambda_1,\dots,\lambda_r$ are the nonzero eigenvectors of $AA^\top$. □

Proposition 7.3.17. *[Cholesky decomposition] Every symmetric positive semidefinite matrix M is a gram matrix of an upper triangular matrix C. $M = C^\top C$ is known as the Cholesky Decomposition.*[28]

Proof. Let M be a symmetric positive semidefinite matrix. Corollary 7.3.2 gives us a decomposition $M = V\Lambda V^\top$ with Λ a diagonal matrix with the eigenvalues of M in the diagonal. Since M is PSD, the diagonal entries of Λ are non-negative and so we can build $\Lambda^{1/2}$ by taking the square root of each diagonal entry of Λ. Then $M = \left(V\Lambda^{1/2}\right)\left(V\Lambda^{1/2}\right)^\top$. To make the matrices in the decomposition be upper triangular, simply take the QR decomposition (recall Definition 5.4.11) $\left(V\Lambda^{1/2}\right)^\top = QR$ with Q such that $Q^\top Q = I$ and R upper triangular. We have $M = \left(V\Lambda^{1/2}\right)\left(V\Lambda^{1/2}\right)^\top = (QR)^\top (QR) = R^\top Q^\top QR = R^\top R$. Taking $C = R$ establishes the Proposition.[29] □

Further Remark 54. At first glance, Symmetric matrices look very special (since we must have $A^\top = A$) but they they actually appear very often in both applications and pure mathematics. For example, in my own work, I rarely encounter non-symmetric matrices. There are (at least) two reasons for this: (i) For any matrix B we can form a symmetric matrix $B^\top B$ from which we can study B, this is going to be the key idea behind the Singular Value Decomposition. (ii) In many instances, matrices represent relationship between objects — for example, A_{ij} can represent a friendship connection (or a similarity measure) between person (or data point) i and j and in many cases such relationships are symmetric.

Exploratory Challenge 55. Recall the symmetric LU decomposition from the first part of the course, what can you say of such a decomposition for PSD matrices? How is it related to the Cholesky Decomposition?

8. Singular Value Decomposition; and some open questions in Linear Algebra

8.1. The Singular Value Decomposition.

[29] This is not the classical construction of the Cholesky Decomposition. The classical construction is with Gaussian Elimination, but at this stage of the course I think this is more transparent. Note also that when using Gaussian Elimination C will be a square matrix, while here R can be rectangular if M is not full rank (which makes it a more economical decomposition).

We are now reaching "the ultimate theorem of our class", the Singular Value Decomposition (SVD). The SVD is a way to generalize the eigendecomposition to non-symmetric, and even non-square, matrices. Instead of eigenvalues we will have singular values and instead of eigenvectors we will have (right and left) singular vectors.

Definition 8.1.1 (SVD — Singular Value Decomposition)**.** *Let $A \in \mathbb{R}^{m\times n}$. There exist orthogonal matrices $U \in \mathbb{R}^{m\times m}$ and $V \in \mathbb{R}^{n\times n}$ such that*

$$A = U\Sigma V^\top, \tag{40}$$

where $\Sigma \in \mathbb{R}^{m\times n}$ is a diagonal matrix, in the sense that $\Sigma_{ij} = 0$ when $i \neq j$, and the diagonal elements are non-negative and ordered in descending order. $U^\top U = I$ and $V^\top V = I$.

The columns $u_1, \dots u_m$ of U are called the left singular vectors of A and are orthonormal. The columns $v_1, \dots v_n$ of V are called the right singular vectors of A and are orthonormal. The diagonal elements of Σ, $\sigma_i = \Sigma_{ii}$ are called the singular values of A and are ordered as

$$\sigma_1 \geq \cdots \geq \sigma_{\min\{m,n\}}.$$

Remark 8.1.2. *If A has rank r we can write the SVD in a more compact form:*

$$A = U_r\Sigma_r V_r^\top, \tag{41}$$

where $U_r \in \mathbb{R}^{m\times r}$ contains the first r left singular vectors, $V_r \in \mathbb{R}^{n\times r}$ contains the first r right singular vectors and $\Sigma_r \in \mathbb{R}^{r\times r}$ is a diagonal matrix with the first r singular values. Notice that storing such a decomposition in the computer requires storing $r \times (m+n+1)$ real numbers rather than $m \times n$ real numbers which would be required to store A naively. When a matrix has small rank these are crucial savings.[30].

Oftentimes the subscript is omitted and the compact SVD is simply written as $U\Sigma V^\top$ while specifying the dimensions of the matrices involved to specify which form of the SVD is being considered.

Remark 8.1.3. *Let $A \in \mathbb{R}^{m\times n}$ and $A = U\Sigma V^\top$ be its SVD (as in* (40)*) then*

$$AA^\top = U\left(\Sigma\Sigma^\top\right)U^\top,$$

and so the left singular vectors of A, the columns of U, are the eigenvectors of $AA^\top$ and the singular values of A are the square-root of the eigenvalues of $AA^\top$ (note that $\Sigma\Sigma^\top$ is $m \times m$ diagonal). If $m > n$, A has n singular values and $AA^\top$ has m eigenvalues (which is larger than n), but the "missing" ones are 0.

[30] Taking this one step forward, when a matrix is well approximated by a low rank matrix, oftentimes one stores only a small rank approximation of a matrix A, this is a crucial idea in tasks ranging from Image Compressions, Numerical Analysis, and Machine Learning, see Section **??**.

Analogously,

$$A^\top A = V\left(\Sigma^\top \Sigma\right)V^\top,$$

and so the right singular vectors of A, the columns of V, are the eigenvectors of $A^\top A$ and the singular values of A are the square-root of the eigenvalues of $A^\top A$ (note that $\Sigma^\top\Sigma$ is $n\times n$ diagonal). If $n > m$, A has m singular values and $A^\top A$ has n eigenvalues (which is larger than m), but the "missing" ones are 0.

This observation makes it easier to write the singular values and singular vectors of A in terms of eigenvalues and eigenvectors of $AA^\top$ and $A^\top A$, which are symmetric matrices (and directly implies, e.g., uniqueness of singular values; and the fact that the rank of a matrix is the number of nonzero singular values). In fact, the proof of the existence SVD will heavily rely on the Spectral Theorem.

An important direct consequence of the SVD, and in particular of (41) is that we can write any rank-r matrix $A \in \mathbb{R}^{m\times n}$ as a sum of r rank-1 matrices:

Proposition 8.1.4. *Let $A \in \mathbb{R}^{m\times n}$ be a matrix with rank r. Let $\sigma_1,\ldots,\sigma_r$ be the non-zero singular values of A, $u_1,\ldots,u_r$ the corresponding left singular vectors and $v_1,\ldots,v_r$ the corresponding right singular vectors. Then*

$$A = \sum_{k=1}^{r} \sigma_k u_k v_k^\top. \tag{42}$$

Challenge 56. The SVD is a powerful tool. Many of the things we did in this course become significantly simpler with the SVD. Now that you have the SVD, try to reread these notes and try to re-interpret the results we derived in terms of the SVD. For example, the Moore-Penrose Pseudoinverse has a very simple description of the SVD, it corresponds to swapping U and V and replacing the non-zero singular values by their inverses, while keeping the zero ones zero. Try to derive this!

Theorem 8.1.5. *[The SVD – the Ultimate Theorem of `ETHZ 401-0131-00L`]*

Every matrix $A \in \mathbb{R}^{m\times n}$ has an SVD decomposition of the form (40).

In other words:

Every linear transformation is diagonal when viewed in the bases of the singular vectors.

Proof. Let $A^{m\times n}$. Let r be the rank of $A^{m\times n}$. We will build a compact SVD as in (41). It is easy to see that we can get an SVD in the sense of (40) from a compact one by adding singular values that are zero and extending the singular vectors in both U_r and V_r to orthonormal bases.

By Theorem 7.3.1 and Corollary 7.3.2 the matrix $AA^\top$ has a complete set of orthonormal eigenvectors and can be written as

$$AA^\top = U\Lambda U^\top, \tag{43}$$

where $U \in \mathbb{R}^{m\times m}$ is orthogonal and Λ is diagonal. Let us write (43) ordering the diagonal entries of Λ in decreasing order. Furthermore, let us write (43) also in a compact form, by keeping only the r non-zero eigenvalues (and corresponding eigenvectors), so

$$AA^\top = U_r\Lambda_r U_r^\top$$

for $U_r \in \mathbb{R}^{m\times r}$ such that $U_r^\top U_r = I$ and Λ_r is $r\times r$ diagonal with the non-zero eigenvalues of $AA^\top$. By Proposition 7.3.16 the eigenvalues of $AA^\top$ are non-negative and so the diagonal entries of Λ_r are positive. Let $\Sigma_r \in \mathbb{R}^{r\times r}$ be the diagonal matrix with diagonal entries $\sigma_i := (\Sigma_r)_{ii} = \sqrt{\Lambda_{ii}}$. Our goal is to show that there is a $n\times r$ matrix V_r, with orthonormal columns, such that $A = U_r\Sigma_r V_r^\top$. We would have $\Sigma_r^{-1}U_r^\top A = \Sigma_r^{-1}U_r^\top U_r\Sigma_r V_r^\top = V_r^\top$, or equivalently $V_r = A^\top U_r\Sigma_r^{-1}$. Motivated by this, let's set

$$V_r := A^\top U_r\Sigma_r^{-1},$$

this corresponds to a matrix with columns $v_1,\dots,v_r$ given by $v_k = \frac{1}{\sigma_k}A^\top u_k$. To conclude we need to show that this construction indeed gives a compact SVD, for this we still need to show two things:

(1) $V_r^\top V_r = I$. This can be verified by direct computation, while recalling that $AA^\top = U_r\Lambda_r U_r^\top$:

$$V_r^\top V_r = \left(A^\top U_r\Sigma_r^{-1}\right)^\top A^\top U_r\Sigma_r^{-1} = \Sigma_r^{-1}U_r^\top AA^\top U_r\Sigma_r^{-1} = \Sigma_r^{-1}U_r^\top U_r\Lambda_r U_r^\top U_r\Sigma_r^{-1} = \Sigma_r^{-1}\Lambda_r\Sigma_r^{-1} = I$$

(2) $A = U_r\Sigma_r V_r^\top$. Note that

$$U_r\Sigma_r V_r^\top = U_r\Sigma_r\left(A^\top U_r\Sigma_r^{-1}\right)^\top = U_rU_r^\top A.$$

Let us simply verify that $A = U_rU_r^T A$.

- Let $x \in N(A)$. Then $Ax = 0 = U_rU_r^T x$
- Let $x \in C(A^T)$. It follows that $x = A^T y$ for $y \in \mathrm{R}^m$ and hence,

$$Ax = AA^T y = U_r\Lambda_r U_r^T y = U_r I\Lambda_r U_r^T y = U_rU_r^T U_r\Lambda_r U_r^T y = U_rU_r^T AA^T y = U_rU_r^T Ax.$$

Hence, for all $x \in \mathrm{R}^n$ we have verified that $Ax = U_rU_r^T Ax$. Then $A = U_rU_r^T A$ follows.

□

8.2. **Vector and Matrix Norms.**

A short section on vector and matrix norms. So far, the norm of a vector $x \in \mathbb{R}^n$ was simply given by $\|x\| = x^\top x$ but there are instances where it makes sense to measure the "lenght" of vectors in other ways. One popular way is called the "Manhattan distance" since when traveling in Manhattan one cannot take advantage of Pythagoras Theorem because that would involve cutting through buildings, that norm is given by $\|x\|_1 = \sum_{i=1}^n |x_i|$. In general, for $1 \le p \le \infty$ the ℓ_p norm is given by

$$\|x\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{1/p}, \tag{44}$$

for $p < \infty$, and $\|x\|_\infty = \max_i |x_i|$. Notice that $\|\cdot\|_2$ corresponds to the Euclidean norm that we have used in this course.[31]

Challenge 57 ($\star$)**.** Prove that, for all $x \in \mathbb{R}^n$, we have $\|x\|_2 \le \|x\|_1 \le \sqrt{n}\|x\|_2$.

In several situations one also needs to "measure" the size of matrices (for example, when talking about a matrix being close to another one, we need a notion of distance, or norm of the difference).

Definition 8.2.1 (Two matrix norms)**.** *Given a matrix $A \in \mathbb{R}^{m\times n}$ we define two matrix norms:*

- $\|A\|_F$*, known as the Frobenius norm, is defined as*

$$\|A\|_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^n A_{ij}^2},$$

- $\|A\|_{op}$*, known as operator or specral norm, is defined as*

$$\|A\|_{op} = \max_{\substack{x\in\mathbb{R}^n \\ s.t. \|x\|=1}} \|Ax\|.$$

Further Proposition 58. Given $A \in \mathbb{R}^{m\times n}$ with singular values $\sigma_1 \ge \cdots \ge \sigma_{\min\{m,n\}}$. We have

(1) $\|A\|_F^2 = \operatorname{Tr}\left(A^TA\right)$

(2) $\|A\|_F^2 = \sum_{i=1}^{\min\{m,n\}} \sigma_i^2$

(3) $\|A\|_{op} = \sigma_1$

[31] The ℓ_1 norm is notable for promoting sparsity when one attempts to minimize it to solve underdetermined linear systems. This is the key idea behind "Compressed Sensing", and plays a crucial role in many imaging/sensing technologies. You can read more about it in Section 12 of [BM23] or Chapter 10 of [BSS] and references therein.

(4) $\|A\|_{op} \leq \|A\|_F \leq \sqrt{\min\{m,n\}}\|A\|_{op}$.

Challenge 59 ($\star$)**.** Prove Further Proposition 58.[32]

8.3. **Some Mathematical Open Problems.** Now that we have covered the notion of eigenvalues and eigenvectors, there are a few fascinating open questions we can state. These are questions (or conjectures), that we currently do now know the answer to (or that we are not sure they are true). I have a list of 42 open problems in some lecture notes [Ban16] I wrote almost a decade ago, some have been solved in the meantime, but many remain open. I write below a few for which you have all the necessary background to understand: Let me know if you solve any of them; regardless of whether its days or decades from now, I will be very happy to hear about your solution!

Conjecture 60 (Hadamard conjecture)**.** For any n multiple of 4 there exists an Hadamard matrix H that is $n \times n$.

An Hadamard matrix $H \in \mathbb{R}^{n\times n}$ is a matrix with only entries 1 or -1 that is a multiple of an orthogonal matrix. In other words $H_{i,j} = \pm 1$ for all i, j and $H^\top H = nI$. Yet in other words: the columns of H are an orthogonal basis for $\mathbb{R}^n$ formed with only vectors with entries ± 1.

Open Problem 61 (Mutually Unbiased Bases)**.** See Open Problem 6.2 in [Ban16].

Conjecture 62 (Zauner's Conjecture)**.** See Open Problem 6.3 in [Ban16].

Conjecture 63 (Komlos Conjecture)**.** See Open Problem 0.1 in [Ban16].

Conjecture 64 (Matrix Spencer Conjecture)**.** See Open Problem 4.3 in [Ban16].

Open Problem 65 (Rank of the Matrix Multiplication Tensor)**.** What is the rank of the Matrix Multiplication Tensor corresponding to multiplication of 3×3 matrices.

A $d_1 \times d_2 \times d_3$ tensor T is what we can think of as a cubic matrix. It has $d_1 d_2 d_3$ entries given by T_{ijl}. We say T has rank r if r is the smallest integer such that we can write

$$T = \sum_{k=1}^{r} a_k \otimes b_k \otimes c_k,$$

[32] Hint: The order I chose for Further Proposition 58 was so that it is easiest to prove these properties in this order. This is a good exercise to help consolidate your understanding of the SVD, and other concepts in this course.

for $a_k \in \mathbb{R}^{d_1}, b_k \in \mathbb{R}^{d_2}, c_k \in \mathbb{R}^{d_3}$, for $k = 1, \dots, r$. In other words

$$T_{ijl} = \sum_{k=1}^{r} (a_k)_i (b_k)_j (c_k)_l.$$

Recall Proposition 8.1.4 to see why for matrices this corresponds to the notion of rank we have been using. While computing the rank of a matrix is computationally easy, doing so for tensors is notoriously difficult (because they lack a spectral theory of eigenvalues and eigenvectors).

There is a way to think of Strassen's algorithm (that you saw in a CS Lens in Part I of the course) in terms of a decomposition of a certain Tensor in terms of rank-1 tensors. In this description we focus on $n \times n$ matrices, but the same thing can be done for rectangular matrices.

The $n \times n$ matrix multiplication tensor is a $n^2 \times n^2 \times n^2$ tensor, where each dimension is indexed by pairs $(i_1, i_2), (j_1, j_2), (l_1, l_2)$ and T is given by

$$T_{(i_1,i_2),(j_1,j_2),(l_1,l_2)} = \begin{cases} 1 & \text{if} \quad i_1 = j_1, j_2 = l_1, l_2 = i_2 \\ 0 & \text{o.w.} \end{cases}.$$

Strassen's algorithm can be viewed as the fact that the rank of the 2×2 matrix multiplication tensor (a $4 \times 4 \times 4$ tensor) is ≤ 7. The rank of the 3×3 matrix multiplication tensor (a $9 \times 9 \times 9$ tensor) remains unknown.[33] [34]

Conjecture 66 (The Paley ETF Conjecture)**.** See Open Problem 6.4 in [Ban16] (see also Open Problem 5.1. in the same reference).[35]

Conjecture 67 (Ellipsoid Problem)**.** See Conjecture 1.1. in either https://arxiv.org/pdf/2307.01181.pdf or https://arxiv.org/pdf/2310.05787.pdf.[36]

[33] To the best of my knowledge, the current "world records" for lower and upper bounds are 19 and 23, see for example https://mathoverflow.net/questions/249256/best-known-bounds-on-border-ranks-of-small-matrix-multiplication-tensors?noredirect=1&lq=1 or https://mathoverflow.net/questions/151058/best-known-bounds-on-tensor-rank-of-matrix-multiplication-of-3x3-matrices.

[34] See https://www.youtube.com/watch?v=fDAPJ7rvcUw for a very nice description of how AI methods found a better low rank decomposition for the matrix multiplication tensor for some dimensions, and https://www.nature.com/articles/s41586-022-05172-4 for the paper the video discusses (make sure to take a look at the table in Figure 3 in that article).

[35] This one needs some (light) Number Theory background to understand. I posed this one (with collaborators) and spent many hours trying to make progress on it...

[36] This one needs some (light) Probability Theory to understand

Acknowledgements. Many thanks to all the Linear Algebra teaching team! A particularly shout out to many of you that caught countless typos on these notes and gave countless suggestions that improve them! Thanks (a partial list): Bernd Gärtner, Sebastian Haslebacher, Stefan Kuhlmann, Felix Breuer, Till Schnabel, Mattia Taiana, Tanguiy Magne, Aviv Segall, Matthieu Croci, Sergey Prokudin, Mia Filic, Sofia Giampietro, Seyedmorteza Sadat, Mark Sosman, Elia Trachsel, Silvan Bolt.

Appendix A. Some Important Preliminaries and Remarks on Notation

To follow these notes the reader needs to be familiar with basics of vector and matrix operations and manipulations; understand what is dimension of a subspace, and in particular that is well-defined (that every basis of a subspace has the same size); and understand what is the rank of a matrix (and in particular that the dimension of the column space and the row space are the same). Even though Gaussian Elimination is not a core ingredient of this part of the course, we still assume that the reader is familiar with it. The students of 401-0131-00L are familiar with all this via Part I of this course.

Some further important preliminaries and/or remarks:

(1) The dot product $x \cdot y$ between two real valued vectors is sometimes also called inner product and written as $\langle x, y \rangle$ (it is equal to $x^\top y$). For $\mathbb{C}^n$ the inner product is given by $\langle x, y \rangle = y^* x$.

(2) Matrix Factorization for A an $m \times n$ matrix with rank r:
$A = CR$,
C is $m \times r$ with linearly independent columns (they are the first r linearly independent columns of A). R is $r \times n$, it is upper triangular (i.e. $R_{ij} = 0$ if $i > j$), and it has an $r \times r$ identity as a submatrix, corresponding to the locations of the first r linearly independent columns of A.

(3) For V a subspace (or a vector space) with dimension n the following holds:
- Any basis of V has size n.
- Any spanning set of V has size $\geq n$.
- Any spanning set of V with size n is also a basis.
- Any set of linearly independent vectors in V has size $\leq n$.
- Any set of linearly independent vectors in V with size n is also a basis.

Appendix B. A "Simple proof" of the Fundamental Theorem of Algebra

In this appendix we present a brief sketch of a (relatively) simple proof of the Fundamental Theorem of Algebra I learned from Alessio Figalli.

Let $P(z)$ be a polynomial of degree n. Without loss of generality we can assume it is monic $P(z) = z^n + \alpha_{n-1}z^{n-1} + \cdots + \alpha_0$. Suppose $P(z)$ has no zeros/roots. There is a $r \in \mathbb{R}$ large enough such that the infimum of $|P(z)|$ inside the close disc D_r of radius r centered at zero is smaller than that outside the disc D_r (because far from the origin the term z^n dominates and forces $|P(z)|$ to be large outside of D_r. Since D_r is a compact set and $|P(z)|$ is continuous it needs to attain its minimum[37] at a point $z_0 \in D_r$. Note that $P(z_0) \neq 0$. Write $Q(z) = P(z - z_0)$, it is also a polynomial of degree n, $Q(z) = \beta_0 + \beta_1 z + \beta_2 z^2 + \cdots + z^n$. Notice that $\beta_0 = P(z_0)$. let k be the first coefficient of $Q(z)$ (not including β_0) that is nonzero (meaning that $\beta_k \neq 0$ but $\beta_i = 0$ for all $0 < i < k$. Then $Q(z) = \beta_0 + \beta_k z^k + \beta_{k+1} z^k + \cdots$. Take $\varepsilon > 0$ arbitrarily small and consider $Q\left(\varepsilon\left(-\frac{\beta_0}{\beta_k}\right)^{\frac{1}{k}}\right)$. It is not difficult to see that for ε small enough the higher order terms are negligible and the term $\beta_0 + \beta_k z^k$ has smaller modulus and so one can pick ε such that $\left|Q\left(\varepsilon\left(-\frac{\beta_0}{\beta_k}\right)^{\frac{1}{k}}\right)\right| < |Q(0)|$ which is a contradiction with the fact that $|P(z_0)|$ was minimum.

References[38]

[Ban16] Afonso S. Bandeira. Ten lectures and forty-two open problems in the mathematics of data science. *Available online at:* `https://people.math.ethz.ch/~abandeira/TenLecturesFortyTwoProblems.pdf`. *See also* `https://ocw.mit.edu/courses/18-s096-topics-in-mathematics-of-data-science-fall-2015/`, 2016.

[BM23] Afonso S. Bandeira and Antoine Maillard. Mathematics of signals, networks, and learning. *Available online at:* `https://anmaillard.github.io/teaching/msnl_spring_2023.pdf`. *Videos from an earlier version of the course available at* `https://youtube.com/playlist?list=PLiud-28tsatL0MbfJFQQS7MYkrFrujCYp`, 2023.

[BSS] A. S. Bandeira, A. Singer, and T. Strohmer. Mathematics of data science. *Book draft available at* `https://people.math.ethz.ch/~abandeira/BandeiraSingerStrohmer-MDS-draft.pdf`. *Videos available at:* `https://www.youtube.com/playlist?list=PLiud-28tsatIKUitdoH3EEUZL-9i516IL`.

[Str23] Gilbert Strang. *Introduction to Linear Algebra. (Table of contents available at* `https://math.mit.edu/~gs/linearalgebra/ila6/indexila6.html`*).* Wellesley - Cambridge Press., sixth edition, 2023.

[37] This part needs some extra analysis/topology background: the fact that continuous functions on a compact (think closed and bounded) set needs to attain a minimum. You will learn about this in Analysis. Perhaps not surprisingly, the "other proof" of Corollary 7.3.8 that does not involve complex numbers, also needs this fact.

[38] In some PDF viewers the ∼ in the urls above does not show as the correct character, if the link appears broken delete the ˜ and write a new ∼ on the url.