

LINEAR ALGEBRA

Dinh Huu Nguyen, Fall 2014

Abstract: lecture notes for Advanced Linear Algebra at John von Neumann Institute, Vietnam, Fall 2014.

CONTENTS

Part 1. Linear Algebra	1
1. Vector Spaces	1
1.1. Basic Objects	1
1.2. Inner Product	4
1.3. Norm	5
1.4. Distance between Vectors	6
1.5. Angle between Vectors	6
2. Linear Maps between Vector Spaces	7
2.1. Linear Maps	7
2.2. Kernel, Nullity, Image, Rank	11
3. Matrices	13
3.1. Partition	14
3.2. Addition	14
3.3. Multiplication	14
3.4. Transposition	17
3.5. Some Matrices	17
3.6. Invertible Matrices and Their Inverses	19
3.7. Row Operations	22
3.8. Determinant	24
3.9. Trace	27
3.10. Eigenvalues, Eigenvectors and Eigenvalue Decompositions	28
3.11. Singular Values, Singular Vectors and Singular Value Decomposition	31
Part 2. Matrix Algorithms	33
4. Complexity of Matrix Algorithms	33
5. Cholesky Decomposition	34
6. LU Decomposition	35
6.1. LU Decomposition without Pivoting	37
6.2. Permutation Matrices	38
6.3. LU Decomposition with Pivoting	38
6.4. Effect of Rounding in Using LU Decomposition	39
7. QR Decomposition	40

8.	Least Square Problem	41
8.1.	Cholesky Decomposition to Solve Least Square Problem	42
8.2.	QR Decomposition to Solve Least Square Problem	43
9.	Least Norm Problem	44
9.1.	Cholesky Decomposition to Solve Least Norm Problem	45
9.2.	QR Decomposition to Solve Least Norm Problem	46

Part 1. Linear Algebra

Linear algebra is central to both pure and applied mathematics. We study vector spaces and linear maps between them over a field. Most of the times, this field is a general field F . Other times, this field is the real numbers \mathbb{R} .

1. VECTOR SPACES

1.1. **Basic Objects.** We begin with the usual Euclidean spaces

$$\mathbb{R} = \{\text{all real numbers}\}$$

$$\mathbb{R} \times \dots \times \mathbb{R} = \mathbb{R}^n = \{\text{all } (x_1, \dots, x_n), x_i \in \mathbb{R}\}, n \geq 2$$

Each element (x_1, \dots, x_n) is called an n -tuple and each x_i is called its i^{th} component or i^{th} coordinate. Like real numbers, the elements in \mathbb{R}^n can be added

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

and scaled by a real number

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$$

for all $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n, a \in \mathbb{R}$. These algebraic operations impose a structure on \mathbb{R}^n . We consider its abstract generalization.

Definition 1.1. A vector space over a field F is a set V together with a binary operation $+$ and a scalar multiplication \cdot that satisfy the following axioms

1. (closure under addition) $v + w \in V$ for any $v, w \in V$.
2. (associativity of addition) $(u + v) + w = u + (v + w)$ for all $u, v, w \in V$.
3. (commutativity of addition) $v + w = w + v$.
4. (identity element under addition) there exists an element $0 \in V$ such that $0 + v = v + 0 = v$ for all $v \in V$.
5. (inverse element under addition) there exists an element $-v$ such that $v + (-v) = -v + v = 0$ for all $v \in V$.
6. (closure under scalar multiplication) $a \cdot v \in V$ for any $a \in F$ and $v \in V$.
7. (distributivity of scalar multiplication with respect to vector addition) $a \cdot (v + w) = a \cdot v + a \cdot w$.
8. (distributivity of scalar multiplication with respect to field addition) $(a + b) \cdot v = a \cdot v + b \cdot v$.
9. (compatibility of scalar multiplication with field multiplication) $(ab) \cdot v = a \cdot (b \cdot v)$.
10. (identity element of scalar multiplication) $1 \cdot v = v$ for $1 \in F$ and any $v \in V$.

For those who have studied abstract algebra, the first five axioms mean V is a group under $+$ and the next five axioms mean V is an F -module. The elements in V are called vectors while the elements in F are called scalars. We denote this vector space structure by $(V, +, \cdot_F)$ or $(V, +, \cdot)$ or V/F or simply V . Below are some examples.

Example 1.2. The set $V = \{*\}$ a single point over the field \mathbb{Q} under the trivial $+$ and \cdot is a vector space. It is called the zero vector space and denoted by $\{0\}$. The same holds when we replace \mathbb{Q} with any field F .

Example 1.3. The plane $\mathbb{R}^2 = \{(x, y) \text{ with } x, y \in \mathbb{R}\}$ over the field \mathbb{R} under the usual operations $+$ and \cdot is a vector space. More generally, the space $\mathbb{R}^n = \{(x_1, \dots, x_n) \text{ with } x_i \in \mathbb{R}\}$ over the field \mathbb{R} under the usual operations $+$ and \cdot is a vector space.

Example 1.4. The rational plane $\mathbb{Q}^2 = \{(x, y) \text{ with } x, y \in \mathbb{Q}\}$ over the field \mathbb{R} under the usual operations $+$ and \cdot is not a vector space.

Example 1.5. The set $S = \{\sum_{i=1}^n a_i x^i\}$ of all finite sums of length n where $a_i \in \mathbb{C}$ and x is an indeterminate over the field \mathbb{C} under the usual operations $+$ and \cdot is a vector space.

Example 1.6. We consider different classes of maps from \mathbb{R}^n to \mathbb{R} .

- A map $\mathbb{R}^n \xrightarrow{f} \mathbb{R}, (x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$ is called linear if $f(av + bw) = af(v) + bf(w)$ for any $a, b \in \mathbb{R}, v, w \in \mathbb{R}^n$. If we define addition $f + g$ as $(f + g)(v) = f(v) + g(v)$ and scalar multiplication as $(a \cdot f)(v) = af(v)$ then the set $L(\mathbb{R}^n, \mathbb{R}) = \{\text{all linear maps } \mathbb{R}^n \xrightarrow{f} \mathbb{R}\}$ over the field \mathbb{R} under $+$ and \cdot is a vector space.
- More generally, a map $\mathbb{R}^n \xrightarrow{g} \mathbb{R}, (x_1, \dots, x_n) \mapsto g(x_1, \dots, x_n)$ is called affine if $g(v) = f(v) + a$ for some linear map f and some $a \in \mathbb{R}$. One can verify that this condition is equivalent to the condition $g(av + bw) = af(v) + bf(w)$ for any $a + b = 1$ and $v, w \in \mathbb{R}^n$. The set $M(\mathbb{R}^n, \mathbb{R}) = \{\text{all affine maps } \mathbb{R}^n \xrightarrow{g} \mathbb{R}\}$ over the field \mathbb{R} under operations $+$ and \cdot is a vector space.
- Most generally, the set $N(\mathbb{R}^n, \mathbb{R}) = \{\text{all maps } \mathbb{R}^n \xrightarrow{h} \mathbb{R}\}$ over the field \mathbb{R} under same operations is a vector space.

One can see that $L(\mathbb{R}^n, \mathbb{R}) \subset M(\mathbb{R}^n, \mathbb{R}) \subset N(\mathbb{R}^n, \mathbb{R})$ and the operations on each subset agree with the operations from the larger set. So in a sense $L(\mathbb{R}^n, \mathbb{R})$ is a subspace of $M(\mathbb{R}^n, \mathbb{R})$ which is a subspace of $N(\mathbb{R}^n, \mathbb{R})$. Abstractly, whenever we have objects with some structure, we also consider subobjects with the same structure.

Definition 1.7. A subset $U \subset V$ of a vector space $(V, +, \cdot)$ is called a subspace if U under $+$ and \cdot is also a vector space over F .

Example 1.8. In example 1.6 $L(\mathbb{R}^n, \mathbb{R}) \subset M(\mathbb{R}^n, \mathbb{R}) \subset N(\mathbb{R}^n, \mathbb{R})$ as subspaces over \mathbb{R} . We will know more about them later.

Example 1.9. We can view \mathbb{R}^2 as a subspace $U = \{(x, y, 0), x, y \in \mathbb{R}\} \subset \mathbb{R}^3$. Why isn't $U' = \{(x, y, 1), x, y \in \mathbb{R}\} \subset \mathbb{R}^3$ a subspace?

We associate the first invariant to each vector space V over a field F , generalizing the notion of dimension that we often speak of for \mathbb{R}^n .

Definition 1.10. A finite sum $\sum_{i=1}^n a_i v_i = a_1 v_1 + \dots + a_n v_n$ with $a_i \in F, v_i \in V$ is called a linear combination of v_1, \dots, v_n . The set of all linear combinations of v_1, \dots, v_n is called their span and denoted by $\text{Span}(v_1, \dots, v_n)$. If there exist a_1, \dots, a_n , not all zero, such that $a_1 v_1 + \dots + a_n v_n = 0$ then we say the v_1, \dots, v_n are linearly dependent. Else we say they are linearly independent.

Example 1.11. It is easy to verify that $(1, 0), (0, 1)$ are linearly independent in \mathbb{R}^2 while $(2, 1, 1), (0, 1, 2), (4, 5, 8)$ are linearly dependent in \mathbb{R}^3 .

Example 1.12. Any pair $x^i, x^j, i \neq j$ in example 1.5 are linearly independent.

Definition 1.13. A subset $B = \{v_i\}_{i \in I}, I$ an indexing set and $v_i \in V$, is called a basis for V if B is linearly independent and $\text{Span}(B) = V$.

In this course, we only consider vector spaces with finite basis $B = \{v_1, \dots, v_n\}$. By definition, every $v \in V$ can be written as a linear combination $v = \sum_{i=1}^n a_i v_i$ and such representation is unique by linear independence of B . The tuple (a_1, \dots, a_n) is called the coordinate form of v . One can imagine that it has different representations and different coordinate forms in different bases.

Example 1.14. If we choose $B = \{(1, 0), (0, 1)\}$ as basis for \mathbb{R}^2 then $v = (3, 4)$ can be written as $3(1, 0) + 4(0, 1)$ with coordinate form $(3, 4)$. If we choose $B' = \{(0, 1), (1, 0)\}$ then $v = 4(0, 1) + 3(1, 0)$ with coordinate form $(4, 3)$. If we choose $B'' = \{(1, 0), (0, 2)\}$ then $v = 3(1, 0) + 2(0, 2)$ with coordinate form $(3, 2)$.

Exercise 1.15. Find the linear representation and coordinate form for $(3, 4)$ in basis $B''' = \{(1/\sqrt{2}, 1/\sqrt{2}), (-1/\sqrt{2}, 1/\sqrt{2})\}$.

The previous examples show no basis is more special than the rest, only some bases are nicer for computation than others. Moreover, the order in each basis affects coordinate form representation. What is true is every vector space has a basis and all bases of V have the same size. This is the first invariant we associate to each vector space V over a field F .

Definition 1.16. We define the dimension $\dim(V/F)$ of V/F as the size of any basis for V .

Example 1.17. The vectors $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ form a basis for \mathbb{R}^n over \mathbb{R} since they are clearly linearly independent and any (x_1, \dots, x_n) can be written as $x_1(1, 0, \dots, 0) + \dots + x_n(0, \dots, 1), x_i \in \mathbb{R}$. Therefore the dimension of \mathbb{R}^n over \mathbb{R} is n as conventionally known. They do not form a basis for \mathbb{R}^n over \mathbb{Q} .

Example 1.18. The vectors x, x^2, \dots, x^n together form a basis for our vector space V over \mathbb{C} in example 1.5. Its dimension is n . Viewed as a vector space over \mathbb{R} , however V has dimension $2n$ since one of its bases is $x, ix, x^2, ix^2, \dots, x^n, ix^n$.

Example 1.19. The vector space N in example 1.6 does not have a finite basis. In fact, any of its bases must be uncountable. We say it has infinite dimension over \mathbb{R} .

1.2. Inner Product. We begin this subsection by considering vector spaces over \mathbb{R} . If they are to enjoy multiplication $V \times V \longrightarrow \mathbb{R}, (v, w) \mapsto v \cdot w$, we expect the following.

Definition 1.20. An inner product on a vector space V over \mathbb{R} is any map $V \times V \xrightarrow{\langle -, - \rangle} \mathbb{R}$ that satisfies the following axioms,

1. (symmetry) $\langle v, w \rangle = \langle w, v \rangle$.
2. (linearity) $\langle a \cdot u + b \cdot v, w \rangle = a \langle u, w \rangle + b \langle v, w \rangle$.
3. (positive definiteness) $\langle v, v \rangle \geq 0$ for all $v \in V$, with equality iff $v = 0$.

A vector space V over \mathbb{R} equipped with an inner product is called an inner product space. Note that the product of two vectors is a scalar in \mathbb{R} .

Example 1.21. We can turn \mathbb{R}^n into an inner product space as follows. Given two vectors $v = (x_1, \dots, x_n), w = (y_1, \dots, y_n) \in \mathbb{R}^n$ we define their inner product to be $\langle v, w \rangle = \sum_{i=1}^n x_i y_i = x_1 y_1 + \dots + x_n y_n$. One can verify that this newly minted product satisfies the above three axioms.

- a. If $v = (3, 4)$ and $w = (5, 6)$ in \mathbb{R}^2 then $\langle v, w \rangle = 3 \cdot 5 + 4 \cdot 6 = 39$
- b. If $v = (x_1, \dots, x_n)$ and $w = (y_1, \dots, y_n)$ in \mathbb{R}^n where $x_i, y_i \in \{0, 1\}$ then $\langle v, w \rangle$ is the number of indices i where $a_i = b_i = 1$.
- c. If $v = (x_1, \dots, x_n)$ then $\langle v, e_i \rangle = x_i$ its i^{th} coordinate.

If we look closely, we will see that any inner product $V \times V \xrightarrow{\langle -, - \rangle} \mathbb{R}$ is completely determined by $\langle v_i, v_j \rangle, 1 \leq i, j \leq n$ for any basis $B = \{v_1, \dots, v_n\}$ by linearity. So if we drop the requirement of positive definiteness, we can define other inner products for V by setting $\langle v_i, v_j \rangle = \langle v_j, v_i \rangle = \alpha_{ij}$ (for symmetry) and extending by linearity.

$$V \times V \xrightarrow{\langle -, - \rangle} \mathbb{R}$$

$$(v, w) = \left(\sum_{i=1}^n a_i v_i, \sum_{i=1}^n b_i v_i \right) \mapsto \sum_{i,j} a_i b_j \alpha_{ij}$$

Example 1.22. For \mathbb{R}^n over \mathbb{R} , if we set $\langle e_i, e_j \rangle = \delta_{ij}$ then we get the inner product in example 1.21. On the other hand, if we set $\langle e_i, e_j \rangle = i + j$ then $\langle (3, 4), (5, 6) \rangle = \langle 3e_1 + 4e_2, 5e_1 + 6e_2 \rangle = 15 \langle e_1, e_1 \rangle + (18 + 20) \langle e_1, e_2 \rangle + 24 \langle e_2, e_2 \rangle = 15 \cdot 2 + 38 \cdot 3 + 24 \cdot 4 = 240$.

We can use this approach to define inner products for vectors space over a general F .

$$V \times V \xrightarrow{\langle -, - \rangle} F$$

$$(v_i, v_j) \mapsto \alpha_{ij}$$

$$(v_j, v_i) \mapsto \alpha_{ij}$$

$$(v, w) = \left(\sum_{i=1}^n a_i v_i, \sum_{i=1}^n b_i v_i \right) \mapsto \sum_{i,j} a_i b_j \alpha_{ij}$$

1.3. Norm. Given a vector space V over \mathbb{R} we want to make precise how large each vector $v \in V$ is. Of course, there are different ways to do so but they all must meet certain expectations.

Definition 1.23. A norm on V over \mathbb{R} is a map $V \xrightarrow{\|-\|} \mathbb{R}$ that satisfies,

1. (positive definiteness) $\|v\| \geq 0$, with equality iff $v = 0$.
2. (homogeneity) $\|a \cdot v\| = |a| \|v\|$.
3. (triangle inequality) $\|v + w\| \leq \|v\| + \|w\|$.

Any vector space V over \mathbb{R} with norm is called a normed space.

Example 1.24. One obvious way to define a norm on \mathbb{R}^n is $\|(x_1, \dots, x_n)\| = |x_1| + \dots + |x_n|$. This is called the 1-norm and denoted by $\| - \|_1$.

Example 1.25. Another norm we have on \mathbb{R}^n is the usual Euclidean norm $\|(x_1, \dots, x_n)\| = \sqrt{x_1^2 + \dots + x_n^2} = \sqrt{\langle v, v \rangle}$ where $\langle -, - \rangle$ is the usual inner product for \mathbb{R}^n . This is called the 2-norm and denoted by $\| - \|_2$. The Euclidean norm is related to the root mean square value RMS of a vector v (instead of mean or mean square), defined as $\text{RMS}(v) = \sqrt{\frac{1}{n}(x_1^2 + \dots + x_n^2)} = \frac{1}{\sqrt{n}}\|v\|$. This quantity roughly tells us about the typical value of the coordinates x_i with respect to n .

Example 1.26. More generally we define the p -norm on \mathbb{R}^n as $\|(x_1, \dots, x_n)\|_p = \sqrt[p]{|x_1|^p + \dots + |x_n|^p}$ for any $1 \leq p < \infty$.

Example 1.27. We define the ∞ -norm on \mathbb{R}^n as $\|(x_1, \dots, x_n)\|_\infty = \max\{|x_1|, \dots, |x_n|\}$.

Exercise 1.28. Draw all the vectors of norm 1 in \mathbb{R}^2 , where norm here is the 1-norm, the p -norm for $1 < p < 2$, the 2-norm, the p -norm for $2 < p < \infty$, and the ∞ -norm.

We just saw that $\|v\|_2 = \sqrt{\langle v, v \rangle}$ where $\langle -, - \rangle$ is the usual inner product for \mathbb{R}^n . In general, any inner product $\langle -, - \rangle$ on a vector space V over \mathbb{R} induces a map $V \xrightarrow{\| - \|} \mathbb{R}, v \mapsto \|v\| = \sqrt{\langle v, v \rangle}$. Such definition easily clears the first two axioms of being a norm due to the properties of inner product. We establish a nice theorem that would imply the triangle inequality axiom.

Theorem 1.29. (Cauchy-Schwarz Inequality) *For all v, w in an inner product space V with induced norm $\| - \|$ we have $|\langle v, w \rangle| \leq \|v\| \|w\|$. Moreover, equality holds iff v, w are linearly dependent.*

Proof. If either $v = 0$ or $w = 0$ then inequality holds. Else consider the quadratic polynomial $p(t) = \|tv + w\|^2 = \langle tv + w, tv + w \rangle = \langle v, v \rangle t^2 + 2\langle v, w \rangle t + \langle w, w \rangle$. Being a square, $p(t) \geq 0$, hence its discriminant $4\langle v, w \rangle^2 - 4\langle v, v \rangle \langle w, w \rangle \leq 0$, or $\langle v, w \rangle^2 \leq \langle v, v \rangle \langle w, w \rangle$. Equality holds iff the discriminant is 0 iff $p(t) = 0$ iff $tv + w = 0$ iff w is a multiple of v . \square

Do you see why we considered such polynomial $p(t)$ as to show us exactly what we needed?

Corollary 1.30. (Triangle Inequality) *The induced norm $\| - \|$ from an inner product on V satisfies triangle inequality $\|v + w\| \leq \|v\| + \|w\|$, all $v, w \in V$.*

Proof. Clearly $\|v + w\|^2 = \langle v + w, v + w \rangle = \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle = \|v\|^2 + 2\langle v, w \rangle + \|w\|^2 \leq \|v\|^2 + 2\|v\| \|w\| + \|w\|^2 = (\|v\| + \|w\|)^2$, from which our claim follows. \square

Thus an inner product on V induces a norm.

1.4. Distance between Vectors. A norm in turn induces distance.

Definition 1.31. For any vectors v, w in a vector space V equipped with norm $\| - \|$ we define their distance to be $\text{dist}(v, w) = \|v - w\|$.

Example 1.32. All the above norms on \mathbb{R}^n induce different distances between vectors in \mathbb{R}^n , though some of them are rather antiintuitive.

1.5. Angle between Vectors. As an inner product $\langle -, - \rangle$ induces a norm $\| - \|$ for V , we notice there is a relationship between $\langle v, w \rangle$ and $\|v\|\|w\|$ for any pair $v, w \in V$.

Example 1.33. When v, w are in the same direction, $w = av \in V$ for some positive $a \in \mathbb{R}$ and $\langle v, w \rangle = a\langle v, v \rangle = a\|v\|^2 = |a|\|v\|\|v\| = \|v\|\|w\|$. When v, w are in opposite direction, $w = -av$ for some positive a and $\langle v, w \rangle = -\|v\|\|w\|$.

Hence we suspect that the ratio $\frac{\langle v, w \rangle}{\|v\|\|w\|}$ bears some correlation between v and w , perhaps how v lines up against w .

Definition 1.34. For any nonzero vectors v, w in a vector space V equipped with inner product $\langle -, - \rangle$ and induced norm $\| - \|$ we define their correlation coefficient to be $\rho(v, w) = \frac{\langle v, w \rangle}{\|v\|\|w\|}$.

This correlation coefficient, viewed as a map $V \times V \xrightarrow{\rho} \mathbb{R}$ is surely symmetric. Its range is $[-1, 1]$ by Cauchy-Schwarz inequality. Two vectors v, w are said to be highly correlated if $\rho(v, w)$ is close to 1, uncorrelated if $\rho(v, w) = 0$, and highly anticorrelated if $\rho(v, w)$ is close to -1.

Example 1.35. Consider $u = (0.1, -0.3, 1.3, -0.3, -3.3)$, $v = (0.2, -0.4, 3.2, -0.8, -5.2)$, $w = (1.8, -1.0, -0.6, 1.4, -0.2)$. Then $\|u\| = 3.57$, $\|v\| = 6.17$, $\|w\| = 2.57$, $\langle u, v \rangle = 21.7$, $\langle u, w \rangle = -0.06$, $\rho(u, v) = 0.98$, $\rho(u, w) = -0.007$. Therefore u and v are more correlated than u and w are (v is roughly twice u).

Example 1.36. The set $RV((\Omega, \mathcal{F}, P), (\mathbb{R}, \mathcal{B}(\mathbb{R})))$ of all random variables from (Ω, \mathcal{F}, P) to $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ form a vector space over \mathbb{R} . The subset $RVF((\Omega, \mathcal{F}, P), (\mathbb{R}, \mathcal{B}(\mathbb{R})))$ of all random variables with finite second moment and zero mean form a subspace of $RV((\Omega, \mathcal{F}, P), (\mathbb{R}, \mathcal{B}(\mathbb{R})))$. If we define $\langle X, Y \rangle = \text{cov}(X, Y)$ then

1. (symmetry) $\langle X, Y \rangle = \langle Y, X \rangle$.
2. (linearity) $\langle aX + bY, Z \rangle = a\langle X, Z \rangle + b\langle Y, Z \rangle$.
3. (positive semidefiniteness) $\langle X, X \rangle \geq 0$ with equality iff X is constant.

Therefore, $\langle -, - \rangle$ is not quite an inner product for $RV((\Omega, \mathcal{F}, P), (\mathbb{R}, \mathcal{B}(\mathbb{R})))$. However, it is an inner product for the subspace $RVF((\Omega, \mathcal{F}, P), (\mathbb{R}, \mathcal{B}(\mathbb{R})))$ of all random variables with finite second moment and zero mean. This inner product induces the norm $\|X\| = \sqrt{\langle X, X \rangle} = \sqrt{\text{cov}(X, X)} = \sqrt{\text{var}(X)} = \sigma_X$ and the correlation coefficient $\rho(X, Y) = \text{corr}(X, Y)$ in probability theory.

From correlation coefficient we define angle between two vectors.

Definition 1.37. For any nonzero vectors v, w in a vector space V equipped with inner product $\langle -, - \rangle$, induced norm $\| - \|$ and correlation coefficient $\rho(-, -)$ we define their angle to be $\angle(v, w) = \arccos(\rho(v, w)) = \arccos\left(\frac{\langle v, w \rangle}{\|v\|\|w\|}\right)$.

Example 1.38. The usual inner product for \mathbb{R}^n and its induced norm, distance, correlation coefficient and angle give us the usual geometry for $\mathbb{R}^n, 0 \leq n \leq 3$ while generalizing to $\mathbb{R}^n, n \geq 4$. Another inner product for \mathbb{R}^n would give us another, albeit strange geometry.

For two vectors v, w in an inner product space V with induced norm, correlation coefficient and angle, if $\angle(v, w) = 0^\circ$, i.e. they have correlation coefficient 1 then each vector is a positive multiple of the other and we say v, w are aligned. If $0^\circ < \angle(v, w) < 90^\circ$, i.e. they have positive correlation coefficient then we say v, w make an acute angle. If $\angle(v, w) = 90^\circ$, i.e. they have correlation coefficient 0 then we say v, w are orthogonal and write $v \perp w$. If $90^\circ < \angle(v, w) < 180^\circ$, i.e. they have negative correlation coefficient then we say v, w make an obtuse angle. Lastly, if $\angle(v, w) = 180^\circ$, i.e. they have correlation coefficient -1 then each vector is a negative multiple of the other and we say v, w are antialigned. We are more interested in orthogonal vectors of norm 1 because they make excellent bases.

Definition 1.39. A vector v in a normed space V is called a unit vector if $\|v\| = 1$.

Any vector $v \in V$ can be easily normalized and replaced by an aligned unit vector $\frac{v}{\|v\|}$.

Definition 1.40. A collection of vectors $\{v_1, \dots, v_n\}$ in an inner product space V with induced norm are said to be orthonormal if each v_i is a unit vector and $v_i \perp v_j$ for any $i \neq j$.

Example 1.41. Both collections $A = \{(1, 0, 0), (0, 1, 0)\}$ and $B = \{(0, 0, -1), (1/\sqrt{2}, 1/\sqrt{2}, 0), (1/\sqrt{2}, -1/\sqrt{2}, 0)\}$ are orthonormal while $C = \{(1, -1, 0), (1, 1, 1)\}$ can be normalized into an orthonormal one.

We can even say a collection $\{v_1, \dots, v_n\}$ are orthonormal if $\langle v_i, v_j \rangle = \delta_{ij}$ for an inner product that does not induce norm and angle. If $v = a_1 v_1 + \dots + a_n v_n$ is a linear combination then surely $\langle v_i, v \rangle = \langle v_i, a_1 v_1 + \dots + a_n v_n \rangle = \sum_{j=1}^n \langle v_i, a_j v_j \rangle = a_i \|v_i\| = a_i$. So taking inner product with v_i picks out the i^{th} coefficient in the linear combination for v , see example 1.21(c). It implies any orthonormal collection $\{v_1, \dots, v_n\}$ are linearly independent. This is most useful when $n = \dim(V)$ and $\{v_1, \dots, v_n\}$ form a basis for V .

2. LINEAR MAPS BETWEEN VECTOR SPACES

2.1. Linear Maps. We step back from vectors within a vector space V/F and consider the relationships between finite dimensional vector spaces over the same field F . Given two vector spaces V/F and W/F we would expect any map between them to respect their linear structures.

Definition 2.1. A map $V \xrightarrow{f} W$ between two vector spaces V, W over F is called linear if $f(av + bw) = af(v) + bf(w)$ for all $v, w \in V$ and $a, b \in F$.

The set of all linear maps from V to W is denoted by $L(V, w)$. We can give it a vector space structure by defining addition $f + g$ where $(f + g)(v) = f(v) + g(v)$ and scalar multiplication $a \cdot f$ where $(a \cdot f)(v) = a \cdot f(v)$. That addition of linear maps is commutative and associative follows from analogous properties for additions in V and in W .

1. (commutativity) $f + g = g + f$.

2. (associativity) $(f + g) + h = f + (g + h)$.

Moreover, composition $U \xrightarrow{f} V \xrightarrow{g} W$ of two linear maps is also linear. One can verify that

1. (distributivity) $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$ and $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$.
2. (associativity) $(f \circ g) \circ h = f \circ (g \circ h)$.

Example 2.2. The trivial map $V \xrightarrow{f} W, v \mapsto 0$ between any two vector spaces is certainly linear.

Example 2.3. The map $\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^3, (x, y) \mapsto (x, y, 0)$ is linear. The image of f is the subspace we described in example 1.9 and this is how we often embed \mathbb{R}^2 into \mathbb{R}^3 . In similar fashion can \mathbb{R}^m be embedded into $\mathbb{R}^n, m \leq n$. The map $\mathbb{R}^2 \xrightarrow{g} \mathbb{R}^3, (x, y) \mapsto (x, y, 1)$ however is not linear.

Example 2.4. Let V be vector space V over F with basis $B = \{v_1, \dots, v_n\}$ and inner product $\langle v_i, v_j \rangle = \langle v_j, v_i \rangle = \alpha_{ij}$. For $v \in V$, the map $V \xrightarrow{f_v} F, w \mapsto \langle v, w \rangle$ is linear by definition of $\langle -, - \rangle$. In particular, if $\langle v_i, v_j \rangle = \delta_{ij}$ and $w = b_1 v_1 + \dots + b_n v_n$ then $f_{v_i}(w) = \langle w, v_i \rangle = b_i$ its i^{th} coordinate with respect to B . See example 1.21(c).

Such maps f_v in fact account for all linear maps from V to F .

Proposition 2.5. For any vector space V over F with basis $B = \{v_1, \dots, v_n\}$ and $\langle v_i, v_j \rangle = \delta_{ij}$, a map $V \xrightarrow{f} F$ is linear iff $f = f_v$ for some $v \in V$.

Proof. It remains to show that for any linear map $V \xrightarrow{f} F$ and any $w = b_1 v_1 + \dots + b_n v_n \in V$ we have $f(w) = b_1 f(v_1) + \dots + b_n f(v_n) = f_{v_1}(w) f(v_1) + \dots + f_{v_n}(w) f(v_n) = (f(v_1) f_{v_1} + \dots + f(v_n) f_{v_n})(w) = f_v(w)$ where $v = f(v_1) v_1 + \dots + f(v_n) v_n$. \square

Corollary 2.6. The vector space $L(V, F)$ has dimension n .

Proof. From the proof of the proposition, any linear map $f = f_v = f(v_1) f_{v_1} + \dots + f(v_n) f_{v_n}$ for $v = f(v_1) v_1 + \dots + f(v_n) v_n$. Furthermore, these $\{f_{v_1}, \dots, f_{v_n}\}$ are linearly independent, hence they form a basis for $L(V, F)$. Summarily, every basis $\{v_1, \dots, v_n\}$ for V corresponds to a basis $\{f_{v_1}, \dots, f_{v_n}\}$ for $L(V, F)$. Therefore V and $L(V, F)$ share the same dimension n . \square

Each f_v is called the dual of v and denoted by v^* . The space $L(V, F)$ is called the dual of V and denoted by V^* . We now look at some examples.

Example 2.7. Taking average of the coordinates $\mathbb{R}^n \xrightarrow{f} \mathbb{R}, (x_1, \dots, x_n) \mapsto (x_1 + \dots + x_n)/n$ is linear. One sees $f = f_v$ where $v = (1/n, \dots, 1/n)$.

Example 2.8. Taking maximum of the coordinates $\mathbb{R}^n \xrightarrow{f} \mathbb{R}, (x_1, \dots, x_n) \mapsto \max\{x_1, \dots, x_n\}$ is not linear. To see this, pick $n = 2, v = (1, -1), w = (-1, 1)$. Then $f(v + w) \neq f(v) + f(w)$. Hence $f \neq f_v$ for all $v \in \mathbb{R}^n$.

Corollary 2.6 tells us that $L(\mathbb{R}^n, \mathbb{R})$ has dimension n and $M(\mathbb{R}^n, \mathbb{R})$ has dimension $(n+1)$ in example 1.6. While $M(\mathbb{R}^n, \mathbb{R})$ is much smaller than $N(\mathbb{R}^n, \mathbb{R})$, every continuously

differentiable map $f \in N(\mathbb{R}^n, \mathbb{R})$ has a good affine approximation in $M(\mathbb{R}^n, \mathbb{R})$. Recall that if $\mathbb{R}^n \xrightarrow{f} \mathbb{R}, x \mapsto f(x)$ is a continuously differentiable then we can take the continuous partial derivatives $\frac{\partial f(x)}{\partial x_i}, i = 1, \dots, n$ and form its gradient $\nabla f(x) = (\frac{\partial f(x)}{\partial x_1}, \dots, \frac{\partial f(x)}{\partial x_n})$. The first-order Taylor approximation of f near x is defined as

$$\begin{aligned} f_{\text{aff}}(x') &= (\frac{\partial f(x)}{\partial x_1}, \dots, \frac{\partial f(x)}{\partial x_n})(x' - x)^t + f(x) \\ &= \sum_{i=1}^n \frac{\partial f(x)}{\partial x_i} (x'_i - x_i) + f(x) \\ &= \langle \nabla f(x), (x' - x) \rangle + f(x) \end{aligned}$$

This map f_{aff} is certainly affine and gives a good approximation of f when x' is near x .

Example 2.9. When $n = 1$ this is none other than the usual Taylor approximation $f_{\text{aff}}(x') = f'(x)(x' - x) + f(x)$ we often see.

Example 2.10. Consider $\mathbb{R}^2 \xrightarrow{f} \mathbb{R}, (x_1, x_2) \mapsto e^{x_1+x_2-1} + e^{x_1-x_2-1} + e^{-x_1-1}$. Then

$$\nabla f(x) = (e^{x_1+x_2-1} + e^{x_1-x_2-1} - e^{-x_1-1}, e^{x_1+x_2-1} - e^{x_1-x_2-1})$$

At $(0, 0)$

$$\nabla f((0, 0)) = (1/e, 0)$$

Hence the first-order Taylor approximation of f near $(0, 0)$ is

$$\begin{aligned} f_{\text{aff}}(x) &= \langle \nabla f((0, 0)), x - (0, 0) \rangle + f((0, 0)) \\ &= x_1/e + 3/e \end{aligned}$$

The most notable thing about a linear map $V \xrightarrow{f} W$ is that it is completely determined by what it does to a basis $B = \{v_1, \dots, v_n\}$ for V . More precisely, if we write $v = a_1v_1 + \dots + a_nv_n$ then $f(v) = a_1f(v_1) + \dots + a_nf(v_n)$ by linearity of f . If we also choose a basis $C = \{w_1, \dots, w_m\}$ for W then we can write $f(v_i) = b_{1i}w_1 + \dots + b_{mi}w_m = (b_{1i}, \dots, b_{mi})^t$. Hence

$$\begin{aligned} f(v) &= a_1f(v_1) + \dots + a_nf(v_n) \\ &= a_1(b_{11}, \dots, b_{m1})^t + \dots + a_n(b_{1n}, \dots, b_{mn})^t \\ &= (a_1b_{11} + \dots + a_nb_{1n}, \dots, a_1b_{m1} + \dots + a_nb_{mn})^t \\ &= \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & \vdots & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} (a_1, \dots, a_n)^t \end{aligned}$$

if we define multiplication between an $m \times n$ matrix and an $n \times 1$ matrix as such. We have used the transpose notation t here without having introduced it yet. We state this in a theorem.

Theorem 2.11. Any linear map $V \xrightarrow{f} W$ can be represented by a matrix A_f once V, W are given bases. Conversely any $m \times n$ matrix A is a linear map between a vector space V of dimension n and a vector space W of dimension m .

Proof. It remains to show that as a map, $A(av + a'v') = aA(v) + a'A(v')$, but this follows from definition of matrix multiplication above. \square

When we are given a matrix A without mention of domain V with basis B and codomain W with basis C , they are understood to be F^n with canonical basis $\{e_1, \dots, e_n\}$ and F^m with canonical basis $\{e_1, \dots, e_m\}$. Let us look at some examples.

Example 2.12. The trivial map $V \xrightarrow{0} W, v \mapsto 0$ is linear and represented by the zero matrix 0 with respect to any basis for V and any basis for W .

Example 2.13. For any linear map $V \xrightarrow{A} W$ with respect to basis $\{v_1, \dots, v_n\}$ for V and basis $\{w_1, \dots, w_m\}$ for W , $A(v_i)$ equals the i^{th} column of A .

$$\begin{pmatrix} b_{11} & \dots & b_{1i} & \dots & b_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1} & \dots & b_{ni} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1_i \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} b_{1i} \\ \vdots \\ b_{ni} \end{pmatrix}$$

Exercise 2.14. Consider an inner product space V with basis $B = \{v_1, \dots, v_n\}$ and the vector space F with basis $C = \{1\}$. If $\langle v_i, v_j \rangle = \langle v_j, v_i \rangle = \alpha_{ij}$ and $v = a_1v_1 + \dots + a_nv_n$, find the matrix representation for $V \xrightarrow{f_v} F, w \mapsto \langle v, w \rangle$ in example 2.4 with respect to these bases.

Example 2.15. (Change of basis matrix) The identity map $V \xrightarrow{id} V, v \mapsto v$ is linear. If we choose a basis $B = \{v_1, \dots, v_n\}$ for both domain and codomain then $id(v_i) = v_i = 0v_1 + \dots + 1v_i + \dots + 0v_n$ and id is represented by the identity matrix I . On the other hand, if we choose a different basis $B' = \{v'_1, \dots, v'_n\}$ for codomain then $id(v_i) = v_i = b_{1i}v'_1 + \dots + b_{ni}v'_n$. Hence id is represented by the matrix (b_{ij}) and not I . We call this matrix the change of basis matrix and denote it by $A_{BB'}$. Moreover, the identity map going in the opposite direction is represented by the change of basis matrix $A_{B'B}$. Since composition of these two identity maps is represented by the identity matrix I , it follows that $A_{BB'}A_{B'B} = A_{B'B}A_{BB'} = I$.

Example 2.16. Conversely, the identity matrix I with respect to certain bases for domain and codomain may not represent the identity map. Consider the linear map

$$\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2, (1, 0) \mapsto (1, 0), (0, 1) \mapsto (0, 2)$$

If we choose basis $B = \{e_1, e_2\}$ for both domain and codomain then $(1, 0), (0, 1), (0, 2)$ have coordinates form $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ and the matrix representation for f with

respect to this basis is

$$\begin{aligned} \mathbb{R}^2 &\xrightarrow{\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}} \mathbb{R}^2 \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} &\mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} &\mapsto \begin{pmatrix} 0 \\ 2 \end{pmatrix} \end{aligned}$$

However, if we choose basis $B = \{e_1, e_2\}$ for domain and basis $C = \{e_1, 2e_2\}$ for codomain then $(1, 0), (0, 2)$ have coordinate forms $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and the matrix representation for f with respect to these bases is

$$\begin{aligned} \mathbb{R}^2 &\xrightarrow{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \mathbb{R}^2 \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} &\mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} &\mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$

Example 2.17. (Change of basis for vectors) We continue with example 2.15. For a vector $v = a_1v_1 + \dots + a_nv_n$ with coordinate form (a_1, \dots, a_n) with respect to B , we have

$$\begin{aligned} v &= a_1v_1 + \dots + a_nv_n \\ &= a_1(b_{11}v'_1 + \dots + b_{n1}v'_n) + \dots + a_n(b_{1n}v'_1 + \dots + b_{nn}v'_n) \\ &= (a_1b_{11} + \dots + a_nb_{1n})v'_1 + \dots + (a_1b_{n1} + \dots + a_nb_{nn})v'_n \end{aligned}$$

Hence its new coordinate form with respect to B' is

$$(a_1b_{11} + \dots + a_nb_{1n}, \dots, a_1b_{n1} + \dots + a_nb_{nn})^t = A_{BB'}(a_1, \dots, a_n)^t$$

Exercise 2.18. Compute the change of basis matrix $A_{B''B'''}$ when we move from basis B'' in example 1.14 to basis B''' in exercise 1.15. Use it to compute coordinate form for $(3, 4)$ with respect to B''' and compare it with the result there.

Example 2.19. Reflection across any line in the plane \mathbb{R}^2 with the usual inner product is linear. If we choose an orthonormal basis $\{u_1, u_2\}$ such that $r(u_1) = u_2$ and $r(u_2) = u_1$ then clearly it is represented as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Similarly, reflection across u_1 is linear and represented by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ while projection onto u_1 is represented by $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

2.2. Kernel, Nullity, Image, Rank. The first thing we look at in each linear map $V \xrightarrow{f} W$ is what it annihilates in V and what it covers in W .

Definition 2.20. For any linear map $V \xrightarrow{f} W$ we define $\ker(f) = \{v \in V \text{ such that } f(v) = 0\}$ and $\text{im}(f) = \{w \in W \text{ such that } w = f(v) \text{ for some } v \in V\}$.

One can verify that $\ker(f)$ is a subspace of V and $\text{im}(f)$ is a subspace of W . We say f is injective if $\ker(f) = \{0\}$, f is surjective if $\text{im}(f) = W$, and f is bijective if it is both injective and surjective.

Definition 2.21. For any linear map $V \xrightarrow{f} W$ we define $\text{nullity}(f) = \dim(\ker(f))$, called the nullity of f . We define $\text{rank}(f) = \dim(\text{im}(f))$, called the rank of f .

Clearly f is injective iff $\text{nullity}(f) = 0$ and f is surjective iff $\text{rank}(f) = \dim(W)$. Furthermore, if $\{v_1, \dots, v_k\}$ is a basis for $\ker(f)$ then it can be completed to a basis $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ for V . Write any $V \ni v = a_1v_1 + \dots + a_kv_k + a_{k+1}v_{k+1} + \dots + a_nv_n$ then $f(v) = a_1f(v_1) + \dots + a_kf(v_k) + a_{k+1}f(v_{k+1}) + \dots + a_nf(v_n) = a_{k+1}f(v_{k+1}) + \dots + a_nf(v_n)$. Therefore $\text{im}(f) = \text{Span}(f(v_{k+1}), \dots, f(v_n))$. While $\dim(\ker(f)) = k$, we see $\dim(\text{im}(f)) \leq n - k$. Equality follows from the following theorem.

Theorem 2.22. (*Rank-Nullity*) If $V \xrightarrow{f} W$ is a linear map then $\dim(V) = \text{nullity}(f) + \text{rank}(f)$.

Proof. It remains to show $\{f(v_{k+1}), \dots, f(v_n)\}$ are linearly independent and thus form a basis for $\text{im}(f)$. Suppose $b_{k+1}f(v_{k+1}) + \dots + b_nf(v_n) = 0$ for some $b_{k+1}, \dots, b_n \in F$, then $f(b_{k+1}v_{k+1} + \dots + b_nv_n) = 0$. So $b_{k+1}v_{k+1} + \dots + b_nv_n \in \ker(f)$ and we can write $b_{k+1}v_{k+1} + \dots + b_nv_n = b_1v_1 + \dots + b_kv_k$ for some $b_1, \dots, b_k \in F$. Since the v_i form a basis for V , the b_i must all be 0. In particular, $b_{k+1} = \dots = b_n = 0$. \square

Example 2.23. The zero map $V \xrightarrow{0} W$ has $\text{nullity}(0) = \dim(V)$ and $\text{rank}(0) = 0$ while for $\lambda \neq 0$ scaling $V \xrightarrow{\lambda} V$ has $\text{nullity}(\lambda, \dots, \lambda) = 0$ and $\text{rank}(\lambda, \dots, \lambda) = \dim(V)$.

Example 2.24. Reflections in example 2.19 has nullity 0 and rank 2. On the other hand, projection onto u_1 has nullity 1 and rank 1. In general, if $\{u_1, \dots, u_k\}$ are linearly independent in V then projection onto $\text{Span}(u_1, \dots, u_k)$ has $\text{rank} = k$ and $\text{nullity} = \dim(V) - k$.

If we view each $m \times n$ matrix A as a linear map $F^n \xrightarrow{A} F^m$ then from example 2.13 and theorem 2.22, $n - k$ of its columns will form a basis for its image while the other k columns are linearly dependent upon those. Looking closely at columns of a matrix reveals information about that matrix.

Example 2.25. The matrix $\begin{pmatrix} 1 & 2 & 5 \\ -1 & 0 & -1 \\ 2 & -1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ has rank 2 and nullity 1. It is neither injective nor surjective.

If linear map $V \xrightarrow{f} W$ is bijective then its inverse $W \xrightarrow{f^{-1}} V, w \mapsto v$ the unique element in V such that $f(v) = w$ is also linear. We call such f an isomorphism and say V and W are isomorphic. If A_f is the matrix representation for f with respect to some bases for V and W and $A_{f^{-1}}$ the matrix representation for f^{-1} then surely $A_f A_{f^{-1}} = A_{f^{-1}} A_f = I$.

Moreover, $\text{nullity}(f) = \text{nullity}(f^{-1}) = 0$ and $\dim(V) = \text{rank}(f) = \text{rank}(f^{-1}) = \dim(W)$ in that case.

Example 2.26. The identity map $V \xrightarrow{id} V$ in example 2.15 is an isomorphism. With basis B for domain V and basis B' for codomain V , it has matrix representation $A_{BB'}$ and its inverse has matrix representation $A_{B'B}$ with $A_{BB'}A_{B'B} = A_{B'B}A_{BB'} = I$.

Example 2.27. The association $V \longrightarrow L(V, F), v \mapsto f_v$ in example 2.4 is an isomorphism.

Exercise 2.28. If $V \xrightarrow{f} W$ is a bijective linear map, show that its inverse $W \xrightarrow{f^{-1}} V, w \mapsto v$ the unique element in V such that $f(v) = w$ is also linear.

Exercise 2.29. Show that

- If V and W have the same dimension over F then they are isomorphic.
- If V and W have different dimensions over F then they are not isomorphic.

We end this subsection with a look at what happens to a linear map and its matrix representations with respect to different bases.

Theorem 2.30. (*Change of Basis for Linear Maps*) If $V \xrightarrow{f} W$ is a linear map with matrix presentation A_f with respect to bases B, C for V, W and with matrix representation A'_f with respect to bases B', C' for V, W then $A'_f = A_{CC'}A_fA_{BB'}^{-1}$ where $A_{BB'}$ and $A_{CC'}$ are the change of basis matrices.

Proof. It follows immediately from the following commutative diagram of maps and the commutative diagram of their matrix representations with respect to different bases.

$$\begin{array}{ccc}
 V & \xrightarrow{f} & W \\
 \downarrow id_V & & \downarrow id_W \\
 V & \xrightarrow{f} & W
 \end{array}
 \qquad
 \begin{array}{ccc}
 V & \xrightarrow{A_f} & W \\
 \downarrow A_{BB'} & & \downarrow A_{CC'} \\
 V & \xrightarrow{A'_f} & W
 \end{array}$$

□

When $W = V$ and $C' = B'$, the theorem says $A'_f = A_{BB'}A_fA_{BB'}^{-1}$ which is often written as $A'_f = U A_f U^{-1}$ in literature.

3. MATRICES

As any linear map between vector spaces over F with fixed bases is represented by a matrix, we study matrices more closely. First goes a formal definition of matrix.

Definition 3.1. A matrix M is a rectangular array of $(a_{ij})_{m \times n}$ of m rows and n columns, where each entry a_{ij} in the i^{th} row and j^{th} column is an element in F . We denote the set of all $m \times n$ matrices over F by $M(m, n, F)$.

Example 3.2. We have

1. $\begin{pmatrix} 1/2 \\ 2 \\ 2/3 \end{pmatrix} \in M(3, 1, \mathbb{Q})$ with $a_{3,1} = 2/3$
2. $M = \begin{pmatrix} \sin(\pi/10) & \cos(\pi/10) \end{pmatrix} \in M(1, 2, \mathbb{R})$ with $a_{1,2} = \cos(\pi/10)$
3. $M = \begin{pmatrix} i & e & 1 \\ \pi & 0 & 1/2 \\ \ln 5 & 1 & 3 \end{pmatrix} \in M(3, \mathbb{C})$ with $a_{2,2} = 0$

Below are what we can do with matrices.

3.1. Partition. We can partition a matrix into submatrices. This will be useful later when we multiply matrices by blocks without fretting too much about entries.

Example 3.3. If $A \in M(n, F)$ then it can be partitioned into blocks $A_{4 \times 5} = \begin{pmatrix} A_{3 \times 3} & A_{3 \times 2} \\ A_{1 \times 3} & A_{1 \times 2} \end{pmatrix}$.

Example 3.4. If $A \in M(4, 5, F)$ and $B \in M(r + s, 4, F)$ then they can be partitioned into blocks for multiplication as follows

$$\begin{pmatrix} B_{r \times 3} & B_{r \times 1} \\ B_{s \times 3} & B_{s \times 1} \end{pmatrix} \begin{pmatrix} A_{3 \times 3} & A_{3 \times 2} \\ A_{1 \times 3} & A_{1 \times 2} \end{pmatrix} = \begin{pmatrix} B_{r \times 3}A_{3 \times 3} + B_{r \times 1}A_{1 \times 3} & B_{r \times 3}A_{3 \times 2} + B_{r \times 1}A_{1 \times 2} \\ B_{s \times 3}A_{3 \times 3} + B_{s \times 1}A_{1 \times 3} & B_{s \times 3}A_{3 \times 2} + B_{s \times 1}A_{1 \times 2} \end{pmatrix}$$

3.2. Addition. As the set $L(V, w)$ of all linear maps between V and W can be given a vector space structure, so can their matrix representations $M(m, n, F)$ with respect to some fixed bases.

Definition 3.5. For $A = (a_{ij}), B = (b_{ij}) \in M(m, n, F)$ we define $A + B = (c_{ij}) \in M(m, n, F)$ where $c_{ij} = a_{ij} + b_{ij}$.

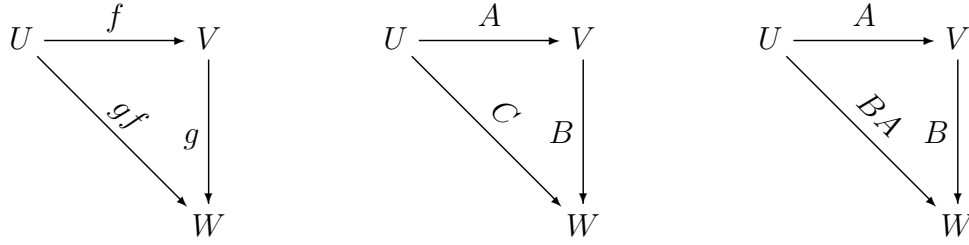
Example 3.6. $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 0 \\ 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 2 \\ 0 & 0 & -3 \end{pmatrix}$.

Addition of matrices $A + B$ clearly corresponds to addition of linear maps $V \xrightarrow{f_A + f_B} W$. Thus it enjoys commutativity and associativity as well.

1. (commutativity) $A + B = B + A$.
2. (associativity) $(A + B) + C = A + (B + C)$.

3.3. Multiplication. Next question is how to define scalar multiplication $a \cdot A_f$ to represent the linear map $a \cdot f$. If we represent scaling by a by the matrix (a, \dots, a) then we are looking at how to define the product $(a, \dots, a)A$ to represent the composition $U \xrightarrow{f} V \xrightarrow{a} V$. More generally, if $U \xrightarrow{f} V \xrightarrow{g} W$ are represented by A, B with respect to some chosen bases for U, v, w then we must define the right product BA to represent gf . Here is the

picture.



Definition 3.7. For $A = (a_{ij}) \in M(m, n, F)$ and $B = (b_{ij}) \in M(l, m, F)$ we define $BA = (c_{ij}) \in M(l, n, F)$ where $c_{ij} = a_{1j}b_{i1} + a_{2j}b_{i2} + \dots + a_{mj}b_{im} = \sum_{k=1}^m a_{kj}b_{ik}$ is the inner product of i^{th} row of B and j^{th} column of A .

Proposition 3.8. Consider U, V, W over F with dimensions n, m, l and bases $\{u_1, \dots, u_n\}$, $\{v_1, \dots, v_m\}$, $\{w_1, \dots, w_l\}$. If $U \xrightarrow{f} V$ is represented by $A = (a_{ij}) \in M(m, n, F)$ and $V \xrightarrow{g} W$ is represented by $B = (b_{ij}) \in M(l, m, F)$ then $U \xrightarrow{gf} W$ is represented by BA .

Proof. We write out $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & & \vdots \\ b_{l1} & \dots & b_{lm} \end{pmatrix}$. Then

$$\begin{aligned} f(u_1) &= A(1, 0, \dots, 0)^t = (a_{11}, \dots, a_{m1})^t = a_{11}v_1 + \dots + a_{m1}v_m \\ &\vdots \\ f(u_n) &= A(0, \dots, 0, 1)^t = (a_{1n}, \dots, a_{mn})^t = a_{1n}v_1 + \dots + a_{mn}v_m \\ gf(u_1) &= a_{11}B(v_1) + \dots + a_{m1}B(v_m) = a_{11}(b_{11}, \dots, b_{l1})^t + \dots + a_{m1}(b_{1m}, \dots, b_{lm})^t \\ &\vdots \\ gf(u_n) &= a_{1n}B(v_1) + \dots + a_{mn}B(v_m) = a_{1n}(b_{11}, \dots, b_{l1})^t + \dots + a_{mn}(b_{1m}, \dots, b_{lm})^t \end{aligned}$$

Hence gf is represented by $\begin{pmatrix} a_{11}b_{11} + \dots + a_{m1}b_{1m} & \dots & a_{1n}b_{11} + \dots + a_{mn}b_{1m} \\ \vdots & & \vdots \\ a_{11}b_{l1} + \dots + a_{m1}b_{lm} & \dots & a_{1n}b_{l1} + \dots + a_{mn}b_{lm} \end{pmatrix}$ which is precisely BA . \square

Note that the number of columns of A must equal the number of rows of B . This definition agrees with our earlier one in 2.1.

Example 3.9. $\begin{pmatrix} 1 & 4 & 2 & 0 \\ 2 & 1 & 5 & 6 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 3 & 0 & 1 \\ 4 & 0 & 5 \\ 1 & 2 & 0 \end{pmatrix} = C_{2 \times 3}$ where $c_{21} = 2 \cdot 2 + 1 \cdot 3 + 5 \cdot 4 + 6 \cdot 1 = 33$

As a special case we define scalar multiplication as $aA = \begin{pmatrix} a & \dots & 0 \\ \vdots & a & \vdots \\ 0 & \dots & a \end{pmatrix} A$.

Example 3.10. $5 \begin{pmatrix} 2 & 1 & 3 \\ 3 & 0 & 1 \\ 4 & 0 & 5 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 3 & 0 & 1 \\ 4 & 0 & 5 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 10 & 5 & 15 \\ 15 & 0 & 5 \\ 20 & 0 & 25 \\ 5 & 10 & 0 \end{pmatrix}$

This scalar multiplication together with matrix addition turn $M(m, n, F)$ into a vector space over F , just as $L(F^n, F^m)$ is a vector space over F . More is true.

Theorem 3.11. For F^n and F^m with bases $\{e_1, \dots, e_n\}$ and $\{e_1, \dots, e_m\}$, the linear maps $(L(F^n, F^m), +, \cdot) \xrightleftharpoons[\varphi]{\phi} (M(m, n, F), +, \cdot), f \mapsto A_f, A \mapsto A$ are inverses of each other.

Proof. This is obvious. \square

Corollary 3.12. The vector space $L(F^n, F^m)$ has dimension mn .

Proof. The collection $\{E_{ij} = (1_{ij}), 1 \leq i \leq m, 1 \leq j \leq n\}$ form a basis for $M(m, n, F)$. \square

It follows from analogous properties for composition and addition of linear maps that

1. (associativity) $(AB)C = A(BC)$
2. (distributivity) $A(B + C) = AB + AC$ and $(A + B)C = AC + BC$
3. (identity element) $I_{m \times m}A_{m \times n} = A_{m \times n}I_{n \times n} = A$ for all $A_{m \times n}$ (best when $m = n$)
4. (scalar multiplication) $aA = Aa$

If $m = n$ then (3) and (4) mean commutativity $(aI_{m \times m})A_{m \times m} = A_{m \times m}(aI_{m \times m})$ for all $a \in F$ and $I, A \in M(m, F)$. Here are a few more examples to illuminate matrix multiplication.

Example 3.13. One can see $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ through direct multiplication or through geometry in \mathbb{R}^2 . Matrix multiplication is not commutative in general.

Example 3.14. Matrix multiplication fails to cancel

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

but clearly

$$\begin{pmatrix} 3 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

Example 3.15. Matrix multiplication has zero divisors $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Example 3.16. Matrix multiplication has idempotents $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Example 3.17. Given $a_1, \dots, a_k \in F$ and $A_1, \dots, A_k \in M(m, n, F)$ we can form a linear combination $a_1A_1 + \dots + a_kA_k \in M(m, n, F)$.

Example 3.18. Given a polynomial such as $p(x) = x^2 + 2x + 3 \in \mathbb{R}[x]$, we can view it as map $\mathbb{R} \xrightarrow{p(x)} \mathbb{R}, 4 \mapsto 4^2 + 2 \cdot 4 + 3 = 27$. Now we can also view it as map $M(n, \mathbb{R}) \xrightarrow{p(x)} M(n, \mathbb{R}), A \mapsto A^2 + 2 \cdot A + 3$.

3.4. Transposition. Next we attribute to each matrix $A \in M(m, n, F)$ a companion, it helps us develop matrix theory.

Definition 3.19. For $A = (a_{ij}) \in M(m, n, F)$, we define its transpose $A^t = (b_{ij}) \in M(n, m, F)$ where $b_{ij} = a_{ji}$.

Proposition 3.20. *Transposition has the following properties*

1. $(A^t)^t = A$.
2. $(A + B)^t = A^t + B^t$.
3. $(aA)^t = aA^t$.
4. $(AB)^t = B^t A^t$.

Proof. Straightforward. □

Can you interpret these properties in terms of behavior of the associated linear maps? Noteworthy is the fact that if a linear map $V \xrightarrow{f} W$ is represented by $A \in M(m, n, F)$ with respect to basis $\{v_1, \dots, v_n\}$ for V and basis $\{w_1, \dots, w_m\}$ for W then its dual $W^* \xrightarrow{f^*} V^*$ is represented by $A^t \in M(n, m, F)$ with respect to basis $\{w_1^*, \dots, w_m^*\}$ for W^* and basis $\{v_1^*, \dots, v_n^*\}$ for V^* .

Example 3.21.
$$\begin{pmatrix} 2 & 1 & 4 \\ 3 & 4 & 1 \\ 5 & 3 & 1 \end{pmatrix}^t = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 3 \\ 4 & 1 & 1 \end{pmatrix}$$

Example 3.22.
$$\begin{pmatrix} 2 & 1 & 7 \end{pmatrix}^t = \begin{pmatrix} 2 \\ 1 \\ 7 \end{pmatrix}$$

3.5. Some Matrices. We use transposition to describe some interesting classes of matrices.

3.5.1. Orthogonal Matrices. The first class is orthogonal matrices.

Definition 3.23. A matrix $A \in M(m, n, F)$ is called orthogonal (or more descriptively orthonormal) if $A^t A = I_n$.

It follows that if we consider the i^{th} column as coordinate form of vector $v_i \in F^m$ with respect to canonical basis $\{e_1, \dots, e_m\}$ and inner product $\langle e_i, e_j \rangle = \delta_{ij}$ then $\langle v_i, v_j \rangle = \delta_{ij}$. Hence $\{v_1, \dots, v_n\}$ are an orthonormal collection of vectors in F^m , recall the discussion after example 1.41. It follows that these v_i are linearly independent and $m \geq n$.

3.5.2. Triangular Matrices. The second class is triangular matrices.

Definition 3.24. A matrix $A \in M(n, F)$ is called lower triangular if all entries above the diagonal are zero, i.e. $a_{ij} = 0$ for all $i < j$. A matrix $A \in M(n, F)$ is called upper triangular if $a_{ij} = 0$ for all $i > j$. And if $a_{11} = \dots = a_{nn} = 1$ then it is called unit lower triangular or unit upper triangular.

Example 3.25. We have $A = \begin{pmatrix} 4 & 0 & 0 \\ 5 & 2 & 0 \\ 3 & 6 & 1 \end{pmatrix}$ is lower triangular and $A = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 2 & 5 \\ 0 & 0 & 1 \end{pmatrix}$ is upper triangular.

By definition, a matrix A is lower triangular iff A^t is upper triangular and vice versa, while it is both lower triangular and upper triangular iff all of its nondiagonal entries are zero.

Definition 3.26. A matrix $A \in M(n, F)$ is called diagonal if $a_{ij} = 0$ whenever $i \neq j$.

Example 3.27. These matrices are all diagonal,

$$A = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } A^n = \begin{pmatrix} 4^n & 0 & 0 \\ \vdots & 2^n & \vdots \\ 0 & \dots & 1^n \end{pmatrix}$$

$$B = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B^{-1} = \begin{pmatrix} 1/4 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Example 3.28. One can verify that if $A = (a_{11}, \dots, a_{nn}) \in M(n, F)$ is a diagonal matrix and $M \in M(n, F)$ is any matrix then AM is the matrix whose i^{th} row is the i^{th} row of A multiplied by a_{ii} .

We denote the set of all lower triangular matrices, upper triangular matrices and diagonal matrices as $L(n, F)$, $U(n, F)$, $D(n, F)$. Each set is closed under addition, multiplication and inverse. For example, if $A, B \in L(n, F)$ then $AB \in L(n, F)$. Or if $A \in U(n, F)$ is invertible then $A^{-1} \in U(n, F)$.

3.5.3. *Symmetric Matrices.* Another class of matrices that transposition helps describe is symmetric matrices.

Definition 3.29. A square matrix $A \in M(n, F)$ is called symmetric if $A = A^t$, or equivalently if $a_{ij} = a_{ji}$ for all i, j .

Example 3.30. We have

a. $A = \begin{pmatrix} 0 & 4 & 1 \\ 4 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ is symmetric.

b. Every diagonal matrix is symmetric while other triangular matrices are not. Draw a Venn's diagram of $L(n, F)$, $U(n, F)$, $D(n, F)$, $S(n, F)$.

The set of all symmetric matrices is denoted by $S(n, F)$. It is closed under addition and inverse, but not under multiplication. One sure source for symmetric matrices is taking inner products of vectors. If $u = a_1v_1 + \dots + a_nv_n$ and $w = b_1v_1 + \dots + b_nv_n$ are two vectors in an inner product space V with basis $\{v_1, \dots, v_n\}$ then $\langle u, w \rangle = \langle a_1v_1 + \dots + a_nv_n, b_1v_1 + \dots + b_nv_n \rangle = (a_1, \dots, a_n)A(b_1, \dots, b_n)^t$ where $A = (\langle v_i, v_j \rangle)$. Even if v_1, \dots, v_n are not a basis for V , we can still form $A = (\langle v_i, v_j \rangle)$.

Definition 3.31. A symmetric matrix $A \in M(n, \mathbb{R})$ is called definite if all $v^tAv, v \in V \setminus \{0\}$ are either positive or negative. Otherwise, we say A is indefinite.

If all $v^tAv, v \in V \setminus \{0\}$ are positive then we say A is positive definite. If all $v^tAv, v \in V \setminus \{0\}$ are negative then we say A is negative definite. And if there are some equalities to 0 then we prefix semi to the word definite.

Example 3.32. The identity matrix I is positive definite, since $(a_1, \dots, a_n)I(a_1, \dots, a_n)^t = a_1^2 + \dots + a_n^2$.

Example 3.33. The matrix $A = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$ is positive definite, since

$$\begin{aligned} (a_1, a_2, a_3)A(a_1, a_2, a_3)^t &= 2a_1^2 - 2a_1a_2 + 2a_2^2 - 2a_2a_3 + 2a_3^2 \\ &= a_1^2 + (a_1 - a_2)^2 + (a_2 - a_3)^2 + a_3^2 \end{aligned}$$

Exercise 3.34. Show that the matrix $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ is indefinite and compute $p(A)$ where $p(t) = t^2 - 4t + 3$.

Exercise 3.35. Find a 3×3 negative definite matrix.

The source taking inner products of vectors for symmetric matrices is certainly a possible source for positive semidefinite matrices. A matrix G is called a Gram matrix for vectors $v_1, \dots, v_n \in \mathbb{R}^m$ if $g_{ij} = \langle v_i, v_j \rangle$, $1 \leq i, j \leq n$ the usual inner products between v_1, \dots, v_n . In other words, $G = A^t A$ where $A \in M(m, n, \mathbb{R})$ has i^{th} column v_i .

Proposition 3.36. A matrix $G \in M(n, \mathbb{R})$ is positive semidefinite iff it is a Gram matrix for some vectors $v_1, \dots, v_n \in \mathbb{R}^m$.

Proof. If $G = A^t A$ is a Gram matrix then $v^t G v = v^t A^t A v = (Av)^t (Av) = \langle Av, Av \rangle = \|Av\|^2 \geq 0$ for all $v \in \mathbb{R}^n$. So $A^t A$ is positive semidefinite. Conversely, if G is positive semidefinite then by the eigenvalue decomposition for symmetric matrices that we will learn in theorem 3.98, $G = U D U^{-1}$ where U is orthogonal and $D = (\lambda_1, \dots, \lambda_n)$ is diagonal with nonnegative diagonal entries. Take $B = (\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})$ then $G = U B B U^{-1} = (U^{-1})^t B^t B U^{-1} = (B U^{-1})^t (B U^{-1})$ a Gram matrix for vectors v_1, \dots, v_n the columns of $B U^{-1}$. \square

3.6. Invertible Matrices and Their Inverses.

3.6.1. Invertibility for Square Matrices. When $V \xrightarrow{f} W$ is a linear map between vector spaces of equal dimension n , its matrix representation A with respect to a basis is square and it is quick to determine whether f is bijective by looking at A . Or abstractly, $M(n, F)$ has been equipped with multiplication and we want to consider those matrices that are invertible under this operation

$$\begin{aligned} A_f A_{f^{-1}} &= A_{f f^{-1}} = A_{id_W} = I_n \\ A_{f^{-1}} A_f &= A_{f^{-1} f} = A_{id_V} = I_n \end{aligned}$$

Definition 3.37. A square matrix $A \in M(n, F)$ is called invertible (or nonsingular) if there exists $B \in M(n, F)$ such that $AB = BA = I$, in which case we denote B by A^{-1} . Else we say A is noninvertible (or singular).

Example 3.38. The inverse of $I \in M(n, F)$ is I itself. More generally, for $a \neq 0 \in F$,

$$\begin{pmatrix} a & \dots & 0 \\ \vdots & a & \vdots \\ 0 & \dots & a \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & \dots & 0 \\ \vdots & 1/a & \vdots \\ 0 & \dots & 1/a \end{pmatrix}$$

Example 3.39. The change of basis matrices $A_{BB'}$ and $A_{B'B}$ in example 2.15 are invertible. They are inverses of each other.

Example 3.40. One can verify that $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} -5/12 & 3/12 & 4/12 \\ 7/12 & 3/12 & -8/12 \\ 1/12 & -3/12 & 4/12 \end{pmatrix}$ are inverses of each other.

Example 3.41. Any matrix with a whole row of zeros or a whole column of zeros is singular. For example, if $M(3, \mathbb{R}) \ni A = \begin{pmatrix} c_1 & c_2 & 0 \end{pmatrix}$ then $BA = B \begin{pmatrix} c_1 & c_2 & 0 \end{pmatrix} = \begin{pmatrix} Bc_1 & Bc_2 & 0 \end{pmatrix} \neq I$ for any matrix B , so A is noninvertible. Or one can look at what A does to the basis $\{e_1, e_2, e_3\}$ to see its kernel and range.

We will learn three ways to find the inverse of an invertible matrix by hand. Or we can use wolframalpha. Now let us look at some properties about inverse.

Theorem 3.42. Any invertible matrices $A, B \in M(n, F)$ satisfy the following,

1. A has unique inverse A^{-1} and $(A^{-1})^{-1} = A$.
2. $(AB)^{-1} = B^{-1}A^{-1}$
3. $(A^n)^{-1} = (A^{-1})^n$.
4. $(aA)^{-1} = \frac{1}{a}A^{-1}$ for $a \neq 0 \in \mathbb{R}$.
5. $(A^t)^{-1} = (A^{-1})^t$.

Proof. prove a few of these in class. □

Example 3.43. We reuse A and A^{-1} in example 3.40. One can verify that

$A^2 = \begin{pmatrix} 13 & 9 & 14 \\ 11 & 11 & 14 \\ 11 & 9 & 16 \end{pmatrix}$ and $(A^{-1})^2 = \begin{pmatrix} 25/72 & -9/72 & -14/72 \\ -11/72 & 27/72 & -14/72 \\ -11/72 & -9/72 & 22/72 \end{pmatrix}$ are inverses of each other.

Example 3.44. Or $12A^{-1} = \begin{pmatrix} -5/12 & 3/12 & 4/12 \\ 7/12 & 3/12 & -8/12 \\ 1/12 & -3/12 & 4/12 \end{pmatrix} = \begin{pmatrix} -5 & 3 & 4 \\ 7 & 3 & -8 \\ 1 & -3 & 4 \end{pmatrix}$ is the inverse of $\frac{1}{12}A$.

Example 3.45. Or $(A^{-1})^t = \begin{pmatrix} -5/12 & 7/12 & 1/12 \\ 3/12 & 3/12 & -3/12 \\ 4/12 & -8/12 & 4/12 \end{pmatrix}$ is the inverse of $A^t = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 2 & 1 \\ 3 & 1 & 3 \end{pmatrix}$

We relate invertibility of a matrix with its behavior as a linear map.

Theorem 3.46. A matrix $A \in M(n, F)$ is invertible iff $F^n \xrightarrow{A} F^n$ has trivial kernel iff it has full image iff its columns are linearly independent.

Proof. show in class. □

It follows from the theorem that A is invertible iff its transpose is invertible iff its rows are linearly independent. We get the following result for positive semidefinite matrices.

Corollary 3.47. Positive definite matrices $A \in M(n, \mathbb{R})$ are invertible while positive semidefinite matrices $A \in M(n, \mathbb{R})$ that are not positive definite are noninvertible.

Proof. If A is positive definite and $v \in \ker(A)$ then $v^t Av = v^t 0 = 0$ implies $v = 0$. Hence A has trivial kernel and is invertible by the theorem. On the other hand, if A is positive semidefinite but not positive definite then there exists some $v \neq 0$ such that $v^t Av = 0$. We have the quadratic polynomial $p(x) = (v + xAv)^t A(v + xAv) = (v^t + xv^t A^t)(Av + xA^2 v) = v^t Av + xv^t A^2 v + xv^t A^t Av + x^2 v^t A^t A^2 v = 0 + 2xv^t A^2 v + x^2 v^t A^3 v = 2xv^t A^2 v + x^2 v^t A^3 v \geq 0$ with minimum 0 at $t = 0$. It follows that $p'(0) = 2v^t A^2 v = 2v^t A^t Av = 2(Av)^t Av = 2\langle Av, Av \rangle = 2\|Av\|^2 = 0$. By positive definiteness of inner product, $Av = 0$. So A has nontrivial kernel and is noninvertible by the theorem. \square

Corollary 3.48. *A Gram matrix $G = A^t A \in M(n, \mathbb{R})$ for vectors $v_1, \dots, v_n \in \mathbb{R}^m$ is positive definite iff $A \in M(m, n, \mathbb{R})$ has trivial kernel iff $A^t \in M(n, m, \mathbb{R})$ has full image.*

Proof. Surely G is positive definite iff $v^t Gv = v^t A^t Av = \|Av\|^2 > 0$ for all nonzero v iff $Av \neq 0$ for all nonzero v iff A has trivial kernel. For the second equivalence, assume G is positive definite, then it is invertible by corollary 3.47. So every $v = I_n v = GG^{-1}v = (A^t A)(A^t A)^{-1}v = A^t(A(A^t A)^{-1}v)$ and A^t has full image. Conversely, if A^t has full image then every nonzero $v = A^t w$ with $\|v\|^2 = v^t v = w^t Av > 0$. This means $Av \neq 0$. So $v^t Gv = v^t A^t Av = \|Av\|^2 > 0$ and G is positive definite. \square

The second iff is a nice result in linear algebra.

3.6.2. Invertibility for General Matrices. When $V \xrightarrow{f} W$ is a linear map between vector spaces V and W of possibly different dimensions n and m then its matrix representation A has size $m \times n$ and we have more to keep track of. If $m > n$ then A has more rows than columns and is called a tall matrix. If $m < n$ then A has more columns than rows and is called a wide matrix.

Definition 3.49. A matrix $A \in M(m, n, F)$ is called left invertible if there exists a matrix $B \in M(n, m, F)$ such that $BA = I_n$. It is called right invertible if there exists a matrix $B \in M(n, m, F)$ such that $AB = I_m$.

Again we relate one-sided invertibility of a matrix with its behavior as a linear map.

Theorem 3.50. *A matrix $A \in M(m, n, F)$ is left invertible iff A has trivial kernel iff $A^t A$ is positive definite iff A^t has full image iff A^t is right invertible.*

Proof. If A has a left inverse B then $Av = 0$ implies $v = I_n v = BAv = B0 = 0$, so A has trivial kernel. Conversely, if A has trivial kernel then $A^t A$ is positive definite by corollary 3.48. By 3.47, it is invertible with inverse $(A^t A)^{-1}$. But then $((A^t A)^{-1} A^t)A = (A^t A)^{-1}(A^t A) = I_n$, so A is left invertible. If A^t has right inverse then $v = I_n v = A^t(A^t)^{-1}v = A^t((A^t)^{-1}v)$ and A^t has full image. Conversely, if A^t has full image then $A^t A$ is positive definite by corollary 3.48. By 3.47, it is invertible with inverse $(A^t A)^{-1}$. But then $A^t(A(A^t A)^{-1}) = (A^t A)(A^t A)^{-1} = I_n$, so A^t is right invertible. \square

Written in a separate statement, a matrix A is right invertible iff A has full image iff AA^t is positive definite. From the proof, a left invertible matrix A has left inverse $(A^t A)^{-1} A^t$ while a right invertible matrix A has right inverse $A^t(AA^t)^{-1}$. Both of these one-sided inverses are called Moore-Penrose pseudoinverses. They are not unique, we will learn a second way to find them later.

Corollary 3.51. *Any left invertible matrix must be square or tall while any right invertible matrix must be square or wide.*

Proof. By theorem 3.50, any left invertible matrix $\mathbb{R}^n \xrightarrow{A} \mathbb{R}^m$ has trivial kernel and \mathbb{R}^n embeds into \mathbb{R}^m , so $m \geq n$. The second claim follows through transposition. \square

Example 3.52. The tall matrix $A = \begin{pmatrix} 2 & 0 \\ 0 & 1/3 \\ 0 & 0 \end{pmatrix}$ has left inverse $A = (A^t A)^{-1} A^t = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$.

Example 3.53. Recall that a matrix $A \in M(m, n, \mathbb{R})$ is called orthogonal if $A^t A = I_n$, so it is left invertible with left inverse $A^t \in M(n, m, \mathbb{R})$. Consequently, it has as many or more rows than columns, we knew this before.

Example 3.54. The wide matrix $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}$ has right inverse $A^t (A A^t)^{-1} = \begin{pmatrix} 7/11 & -4/11 \\ -4/11 & 7/11 \\ 1/11 & 1/11 \end{pmatrix}$.

Exercise 3.55. Consider the map $\mathbb{R}^3 \xrightarrow{f} \mathbb{R}^2, (x, y, z) \mapsto (2x, y + z)$.

- Show that f is linear.
- Find the matrix representation A for f with respect to $B = \{e_1, e_2, e_3\}$ for \mathbb{R}^3 and $C = \{e_1, e_2\}$ for \mathbb{R}^2 .
- Determine whether A is left invertible or right invertible.
- Find a left inverse or right inverse for A .
- Find another left inverse or right inverse for A .

3.7. Row Operations. We can also determine invertibility and inverse for a square matrix $A \in M(n, F)$ by looking at the columns and rows of A without referring to its linear map. This is done by studying A through simple row modifications and column modifications.

Definition 3.56. We define an elementary row operation for a matrix A to be either interchanging two rows, multiplying a row by a nonzero constant $a \in F$, or adding a constant a times a row to another row.

For convenience, we denote each elementary row operation by O and its reverse operation by O^{-1} . This reverse operation is also an elementary operation.

Definition 3.57. A matrix $A \in M(n, F)$ is called elementary if it differs from I by a single elementary row operation.

Theorem 3.58. *If $E = O(I)$ is an elementary matrix then $EA = O(A)$, that is multiplying A by E on the left is the same as performing O to A .*

Proof. book. \square

Corollary 3.59. *Any elementary matrix E is invertible with inverse $E^{-1} = O^{-1}(I)$.*

Proof. If $E = O(I)$ then $E \cdot O^{-1}(I) = O(O^{-1}(I)) = I$. \square

Exercise 3.60. Determine what the linear map $F^3 \xrightarrow{O(I)} F^3$ does where

- O is interchanging the first two rows.
- O is multiplying row 3 by 2.
- O is adding 2 times row 3 to row 1.

The elementary row operations allow us to modify a matrix $A \in M(n, F)$ for our purpose.

Definition 3.61. Two matrices $A, B \in M(n, F)$ are called row equivalent if they differ by a sequence of elementary row operations, in which case we write $A \sim B$.

Note that this relation \sim is an equivalence relation, i.e. it satisfies

- (reflexivity) $A \sim A$.
- (symmetry) $A \sim B$ then $B \sim A$.
- (transitivity) $A \sim B$ and $B \sim C$ then $A \sim C$.

The set of all matrices row equivalent to I form an equivalence class in $M(n, F)$.

Example 3.62. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{4r_2} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \xrightarrow{r_1+r_2 \text{ to } r_1} \begin{pmatrix} 1 & 4 \\ 0 & 4 \end{pmatrix} \xrightarrow{r_1 \leftrightarrow r_2} \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}$. Hence $\begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix} \sim I$. However, it is not an elementary matrix and you can not go from one to the other by a single elementary row operation.

Theorem 3.63. A matrix $A \in M(n, F)$ is invertible iff $A \sim I$.

Proof. If A is invertible then we can reduce it to I through a sequence of elementary row operations. Conversely, if $A = O_r(\dots(O_1(I))) = E_r \dots E_1 I$ then as composition of invertible linear maps, A is invertible. \square

Hence, the row equivalence class of I consists of all invertible matrices.

Corollary 3.64. If A is invertible and the elementary operations O_r, \dots, O_1 reduce A to I then the same operations will reduce I to A^{-1} .

Proof. By theorem 3.63, there exist operations O_1, \dots, O_r such that $O_r(\dots O_1(A)) = E_r \dots E_1 A = I$. But then $A^{-1} = E_r \dots E_1 = O_r \dots O_1(I)$. \square

This corollary gives us an algorithm to invert any invertible matrix. It will stall on a noninvertible matrix.

Example 3.65. Given $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$, we perform

$$\begin{aligned} & \left(\begin{array}{ccc|ccc} 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{array} \right) \xrightarrow{r_1/2, r_2-r_1, r_3-r_1} \left(\begin{array}{ccc|ccc} 1 & 1/2 & 1/2 & 1/2 & 0 & 0 \\ 0 & 3/2 & 1/2 & -1/2 & 1 & 0 \\ 0 & 1/2 & 3/2 & -1/2 & 0 & 1 \end{array} \right) \xrightarrow{2r_2/3, r_3-r_2/2} \\ & \left(\begin{array}{ccc|ccc} 1 & 1/2 & 1/2 & 1/2 & 0 & 0 \\ 0 & 1 & 1/3 & -1/3 & 2/3 & 0 \\ 0 & 0 & 4/3 & -1/3 & -1/3 & 1 \end{array} \right) \xrightarrow{3r_3/4, r_2-r_3/3, r_1-r_3/2} \left(\begin{array}{ccc|ccc} 1 & 1/2 & 0 & 5/8 & 1/8 & -3/8 \\ 0 & 1 & 0 & -1/4 & 3/4 & -1/4 \\ 0 & 0 & 1 & -1/4 & -1/4 & 3/4 \end{array} \right) \xrightarrow{r_1-r_2/2} \\ & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3/4 & -1/4 & -1/4 \\ 0 & 1 & 0 & -1/4 & 3/4 & -1/4 \\ 0 & 0 & 1 & -1/4 & -1/4 & 3/4 \end{array} \right) = (I \mid A^{-1}) \end{aligned}$$

This is the first way to find inverse of an invertible matrix.

3.8. Determinant. A third way to determine invertibility and inverse for $A \in M(n, F)$ is through one of its most important invariants.

Definition 3.66. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, F)$ we define its determinant $\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$.

Example 3.67. $\det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1 \cdot 4 - 2 \cdot 3 = -2$

We choose this definition $\det(A) = ad - bc$ because $ad - bc = 0$ iff $(a, b) = a(b, d)$ for some $a \neq 0$ iff A is noninvertible. Suppose we have defined determinant for $A \in M(n-1, F)$. We consider two more ingredients for determinant of a general $n \times n$ matrix.

Definition 3.68. For $A = (a_{ij}) \in M(n, F)$ we define the minor M_{ij} of entry a_{ij} to be the determinant of the $(n-1) \times (n-1)$ submatrix that remains after deleting the i^{th} row and j^{th} column from A . We define the cofactor C_{ij} of entry a_{ij} to be $(-1)^{i+j} M_{ij}$.

Definition 3.69. For $A = (a_{ij}) \in M(n, F)$ we define its cofactor expansion along row i^{th} to be $\sum_{j=1}^n a_{ij} C_{ij}$ and its cofactor expansion along column j^{th} to be $\sum_{i=1}^n a_{ij} C_{ij}$.

One obvious question is whether cofactor expansion depends on the choice of row vs. column, or the choice of which row, or the choice of which column. Here is the answer.

Theorem 3.70. *Cofactor expansion of $A = (a_{ij}) \in M(n, F)$ is independent of the choice of row vs. column, or the choice of row, or the choice of column.*

Proof. One way is to explicitly write out any two cofactor expansions in terms of the a_{ij} and compare. It is tedious bookkeeping. \square

Finally we can define determinant of a general $n \times n$ matrix A .

Definition 3.71. For a matrix $A = (a_{ij}) \in M(n, F)$ we define its determinant $\det(A) = \sum_{j=1}^n a_{ij}C_{ij} = \sum_{i=1}^n a_{ij}C_{ij}$ any cofactor expansion along any row or any column.

It takes us long to define determinant but it is not hard to compute.

Example 3.72.

$$\det \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 5 \\ 3 & 1 & 2 & 6 \\ 2 & 1 & 3 & 7 \end{pmatrix} = 7 \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{vmatrix} - 6 \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{vmatrix} + 5 \begin{vmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 1 & 3 \end{vmatrix} - 4 \begin{vmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 2 & 1 & 3 \end{vmatrix}$$

Computation of determinant is easier for matrices full of zeros. If A has a row or a column full of zeros then we can choose to calculate cofactor expansion along that row or column. For instance, if A is an upper triangular matrix then we can choose to compute cofactor expansion along the first column and get $\det(A) = \prod_{i=1}^n a_{ii}$ by induction. To facilitate computation of determinant of a general matrix, we establish some primary properties for determinant.

Theorem 3.73. For matrices $A, b, c \in M(n, F)$,

1. If an operation O multiplies a row (column) of A by a then $\det(O(A)) = a \det(A)$.
2. If the i^{th} row (column) of A is the sum of the i^{th} row (column) of B and the i^{th} row (column) of C and all the other rows (columns) of B and C are the same then $\det(A) = \det(B) + \det(C)$.
3. If two rows (columns) of A are linearly independent then $\det(A) = 0$.
4. If O adds a multiple of one row (column) to another then $\det(O(A)) = \det(A)$.
5. If O interchanges two rows (columns) of A then $\det(O(A)) = -\det(A)$.

Proof. For (1), assume row i^{th} is multiplied by a , then along this row, $\det(O(A)) = \sum_{i=1}^n aa_{ij}C_{ij} = a \sum_{i=1}^n a_{ij}C_{ij} = a \det(A)$. For (2), calculate along that row. For (3) use permutation in cofactor expansion of determinant. For (4), use (2) and (3). For (5), use (4) and (1) via a sequence of addition, subtraction, multiplication. \square

Example 3.74. $\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{vmatrix} = 2$, $\begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix} = 1$, and $\begin{vmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1$. In any case, if $E = O(I)$ is an elementary matrix then $\det(E) = \pm a \det(I) = \pm a \neq 0$.

Example 3.75. $\begin{vmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 3 & 6 & 9 \end{vmatrix} = 0$ by 3.73(3).

Example 3.76. Reduce $\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{pmatrix}$ to diagonal form by elementary row operations, keeping track of how \det changes along the way. This could have been done with column operations as well.

We consider some examples to see how determinant interacts with matrix addition and matrix multiplication.

Example 3.77. $\left| \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right| + \left| \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right| \neq \left| \begin{pmatrix} 1 & 0 & 4 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right|.$

Example 3.78. $\left| \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right| = \left| \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right| \left| \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right|$

So determinant does not respect addition but it may respect matrix multiplication. Toward the general statement, we have a prelude.

Lemma 3.79. *If E is an elementary matrix then $\det(EA) = \det(E)\det(A)$ for any $A \in M(n, F)$.*

Proof. If $E = O(I)$ then $EA = O(A)$ and the result follows from theorem 3.73. \square

We now list more properties of determinant.

Theorem 3.80. *For matrices $A, B, C \in M(n, F)$,*

1. *(compatibility with transpose) $\det(A^t) = \det(A)$.*
2. *$\det(aA) = a^n \det(A)$.*
3. *(invertibility) A is invertible iff $\det(A) \neq 0$.*
4. *(compatibility with multiplication) $\det(AB) = \det(A)\det(B)$.*
5. *If A is invertible then $\det(A^{-1}) = \det(A)^{-1}$.*

Proof. Clearly (1) and (2) follow from definition of determinant. If A is noninvertible then one of its rows, say $r_1 = a_2r_2 + \dots + a_nr_n$ a linear combination of the remaining row. Thus we can add $-a_2r_2, \dots, -a_nr_n$ to r_1 to get a matrix with first row full of zeros without changing determinant. Hence $\det(A) = 0$. Conversely, if A is invertible then $A \sim I$, i.e. $A = E_r \dots E_1 I$, so $\det(A) = \det(E_r) \dots \det(E_1) 1 \neq 0$ by lemma 3.79 and example 3.74. This is (3). For (4) we consider two cases. If A is noninvertible then so is AB and $\det(AB) = 0 = \det(A)\det(B)$ by (3). If A is invertible then we write $A = E_k \dots E_1$, hence $\det(AB) = \det(E_k \dots E_1 B) = \det(E_k) \dots \det(E_1) \det(B) = \det(A)\det(B)$ by lemma 3.79. Lastly, $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(I) = 1$ and (5) follows. \square

Corollary 3.81. *A triangular matrix $A = (a_{ij}) \in M(n, F)$ is invertible iff all its diagonal entries are nonzero.*

Proof. Since $\det(A) = \prod_{i=1}^n a_{ii}$, the claim follows theorem 3.80(3). \square

Therefore, whether $\det(A) = 0$ or $\det(A) \neq 0$ tells us whether A is singular or A is nonsingular before we perform row reduction to find its inverse.

There is another way to find inverse of an invertible matrix. We have actually seen it in the 2×2 case $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Can we guess the general form for A^{-1} ?

Definition 3.82. For a matrix $A = (a_{ij}) \in M(n, F)$, the matrix (C_{ij}) where C_{ij} the cofactor of a_{ij} is called the matrix of cofactors of A and its transpose $(C_{ij})^t$ is called the adjugate (or adjoint in some literature) of A , denoted by $\text{adj}(A)$.

Example 3.83. The matrix $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$ has cofactors

$$\begin{aligned} C_{11} &= 5 & C_{12} &= -7 & C_{13} &= -1 \\ C_{21} &= -3 & C_{22} &= -3 & C_{23} &= 3 \\ C_{31} &= -4 & C_{32} &= 8 & C_{33} &= -4 \end{aligned}$$

Hence its matrix of cofactors is $\begin{pmatrix} 5 & -7 & -1 \\ -3 & -3 & 3 \\ -4 & 8 & -4 \end{pmatrix}$ and its adjugate is $\begin{pmatrix} 5 & -3 & -4 \\ -7 & -3 & 8 \\ -1 & 3 & -4 \end{pmatrix}$

We state and prove our suspicion for the general case.

Theorem 3.84. If $A \in M(n, F)$ is invertible then $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$.

Proof. Consider $A \cdot \text{adj}(A) = (a_{ij})(C_{ij})^t = (d_{ij})$ where $d_{ij} = a_{i1}C_{j1} + \dots + a_{jn}C_{jn}$. If $i = j$ then d_{ij} is precisely $\det(A)$, else d_{ij} is the determinant of the matrix from replacing the j^{th} row of A with its i^{th} row. Since this matrix has two rows that are the same, its determinant is 0. Hence $A \cdot \text{adj}(A) = \det(A)I$ and we are done. \square

Example 3.85. Since $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$ has determinant -12 , it is invertible with inverse

$A^{-1} = \frac{1}{-12} \begin{pmatrix} 5 & -3 & -4 \\ -7 & -3 & 8 \\ -1 & 3 & -4 \end{pmatrix} = \begin{pmatrix} -5/12 & 3/12 & 4/12 \\ 7/12 & 3/12 & -8/12 \\ 1/12 & -3/12 & 4/12 \end{pmatrix}$. This is the second way to find inverse of an invertible matrix.

Exercise 3.86. Consider the matrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$.

- Compute its cofactor expansion along the first row and its cofactor expansion along the first column. This is $\det(A)$.
- Determine if A is invertible.
- Compute its adjugate matrix and its inverse.
- Use elementary row operation to reduce $(A|I)$ to $(I|A^{-1})$.
- Record how each elementary row operation changes $\det(A)$ along the way.

3.9. Trace. We give each square matrix another invariant.

Definition 3.87. For a matrix $A = (a_{ij}) \in M(n, F)$, we define its trace $\text{tr}(A) = \sum_{i=1}^n a_{ii}$.

There is not much we want to say about trace.

Theorem 3.88. For matrices $A, b \in M(n, F)$,

1. $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$.
2. $\text{tr}(aA) = a\text{tr}(A)$.
3. $\text{tr}(AB) = \text{tr}(BA)$.
4. $\text{tr}(A) = \text{tr}(A^t)$.

Proof. prove some of these in class. □

The first three properties actually characterize trace. If $M(n, F) \xrightarrow{f} F$ is a linear map such that $f(AB) = f(BA)$ then it is proportional to trace.

3.10. Eigenvalues, Eigenvectors and Eigenvalue Decompositions. Now that we have seen the utility of matrix representation for a linear map $F^n \xrightarrow{f} F^n$ with respect to some basis B for domain and codomain, the question is whether we can find another basis B' such that f has a simple representation from which we can read off its information. In particular, can we find a basis $B' = \{v_1, \dots, v_n\}$ with respect to which f is represented by a diagonal matrix $D = (\lambda_1, \dots, \lambda_n)$? In such case we can see that

- $f(v_i) = \lambda_i v_i$ extension along the direction of v_i .
- $\text{im}(f) = \text{Span}(v_i, \lambda_i \neq 0)$.
- $\text{rank}(f)$ is the number of nonzero λ_i .
- $\det(f) = \prod_i \lambda_i$.
- $\text{tr}(f) = \sum_i \lambda_i$, etc.

Conversely, if there exist n linearly independent $\{v_1, \dots, v_n\}$ such that $f(v_i) = \lambda_i v_i$ then we can use them as basis B' and f has matrix representation $D = (\lambda_1, \dots, \lambda_n)$ with respect to B' . This leads us to eigenvalues and eigenvectors.

Definition 3.89. For $F^n \xrightarrow{f} F^n$, a scalar $\lambda \in F$ is called an eigenvalue of f if there exists a nonzero vector $v \in F^n$ such that $f(v) = \lambda v$. Such v is called an eigenvector corresponding to λ .

Note that eigenvalues may be zero but eigenvectors must be nonzero. Firstly, eigenvalues and eigenvectors may not exist. Secondly, if v is an eigenvector corresponding to an eigenvalue λ then for any $a \neq 0 \in F$, av is also an eigenvector corresponding to λ . Thirdly, $(\lambda I - A)(v) = 0$ for any matrix representation A for f with respect to any basis. This implies $(\lambda I - A)$ is noninvertible, or equivalently $\det(\lambda I - A) = 0$. If we view λ as an unknown then this polynomial is monic of degree n and independent of basis. It is called the characteristic polynomial of f and denoted by $\text{char}_f(\lambda)$. The span of all eigenvectors corresponding to an eigenvalue λ is denoted by V_λ .

Example 3.90. If $F^n \xrightarrow{f} F^n$ is noninvertible with nonzero $v \in \ker(f)$ then v is an eigenvector with eigenvalue 0.

Example 3.91. If $F^n \xrightarrow{f} F^n$ is represented by a triangular matrix $A = (a_{ij})$ with respect to some basis then $\text{char}_f(\lambda) = \det(\lambda I - A) = \prod_{i=1}^n (\lambda - a_{ii})$ as seen in the proof of corollary 3.81 and the a_{ii} are its eigenvalues.

Example 3.92. If $\mathbb{R}^3 \xrightarrow{f} \mathbb{R}^3$ has matrix representation matrix $A = \begin{pmatrix} 7 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 9 \end{pmatrix}$ with respect to $B = \{e_1, e_2, e_3\}$ then $\text{char}_f(\lambda) = \lambda^3 + 24\lambda^2 - 191\lambda + 504$ with roots $\lambda_1 = 7, \lambda_2 = 8, \lambda_3 = 9$ and corresponding eigenvectors $v_1 = e_1, v_2 = e_2, v_3 = e_3$.

Example 3.93. If $\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2$ has matrix representation matrix $A = \begin{pmatrix} 2 & -4 \\ -1 & -1 \end{pmatrix}$ with respect to $B = \{e_1, e_2\}$ then $\text{char}_A(\lambda) = \lambda^2 - \lambda - 6$ with roots $\lambda_1 = -2, \lambda_2 = 3$ and corresponding eigenvectors $v_1 = (1, 1), v_2 = (-4, 1)$. With respect to basis $B' = \{(1, 1), (-4, 1)\}$, f has matrix form $A' = \begin{pmatrix} -2 & 0 \\ 0 & 3 \end{pmatrix}$. Note that $\text{char}_{A'}(\lambda) = \text{char}_A(\lambda)$.

Theorem 3.94. (*Eigenvalue Decomposition*) Every matrix $A \in M(n, \mathbb{R})$ with n linearly independent eigenvectors v_1, \dots, v_n can be decomposed as $A = UDU^{-1}$ where $U \in M(n, \mathbb{R})$ is invertible and $D \in D(n, \mathbb{R})$ is diagonal.

Proof. As linear map, A has matrix representation D with respect to basis $B' = \{v_1, \dots, v_n\}$. By theorem 2.30, we get $D = A_{BB'}AA_{BB'}^{-1}$, or $A = A_{BB'}^{-1}DA_{BB'} = A_{B'B}DA_{B'B}^{-1}$ where $A_{BB'}$ is the change of basis matrix with i^{th} column v_i . \square

The diagonal entries of D are the eigenvalues of both D and A and their corresponding eigenvectors are the columns v_i of $A_{B'B}$.

Example 3.95. In example 3.93, $A_{B'B} = \begin{pmatrix} 1 & -4 \\ -1 & -1 \end{pmatrix}$ with inverse $A_{B'B}^{-1} = A_{BB'} = \begin{pmatrix} 1/5 & 4/5 \\ -1/5 & 1/5 \end{pmatrix}$. So $\begin{pmatrix} 2 & -4 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -4 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1/5 & 4/5 \\ -1/5 & 1/5 \end{pmatrix}$.

Example 3.96. If $\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2$ is rotation by θ counterclockwise then it has matrix representation $A = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ with respect to $B = \{e_1, e_2\}$. It has characteristic polynomial $\text{char}_A(\lambda) = \lambda^2 - 2\cos \theta \lambda + 1$ with discriminant $\Delta = -4\sin^2 \theta \leq 0$. When $\theta = n\pi, n$ even then $\lambda_1 = \lambda_2 = 1$ and $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. When $\theta = n\pi, n$ odd then $\lambda_1 = \lambda_2 = -1$ and $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. When $\theta \neq n\pi$ then $\text{char}_A(\lambda)$ has no real root and A does not have real eigenvalues, eigenvectors and such decomposition.

The above example shows that a real matrix may not satisfy the hypothesis of theorem 3.94 because a polynomial over \mathbb{R} may not have real roots. But it always has complex roots and this leads to the following result.

Theorem 3.97. (*Schur Decomposition*) Every matrix $A \in M(n, \mathbb{C})$ can be decomposed as $A = UDU^{-1}$ where $U \in M(n, \mathbb{C})$ is unitary and $D \in U(n, \mathbb{C})$ is upper triangular.

Proof. Over \mathbb{C} , every polynomial has a root, so A has an eigenvalue λ corresponding to an eigenspace V_λ . Let V_λ^\perp be its orthogonal complement. Let B_1, B_2 and $\{B_1, b_2\}$ be

orthonormal bases for V_λ , V_λ^\perp and $V_\lambda \oplus V_\lambda^\perp$. Then A has representation $\begin{pmatrix} B_1 & B_2 \end{pmatrix}^* A \begin{pmatrix} B_1 & B_2 \end{pmatrix} = \begin{pmatrix} \lambda I_\lambda & A_{12} \\ 0 & A_{22} \end{pmatrix}$ with respect to this basis. Induction on n finishes the proof. \square

A unitary matrix $U \in M(n, \mathbb{C})$ by definition satisfies $U^{-1} = U^*$ where U^* denotes the conjugate transpose of U . Again, the diagonal entries of D are the eigenvalues of both D and A .

Theorem 3.98. (*Eigenvalue Decomposition for Symmetric Matrices*) Every symmetric matrix $A \in M(n, \mathbb{R})$ can be decomposed as $A = UDU^{-1}$ where $U \in M(n, \mathbb{R})$ is orthogonal and $D \in D(n, \mathbb{R})$ is diagonal.

Proof. By theorem 3.97 and symmetry, we have $D = U^*AU = U^*A^*U = U^*(UDU^*)^*U = U^*U^{**}D^*U^*U = U^*UD^*U^*U = D^*$. So D is real diagonal. Similar argument shows U is real. \square

This theorem implies every symmetric matrix has real eigenvalues corresponding to n orthonormal eigenvectors. Here are some additional facts.

- $\text{rank}(A) = \text{rank}(D) =$ number of nonzero eigenvalues.
- the image of A is spanned by the v_i with nonzero eigenvalues.
- the kernel of A is spanned by the v_i with zero eigenvalues.

When A is positive semidefinite, $0 \leq v_i^t A v_i = v_i^t U D U^{-1} v_i = v_i^t U D e_i = v_i^t U \lambda_i e_i = \lambda_i v_i^t v_i = \lambda_i$. Hence all eigenvalues are nonnegative and they are positive iff A is positive definite. We will need the following application of the theorem to positive semidefinite matrices later.

Theorem 3.99. (*LDU Decomposition for Positive Semidefinite Matrices*) Every positive semidefinite matrix $A \in M(n, \mathbb{R})$ can be decomposed as $A = LDL^t$ where $L \in L(n, \mathbb{R})$ is unit lower triangular and $D \in D(n, \mathbb{R})$ is diagonal.

Proof. use theorem 3.98. \square

This LDU decomposition is unique for positive definite matrices. Note that we do not claim L to be orthogonal, otherwise we would have $L^t = L^{-1}$ above.

Exercise 3.100. Consider $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ in example 3.65.

- a. Compute its characteristic polynomial.
 - b. Compute its eigenvalues and eigenvectors.
 - c. Compute its eigenvalue decomposition.
 - d. Use this decomposition to compute its inverse and compare with previous result.
- This is the third way to find inverse of an invertible matrix.
- e. Read off its determinant and trace.

Matrices A and D in these decompositions are said to be similar. In general, we say two matrices $A, B \in M(n, F)$ are similar if there exists an invertible matrix $U \in M(n, F)$ such that $A = UBU^{-1}$. Such an equality corresponds to a change of basis in matrix representation for a linear map. Similarity is an equivalence relation for matrices and each similarity class represent the same linear map, given a basis has been fixed for F^n .

It is obvious that determinant is an invariant of the similarity classes, i.e. it is basis independent. The same holds for trace. This implies

- $\det(A) = \prod_{i=1}^n \lambda_i.$
- $\operatorname{tr}(A) = \sum_{i=1}^n \lambda_i.$
- $\operatorname{char}_A(\lambda) = \lambda^n - \operatorname{tr}(A)\lambda^{n-1} + \dots + (-1)^n \det(A).$

Exercise 3.101. Show that similarity is an equivalence relation on $M(n, F)$.

3.11. Singular Values, Singular Vectors and Singular Value Decomposition.

Eigenvalue decomposition for symmetric matrices paves the way for us to seek a decomposition for general matrix $A \in M(m, n, F)$.

Theorem 3.102. (*Singular Value Decomposition*) Every matrix $A \in M(m, n, \mathbb{R})$ can be decomposed as $A = UDV^{-1}$ where $U \in M(m, \mathbb{R})$ and $V \in M(n, \mathbb{R})$ are orthogonal and $D \in M(m, n, \mathbb{R})$ is diagonal with nonnegative entries.

Proof. Assume $n \leq m$ without loss of generality and consider the positive semidefinite Gram matrix $A^t A \in M(n, \mathbb{R})$. By theorem 3.98, it has eigenvalues $\lambda_1, \dots, \lambda_n$ corresponding to orthonormal eigenvectors $v_1, \dots, v_n \in \mathbb{R}^n$ where the first $r \leq n$ eigenvalues are nonzero. For $1 \leq j \leq r$, set $\sigma_j = \sqrt{\lambda_j}$ and $u_j = \sigma_j^{-1} A v_j \in \mathbb{R}^m$. Complete u_1, \dots, u_r to an orthonormal basis $\{u_1, \dots, u_m\}$ for \mathbb{R}^m . If we use the u_i as columns for $U \in M(m, \mathbb{R})$ and the v_j as columns for $V \in M(n, \mathbb{R})$ then they are orthogonal matrices and

$$(U^t A V)_{ij} = u_i^t A v_j = \begin{cases} u_i^t 0 = 0 & \text{if } j > r \\ u_i^t \sigma_j u_j = \sigma_j \delta_{ij} & \text{if } j \leq r \end{cases}$$

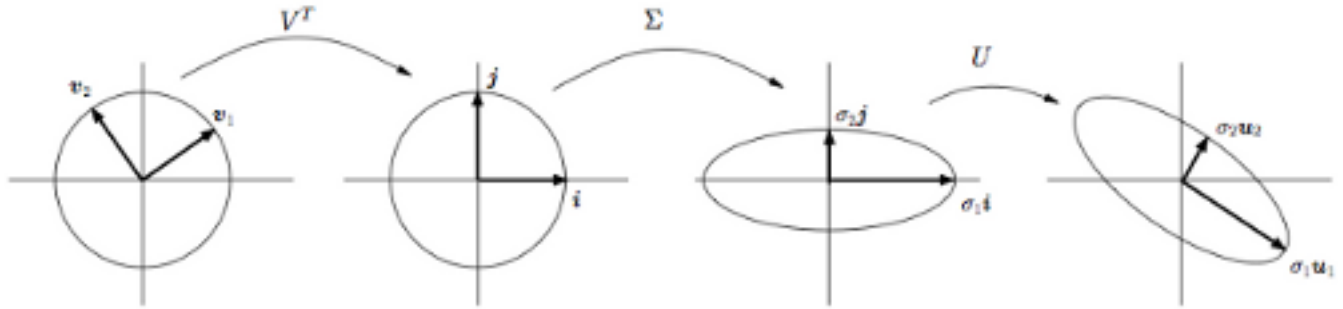
Hence $U^t A V = D$ is our upper triangular matrix and $A = U D V^t$ as desired. \square

The columns u_i of U are eigenvectors of $A A^t$ and the diagonal entries σ_j of D are square roots of the nonnegative eigenvalues λ_j shared by both $A^t A$ and $A A^t$, often arranged in decreasing order via a permutation of the u_i and the v_j . They are called singular values while the columns of U are called left singular vectors and the columns of V are called right singular vectors, hence the name singular value decomposition. Here is a summary plus some other facts.

- $A^t A v_j = \lambda_j v_j, 1 \leq j \leq n$ where $\lambda_j > 0$ for $1 \leq j \leq r$ and $\lambda_j = 0$ for $r + 1 \leq j \leq n$.
- $\sigma_j = \sqrt{\lambda_j} > 0, 1 \leq j \leq r$.
- $A v_j = \sigma_j u_j, 1 \leq j \leq r$.
- $A v_j = 0, r + 1 \leq j \leq n$.
- u_{n+1}, \dots, u_m can vary so long as $\{u_1, \dots, u_m\}$ are orthonormal.
- $\operatorname{rank}(A) = \operatorname{rank}(D) = r$ the number of nonzero singular values.
- the image of A is spanned by the first r columns of U .
- the kernel of A is spanned by the last $(n - r)$ columns of V .
- the image of A^t is spanned by the first r columns of V .
- the kernel of A^t is spanned by the last $(m - r)$ columns of V .
- all singular values are positive iff all eigenvalues of $A^t A$ is positive iff $A^t A$ is positive definite iff $A^t A$ is invertible iff it has rank n iff A has rank n iff $r = n$.

- singular value decomposition and eigenvalue decomposition coincide iff A is positive semidefinite.

The case $m \leq n$ is analogous. The next figure illustrates how singular value decomposition works when $n = m = 2$. Choose the columns v_1 and v_2 of V as basis vectors, then there are two rotations $V^t(v_1) = e_1$ and $V^t(v_2) = e_2$. After that, there are two extensions $D(e_1) = \sigma_1 e_1$ and $D(e_2) = \sigma_2 e_2$. Lastly, there are two rotations $U(\sigma_1 e_1) = \sigma_1 u_1$ and $U(\sigma_2 e_2) = \sigma_2 u_2$.



Example 3.103. Consider the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix}$. The matrix $A^t A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$ has characteristic polynomial $\text{char}_{A^t A}(\lambda) = \lambda^2 - 6\lambda + 8$ with eigenvalues 4 and 2 corresponding to orthonormal eigenvectors $v_1 = (\sqrt{2}/2, \sqrt{2}/2)$ and $v_2 = (\sqrt{2}/2, -\sqrt{2}/2)$. Hence $\sigma_1 = 2, \sigma_2 = \sqrt{2}$ and $u_1 = \sigma_1^{-1} A v_1 = (\sqrt{2}, \sqrt{2}, 0), u_2 = \sigma_2^{-1} A v_2 = (0, 0, \sqrt{2})$. If we add $u_3 = u_1 \times u_2$ to complete u_1, u_2 to an orthonormal basis then

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \sqrt{2}/2 & 0 & \sqrt{2}/2 \\ \sqrt{2}/2 & 0 & -\sqrt{2}/2 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & \sqrt{2} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{2}/2 & \sqrt{2}/2 \\ \sqrt{2}/2 & -\sqrt{2}/2 \end{pmatrix}$$

We could use $u_3 = (-\sqrt{2}/2, \sqrt{2}/2)$ and the above equation would still hold, demonstrating the nonuniqueness of U and as well of V in general cases. Moreover, $\text{rank}(A) = \text{rank}(D) = r = 2$ while $\ker(A) = \{0\}$ and $\text{im}(A) = \text{Span}(v_1, v_2) \subsetneq \mathbb{R}^3$.

Example 3.104. Consider the total least squares problem of finding $w \in \mathbb{R}^n$ such that $\|Aw\|_2 = \min\{\|Av\|_2, \|v\|_2 = 1\}$ for any matrix $A \in M(m, n, \mathbb{R})$. The solution turns out to be the right singular vector of A corresponding to the smallest singular value. One can find other applications of singular value decomposition to data compression and principal component analysis in various fields.

Exercise 3.105. Reconsider the wide matrix $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}$ in example 3.54.

- Compute the characteristic polynomial, eigenvalues and orthonormal eigenvectors for AA^t .
- Compute the characteristic polynomial, eigenvalues and orthonormal eigenvectors for $A^t A$.

- c. Compute the singular values and orthonormal left singular vectors.
- d. Compute the singular value decomposition.
- e. Use this decomposition to compute right inverse for A and compare with previous result. This is the second way to find right inverse of a right invertible matrix.

Part 2. Matrix Algorithms

Linear algebra has extensive applications in many modern disciplines, especially those that work with data in Euclidean spaces. One major application is to solve a system of equations

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

where $a_{ij}, b_i \in F$. If we view $A = (a_{ij}) \in M(m, n, F)$ as a linear map $F^n \xrightarrow{A} F^m$ then we are looking to find solution $x = (x_1, \dots, x_n) \in F^n$ such that $Ax = b$ where $b = (b_1, \dots, b_m) \in F^m$. Below are some of the scenarios, but not all.

- i. for each $b \in F^m$ there are infinitely many solutions. This means $m < n$ and A is right invertible with full image.
- ii. for each $b \in F^m$ there is a unique solution. This means $m = n$ and A is invertible.
- iii. for some $b \in F^m$ there is no solution. This means $\text{im}(A) \subsetneq F^m$. The reason may be $m > n$ even though A is left invertible with trivial kernel. Or it may be $m \leq n$ but $\text{rank}(A) < m \leq n$ and A is not left invertible.

4. COMPLEXITY OF MATRIX ALGORITHMS

As engineers, you devise efficient ways to solve such systems of equations when A falls into one of these scenarios. You also care about the cost to solve them.

Definition 4.1. A flop is an execution of either $+$ or \cdot in F .

To evaluate the complexity of an algorithm, we write the total number of flops in that algorithm as a function of the sizes of objects at hand, for example $f(m, n)$ for matrices $A \in M(m, n, F)$, and simplify the expression by discarding minor terms. Flop count played a larger role when flops were slow and their count gave an accurate prediction of time cost. Nowadays that is no longer the case and flop count gives a rough estimate of time cost, especially when we consider its order.

Example 4.2. Taking inner product $\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle$ takes n multiplications and $n - 1$ additions for $2n - 1$ flops. We only keep $f(n) = 2n$ as a polynomial of the size n of our vectors.

Example 4.3. Adding $A, B \in M(m, n, F)$ takes mn additions for mn flops. We keep $f(m, n) = mn$ as a polynomial of the size of our matrices.

Example 4.4. If $A \in M(m, n, F)$ and $x \in F^n$ then computing Ax takes m inner products, hence $m(2n - 1)$ flops. We keep $f(m, n) = 2mn$. In case $A \in M(n, F)$ is diagonal then computing Ax takes only n flops. In another case $A = BC$ where $B \in M(m, p, F)$ and $C \in M(p, n, F)$ then computing $Ax = BCx$ takes $2pn + 2mp = 2p(m + n)$ flops, much fewer than $2mn$ when $p \ll \min\{m, n\}$.

Example 4.5. Multiplying two matrices $A \in M(m, n, F)$, $B \in M(n, p, F)$ takes mn inner products of vectors of size n for $mp(2n-1)$ flops, or $2mnp$ if $n \gg 1$. In case $m = p$ and AB is symmetric, this number decreases to $(m^2/2 + m)(2n-1) = m(m+1)(2n-1)/2$, or m^2n as the leading term. Flop count in multiplying more than two matrices depends on how we parse the product. For $A \in M(m, n, F)$, $B \in M(n, p, F)$, $C \in M(p, q, F)$, computing $(AB)C$ takes $2mp(n+q)$ flops while computing $A(BC)$ takes $2nq(m+p)$ flops. The first computation is better when $2mp(n+q) < 2nq(m+p)$, i.e. when $1/n + 1/q < 1/m + 1/p$.

Example 4.6. Consider the system $Ax = b$ where $A \in M(n, F)$ is triangular. Assume A is lower triangular.

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Surely $x_1 = b_1/a_{11}$, $x_2 = (b_2 - a_{21}x_1)/a_{22}$, $x_3 = (b_3 - a_{31}x_1 - a_{32}x_2)/a_{33}$, \dots , $x_n = (b_n - a_{n1}x_1 - a_{n2}x_2 - \dots - a_{n(n-1)}x_{n-1})/a_{nn}$, each step taking $1, 3, 5, \dots, (2n-1)$ flops for a total of n^2 flops. This algorithm is called forward substitution. If A is diagonal then there are only n divisions, so the algorithm takes n flops. Or if A is sparse with at most k nonzeros in each row then each substitution step takes $2k-1$ flops and the algorithm takes $2(k-1)n \approx 2kn$ flops. If A is upper triangular, the algorithm is called backward substitution and works in a transposed fashion. Whether we get through all the substitution steps, i.e. whether $Ax = b$ is solvable depends on the innate properties of A . By corollary 3.81, the system has unique solution iff A is invertible iff all its diagonal entries are nonzero. If we write $A^{-1} = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}$ in that case then $AA^{-1} = I$ sets up n systems of linear equations $Ax_1 = e_1, \dots, Ax_n = e_n$. We can perform either algorithm above to solve each equation for x_i and get A^{-1} .

5. CHOLESKY DECOMPOSITION

We consider solving a system of equations $Ax = b$ where $A \in M(n, \mathbb{R})$ is positive definite.

Theorem 5.1. (*Cholesky Decomposition*) Every positive semidefinite matrix $A \in M(n, \mathbb{R})$ can be decomposed as $A = LL^t$ where $L \in M(n, \mathbb{R})$ is lower triangular.

Proof. By theorem 3.99, $A = L'DL^t = L'BBL^t = L'BB^tL^t = (L'B)(L'B)^t = LL^t$ where $B = \sqrt{D}$ is triangular and L, L' are lower triangular. \square

This Cholesky decomposition is unique for positive definite matrices and this is their form as a Gram matrix, recall 3.36. All matrices involved are then invertible. Again we do not claim L to be orthogonal, otherwise we would have $L^t = L^{-1}$ above.

Example 5.2. Positive semidefinite $A = (a_1, \dots, a_n) \in M(n, F)$ with nonnegative a_i has Cholesky decomposition $(\sqrt{a_1}, \dots, \sqrt{a_n})(\sqrt{a_1}, \dots, \sqrt{a_n})$. When A has some zero a_i then perhaps we can find another decomposition, showing nonuniqueness.

Example 5.3. Positive definite $\begin{pmatrix} 4 & 2 \\ 2 & 10 \end{pmatrix}$ has unique Cholesky decomposition $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$.

We will return to how Cholesky decomposition works and how it takes $n^3/3$ flops. Meanwhile, let's see what it does for us. Suppose we had to solve a system of linear equations $Ax = b$ where A is positive definite. If we write $Ax = LL^t x = Ly = b$ then we see,

- Cholesky decomposition takes $n^3/3$ flops.
- Solving $Ly = b$, L lower triangular takes n^2 flops.
- Solving $L^t x = y$, L upper triangular takes n^2 flops.
- Hence the total cost is $n^3/3 + 2n^2 \approx n^3/3$ flops.

Example 5.4. Suppose we had to solve $4x_1 + 2x_2 = 3, 2x_1 + 10x_2 = 5$. Factoring $\begin{pmatrix} 4 & 2 \\ 2 & 10 \end{pmatrix}$ into $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ takes $2^3/3$ flops. Solving $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$ to get $(y_1, y_2) = (3/2, 7/6)$ takes 2^2 flops. Lastly solving $\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3/2 \\ 7/6 \end{pmatrix}$ to get $(x_1, x_2) = (5/9, 7/18)$ takes another 2^2 flops. The total cost is $8/3 + 2 \cdot 2^2$ flops.

Suppose we had to solve multiple systems $Ax_1 = b_1, \dots, Ax_m = b_m$, which is equivalent to solving the matrix equation $A_{n \times n} X_{n \times m} = B_{n \times m}$ where X has i^{th} column x_i and B has j^{th} column b_j . Of course we don't repeat Cholesky decomposition, so the total flop count is $n^3/3 + 2mn^2$. The effort of solving a small number of systems with the same A is roughly the effort of solving one system. This applies to finding the inverse of A , i.e. finding X such that $AX = I$ since we know any positive definite matrix $A = LL^t$ is invertible by corollary 3.48 with inverse $A^{-1} = (L^t)^{-1}L^{-1} = (L^{-1})^t L^{-1}$. The cost for A^{-1} is then $n^3/3 + 2n \cdot n^2 = 7n^3/3$. Is this cheaper than finding L^{-1} and multiplying with $(L^{-1})^t$?

We can also prove existence of Cholesky decomposition for positive definite matrix $A = LL^t$ by recursion, starting with the partition

$$\begin{pmatrix} a_{11} & A_{21}^t \\ A_{21} & A_{22} \end{pmatrix} = \begin{pmatrix} l_{11} & 0 \\ L_{21} & L_{22} \end{pmatrix} \begin{pmatrix} l_{11}^t & L_{21}^t \\ 0 & L_{22}^t \end{pmatrix} = \begin{pmatrix} l_{11}^2 & l_{11} L_{21}^t \\ l_{11} L_{21} & L_{21} L_{21}^t + L_{22} L_{22}^t \end{pmatrix}$$

Hence $l_{11} = \sqrt{a_{11}}$, $L_{21} = \frac{1}{l_{11}} A_{21}$, and $L_{22} L_{22}^t = A_{22} - L_{21} L_{21}^t$. This means we now must find L_{22} in Cholesky decomposition of the positive definite matrix $A_{22} - L_{21} L_{21}^t = A_{22} - \frac{1}{a_{11}} A_{21} A_{21}^t$ of smaller size $(n-1) \times (n-1)$. Eventually we arrive at Cholesky decomposition of a 1×1 matrix, which is just taking square root. As a process

1. Compute the first column of $l_{11} = \sqrt{a_{11}}$ and $L_{21} = \frac{1}{l_{11}} A_{21}$ of L .
2. Compute Cholesky decomposition $A_{22} - L_{21} L_{21}^t = L_{22} L_{22}^t$.

The whole algorithm takes $n^3/3$ flops. It also verifies whether a matrix A is positive definite, as it will stall at some recursive step with $a_{11} = 0$ if A is not.

Exercise 5.5. Perform Cholesky decomposition for $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$.

6. LU DECOMPOSITION

Next, we consider solving $Ax = b$ where $A \in M(n, \mathbb{R})$ is invertible, using the same factor-solve approach as in the previous subsection. Suppose we can factor $A = A_1 \dots A_k$

where each A_i is special and k is small in f flops. Then we can solve $A_1x_1 = b, A_2x_2 = x_1, \dots, A_kx_k = x_{k-1}$ sequentially in g flops. The total flop count is $f + g \approx f$ when f is dominant.

Example 6.1. Solving $Ax = b$ where $A \in M(n, \mathbb{R})$ is positive definite costs $n^2/3 + 2n^2$ flops.

Again this approach is effective in solving m systems of equations sharing the same coefficient matrix A , as the cost is then $f + mg \approx f$ when f is dominant. We look at the existence of such decomposition.

Theorem 6.2. (*LU Decomposition for Invertible Matrices*) Every invertible matrix $A \in M(n, \mathbb{R})$ can be decomposed as $A = PLU$ where $P \in M(n, \mathbb{R})$ is permuting, $L \in L(n, \mathbb{R})$ is unit lower triangular and $U \in U(n, \mathbb{R})$ is upper triangular.

Proof. use theorem 3.94. □

Example 6.3. $\begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 3 \\ 3 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 3/2 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 0 & -1/2 & -7/2 \\ 0 & 0 & -11 \end{pmatrix}$. Wolframalpha will do this with command “LU decomposition”.

Here is the explicit algorithm to solve a system $Ax = b$ for invertible $A \in M(n, \mathbb{R})$.

1. Factoring $A = PLU$ in $2n^3/3$ flops.
2. Computing $z = P^tb$ where $Pz = b$ in 0 flop.
3. Forward substituting for $Ly = z$ in n^2 flops.
4. Backward substituting for $Ux = y$ in n^2 flops.

Total cost is $2n^3/3 + 2n^2 \approx 2n^3/3$ flops. This is the standard method in the industry.

Example 6.4. Given a system $2x_1 + x_2 + 3x_3 = 4, 0x_1 + 2x_2 + 3x_3 = 2, 3x_1 + x_2 + x_3 = 1$ we form A as in example 6.3 and get its decomposition. Next we calculate

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 3/2 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 4 \\ -5 \\ -18 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 & 3 \\ 0 & -1/2 & -7/2 \\ 0 & 0 & -11 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ -5 \\ -18 \end{pmatrix}, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -24/11 \\ -16/11 \\ 18/11 \end{pmatrix}$$

What step 2 actually does is follow $x = A^{-1}b = U^{-1}L^{-1}P^tb$. Moreover, solving multiple systems of m equations with the same invertible coefficient matrix $A \in M(n, \mathbb{R})$ would cost $2n^3/3 + 2mn^2 \approx 2n^3/3$ flops if $n \gg m$. Lastly, solving for A^{-1} is the same as solving n systems $Ax_1 = e_1, \dots, Ax_n = e_n$ where x_i is the i^{th} column of A^{-1} . This would take $2n^3/3$ flops for LU decomposition plus $n \cdot 2n^2$ flops for n forward substitutions and n backward substitutions.

6.1. LU Decomposition without Pivoting. We can also prove existence of LU decomposition for invertible matrix $A = PLU$ by recursion. Up first is the simple case $P = I$ and $A = LU$, which sets up a matrix equation in blocks,

$$\begin{pmatrix} a_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ L_{21} & L_{22} \end{pmatrix} \begin{pmatrix} u_{11} & U_{12} \\ 0 & U_{22} \end{pmatrix}$$

where $L_{21} \in M(n-1, 1, \mathbb{R})$, $U_{12} \in M(1, n-1, \mathbb{R})$, $L_{22} \in M(n-1, n-1, \mathbb{R})$ is unit lower triangular and $U_{22} \in M(n-1, n-1, \mathbb{R})$ is invertible upper triangular. This reduces the problem to LU decomposition for an $(n-1) \times (n-1)$ matrix $A_{22} - \frac{1}{a_{11}}A_{21}A_{12} = L_{22}U_{22}$. Repeat until we arrive at an 1×1 matrix, whose factors are square roots. This algorithm works only if $a_{11} \neq 0$ at each recursive step and no permutation is needed to permute a nonzero with a_{11} , hence the name no pivoting (or no permutation). Step by step

1. Calculate the first row of $u_{11} = a_{11}$, $U_{12} = A_{12}$ of U .
2. Calculate the first column $L_{21} = \frac{1}{a_{11}}A_{21}$ of L .
3. Factor $A_{22} - \frac{1}{a_{11}}A_{21}A_{12}$.

Example 6.5. Consider the invertible matrix $\begin{pmatrix} 4 & 3 & 2 \\ 1 & 0 & 1 \\ 2 & 3 & 4 \end{pmatrix}$.

In step 1

$$u_{11} = a_{11} = 4, U_{12} = A_{12} = \begin{pmatrix} 3 & 2 \end{pmatrix}$$

In step 2

$$L_{21} = \frac{1}{4}A_{12} = \frac{1}{4} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1/4 \\ 1/2 \end{pmatrix}$$

In step 3

$$A_{22} - \frac{1}{4}A_{12}A_{21} = \begin{pmatrix} 0 & 1 \\ 3 & 4 \end{pmatrix} - \frac{1}{4} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \end{pmatrix} = \begin{pmatrix} -3/4 & 1/2 \\ 3/2 & 3 \end{pmatrix}$$

is invertible so we start over recursively.

Again

$$u_{11} = a_{11} = -\frac{3}{4}, U_{12} = A_{12} = \frac{1}{2}$$

Next

$$L_{21} = \frac{1}{a_{11}}A_{21} = -\frac{4}{3} \frac{3}{2} = -2$$

Thirdly

$$A_{22} - \frac{1}{a_{11}}A_{21}A_{12} = 3 + \frac{4}{3} \frac{3}{2} \frac{1}{2} = 4 = 2 \cdot 2$$

Now we put everything together

$$\begin{pmatrix} -3/4 & 1/2 \\ 3/2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & 2 \end{pmatrix} \begin{pmatrix} -3/4 & 1/2 \\ 0 & 2 \end{pmatrix} = L_{22}U_{22}$$

$$\begin{pmatrix} 4 & 3 & 2 \\ 1 & 0 & 1 \\ 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1/4 & 1 & 0 \\ 1/2 & -2 & 2 \end{pmatrix} \begin{pmatrix} 4 & 3 & 2 \\ 0 & -3/4 & 1/2 \\ 0 & 0 & 2 \end{pmatrix} = LU$$

Example 6.6. The matrix $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}$ can not be factored as $\begin{pmatrix} 1 & 0 \\ l_{21} & 1 \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ 0 & u_{22} \end{pmatrix}$ since the algorithm halts at first step with $a_{11} = 0$.

6.2. Permutation Matrices. The above example shows that our algorithm will not start when $a_{11} = 0$. We must swap the first row with another row i^{th} with nonzero a_{i1} in order to proceed. The existence of such a_{i1} is guaranteed by invertibility of A and such movement does not change our solution. This can be done by a permutation matrix P . Let $\sigma \in S_n$ be a permutation of $\{1, \dots, n\}$. We can view it as a map $V \xrightarrow{\sigma} V, (x_1, \dots, x_n) \mapsto (x_{\sigma(1)}, \dots, x_{\sigma(n)})$. This map is linear with matrix representation $A_\sigma = (a_{ij})$ where $a_{ij} = 1$ if $\sigma(i) = j$ and $a_{ij} = 0$ otherwise.

Example 6.7. If $\sigma = (1324)$ then it maps (x_1, x_2, x_3, x_4) to (x_4, x_3, x_1, x_2) in \mathbb{R}^4 and

$$A_\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

If σ^{-1} is the inverse of σ as permutations then $\sigma^{-1}(j) = i$. As linear maps, σ^{-1} is the inverse of σ and $A_{\sigma^{-1}} = (a_{ji}) = A_\sigma^t = A_\sigma^{-1}$. That means solving a system $Ax = b$ where A is a permutation matrix costs 0 flop, with $x = A^t b$.

Exercise 6.8. Show that the map $V \xrightarrow{\sigma} V, (x_1, \dots, x_n) \mapsto (x_{\sigma(1)}, \dots, x_{\sigma(n)})$ is linear.

Exercise 6.9. Given the permutation $\sigma = (1342) \in S_4$,

- Compute $\sigma(e_i)$ and its matrix representation A_σ with respect to $\{e_1, \dots, e_4\}$.
- Compute the inverse permutation σ^{-1} and its matrix representation $A_{\sigma^{-1}}$.
- Verify that $P_{\sigma^{-1}} = P_\sigma^t$ and $P_\sigma P_{\sigma^{-1}} = I$.
- Compute $P_\sigma \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$ to see how it permutes the rows.

6.3. LU Decomposition with Pivoting. We now describe an LU decomposition for invertible A with possibly zero a_{11} by induction. Any invertible $A = (a_{ij}) \in M(1, \mathbb{R})$ can be written as $(1)(1)(a_{11})$. Suppose any invertible matrix $A \in M(n-1, \mathbb{R})$ has an LU decomposition. Consider invertible $A \in M(n, \mathbb{R})$. Since its first column is nonzero, there exists a permutation matrix P_1^t such that $A' = P_1^t A = \begin{pmatrix} a'_{11} & A'_{12} \\ A'_{21} & A'_{22} \end{pmatrix}$ with $a'_{11} \neq 0$. The difference $A'_{22} - \frac{1}{a'_{11}} A'_{21} A'_{12}$ is called the Schur complement of a'_{11} in A' . It is invertible of

size $(n-1) \times (n-1)$ so it has a LU decomposition $P_2 L_{22} U_{22}$ by induction. But then

$$\begin{aligned}
 A &= P_1 A' \\
 &= P_1 \begin{pmatrix} a'_{11} & A'_{12} \\ A'_{21} & A'_{22} \end{pmatrix} \\
 &= P_1 \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix} \begin{pmatrix} a'_{11} & A'_{12} \\ P_2^t A'_{21} & P_2^t A'_{22} \end{pmatrix} \\
 &= P_1 \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix} \begin{pmatrix} a'_{11} & A'_{12} \\ P_2^t A'_{21} & L_{22} U_{22} + \frac{1}{a'_{11}} P_2^t A'_{21} A'_{12} \end{pmatrix} \\
 &= P_1 \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{1}{a'_{11}} P_2^t A'_{21} & L_{22} \end{pmatrix} \begin{pmatrix} a'_{11} & A'_{12} \\ 0 & U_{22} \end{pmatrix}
 \end{aligned}$$

We are done. Summarily, the algorithm takes $2n^3/3$ flops and runs as follows

1. Permute A to A' by a permutation matrix P_1^t so that $a'_{11} \neq 0$.
2. Compute LU decomposition for $A'_{22} - \frac{1}{a'_{11}} A'_{21} A'_{12} = P_2 L_{22} U_{22}$.
3. Put together $P = P_1 \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix}$, $L = \begin{pmatrix} 1 & 0 \\ \frac{1}{a'_{11}} P_2^t A'_{21} & L_{22} \end{pmatrix}$ and $U = \begin{pmatrix} a'_{11} & A'_{12} \\ 0 & U_{22} \end{pmatrix}$.

Example 6.10. Consider the invertible matrix $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 2 & 3 & 3 \end{pmatrix}$.

In step 1, we permute it to $A' = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 2 & 3 & 3 \end{pmatrix}$ with $a'_{11} = 1$ by $P_1^t = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

In step 2, $A'_{22} - \frac{1}{a'_{11}} A'_{21} A'_{12} = \begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix} - \frac{1}{1} \begin{pmatrix} 0 \\ 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is invertible so we start over recursively. This time $a'_{11} = 1$ is already nonzero so $P_2^t = I$.

Next $A'_{22} - \frac{1}{a'_{11}} A'_{21} A'_{12} = -1 - \frac{1}{1} \cdot 1 \cdot 1 = (1)(1)(-2)$.

So in step 3, $P_3 = 1$, $L_3 = 1$ and $U_3 = -2$.

Again in step 3, $P_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $L_{22} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $U_{22} = \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}$.

Lastly $P = P_1 \begin{pmatrix} 1 & 0 \\ 0 & P_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $L = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{a'_{11}} P_2^t A'_{21} & L_{22} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} a'_{11} & A'_{12} \\ 0 & U_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix}$.

Exercise 6.11. Perform LU decomposition for $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$.

6.4. Effect of Rounding in Using LU Decomposition. We discuss the effect of rounding errors on the accuracy of the LU decomposition method for solving a system of

linear equations. Consider the system $10^{-5}x_1 + x_2 = 1, x_1 + x_2 = 0$. Its exact solution is $(\frac{-1}{1-10^{-5}}, \frac{1}{1-10^{-5}})$. On the other hand, $A = \begin{pmatrix} 10^{-5} & 1 \\ 1 & 1 \end{pmatrix}$ has two LU decompositions

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 10^5 & 1 \end{pmatrix} \begin{pmatrix} 10^{-5} & 1 \\ 0 & 1 - 10^5 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 10^{-5} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 - 10^{-5} \end{pmatrix}$$

If we introduce some errors by rounding $a_{22} = 1 - 10^5 = -0.9999 \cdot 10^5$ in the first decomposition to four significant digits $-1.0000 \cdot 10^5 = -10^5$ and proceed to solve the system then we get solution $(0, 1)$. The difference in result is huge. This phenomenon is called numerical instability and an algorithm is called numerically unstable if small errors along the way can cause significant error in the end. Solving linear equations using LU decomposition is numerically unstable.

Similarly, if we round $a_{22} = 1 - 10^{-5} = 0.99999$ in the second decomposition to 1 and solve the system then we get solution $(-1, 1)$. In this case, the difference is tiny, 10^{-5} of the same order as the error we manufactured. This means choice of decomposition, i.e. choice of permutation matrix P , matters. Careful error analysis and extensive practical experience tell us to go with P that permutes the entry of largest absolute value in the first column of A to a'_{11} . Our example agrees with this.

7. QR DECOMPOSITION

Now, we consider solving $Ax = b$ where $A \in M(m, n, \mathbb{R})$ is left invertible, again using the same factor-solve approach as in the previous two subsections. Recall the characterization of left invertible matrices in theorem 3.50 and corollary 3.51.

Theorem 7.1. (*QR Decomposition for Left Invertible Matrices*) Every left invertible matrix $A \in M(m, n, \mathbb{R})$ can be decomposed as $A = QR$ where $Q \in M(m, n, \mathbb{R})$ is orthogonal with $Q^t Q = I_n$ and $R \in U(n, \mathbb{R})$ is upper triangular with positive diagonal entries.

Proof. use theorem 3.94. □

The theorem only shows existence of Q and R . Here is how to get them. If we partition A, Q, R as

$$A = \begin{pmatrix} a_1 & A_2 \end{pmatrix} \quad Q = \begin{pmatrix} q_1 & Q_2 \end{pmatrix} \quad R = \begin{pmatrix} r_{11} & R_{12} \\ 0 & R_{22} \end{pmatrix}$$

then

$$\begin{aligned} \begin{pmatrix} a_1 & A_2 \end{pmatrix} &= \begin{pmatrix} q_1 & Q_2 \end{pmatrix} \begin{pmatrix} r_{11} & R_{12} \\ 0 & R_{22} \end{pmatrix} \\ &= \begin{pmatrix} q_1 r_{11} & q_1 R_{12} + Q_2 R_{22} \end{pmatrix} \end{aligned}$$

where $a_1 \in M(m, 1, \mathbb{R})$, $A_2 \in M(m, n-1, \mathbb{R})$, $q_1 \in M(m, 1, \mathbb{R})$, $Q_2 \in M(m, n-1, \mathbb{R})$, $r_{11} \in M(1, 1, \mathbb{R})$, $R_{12} \in M(1, n-1, \mathbb{R})$, $R_{22} \in M(n-1, n-1, \mathbb{R})$. For Q to be orthogonal

$$\begin{aligned} Q^t Q &= \begin{pmatrix} q_1^t \\ Q_2^t \end{pmatrix} \begin{pmatrix} q_1 & Q_2 \end{pmatrix} \\ &= \begin{pmatrix} q_1^t q_1 & q_1^t Q_2 \\ Q_2^t q_1 & Q_2^t Q_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

we must have $q_1^t q_1 = 1$, $q_1^t Q_2 = 0$, $Q_2^t Q_2 = I$. For R to be upper triangular with positive diagonal entries, we must have $r_{11} > 0$ and R_{22} is upper triangular with positive diagonal entries.

Putting things together, firstly we see $a_1 = q_1 r_{11}$ so we choose $r_{11} = \|a_1\|$, $q_1 = \frac{a_1}{r_{11}}$. Next we see $A_2 = q_1 R_{12} + Q_2 R_{22}$ which implies $q_1^t A_2 = q_1^t q_1 R_{12} + q_1^t Q_2 R_{22} = R_{12}$. So we compute $R_{12} = q_1^t A_2$. Lastly, we see $A_2 - q_1 R_{12} = Q_2 R_{22}$. This is QR decomposition of an $m \times (n-1)$ matrix. Continuing recursively, we arrive at QR decomposition of an $m \times 1$ matrix $A = QR$ where $Q = \frac{1}{\|A\|} A$, $R = \|A\|$. This algorithm is called the modified Gram-Schmidt method. In summary, it runs

1. $r_{11} = \|a_1\|$.
2. $q_1 = \frac{a_1}{r_{11}}$.
3. $R_{12} = q_1^t A_2$.
4. Compute QR decomposition $A_2 - q_1 R_{12} = Q_2 R_{22}$.

The total cost is $2mn^2$ flops. Note that $\|a_1\| \neq 0$ in step 1 because A has trivial kernel. Also $A_2 - q_1 R_{12}$ is left invertible in step 4. Indeed, if $x \neq 0 \in \mathbb{R}^{n-1}$ then $(A_2 - q_1 R_{12})x = A_2 x - \frac{a_1}{r_{11}} R_{12} x = (a_1 \ A_2) \begin{pmatrix} -\frac{1}{r_{11}} R_{12} x & x \end{pmatrix}^t = A \begin{pmatrix} -\frac{1}{r_{11}} R_{12} x & x \end{pmatrix}^t \neq 0$.

Example 7.2. The matrix $A = \begin{pmatrix} 3/5 & -6/5 & 26/5 \\ 4/5 & -8/5 & -7/5 \\ 0 & 4/5 & 4/5 \\ 0 & -3/5 & -3/5 \end{pmatrix}$ has QR decomposition

$$\begin{pmatrix} 3/5 & 0 & 4/5 \\ 4/5 & 0 & -3/5 \\ 0 & 4/5 & 0 \\ 0 & -3/5 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 5 \end{pmatrix}$$

Exercise 7.3. Perform QR decomposition for $\begin{pmatrix} 3 & 3 & 2 \\ 4 & 4 & 1 \\ 0 & 6 & 2 \\ 0 & 8 & 1 \end{pmatrix}$

8. LEAST SQUARE PROBLEM

If our system of equations $Ax = b$ falls into scenario (ii) discussed at the beginning of part 2 then there is a unique x such that $\|Ax - b\| = 0$. If it falls into scenario (iii) then

$Ax \neq b$ and $\|Ax - b\| > 0$ for all $x \in \mathbb{R}^n$ and we can only hope to find an \hat{x} such that this nonzero norm is least. Either way, solving the system becomes minimization of

$$\|Ax - b\|^2 = \sum_{i=1}^m (a_{i1}x_1 + \dots + a_{in}x_n - b_i)^2 = \sum_{i=1}^m r_i(x)^2 \geq 0$$

This explains the name *least square*. The word *linear* is sometimes included to emphasize that each r_i is linear in the x_1, \dots, x_n plus a constant.

Example 8.1. The system

$$Ax = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (x) = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

has no solution. This is the embedding of \mathbb{R} into \mathbb{R}^2 as the x -axis. By geometry, $\hat{x} = 2$ gives smallest $\|Ax - b\|$.

Example 8.2. The system

$$Ax = \begin{pmatrix} 2 & 0 \\ -1 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

has no solution. The corresponding least square problem is to minimize $f(x_1, x_2) = (2x_1 - 1)^2 + (-x_1 + x_2)^2 + (2x_2 + 1)^2$. Taking partial derivatives $\partial f / \partial x_1$ and $\partial f / \partial x_2$ yields solution $\hat{x} = (1/3, -1/3)$ for minimum.

The following theorem tells us when we can expect existence and uniqueness of such \hat{x} .

Theorem 8.3. *If A is a left invertible matrix then the least square problem for $Ax = b$ has unique solution $\hat{x} = (A^t A)^{-1} A^t b$.*

Proof. For $\hat{x} = (A^t A)^{-1} A^t b$ and any $x \in \mathbb{R}^n$, we show $\|Ax - b\|^2 = \|(Ax - A\hat{x}) + (A\hat{x} - b)\|^2 = \langle (Ax - A\hat{x}) + (A\hat{x} - b), (Ax - A\hat{x}) + (A\hat{x} - b) \rangle = \|Ax - A\hat{x}\|^2 + \|A\hat{x} - b\|^2 + 2(Ax - A\hat{x})^t (A\hat{x} - b) = \|A(x - \hat{x})\|^2 + \|A\hat{x} - b\|^2 + 0 \geq \|A\hat{x} - b\|^2$. So \hat{x} is solution to the least square problem. Uniqueness follows from the fact that equality holds iff $\|A(x - \hat{x})\| = 0$ iff $A(x - \hat{x}) = 0$ iff $x - \hat{x} = 0$ iff $x = \hat{x}$. \square

If A is indeed invertible then $\hat{x} = (A^t A)^{-1} A^t b = A^{-1} (A^t)^{-1} A^t b = A^{-1} b$ the precise solution as we would expect. Else, $A^t A \hat{x} = A^t b$ still holds and so we are reduced to solving the system $A^t A x = A^t b$. It is called the system of normal equations associated with the least square problem for $Ax = b$.

8.1. Cholesky Decomposition to Solve Least Square Problem. Since $A^t A$ is positive definite by theorem 3.50, we can apply Cholesky decomposition to solve the least square problem. An algorithm to do so runs as follows

1. Multiply $B = A^t A$ and $c = A^t b$.
2. Compute the Cholesky decomposition $B = LL^t$.
3. Solve $Ly = c$ by forward substitution.
4. Solve $L^t x = y$ by backward substitution.

The cost to form $B = A^t A$ in step 1 is mn^2 flops, note that B is symmetric so we only need to compute $n(n+1)/2 \approx n^2/2$ elements in its lower triangle. The cost to calculate $c = A^t b$ is $2mn$. Step 2 costs $n^3/3$ flops while step 3 and step 4 cost n^2 each. Hence the whole algorithm costs $mn^2 + n^3/3 + 2mn + 2n^2$ flops. Note that left invertibility implies A is square or tall with $m \geq n$, so multiplication of $B = A^t A$ costs the most. If $m \gg n$ then the algorithm costs roughly mn^2 flops.

Example 8.4. Consider the system

$$Ax = \begin{pmatrix} 3/5 & -6/5 & 26/5 \\ 4/5 & -8/5 & -7/5 \\ 0 & 4/5 & 4/5 \\ 0 & -3/5 & -3/5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

where A is from example 7.2. Then

$$B = A^t A = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 5 & -3 \\ 2 & -3 & 30 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 2 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 5 \end{pmatrix}$$

in its Cholesky decomposition and $c = (7/5, -13/5, 4)$. It follows from there that $(y_1, y_2, y_3) = (7/5, 1/5, 1/5)$ by forward substitution and $(x_1, x_2, x_3) = (41/25, 4/25, 1/25)$ by backward substitution.

Exercise 8.5. Consider the system

$$Ax = \begin{pmatrix} 1 & -1 & 4 \\ 1 & 4 & -2 \\ 1 & 4 & 2 \\ 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 1 \end{pmatrix}$$

- Perform Cholesky decomposition for $A^t A$.
- Use it to solve the least square problem for the above system.

8.2. QR Decomposition to Solve Least Square Problem. There is another way to solve the least square problem. By theorem 7.1, we can decompose left invertible $A = QR$ where $Q \in M(m, n, \mathbb{R})$ is orthogonal with $Q^t Q = I_n$ and $R \in U(n, \mathbb{R})$ is upper triangular with positive diagonal entries. Then $A^t A = (QR)^t (QR) = R^t Q^t QR = R^t R$ and $R^t R x = R^t Q^t b$. Since R is invertible, this gives $R x = Q^t b$. Packaged as an algorithm, it is

1. Compute the QR decomposition $A = QR$.
2. Compute $c = Q^t b$.
3. Solve $R x = c$ by backward substitution.

Step 1 costs $2mn^2$ flops while step 2 costs $2mn$ flops and step 3 costs n^2 flops. Total cost is $2mn^2 + 2mn + n^2$ flops. If $m \gg n$ then it is roughly $2mn^2$ flops and this method is slower than Cholesky method by a factor of about 2. However, it is more accurate.

Example 8.6. Again consider the system in example 8.4.

$$Ax = \begin{pmatrix} 3/5 & -6/5 & 26/5 \\ 4/5 & -8/5 & -7/5 \\ 0 & 4/5 & 4/5 \\ 0 & -3/5 & -3/5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

By example 7.2,

$$\begin{pmatrix} 3/5 & -6/5 & 26/5 \\ 4/5 & -8/5 & -7/5 \\ 0 & 4/5 & 4/5 \\ 0 & -3/5 & -3/5 \end{pmatrix} = \begin{pmatrix} 3/5 & 0 & 4/5 \\ 4/5 & 0 & -3/5 \\ 0 & 4/5 & 0 \\ 0 & -3/5 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 5 \end{pmatrix}$$

So

$$c = Q^t b = \begin{pmatrix} 3/5 & 4/5 & 0 & 0 \\ 0 & 0 & 4/5 & -3/5 \\ 4/5 & -3/5 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 7/5 \\ 1/5 \\ 1/5 \end{pmatrix}$$

It follows from there that $(x_1, x_2, x_3) = (41/25, 4/25, 1/25)$.

Exercise 8.7. Again consider the system in exercise 8.5

$$Ax = \begin{pmatrix} 1 & -1 & 4 \\ 1 & 4 & -2 \\ 1 & 4 & 2 \\ 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 1 \end{pmatrix}$$

- Perform QR decomposition for A .
- Use it to solve the least square problem for the above system and compare with previous result.

9. LEAST NORM PROBLEM

If our system falls into scenario (i) at the beginning of part 2 then there are infinitely many solutions $x \in \mathbb{R}^n$ such that $\|Ax - b\| = 0$. If it falls into scenario (ii) then there is a unique x such that $Ax = b$. Either way, we can ask which solution \hat{x} has least norm.

Example 9.1. The system

$$Ax = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

has infinitely many solutions $(2, 1, t), t \in \mathbb{R}$. This is the projection of \mathbb{R}^3 into its xy -plane. By geometry, $\hat{x} = (2, 1, 0)$ has smallest norm.

Example 9.2. The system

$$Ax = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

has infinitely many solutions. The corresponding least norm problem is to minimize $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ subject to relations $x_1 - x_2 + 2x_3 = 1$ and $x_1 + x_2 - x_3 = 0$. We gather information $x_3 = x_1 + x_2$ and $x_2 = 1 - 3x_1$. Hence we need to minimize $f(x_1) = x_1^2 + (1 - 3x_1)^2 + (1 - 2x_1)^2$. Taking derivative yields solution $\hat{x} = (5/14, -1/14, 2/7)$ for minimum.

The following theorem tells us when we can expect existence and uniqueness of such \hat{x} .

Theorem 9.3. *If A is a right invertible matrix then the least norm problem for $Ax = b$ has unique solution $\hat{x} = A^t(AA^t)^{-1}b$.*

Proof. Surely $A\hat{x} = AA^t(AA^t)^{-1}b = b$. And if x is another solution to $Ax = b$ then $\|x\|^2 = \|(x - \hat{x}) + \hat{x}\|^2 = \|x - \hat{x}\|^2 + \|\hat{x}\|^2 + 2\hat{x}^t(x - \hat{x}) = \|x - \hat{x}\|^2 + \|\hat{x}\|^2 + 0 \geq \|\hat{x}\|^2$ because $\hat{x}^t(x - \hat{x}) = (A^t(AA^t)^{-1}b)^t(x - \hat{x}) = b^t(AA^t)^{-1}A(x - \hat{x}) = b^t(AA^t)^{-1}(b - b) = 0$. Uniqueness follows from the fact that equality holds iff $\|x - \hat{x}\| = 0$ iff $x - \hat{x} = 0$ iff $x = \hat{x}$. \square

If A is indeed invertible then $\hat{x} = A^t(AA^t)^{-1}b = A^t(A^t)^{-1}A^{-1}b = A^{-1}b$ the precise solution as we would expect. Else, we can still solve $AA^tz = b$ and $\hat{x} = A^tz$. The first equality is called the system of normal equations associated with the least norm problem for $Ax = b$.

9.1. Cholesky Decomposition to Solve Least Norm Problem. Since AA^t is also positive definite by theorem 3.50, we can apply Cholesky decomposition to solve the least norm problem. An algorithm to do so runs as follows.

1. Multiply $B = AA^t$.
2. Compute the Cholesky decomposition $B = LL^t$.
3. Solve $Lz = b$ by forward substitution.
4. Solve $L^ty = z$ by backward substitution.
5. Compute $x = A^ty$.

The cost to form $B = A^tA$ in step 1 is m^2n , note again that B is symmetric. Steps 2, 3, 4, 5 cost $m^3/3, m^2, m^2, 2mn$ flops. Hence the whole algorithm costs $m^2n + m^3/3 + 2m^2 + 2mn$ flops. Note that right invertibility implies that A is square or wide with $m \leq n$, so again multiplication of $B = AA^t$ costs the most. If $m \ll n$ then the algorithm costs roughly m^2n flops.

Example 9.4. Consider the system

$$Ax = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Then

$$B = AA^t = \begin{pmatrix} 2 & 0 \\ 1 & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1/\sqrt{2} \end{pmatrix}$$

It follows from there that $(z_1, z_2) = (0, \sqrt{x})$ by forward substitution and $(y_1, y_2) = (-1, 2)$ by backward substitution. Finally, $(x_1, x_2) = A^t(y_1, y_2) = (1, 1, 0, 0)$.

Exercise 9.5. Consider the system in example 9.2.

$$Ax = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- a. Perform Cholesky decomposition for AA^t .
- b. Use it to solve the least norm problem for the above system and compare with previous result.

9.2. QR Decomposition to Solve Least Norm Problem. There is another way to solve the least norm problem. By theorem 7.1, we can decompose $A^t = QR$ where $Q \in M(n, m, \mathbb{R})$ is orthogonal with $Q^t Q = I_m$ and $R \in M(m, \mathbb{R})$ is upper triangular with positive diagonal entries. Then $\hat{x} = A^t(AA^t)^{-1}b = QR(R^t Q^t QR)^{-1}b = QR(R^t R)^{-1}b = QRR^{-1}(R^t)^{-1}b = Q(R^t)^{-1}b$. Packaged as an algorithm, it is

1. Compute the QR decomposition $A^t = QR$.
2. Solve $R^t y = b$ by forward substitution.
3. Compute $x = Qy$.

Step 1 costs $2nm^2$ flops while step 2 costs m^2 flops and step 3 costs $2mn$ flops. Total cost is $2m^2n + m^2 + 2mn$ flops. If $m \ll n$ then it is roughly $2m^2n$ flops and this method is slower than the Cholesky method by a factor of about 2. However, it is more accurate.

Example 9.6. Again consider the system in example 9.4.

$$Ax = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The QR factorization for A^t is

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 1 & 1/2 \\ 1 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/\sqrt{2} \\ -1/2 & 1/\sqrt{2} \\ 1/2 & 0 \\ 1/2 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1/\sqrt{2} \end{pmatrix}$$

It follows from there that $(y_1, y_2) = (0, \sqrt{2})$ and $(x_1, x_2, x_3, x_4) = (1, 1, 0, 0)$.

Exercise 9.7. Again consider the system in exercise 9.5.

$$Ax = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- a. Perform QR decomposition for A^t .
- b. Use it to solve the least norm problem for the above system and compare with previous result.

to Aaron Swartz and a free open internet.