Advanced Linear Algebra

B. V. Rajarama Bhat

Statistics and Mathematics Unit
Indian Statistical Institute, Bangalore

Credits and Disclaimer

These notes are based on the course on *Advanced Linear Algebra* taught by Prof. B. V. R. Bhat during the fourth semester of the M.Math programme in the academic year 2024–25.

The LaTeX notes were initialized by

Srivatsa Balaji
Sanchayan Bhowal
Venkat Trivikram

The last three chapters are based on class notes and were LaTeXed with the assistance of ChatGPT.

Warning: These notes may contain factual and/or typographic errors. They should be read as informal course notes, not as an official reference.

M.Math (2023–25)
Indian Statistical Institute, Bangalore

Contents

Chapter 1

Preliminaries

Throughout this chapter V, W are finite dimensional complex inner product spaces unless explicitly stated otherwise. The inner product is linear in the second variable and conjugate-linear in the first variable.

1.1 Orthonormal bases and rank-one operators

Definition 1.1.1 ► Mutually unbiased bases

Two orthonormal bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ of an n-dimensional Hilbert space are called **mutually unbiased** if $|\langle u_i, v_j \rangle|$ is independent of i, j.

If the two bases are mutually unbiased, then for each fixed i,

$$u_i = \sum_{j=1}^{n} \langle v_j, u_i \rangle v_j, \qquad 1 = \|u_i\|^2 = \sum_{j=1}^{n} |\langle v_j, u_i \rangle|^2.$$

Hence the common value is $1/\sqrt{n}$. Thus mutual unbiasedness is equivalently

$$|\langle u_i, v_j \rangle| = \frac{1}{\sqrt{n}}, \qquad 1 \le i, j \le n.$$

Remark 1.1.1. It is a nontrivial open problem whether $\mathbb{C}^6$ admits 7 pairwise mutually unbiased bases. In general, at most $n+1$ pairwise mutually unbiased bases can exist in $\mathbb{C}^n$.

Definition 1.1.2 ► Rank-one operator

For $x, y \in V$, define

$$|x\rangle\langle y| : V \to V, \qquad |x\rangle\langle y|(z) = \langle y, z\rangle x.$$

This is called a **rank-one operator**. Under the standard basis of $\mathbb{C}^n$, its matrix is xy^*.

For $x_i \in V$ and $A \in \mathscr{B}(V)$,

$$\begin{aligned} |x_1\rangle\langle x_2||x_3\rangle\langle x_4| &= \langle x_2, x_3\rangle |x_1\rangle\langle x_4|, \\ A|x\rangle\langle y| &= |Ax\rangle\langle y|, \\ |x\rangle\langle y|A &= |x\rangle\langle A^* y|, \\ (|x\rangle\langle y|)^* &= |y\rangle\langle x|, \\ \mathrm{Tr}(|x\rangle\langle y|) &= \langle y, x\rangle. \end{aligned}$$

If $\{v_1, \ldots, v_n\}$ is an orthonormal basis, then

$$I = \sum_{i=1}^{n} |v_i\rangle\langle v_i|.$$

1.2 Orthogonal projections

Let $M \subseteq V$ be a subspace. Its orthogonal complement is

$$M^{\perp} = \{x \in V : \langle m, x\rangle = 0 \text{ for every } m \in M\}.$$

If $\{v_1,\ldots,v_k\}$ is an orthonormal basis of M, extended to an orthonormal basis $\{v_1,\ldots,v_n\}$ of V, then every $x \in V$ has the orthogonal decomposition

$$x = y + z, \qquad y = \sum_{i=1}^{k} \langle v_i, x\rangle\, v_i \in M, \quad z = \sum_{i=k+1}^{n} \langle v_i, x\rangle\, v_i \in M^{\perp}.$$

Proposition 1.2.1 (Best approximation property)**.** With the above notation,

$$\inf_{w\in M} \|x - w\| = \|x - y\|,$$

and equality is attained uniquely at $w = y$.

Proof. For $w \in M$, $y - w \in M$ and $z \in M^{\perp}$, so

$$\|x-w\|^2 = \|y - w + z\|^2 = \|y-w\|^2 + \|z\|^2 \ge \|z\|^2.$$

Equality holds iff $y - w = 0$. □

The map $P_M x = y$ is the orthogonal projection onto M. It satisfies

$$P_M = P_M^* = P_M^2, \qquad P_M = \sum_{i=1}^{k} |v_i\rangle\langle v_i|.$$

Conversely, if $P = P^* = P^2$, then P is the orthogonal projection onto $\operatorname{ran} P$.

1.3 Isometries and unitary equivalence

Definition 1.3.1 ► Isometry and unitary operator

A linear map $T : V \to W$ is an **isometry** if

$$\langle Tx, Ty\rangle = \langle x, y\rangle, \qquad x, y \in V.$$

Equivalently $T^*T = I_V$. If, in addition, T is onto, then T is called **unitary**. Two matrices $A, B \in M_n(\mathbb{C})$ are **unitarily equivalent** if $B = U^*AU$ for some unitary U.

A unitary maps orthonormal bases to orthonormal bases. Conversely, if a linear map sends one orthonormal basis onto another orthonormal basis, it is unitary.

1.4 Schur triangularization and the spectral theorem

> **Theorem** 1.4.1 (Schur triangularization) For every $A \in M_n(\mathbb{C})$ there is a unitary U such that U^*AU is upper triangular.

Proof. Use induction on n. For $n = 1$ there is nothing to prove. Let $Av = \lambda v$ with $\|v\| = 1$ and extend v to an orthonormal basis. In this basis

$$V^*AV = \begin{pmatrix} \lambda & c^* \\ 0 & C \end{pmatrix}.$$

By induction, $W^*CW = S$ is upper triangular. Then

$$\begin{pmatrix} 1 & 0 \\ 0 & W^* \end{pmatrix} V^*AV \begin{pmatrix} 1 & 0 \\ 0 & W \end{pmatrix} = \begin{pmatrix} \lambda & c^*W \\ 0 & S \end{pmatrix},$$

which is upper triangular. □

Definition 1.4.1 ► Normal and self-adjoint operators

A matrix A is **normal** if $A^*A = AA^*$. It is **self-adjoint** if $A = A^*$.

Lemma 1.4.1 (Triangular normal matrices)

If $T \in M_n(\mathbb{C})$ is upper triangular and normal, then T is diagonal.

Proof. Write

$$T = \begin{pmatrix} \lambda & c^* \\ 0 & S \end{pmatrix}.$$

Then

$$(T^*T)_{11} = |\lambda|^2, \qquad (TT^*)_{11} = |\lambda|^2 + \|c\|^2.$$

Normality gives $c = 0$. Thus $T = \lambda \oplus S$. The lower-right block S is again normal and upper triangular. Induction gives that S is diagonal. □

Theorem 1.4.2 (Spectral theorem) A matrix $A \in M_n(\mathbb{C})$ is normal iff there exist an orthonormal basis $\{u_1, \ldots, u_n\}$ and scalars $\lambda_1, \ldots, \lambda_n$ such that

$$A = \sum_{i=1}^{n} \lambda_i |u_i\rangle\langle u_i|.$$

Equivalently, $A = UDU^*$ with U unitary and D diagonal.

Proof. If A is normal, Schur triangularization gives $U^*AU = T$ upper triangular. Since normality is preserved under unitary conjugacy, T is normal; by the lemma T is diagonal.
Conversely, every diagonal matrix is normal, and normality is preserved under unitary conjugacy. □

Grouping equal eigenvalues gives the unique spectral resolution

$$A = \sum_{j=1}^{r} \lambda_j P_j,$$

where $\lambda_1, \ldots, \lambda_r$ are the distinct eigenvalues, P_j are mutually orthogonal projections, $P_iP_j = \delta_{ij}P_i$, and $\sum_j P_j = I$.
For any function $f : \sigma(A) \to \mathbb{C}$, define the functional calculus

$$f(A) = \sum_{j=1}^{r} f(\lambda_j) P_j.$$

For a normal matrix A:

i. $A = A^*$ iff $\sigma(A) \subseteq \mathbb{R}$.

ii. A is unitary iff $\sigma(A) \subseteq \{z \in \mathbb{C} : |z| = 1\}$.

iii. A is an orthogonal projection iff $\sigma(A) \subseteq \{0, 1\}$.

Every matrix $A \in M_n(\mathbb{C})$ has a unique decomposition

$$A = X + iY, \qquad X = \frac{A + A^*}{2}, \quad Y = \frac{A - A^*}{2i},$$

where X, Y are self-adjoint. These are the real and imaginary parts of A.

1.5 Positive matrices

Definition 1.5.1 ► Positive matrix

A matrix $A \in M_n(\mathbb{C})$ is **positive**, written $A \geq 0$, if $A = A^*$ and $\sigma(A) \subseteq [0, \infty)$.

Theorem 1.5.1 (Equivalent forms of positivity) For $A \in M_n(\mathbb{C})$, the following are equivalent.

i. $A \geq 0$.

ii. $A = B^2$ for some self-adjoint B.

iii. $A = C^*C$ for some $C \in M_n(\mathbb{C})$.

iv. There exist vectors $v_1, \ldots, v_n$ such that $a_{ij} = \langle v_i, v_j \rangle$.

v. $\langle x, Ax \rangle \geq 0$ for all $x \in \mathbb{C}^n$.

Proof. Assume $A \geq 0$. By the spectral theorem, $A = \sum_j \lambda_j P_j$ with $\lambda_j \geq 0$. Then

$$B = A^{1/2} := \sum_j \sqrt{\lambda_j} P_j$$

is self-adjoint and $B^2 = A$, proving (1)⇒(2). Taking $C = B$ gives (2)⇒(3).
If $A = C^*C$, then $\langle x, Ax \rangle = \|Cx\|^2 \geq 0$, so (3)⇒(5). If (5) holds, then first A is self-adjoint: using the polarization identity for the sesquilinear form $\langle x, Ay \rangle$ shows $\langle x, Ay \rangle = \overline{\langle y, Ax \rangle}$. Hence $A = A^*$. Then the spectral theorem gives $A = \sum_j \lambda_j P_j$, and testing on eigenvectors gives $\lambda_j \geq 0$. Thus (5)⇒(1).
Finally, (3)⇒(4) by taking $v_i = Ce_i$, since

$$a_{ij} = \langle e_i, Ae_j \rangle = \langle Ce_i, Ce_j \rangle.$$

Conversely, if $a_{ij} = \langle v_i, v_j \rangle$, then for $x = (x_i)$,

$$\langle x, Ax \rangle = \sum_{i,j} \overline{x_i} x_j \langle v_i, v_j \rangle = \left\| \sum_i x_i v_i \right\|^2 \geq 0.$$

□

Remark 1.5.1. The positive square root $A^{1/2}$ is unique. Indeed, if $B \geq 0$ and $B^2 = A$, then B commutes with A and hence is diagonal in the same spectral resolution as A; its eigenvalues must be the non-negative square roots of those of A.

1.6 Numerical range

The numerical range of $A \in M_n(\mathbb{C})$ is

$$W(A) = \{\langle x, Ax \rangle : \|x\| = 1\}.$$

If $A = A^*$, then $W(A) = [\lambda_{\min}(A), \lambda_{\max}(A)]$. If A is normal, $W(A) = \operatorname{conv} \sigma(A)$; this follows by writing $A = \sum_j \lambda_j |u_j\rangle\langle u_j|$ and observing that

$$\langle x, Ax \rangle = \sum_j |\langle u_j, x \rangle|^2 \lambda_j.$$

For a non-normal matrix, $W(A)$ is still convex; this is the Toeplitz-Hausdorff theorem.

1.7 Exercises

i. Prove that in $\mathbb{C}^n$ there exist at most $n+1$ mutually unbiased bases.

ii. Show that a linear functional $\varphi : M_n(\mathbb{C}) \to \mathbb{C}$ satisfying $\varphi(AB) = \varphi(BA)$ for all A, B is of the form $\varphi(X) = c\,\mathrm{Tr}(X)$.

iii. If $C \geq 0$, prove that $C^{1/2} = p(C)$ for some polynomial p depending on C.

iv. Give a matrix with no square root.

v. If M is normal, show that there exists a normal N such that $N^2 = M$.

vi. Show that all inner products on $\mathbb{C}^n$ are of the form $\langle x, y\rangle_A = \langle x, Ay\rangle$ for a unique strictly positive matrix A.

vii. Show that N is nilpotent iff all eigenvalues of N are zero. Moreover, if $N \in M_n(\mathbb{C})$ is nilpotent, then $N^n = 0$.

viii. Let $Ue_j = e^{2\pi i j/n} e_j$ and $Ve_j = e_{j+1}$ on $\mathbb{C}^n$. Prove that $\{U^j V^k : 0 \leq j, k \leq n-1\}$ is an orthonormal basis of $M_n(\mathbb{C})$ under $\langle A, B\rangle = n^{-1}\,\mathrm{Tr}(A^* B)$.

Chapter 2

Majorization and Doubly Stochastic Matrices

For $x \in \mathbb{R}^n$, write $x^{\downarrow}$ for the coordinates rearranged in decreasing order and $x^{\uparrow}$ for the coordinates rearranged in increasing order.

2.1 Majorization

Definition 2.1.1 ► Majorization

For $x, y \in \mathbb{R}^n$, we say that x is **majorized** by y, and write $x \prec y$, if

$$\sum_{i=1}^{k} x_i^{\downarrow} \le \sum_{i=1}^{k} y_i^{\downarrow}, \qquad 1 \le k \le n-1,$$

and

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i.$$

We say $x \prec_w y$ if only the first family of inequalities holds. We say $x \prec^w y$ if

$$\sum_{i=1}^{k} x_i^{\uparrow} \ge \sum_{i=1}^{k} y_i^{\uparrow}, \qquad 1 \le k \le n-1.$$

Proposition 2.1.1. If $p = (p_1, \ldots, p_n)$ is a probability vector, then

$$\frac{1}{n}(1, \ldots, 1) \prec p \prec (1, 0, \ldots, 0).$$

Proof. Assume $p = p^{\downarrow}$. For the upper bound, $\sum_{i=1}^{k} p_i \le 1$ for every $k < n$. For the lower bound, suppose $\sum_{i=1}^{k} p_i < k/n$ for some $k < n$. Then $p_k < 1/n$, hence $p_i \le p_k < 1/n$ for $i > k$. Therefore

$$1 = \sum_{i=1}^{n} p_i < \frac{k}{n} + \frac{n-k}{n} = 1,$$

a contradiction. □

Proposition 2.1.2. For $x, y \in \mathbb{R}^n$:

i. $x \prec y$ iff $x \prec_w y$ and $x \prec^w y$.

ii. $x \prec_w y$ iff $-x \prec^w -y$.

iii. If $x \prec y$ and $\alpha > 0$, then $\alpha x \prec \alpha y$.

Proof. The only non-immediate point is (1). If $x \prec y$, then for $1 \le k < n$,

$$\sum_{i=1}^{k} x_i^{\uparrow} = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n-k} x_i^{\downarrow} \ge \sum_{i=1}^{n} y_i - \sum_{i=1}^{n-k} y_i^{\downarrow} = \sum_{i=1}^{k} y_i^{\uparrow}.$$

Conversely, weak majorization plus equality at $k = n$ gives the definition of $\prec$. □

Lemma 2.1.1 (Subset formulation)

For $x, y \in \mathbb{R}^n$, $x \prec y$ iff $\sum_i x_i = \sum_i y_i$ and for every $I \subseteq [n]$ there exists $J \subseteq [n]$ with $|J| = |I|$ such that

$$\sum_{i \in I} x_i \le \sum_{j \in J} y_j.$$

Proof. If $|I| = k$, then $\sum_{i \in I} x_i \le \sum_{i=1}^{k} x_i^{\downarrow}$. Under majorization this is at most $\sum_{i=1}^{k} y_i^{\downarrow}$, obtained by choosing J to be the indices of the largest k entries of y.
Conversely, choose I to be the indices of the largest k entries of x. Then there is J of size k with

$$\sum_{i=1}^{k} x_i^{\downarrow} = \sum_{i \in I} x_i \le \sum_{j \in J} y_j \le \sum_{i=1}^{k} y_i^{\downarrow}.$$

Together with equality of total sums, this is $x \prec y$. □

Theorem 2.1.1 (Positive-part criteria) For $x, y \in \mathbb{R}^n$:

i. $x \prec_w y$ iff

$$\sum_{j=1}^{n} (x_j - t)^+ \le \sum_{j=1}^{n} (y_j - t)^+, \qquad t \in \mathbb{R}.$$

ii. $x \prec^w y$ iff

$$\sum_{j=1}^{n} (t - x_j)^+ \le \sum_{j=1}^{n} (t - y_j)^+, \qquad t \in \mathbb{R}.$$

iii. $x \prec y$ iff

$$\sum_{j=1}^{n} |x_j - t| \le \sum_{j=1}^{n} |y_j - t|, \qquad t \in \mathbb{R},$$

and $\sum_j x_j = \sum_j y_j$.

Proof. Assume $x \prec_w y$ and set $x = x^{\downarrow}$. If $x_{k+1} < t \le x_k$, then

$$\sum_j (x_j - t)^+ = \sum_{j=1}^{k} x_j - kt \le \sum_{j=1}^{k} y_j^{\downarrow} - kt \le \sum_j (y_j - t)^+.$$

The remaining cases $t > x_1$ and $t \le x_n$ are immediate. Conversely, take $t = x_{k+1}^{\downarrow}$ and get

$$\sum_{j=1}^{k} x_j^{\downarrow} - kt \le \sum_j (y_j - t)^+ \le \sum_{j=1}^{k} y_j^{\downarrow} - kt.$$

This gives weak majorization. The proof of (2) follows by applying (1) to $-x, -y$. Since

$$|s - t| = (s - t)^+ + (t - s)^+,$$

(3) follows from (1), (2), and equality of total sums. □

2.2 Doubly stochastic matrices

Definition 2.2.1 ► Stochastic matrices

A matrix $A=[a_{ij}]\in M_n(\mathbb{R})$ is **stochastic** if $a_{ij}\geq 0$ and $\sum_j a_{ij}=1$ for each row i. It is **doubly stochastic** if both A and A^T are stochastic.

The doubly stochastic matrices form a convex monoid. If $U=[u_{ij}]$ is unitary, then $B=[|u_{ij}|^2]$ is doubly stochastic; such matrices are called **unistochastic**.

Theorem 2.2.1 (Doubly stochastic matrices contract majorization) For $A\in M_n(\mathbb{R})$ with non-negative entries, the following are equivalent.

i. A is doubly stochastic.

ii. $Ax\prec x$ for every $x\in\mathbb{R}^n$.

Proof. Assume A is doubly stochastic. Since $\sum_i (Ax)_i=\sum_j x_j$, it remains to check the partial sums. Let $x=x^{\downarrow}$ and let $I\subseteq[n]$ with $|I|=k$. Then

$$\sum_{i\in I}(Ax)_i=\sum_{j=1}^{n}t_jx_j,\qquad t_j=\sum_{i\in I}a_{ij}.$$

Here $0\leq t_j\leq 1$ and $\sum_j t_j=k$. Therefore

$$\sum_{j=1}^{k}x_j-\sum_{j=1}^{n}t_jx_j=\sum_{j=1}^{k}(1-t_j)(x_j-x_k)+\sum_{j=k+1}^{n}t_j(x_k-x_j)\geq 0.$$

Taking the maximum over I gives $Ax\prec x$.
Conversely, if $Ax\prec x$ for all x, then $Ae_j\prec e_j$. Hence each column Ae_j is a probability vector, so the columns are non-negative and sum to 1. Also $A1\prec 1$, and the only vector majorized by 1 with total sum n and coordinate upper bound 1 is 1 itself. Thus $A1=1$, so the row sums are 1. □

Definition 2.2.2 ► T-transform

A T-transform is a doubly stochastic matrix which is the identity except on two coordinates i,j, where it acts by

$$(u_i,u_j)\mapsto(tu_i+(1-t)u_j,(1-t)u_i+tu_j),\qquad 0\leq t\leq 1.$$

Theorem 2.2.2 (Hardy-Littlewood-Polya theorem) For $x,y\in\mathbb{R}^n$, the following are equivalent.

i. $x\prec y$.

ii. x is obtained from y by finitely many T-transforms.

iii. x lies in the convex hull of all coordinate permutations of y.

iv. There is a doubly stochastic matrix A such that $x=Ay$.

Proof. (2)⇒(4) and (3)⇒(4) are immediate because T-transforms and permutation matrices are doubly stochastic. The implication (4)⇒(1) follows from the theorem that doubly stochastic matrices contract majorization.
For (1)⇒(2), assume x,y are decreasing. If $x\neq y$, choose k such that $y_1\geq x_1\geq y_k$ and mix the first and kth coordinates of y so that the first coordinate becomes x_1. This produces a vector y' with first coordinate x_1 and with $(x_2,\dots,x_n)\prec(y'_2,\dots,y'_n)$. Induction completes the proof. Finally, finite products of T-transforms lie in the convex hull of permutation matrices, so (2)⇒(3). □

Theorem 2.2.3 (Karamata theorem) For $x, y \in \mathbb{R}^n$,

$$x \prec y \iff \sum_{i=1}^{n} \varphi(x_i) \le \sum_{i=1}^{n} \varphi(y_i)$$

for every convex function $\varphi : \mathbb{R} \to \mathbb{R}$.

Proof. If $x = Ay$ with A doubly stochastic, Jensen's inequality gives

$$\varphi(x_i) = \varphi\left(\sum_j a_{ij} y_j\right) \le \sum_j a_{ij} \varphi(y_j).$$

Summing in i and using the column sums gives the result.
Conversely, apply the hypothesis to the convex functions $\varphi_t(s) = |s - t|$. The positive-part criterion gives $x \prec y$. □

2.3 Birkhoff's theorem

Theorem 2.3.1 (Hall's marriage theorem) A bipartite graph with left vertex set L and right vertex set R, where $|L| = |R|$, has a perfect matching iff

$$|S| \le |N(S)|, \qquad S \subseteq L.$$

Theorem 2.3.2 (Konig-Frobenius theorem) For an $n \times n$ zero-one pattern, the following are equivalent.

i. Every diagonal contains at least one zero.

ii. There is a $k \times \ell$ zero submatrix with $k + \ell > n$.

iii. The bipartite graph of non-zero entries has no perfect matching.

Proof. A diagonal of non-zero entries is exactly a perfect matching in the bipartite graph. Hence (1) is equivalent to (3). If there is no perfect matching, Hall's theorem gives $S \subseteq L$ with $|N(S)| < |S|$. The rows S and the columns $R \setminus N(S)$ form a zero submatrix of size $|S| \times (n - |N(S)|)$ and

$$|S| + n - |N(S)| > n.$$

Conversely, if a $k \times \ell$ zero submatrix has $k + \ell > n$, then in any diagonal one must choose k entries in those k rows but only $n - \ell < k$ columns outside the zero block. Thus every diagonal contains a zero. □

Theorem 2.3.3 (Birkhoff-von Neumann theorem) Every doubly stochastic matrix is a convex combination of permutation matrices. Equivalently, the extreme points of the Birkhoff polytope are the permutation matrices.

Proof. Let A be doubly stochastic. If A is not a permutation matrix, consider the support graph G_A of its positive entries. Since each row and column sum is 1, G_A satisfies Hall's condition and hence contains a perfect matching, i.e. a permutation matrix P with $P_{ij} = 1$ only where $a_{ij} > 0$. Let

$$\epsilon = \min\{a_{ij} : p_{ij} = 1\} > 0.$$

Then $A - \epsilon P$ has non-negative entries and all row and column sums equal $1 - \epsilon$. Hence

$$A = \epsilon P + (1 - \epsilon) B, \qquad B = (1 - \epsilon)^{-1}(A - \epsilon P),$$

where B is again doubly stochastic unless $\epsilon = 1$. Repeating this step terminates because at least one positive entry is killed at each step. □

2.4 Schur, Ky Fan, and Schur-Horn

For a self-adjoint matrix A, let $\lambda(A)=(\lambda_1(A),\dots,\lambda_n(A))$ denote the eigenvalue vector in decreasing order and let $d(A)=(a_{11},\dots,a_{nn})$ be its diagonal vector.

Theorem 2.4.1 (Schur theorem) If $A=A^*\in M_n(\mathbb{C})$, then

$$d(A)\prec\lambda(A).$$

Proof. Let $A=UDU^*$ with $D=\operatorname{diag}(\lambda_1,\dots,\lambda_n)$. Then

$$a_{ii}=\sum_{j=1}^{n}|u_{ij}|^2\lambda_j.$$

Thus $d(A)=B\lambda(A)$, where $B=[|u_{ij}|^2]$ is doubly stochastic. Hence $d(A)\prec\lambda(A)$. □

Theorem 2.4.2 (Ky Fan maximum principle) If $A=A^*$ and $1\le k\le n$, then

$$\sum_{i=1}^{k}\lambda_i(A)=\max\left\{\sum_{i=1}^{k}\langle v_i,Av_i\rangle : v_1,\dots,v_k \text{ orthonormal}\right\}.$$

Proof. Extend $v_1,\dots,v_k$ to an orthonormal basis and let U be the unitary with columns v_i. Schur's theorem applied to U^*AU gives

$$(\langle v_1,Av_1\rangle,\dots,\langle v_n,Av_n\rangle)\prec\lambda(A).$$

Therefore the sum of the first k displayed diagonal entries is at most $\sum_{i=1}^{k}\lambda_i(A)$. Equality is attained by taking $v_1,\dots,v_k$ to be eigenvectors for the k largest eigenvalues. □

Corollary (Weyl-Ky Fan inequalities)

If $A=A^*$ and $B=B^*$, then for $1\le k\le n$,

$$\sum_{i=1}^{k}\lambda_i(A+B)\le\sum_{i=1}^{k}\lambda_i(A)+\sum_{i=1}^{k}\lambda_i(B).$$

Equivalently, $\lambda(A+B)\prec_w\lambda(A)+\lambda(B)$.

Proof. Let $v_1,\dots,v_k$ attain the maximum for $A+B$. Then

$$\sum_{i=1}^{k}\lambda_i(A+B)=\sum_{i}\langle v_i,Av_i\rangle+\sum_{i}\langle v_i,Bv_i\rangle\le\sum_{i=1}^{k}\lambda_i(A)+\sum_{i=1}^{k}\lambda_i(B).$$

□

Theorem 2.4.3 (Schur-Horn theorem) Let $d,\lambda\in\mathbb{R}^n$. There exists a self-adjoint matrix A with diagonal d and eigenvalues λ iff

$$d\prec\lambda.$$

Proof. Necessity is Schur's theorem. For sufficiency, by Hardy-Littlewood-Polya, d can be obtained from λ by finitely many T-transforms. It is enough to realize one T-transform by a unitary conjugation on a two-dimensional coordinate subspace.
For two coordinates a,b, and $0\le t\le 1$, let

$$U_t=\begin{pmatrix}\sqrt{t} & -\sqrt{1-t}\\ \sqrt{1-t} & \sqrt{t}\end{pmatrix}.$$

Then the diagonal of

$$U_t\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}U_t^*$$

is $(ta+(1-t)b,(1-t)a+tb)$. Applying these two-dimensional rotations successively produces a self-adjoint matrix with diagonal d and spectrum λ. □

2.5 Sinkhorn's theorem

> **Theorem** 2.5.1 (Sinkhorn theorem) Let $A\in M_n(\mathbb{R})$ have strictly positive entries. Then there exist positive diagonal matrices R,C such that
>
> $$RAC$$
>
> is doubly stochastic. The pair (R,C) is unique up to replacing (R,C) by $(tR,t^{-1}C)$ with $t>0$.

Proof sketch with the main estimates. Uniqueness is elementary. Suppose R_1AC_1 and R_2AC_2 are doubly stochastic. Put $T=R_2R_1^{-1}$ and $D=C_1^{-1}C_2$. Then $B=R_1AC_1$ and TBD are both doubly stochastic. If t_i and d_j are the diagonal entries of T,D, then

$$\sum_j b_{ij}d_j=t_i^{-1},\qquad \sum_i t_ib_{ij}=d_j^{-1}.$$

Taking a largest t_i and a smallest d_j forces all t_i equal and all d_j equal, since every $b_{ij}>0$.
For existence, alternately normalize rows and columns. Let $A_0=A$. Define A_{2m+1} by normalizing the rows of A_{2m} to sum to 1, and define A_{2m+2} by normalizing the columns of A_{2m+1} to sum to 1. Positivity keeps all normalizing factors finite. Compactness of the normalized matrices gives a convergent subsequence; the monotonicity estimates in Sinkhorn's argument show that all row and column sums of the limit are 1. The accumulated row and column scalings give the desired R,C. □

2.6 Unitary stochastic matrices and Horn's theorem

A doubly stochastic matrix $A=[a_{ij}]$ is called **unitary stochastic** or **unistochastic** if there is a unitary matrix $U=[u_{ij}]$ such that

$$a_{ij}=|u_{ij}|^2.$$

Every unistochastic matrix is doubly stochastic. The converse is false in general, but it is true if one only asks whether a given majorization relation can be realized.

> **Theorem** 2.6.1 (Horn's theorem) For $x,y\in\mathbb{R}^n$,
>
> $$x\prec y$$
>
> if and only if there is a unitary matrix $U=[u_{ij}]$ such that
>
> $$x_i=\sum_{j=1}^n |u_{ij}|^2y_j,\qquad 1\le i\le n.$$
>
> Equivalently, every vector majorized by y is obtained from y by a unistochastic matrix.

Proof. The reverse implication is immediate, since $[|u_{ij}|^2]$ is doubly stochastic.
For the converse, use the Hardy-Littlewood-Polya theorem. It is enough to realize a single T-transform by a unitary. A T-transform changes two coordinates, say a,b, to

$$ta+(1-t)b,\qquad (1-t)a+tb,$$

and fixes the other coordinates. On the corresponding two-dimensional coordinate subspace take

$$U_t = \begin{pmatrix} \sqrt{t} & -\sqrt{1-t} \\ \sqrt{1-t} & \sqrt{t} \end{pmatrix}.$$

Then $|U_t|^{\circ 2}$ is the required two-coordinate T-transform. A finite product of such block unitaries realizes the finite product of T-transforms, so it realizes x from y. □

Remark 2.6.1. The theorem above is the unitary form of the converse to Schur's theorem. It also gives the sufficiency part of Schur-Horn: if $d \prec \lambda$, choose U as above and put $A = U\,\mathrm{diag}(\lambda)U^*$. Then the diagonal of A is d and the eigenvalue vector is λ.

2.7 Doubly stochastic completely positive maps

For self-adjoint matrices $X, Y \in M_n(\mathbb{C})$, write $\lambda(X)$ and $\lambda(Y)$ for their eigenvalue lists in decreasing order.

Definition 2.7.1 ► Doubly stochastic completely positive map

A completely positive map $\tau : M_n \to M_n$ is called **doubly stochastic** if it is both unital and trace preserving. Thus, for a Kraus representation

$$\tau(Z) = \sum_{r=1}^{m} A_r Z A_r^*,$$

we require

$$\sum_r A_r A_r^* = I, \qquad \sum_r A_r^* A_r = I.$$

Theorem 2.7.1 (Majorization through doubly stochastic CP maps) Let $X = X^*$ and $Y = Y^*$ in $M_n(\mathbb{C})$. Then the following are equivalent.

i. $\lambda(X) \prec \lambda(Y)$.

ii. There is a doubly stochastic completely positive map $\tau : M_n \to M_n$ such that

$$X = \tau(Y).$$

Proof. Assume $X = \tau(Y)$, where $\tau(Z) = \sum_r A_r Z A_r^*$ and $\sum_r A_r A_r^* = \sum_r A_r^* A_r = I$. Diagonalize

$$X = U\,\mathrm{diag}(x)U^*, \qquad Y = V\,\mathrm{diag}(y)V^*,$$

where $x = \lambda(X)$ and $y = \lambda(Y)$. Put $B_r = U^* A_r V$. Then

$$\mathrm{diag}(x) = \sum_r B_r\,\mathrm{diag}(y) B_r^*.$$

Taking diagonal entries gives

$$x_i = \sum_{j=1}^{n} d_{ij} y_j, \qquad d_{ij} = \sum_r |(B_r)_{ij}|^2.$$

The matrix $D = [d_{ij}]$ is doubly stochastic because

$$\sum_j d_{ij} = \left(\sum_r B_r B_r^*\right)_{ii} = 1, \qquad \sum_i d_{ij} = \left(\sum_r B_r^* B_r\right)_{jj} = 1.$$

Hence $x = Dy$, so $\lambda(X) \prec \lambda(Y)$.

Conversely, if $\lambda(X) \prec \lambda(Y)$, then by Schur-Horn there is a unitary W such that the diagonal of $W \operatorname{diag}(\lambda(Y))W^*$ is $\lambda(X)$. Equivalently, by Horn's theorem there is a unitary stochastic matrix $D = [|w_{ij}|^2]$ with $\lambda(X) = D\lambda(Y)$. Define a CP map on diagonal matrices by the stochastic transition D, and then conjugate by the spectral unitaries of X and Y. Explicitly, one may take Kraus operators $A_{ij} = \sqrt{d_{ij}}\, u_i v_j^*$, where u_i and v_j are eigenvectors of X and Y. Then

$$\tau(Y) = \sum_{i,j} d_{ij} \lambda_j(Y) |u_i\rangle\langle u_i| = X,$$

and the row and column sum conditions make τ unital and trace preserving. □

2.8 Extreme points of the order interval

Let

$$\mathscr{C} = \{X \in M_n(\mathbb{C}) : 0 \leq X \leq I\}.$$

> **Theorem** 2.8.1 (Extreme points of $\mathscr{C}$) The extreme points of $\mathscr{C}$ are precisely the orthogonal projections.

Proof. Let $X \in \mathscr{C}$ be extreme. Diagonalize

$$X = U \operatorname{diag}(\lambda_1, \ldots, \lambda_n) U^*, \qquad 0 \leq \lambda_i \leq 1.$$

If some $\lambda_i \in (0,1)$, then for sufficiently small $\varepsilon > 0$ both

$$X \pm \varepsilon U E_{ii} U^*$$

belong to $\mathscr{C}$, and X is their non-trivial average. This contradicts extremality. Hence each λ_i is 0 or 1, so X is a projection.
Conversely, let P be a projection and suppose $P = (Y+Z)/2$ with $Y, Z \in \mathscr{C}$. If $v \in \ker P$, then

$$0 = \langle v, Pv \rangle = \frac{1}{2}\langle v, Yv \rangle + \frac{1}{2}\langle v, Zv \rangle.$$

Since $Y, Z \geq 0$, this forces $Yv = Zv = 0$. If $v \in \operatorname{ran} P$, apply the same argument to $I - P = (I - Y + I - Z)/2$ to get $Yv = Zv = v$. Thus $Y = Z = P$, so P is extreme. □

2.9 Hilbert projective metric

Let S be a real Banach space and $K \subset S$ a closed proper cone. Define $x \leq_K y$ iff $y - x \in K$. For $x, y \in K \setminus \{0\}$ set

$$M(x,y) = \inf\{\lambda > 0 : x \leq_K \lambda y\}, \qquad m(x,y) = \sup\{\mu > 0 : \mu y \leq_K x\}.$$

The Hilbert projective distance is

$$d_H(x,y) = \log \frac{M(x,y)}{m(x,y)}.$$

It is a genuine metric on projective classes $[x] = \{\alpha x : \alpha > 0\}$. For the cone of strictly positive matrices, this metric is useful in studying convergence of the Sinkhorn iteration.

Chapter 3

Positive and Completely Positive Maps

Let $M_n = M_n(\mathbb{C})$. We use the Hilbert-Schmidt inner product

$$\langle X, Y\rangle_{HS} = \mathrm{Tr}(X^*Y).$$

3.1 Positive maps

Definition 3.1.1 ► Positive map

A linear map $\tau : M_n \to M_n$ is called **positive** if

$$X \geq 0 \implies \tau(X) \geq 0.$$

It is called **unital** if $\tau(I) = I$ and **trace preserving** if $\mathrm{Tr}\,\tau(X) = \mathrm{Tr}X$ for all X.

Every positive map is $*$-preserving: if $X = X^*$, write $X = X_+ - X_-$ with $X_\pm \geq 0$ by the spectral theorem. Then $\tau(X)$ is self-adjoint, and linearity gives $\tau(X^*) = \tau(X)^*$ for all X.

Definition 3.1.2 ► k-positive and completely positive maps

For $k \geq 1$, a linear map $\tau : M_n \to M_n$ is called **k-positive** if

$$\mathrm{id}_k \otimes \tau : M_k(M_n) \simeq M_k \otimes M_n \to M_k \otimes M_n$$

is positive. It is **completely positive** if it is k-positive for every $k \geq 1$.

Since M_n is finite dimensional, n-positivity already implies complete positivity.

3.2 Kraus form and adjoints

Definition 3.2.1 ► Kraus map

A map of the form

$$\tau(X) = \sum_{j=1}^{r} L_j X L_j^*, \qquad L_j \in M_n,$$

is called a **Kraus map**. The matrices L_j are called Kraus operators.

Every Kraus map is completely positive. Indeed, if $[X_{ab}] \in M_k(M_n)$ is positive, then for each j,

$$[L_j X_{ab} L_j^*] = (I_k \otimes L_j)[X_{ab}](I_k \otimes L_j)^* \geq 0,$$

and sums of positive matrices are positive.

The Hilbert-Schmidt adjoint of a Kraus map is

$$\tau^*(X) = \sum_{j=1}^{r} L_j^* X L_j.$$

Consequently

$$\tau \text{ is unital} \iff \sum_j L_j L_j^* = I, \qquad \tau \text{ is trace preserving} \iff \sum_j L_j^* L_j = I.$$

Thus a map is trace preserving iff its adjoint is unital.

3.3 Choi matrix and Choi-Kraus theorem

Let $E_{ij} = |e_i\rangle\langle e_j|$ be the standard matrix units of M_n.

Definition 3.3.1 ► Choi matrix

The **Choi matrix** of $\tau : M_n \to M_n$ is

$$C_\tau = [\tau(E_{ij})]_{i,j=1}^{n} \in M_n(M_n) \simeq M_n \otimes M_n.$$

Equivalently,

$$C_\tau = (\mathrm{id}_n \otimes \tau)(|\Omega\rangle\langle\Omega|), \qquad \Omega = \sum_{i=1}^{n} e_i \otimes e_i.$$

Theorem 3.3.1 (Choi-Kraus theorem) For a linear map $\tau : M_n \to M_n$, the following are equivalent.

i. τ is completely positive.

ii. τ is n-positive.

iii. $C_\tau \geq 0$.

iv. There exist matrices $L_1, \ldots, L_r \in M_n$ such that

$$\tau(X) = \sum_{j=1}^{r} L_j X L_j^*.$$

Moreover one may take $r = \mathrm{rank}(C_\tau)$, and the minimal number of Kraus operators is called the **Choi rank**.

Proof. (1)⇒(2) is immediate. If τ is n-positive, then

$$|\Omega\rangle\langle\Omega| = [E_{ij}]_{i,j=1}^{n} \geq 0,$$

so $C_\tau = [\tau(E_{ij})] \geq 0$. Thus (2)⇒(3).
Assume $C_\tau \geq 0$. Decompose it as

$$C_\tau = \sum_{\alpha=1}^{r} |v_\alpha\rangle\langle v_\alpha|.$$

Write each $v_\alpha \in \mathbb{C}^n \otimes \mathbb{C}^n$ as

$$v_\alpha = \sum_{i=1}^{n} e_i \otimes L_\alpha e_i$$

for a uniquely determined matrix L_α. Comparing the (i,j) block of C_τ gives

$$\tau(E_{ij}) = \sum_{\alpha=1}^{r} L_\alpha E_{ij} L_\alpha^*.$$

By linearity this holds for every $X \in M_n$, proving the Kraus form. As observed earlier, Kraus form implies complete positivity. □

3.4 Schur product theorem

Theorem 3.4.1 (Schur product theorem) If $A = [a_{ij}] \geq 0$ and $B = [b_{ij}] \geq 0$ in M_n, then their entrywise product

$$A \circ B = [a_{ij} b_{ij}]$$

is positive.

Proof. Since $A \geq 0$, there exist vectors $u_1, \ldots, u_n$ such that $a_{ij} = \langle u_i, u_j \rangle$. Similarly $b_{ij} = \langle v_i, v_j \rangle$. Then

$$a_{ij} b_{ij} = \langle u_i \otimes v_i, u_j \otimes v_j \rangle,$$

so $A \circ B$ is a Gram matrix and hence positive. □

For fixed $A \geq 0$, the map

$$S_A : M_n \to M_n, \qquad S_A(X) = A \circ X,$$

is completely positive. Indeed, by the spectral decomposition $A = \sum_k \lambda_k u_k u_k^*$, one can write

$$A \circ X = \sum_k D_k X D_k^*, \qquad D_k = \sqrt{\lambda_k}\,\mathrm{diag}(u_k).$$

3.5 Quantum channels

Definition 3.5.1 ► Quantum channel

A **quantum channel** on M_n is a completely positive trace-preserving map. Equivalently,

$$\tau(X) = \sum_j L_j X L_j^*, \qquad \sum_j L_j^* L_j = I.$$

A unital completely positive map is also called a **UCP map**.

A unitary channel has the form $X \mapsto UXU^*$. A mixed unitary channel has the form

$$\tau(X) = \sum_{j=1}^{r} p_j U_j X U_j^*, \qquad p_j \geq 0, \quad \sum_j p_j = 1.$$

Every mixed unitary channel is both unital and trace preserving. The converse is false in general.

Remark 3.5.1. The analogy with stochastic matrices is useful but imperfect. Doubly stochastic matrices are convex combinations of permutations by Birkhoff's theorem. The quantum analogue would say that every unital trace-preserving channel is mixed unitary; this fails for matrix algebras of sufficiently large size.

3.6 Adjoints and duality of complete positivity

The Hilbert-Schmidt adjoint of a linear map $\tau : M_n \to M_n$ is the unique map τ^* satisfying

$$\mathrm{Tr}(\tau(X)^* Y) = \mathrm{Tr}(X^* \tau^*(Y)) \qquad (X, Y \in M_n).$$

If

$$\tau(X) = \sum_{r=1}^{m} A_r X A_r^*,$$

then

$$\tau^*(X) = \sum_{r=1}^{m} A_r^* X A_r.$$

Hence τ is CP if and only if τ^* is CP. Moreover

$$\tau \text{ is trace preserving} \iff \tau^* \text{ is unital.}$$

Indeed,

$$\mathrm{Tr}(\tau(X)) = \mathrm{Tr}(X \tau^*(I)),$$

for every X, and this equals $\mathrm{Tr}(X)$ for every X if and only if $\tau^*(I) = I$.

Remark 3.6.1. For a Kraus map, the two normalizations

$$\sum_r A_r A_r^* = I, \qquad \sum_r A_r^* A_r = I$$

are the non-commutative analogues of row and column sum one. This is why unital trace-preserving CP maps are often called doubly stochastic quantum maps.

3.7 Exercises

i. Show that the transpose map $X \mapsto X^T$ is positive but not completely positive on M_n for $n \geq 2$.

ii. Compute the Choi matrix of a unitary channel $X \mapsto UXU^*$.

iii. Show that $S_A(X) = A \circ X$ is trace preserving iff $a_{ii} = 1$ for all i.

iv. Let $\tau(X) = \sum_j L_j X L_j^*$. Prove directly that τ is unital iff τ^* is trace preserving.

v. Prove that if τ is CP and unital, then $\tau(X^*X) \geq \tau(X)^*\tau(X)$. This is Kadison's inequality.

Chapter 4

Quantum Probability

Let $\mathscr{H}$ be a finite dimensional Hilbert space. Quantum probability replaces events by orthogonal projections and probability measures by states.

4.1 Events as projections

A projection is an operator $P \in \mathscr{B}(\mathscr{H})$ satisfying $P = P^* = P^2$. It is the orthogonal projection onto the closed subspace $P\mathscr{H}$. Conversely, every closed subspace has a unique orthogonal projection.
For projections P, Q, define

$$P \wedge Q = \text{projection onto } P\mathscr{H} \cap Q\mathscr{H},$$

$$P \vee Q = \text{projection onto } \overline{P\mathscr{H} + Q\mathscr{H}}, \qquad P^{\perp} = I - P.$$

If $PQ = QP$, then $P \wedge Q = PQ$ and $P \vee Q = P + Q - PQ$. In general, the lattice of projections is not distributive; this is one of the first algebraic differences from classical probability.

Definition 4.1.1 ► Quantum probability measure

A quantum probability measure on the projection lattice is a function

$$\mathbb{P} : \{\text{projections on } \mathscr{H}\} \to [0,1]$$

such that

$$\mathbb{P}(0) = 0, \qquad \mathbb{P}(I - P) = 1 - \mathbb{P}(P),$$

and whenever $P_1, \dots, P_m$ are pairwise orthogonal projections,

$$\mathbb{P}\left(\sum_{j=1}^{m} P_j\right) = \sum_{j=1}^{m} \mathbb{P}(P_j).$$

Theorem 4.1.1 (Gleason theorem) If $\dim \mathscr{H} \geq 3$, then every quantum probability measure has the form

$$\mathbb{P}(P) = \operatorname{Tr}(\rho P),$$

where $\rho \geq 0$ and $\operatorname{Tr} \rho = 1$. The matrix ρ is called a density matrix.

Remark 4.1.1. The theorem fails in dimension 2 without additional regularity assumptions. This exceptional behavior is related to the geometry of the Bloch sphere.

A unit vector $u \in \mathscr{H}$ defines a pure state

$$\rho = |u\rangle\langle u|, \qquad \mathbb{P}(P) = \langle u, Pu\rangle.$$

More generally, any density matrix has a spectral decomposition

$$\rho = \sum_j p_j |u_j\rangle\langle u_j|, \qquad p_j \geq 0, \quad \sum_j p_j = 1,$$

so it is a convex combination of pure states.

4.2 Observables

An observable is a self-adjoint matrix $A = A^*$. If

$$A = \sum_{j=1}^{r} a_j P_j$$

is its spectral decomposition, then A takes value a_j with probability

$$\mathbb{P}(A = a_j) = \mathrm{Tr}\big(\rho P_j\big).$$

Thus

$$\mathbb{E}_\rho[A] = \sum_j a_j \,\mathrm{Tr}\big(\rho P_j\big) = \mathrm{Tr}(\rho A).$$

The variance is

$$\mathrm{Var}_\rho(A) = \mathrm{Tr}\big(\rho A^2\big) - \mathrm{Tr}(\rho A)^2.$$

For a pure state $\rho = |u\rangle\langle u|$, this becomes

$$\mathbb{E}_u[A] = \langle u, Au\rangle, \qquad \mathrm{Var}_u(A) = \|(A - \mathbb{E}_u[A]I)u\|^2.$$

4.3 Heisenberg and Schrodinger uncertainty

Theorem 4.3.1 (Uncertainty principle) Let $u \in \mathscr{H}$ be a unit vector and let $A = A^*$, $B = B^*$. Put

$$a = \langle u, Au\rangle, \qquad b = \langle u, Bu\rangle.$$

Then

$$\mathrm{Var}_u(A)\mathrm{Var}_u(B) \geq \frac{1}{4}|\langle u, [A,B]u\rangle|^2.$$

More precisely,

$$\mathrm{Var}_u(A)\mathrm{Var}_u(B) \geq \frac{1}{4}|\langle u, [A,B]u\rangle|^2 + \frac{1}{4}|\langle u, \{A - aI, B - bI\}u\rangle|^2,$$

where $[A,B] = AB - BA$ and $\{X,Y\} = XY + YX$.

Proof. Set $X = (A - aI)u$ and $Y = (B - bI)u$. By Cauchy-Schwarz,

$$\mathrm{Var}_u(A)\mathrm{Var}_u(B) = \|X\|^2\|Y\|^2 \geq |\langle X, Y\rangle|^2.$$

Now

$$\langle X, Y\rangle = \langle (A - aI)u, (B - bI)u\rangle = \langle u, (A - aI)(B - bI)u\rangle.$$

Its imaginary part is

$$\mathrm{Im}\,\langle X, Y\rangle = \frac{1}{2i}\langle u, [A,B]u\rangle,$$

and its real part is

$$\mathrm{Re}\,\langle X, Y\rangle = \frac{1}{2}\langle u, \{A - aI, B - bI\}u\rangle.$$

Taking only the imaginary part gives the Heisenberg form; keeping both parts gives Schrodinger's stronger inequality. □

4.4 Pauli matrices and Bell's inequality

The Pauli matrices are

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If $x = (x_1, x_2, x_3) \in \mathbb{R}^3$, write

$$\sigma(x) = x_1\sigma_1 + x_2\sigma_2 + x_3\sigma_3.$$

Then

$$\mathrm{Tr}(\sigma_i) = 0, \qquad \sigma_i^2 = I, \qquad \frac{1}{2}\mathrm{Tr}\big(\sigma_i\sigma_j\big) = \delta_{ij},$$

and

$$\sigma(x)^2 = \|x\|^2 I.$$

Thus if $\|x\| = 1$, then $\sigma(x)$ is a self-adjoint unitary with eigenvalues ± 1.

Theorem 4.4.1 (Bell inequality) Let X_1, X_2, X_3 be classical random variables taking values in $[-1, 1]$. Then

$$1 - \mathbb{E}[X_1X_2] \geq |\mathbb{E}[X_1X_3] - \mathbb{E}[X_2X_3]|.$$

Proof. Pointwise,

$$|x_1x_3 - x_2x_3| = |x_3||x_1 - x_2| \leq |x_1 - x_2|.$$

For $x_1, x_2 \in [-1, 1]$ one has $|x_1 - x_2| \leq 1 - x_1x_2$. Taking expectations gives the result. □

Quantum correlations can violate this inequality. In the singlet state on $\mathbb{C}^2 \otimes \mathbb{C}^2$, the correlation of spin measurements in unit directions $x, y \in \mathbb{R}^3$ is

$$\mathbb{E}[\sigma(x) \otimes \sigma(y)] = -\langle x, y \rangle.$$

Hence choosing three unit vectors with a suitable angle, for example separated by 60°, gives correlations which cannot be represented by three classical random variables satisfying Bell's inequality. This is not a contradiction; it shows that the classical joint model does not exist.

4.5 Exercises

i. Show that if projections P, Q commute, then $P \wedge Q = PQ$ and $P \vee Q = P + Q - PQ$.

ii. Give an example showing that the projection lattice of $\mathbb{C}^2$ is not distributive.

iii. Prove that the extreme points of the convex set of density matrices are precisely the rank-one projections.

iv. Verify the Pauli identities $\sigma_i\sigma_j = \delta_{ij}I + i\sum_k \epsilon_{ijk}\sigma_k$.

v. Let $x, y \in \mathbb{R}^3$ be unit vectors. Prove that $\sigma(x)$ and $\sigma(y)$ commute iff $x = \pm y$.

Chapter 5

Differentiators and Geometry of Polynomials

Let $\mathscr{H}$ be an n-dimensional Hilbert space and let $A \in \mathscr{B}(\mathscr{H})$. Write

$$p_A(z) = \det(zI - A)$$

for the characteristic polynomial, and write

$$\tau(X) = \frac{1}{n}\operatorname{Tr}(X)$$

for the normalized trace.

5.1 Differentiators

Definition 5.1.1 ► Differentiator

Let P be an orthogonal projection of rank $n-1$. The compression of A to $P\mathscr{H}$ is

$$A_P = PAP|_{P\mathscr{H}}.$$

We say that P is a **differentiator for** A if

$$p_{A_P}(z) = \frac{1}{n}p_A'(z).$$

Equivalently, the eigenvalues of the compression are the critical points of p_A, counted with multiplicity.

If P has rank $n-1$, then $P = I - |v\rangle\langle v|$ for a unit vector v, unique up to multiplication by a scalar of modulus one. In this case we also say that v is a differentiator vector.

Theorem 5.1.1 (Resolvent criterion) Let v be a unit vector and $P = I - |v\rangle\langle v|$. The following are equivalent.

i. P is a differentiator for A.

ii. For all sufficiently large $|z|$,

$$\left\langle v, (zI - A)^{-1} v \right\rangle = \tau((zI - A)^{-1}).$$

iii. For every $k \geq 0$,

$$\left\langle v, A^k v \right\rangle = \tau(A^k).$$

iv. For every polynomial q,

$$\langle v, q(A)v \rangle = \tau(q(A)).$$

Proof. Choose an orthonormal basis beginning with v. In this basis the compression A_P is the lower-right principal block of A. By the cofactor formula for the inverse,

$$\left\langle v, (zI - A)^{-1} v \right\rangle = \frac{p_{A_P}(z)}{p_A(z)}.$$

Also Jacobi's formula gives

$$\frac{p_A'(z)}{p_A(z)} = \mathrm{Tr}\big((zI - A)^{-1}\big).$$

Thus (1) and (2) are equivalent.
For large z,

$$(zI - A)^{-1} = \sum_{k=0}^{\infty} z^{-k-1} A^k.$$

Comparing coefficients in (2) gives (3), and (3) is exactly (4) by linearity. Conversely, (4) gives equality of the resolvents through the same power series expansion. □

Corollary (Trace vectors for normal matrices)

Suppose A is normal and

$$A = \sum_{j=1}^{r} \lambda_j P_j$$

is its spectral resolution. A unit vector v is a differentiator vector for A iff

$$\|P_j v\|^2 = \frac{\mathrm{rank}\, P_j}{n}, \qquad 1 \leq j \leq r.$$

In particular, if A has simple eigenvalues and $u_1, \ldots, u_n$ is an orthonormal eigenbasis, then

$$v = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} \alpha_j u_j, \qquad |\alpha_j| = 1,$$

is a differentiator vector.

Proof. For a polynomial q,

$$\langle v, q(A)v \rangle = \sum_{j=1}^{r} q(\lambda_j) \|P_j v\|^2, \qquad \tau(q(A)) = \sum_{j=1}^{r} q(\lambda_j) \frac{\mathrm{rank}\, P_j}{n}.$$

Since polynomials separate the finitely many points λ_j, equality for all q is equivalent to equality of the displayed coefficients. □

5.2 Interlacing for real parts

For $A \in M_n(\mathbb{C})$, define

$$\operatorname{Re} A = \frac{A + A^*}{2}.$$

Lemma 5.2.1 (Real part interlacing)

Let $A \in M_n(\mathbb{C})$ and let $\lambda_1(A), \ldots, \lambda_n(A)$ be its eigenvalues. Then, after arranging decreasingly,

$$\lambda(\operatorname{Re} A) \prec \big(\operatorname{Re}\lambda_1(A), \ldots, \operatorname{Re}\lambda_n(A)\big)^{\downarrow}$$

need not hold in general, but the diagonal of a Schur form gives

$$(\operatorname{Re}\lambda_1(A), \ldots, \operatorname{Re}\lambda_n(A)) \prec d(\operatorname{Re} T),$$

where T is any Schur triangular form of A. In particular, eigenvalue real parts of compressions can be represented by convex averages of eigenvalue real parts after a suitable Schur basis.

Proof. Let $A = UTU^*$ with T upper triangular and diagonal entries $\lambda_1(A), \ldots, \lambda_n(A)$. Then $\operatorname{Re} T = (T + T^*)/2$ is self-adjoint and has diagonal entries $\operatorname{Re}\lambda_j(A)$. Schur's theorem applied to the self-adjoint matrix $\operatorname{Re} T$ gives

$$d(\operatorname{Re} T) \prec \lambda(\operatorname{Re} T) = \lambda(\operatorname{Re} A).$$

The displayed relation is the form needed in applications after choosing a Schur basis for a compression. □

Remark 5.2.1. The handwritten notes used this point only as a device for passing from eigenvalues of a compression to convex averages of eigenvalues of a normal dilation. In the final majorization theorem below the needed statement is proved directly, avoiding possible ambiguity about the order of the interlacing relation.

5.3 Gauss-Lucas theorem

Theorem 5.3.1 (Gauss-Lucas theorem) Let p be a non-constant complex polynomial. Every critical point of p lies in the convex hull of the roots of p.

Proof. Let the roots of p be $z_1, \ldots, z_n$, counted with multiplicity, and set

$$A = \operatorname{diag}(z_1, \ldots, z_n).$$

Let

$$v = \frac{1}{\sqrt{n}}(1, \ldots, 1)^T, \qquad P = I - |v\rangle\langle v|.$$

By the trace-vector criterion, P is a differentiator for A. Hence the eigenvalues of the compression $B = PAP|_{P\mathbb{C}^n}$ are exactly the roots of p'/n.
Since A is normal,

$$W(A) = \operatorname{conv}\{z_1, \ldots, z_n\}.$$

For any unit vector $x \in P\mathbb{C}^n$,

$$\langle x, Bx\rangle = \langle x, Ax\rangle \in W(A),$$

so $W(B) \subseteq W(A)$. Every eigenvalue of B belongs to $W(B)$. Therefore every critical point of p lies in $\operatorname{conv}\{z_1, \ldots, z_n\}$. □

5.4 Katsoprinakis' conjecture on real parts

Let p be a polynomial of degree n with roots $z_1,\dots,z_n$ and critical points $w_1,\dots,w_{n-1}$. Let q be the monic polynomial with roots

$$\mathrm{Re}\, z_1,\dots,\mathrm{Re}\, z_n,$$

and let $b_1,\dots,b_{n-1}$ be the critical points of q. Put

$$a_i = \mathrm{Re}\, w_i, \qquad 1 \le i \le n-1.$$

Theorem 5.4.1 (Katsoprinakis' conjecture) With the notation above,

$$(a_1,\dots,a_{n-1}) \prec (b_1,\dots,b_{n-1}).$$

Equivalently, for every convex function $\varphi : \mathbb{R} \to \mathbb{R}$,

$$\sum_{i=1}^{n-1} \varphi(\mathrm{Re}\, w_i) \le \sum_{i=1}^{n-1} \varphi(b_i).$$

Proof. We use a standard eigenvalue majorization lemma. If $T \in M_m(\mathbb{C})$, then

$$(\mathrm{Re}\,\lambda_1(T),\dots,\mathrm{Re}\,\lambda_m(T)) \prec \lambda(\mathrm{Re}\, T).$$

Indeed, take a Schur triangularization $T = URU^*$. Then $\mathrm{Re}\, R$ is self-adjoint and has diagonal entries $\mathrm{Re}\,\lambda_i(T)$. By Schur's theorem, the diagonal vector of $\mathrm{Re}\, R$ is majorized by the eigenvalue vector of $\mathrm{Re}\, R$, which equals $\lambda(\mathrm{Re}\, T)$.
Now let $A = \mathrm{diag}(z_1,\dots,z_n)$ and let $v = n^{-1/2}(1,\dots,1)^T$. Put $H = v^\perp$ and

$$B = P_H A|_H.$$

By the differentiator theorem, the eigenvalues of B are $w_1,\dots,w_{n-1}$. Therefore

$$(\mathrm{Re}\, w_1,\dots,\mathrm{Re}\, w_{n-1}) \prec \lambda(\mathrm{Re}\, B).$$

But

$$\mathrm{Re}\, B = P_H(\mathrm{Re} A)|_H, \qquad \text{where } \mathrm{Re} A = \mathrm{diag}(\mathrm{Re}\, z_1,\dots,\mathrm{Re}\, z_n).$$

Since v is also a trace vector for $\mathrm{Re} A$, this compression is a differentiator for the real diagonal matrix $\mathrm{Re} A$. Hence the eigenvalues of $\mathrm{Re}\, B$ are precisely the critical points $b_1,\dots,b_{n-1}$ of q. This proves the claimed majorization. □

Remark 5.4.1. The equality of means needed for majorization is automatic: by comparing the coefficient of z^{n-2} in p', one has

$$\frac{1}{n-1}\sum_{i=1}^{n-1} w_i = \frac{1}{n}\sum_{j=1}^{n} z_j.$$

Taking real parts gives the corresponding equality for (a_i) and (b_i).

5.5 The de Bruijn-Springer theorem

Definition 5.5.1 ► Rectangular doubly stochastic matrix

An $m\times n$ matrix $S=[s_{ij}]$ is **rectangular doubly stochastic** if

$$s_{ij}\geq 0,\qquad \sum_{j=1}^{n} s_{ij}=1 \quad (1\leq i\leq m),\qquad \sum_{i=1}^{m} s_{ij}=\frac{m}{n} \quad (1\leq j\leq n).$$

For $x\in\mathbb{C}^m$ and $y\in\mathbb{C}^n$, write $x\prec_{\mathrm{r}} y$ if $x=Sy$ for some rectangular doubly stochastic S.

If $x=Sy$ and $\varphi:\mathbb{C}\to\mathbb{R}$ is convex, then Jensen's inequality gives

$$\frac{1}{m}\sum_{i=1}^{m}\varphi(x_i)\leq\frac{1}{n}\sum_{j=1}^{n}\varphi(y_j).$$

Theorem 5.5.1 (de Bruijn-Springer theorem) Let p have roots $z_1,\dots,z_n$ and critical points $w_1,\dots,w_{n-1}$, counted with multiplicity. Then there is a rectangular doubly stochastic matrix $S\in M_{n-1,n}(\mathbb{R})$ such that

$$\begin{pmatrix} w_1\\ \vdots\\ w_{n-1}\end{pmatrix}=S\begin{pmatrix} z_1\\ \vdots\\ z_n\end{pmatrix}.$$

Consequently, for every convex $\varphi:\mathbb{C}\to\mathbb{R}$,

$$\frac{1}{n-1}\sum_{i=1}^{n-1}\varphi(w_i)\leq\frac{1}{n}\sum_{j=1}^{n}\varphi(z_j).$$

Proof. Let $A=\operatorname{diag}(z_1,\dots,z_n)$ on $\mathbb{C}^n$ and $v=n^{-1/2}(1,\dots,1)^T$. Let $H=v^{\perp}$ and $B=P_HA|_H$. By the differentiator theorem, the eigenvalues of B are $w_1,\dots,w_{n-1}$.
By Schur triangularization on H, choose an orthonormal basis $u_1,\dots,u_{n-1}$ of H such that the diagonal entries of the matrix of B are w_i; equivalently,

$$w_i=\langle u_i,Bu_i\rangle=\langle u_i,Au_i\rangle.$$

If $e_1,\dots,e_n$ is the standard basis and $s_{ij}=|\langle e_j,u_i\rangle|^2$, then

$$w_i=\sum_{j=1}^{n}s_{ij}z_j.$$

The row sums are 1 because each u_i is a unit vector. The column sums are

$$\sum_{i=1}^{n-1}s_{ij}=\sum_{i=1}^{n-1}|\langle e_j,u_i\rangle|^2=\|P_He_j\|^2=1-|\langle v,e_j\rangle|^2=1-\frac{1}{n}=\frac{n-1}{n}.$$

Thus $S=[s_{ij}]$ is rectangular doubly stochastic. □

5.6 Exercises

i. Let $A=\operatorname{diag}(z_1,\dots,z_n)$ and $v=n^{-1/2}(1,\dots,1)$. Compute explicitly the compression $PAP|_{v^{\perp}}$ for $n=3$.

ii. Show that if v is a differentiator vector for A, then αv is also a differentiator vector for every $|\alpha|=1$.

iii. Prove the cofactor identity

$$\langle v, (zI - A)^{-1} v \rangle = p_{A_p}(z)/p_A(z)$$

directly from Schur complements.

iv. Deduce the ordinary Gauss-Lucas theorem from de Bruijn-Springer by taking φ to be the distance from a closed half-plane.

Chapter 6

Singular Values and Matrix Factorisations

6.1 Schur's inequality

Let $A \in M_n(\mathbb{C})$ have eigenvalues $\lambda_1, \dots, \lambda_n$, counted with algebraic multiplicity. The Hilbert-Schmidt norm is

$$\|A\|_{HS}^2 = \operatorname{Tr}(A^*A) = \sum_{i,j} |a_{ij}|^2.$$

Theorem 6.1.1 (Schur inequality) For every $A \in M_n(\mathbb{C})$,

$$\sum_{j=1}^n |\lambda_j|^2 \le \|A\|_{HS}^2.$$

Equality holds iff A is normal.

Proof. By Schur triangularization, A is unitarily equivalent to an upper triangular matrix T with diagonal entries λ_j. The Hilbert-Schmidt norm is unitarily invariant, so

$$\|A\|_{HS}^2 = \|T\|_{HS}^2 = \sum_j |\lambda_j|^2 + \sum_{i<j} |t_{ij}|^2 \ge \sum_j |\lambda_j|^2.$$

Equality holds iff T is diagonal, i.e. iff A is unitarily diagonalizable, equivalently normal. □

Applying this to $\operatorname{Re} A$ and $\operatorname{Im} A$ gives

$$\sum_j (\operatorname{Re} \lambda_j)^2 \le \|\operatorname{Re} A\|_{HS}^2, \qquad \sum_j (\operatorname{Im} \lambda_j)^2 \le \|\operatorname{Im} A\|_{HS}^2.$$

6.2 Schoenberg's inequality for critical points

Theorem 6.2.1 (Schoenberg inequality) Let p be a polynomial of degree n with roots $z_1, \dots, z_n$ and critical points $w_1, \dots, w_{n-1}$. Put

$$a = \frac{1}{n} \sum_{j=1}^n z_j = \frac{1}{n-1} \sum_{i=1}^{n-1} w_i.$$

Then

$$\sum_{i=1}^{n-1} |w_i|^2 \le |a|^2 + \frac{n-2}{n} \sum_{j=1}^n |z_j|^2.$$

Equality holds iff the roots $z_1, \dots, z_n$ are collinear.

Proof. Let $A = \operatorname{diag}(z_1, \dots, z_n)$ and let $v = n^{-1/2}(1, \dots, 1)^T$. Let $H = v^\perp$ and $B = P_H A|_H$. The eigenvalues of B are $w_1, \dots, w_{n-1}$.
Write the matrix of A in the orthogonal decomposition $H \oplus \mathbb{C}v$ as

$$A = \begin{pmatrix} B & x \\ y^* & a \end{pmatrix}, \qquad a = \langle v, Av \rangle = \frac{1}{n} \sum_j z_j.$$

Since v is a trace vector for the normal matrices A^*A and AA^*,

$$\|x\|^2 + |a|^2 = \langle v, AA^* v \rangle = \frac{1}{n} \sum_j |z_j|^2,$$

and

$$\|y\|^2 + |a|^2 = \langle v, A^*Av \rangle = \frac{1}{n} \sum_j |z_j|^2.$$

Thus

$$\|B\|_{HS}^2 = \|A\|_{HS}^2 - \|x\|^2 - \|y\|^2 - |a|^2 = \frac{n-2}{n} \sum_j |z_j|^2 + |a|^2.$$

By Schur's inequality applied to B,

$$\sum_i |w_i|^2 \le \|B\|_{HS}^2,$$

which gives the desired bound.
Equality holds iff B is normal. In this compression setting, normality of B is equivalent to $x = y$ up to a unimodular scalar, which is equivalent to all z_j lying on a common line. This gives the equality condition. □

6.3 Polar decomposition

Definition 6.3.1 ► Partial isometry

An operator $V : \mathscr{H} \to \mathscr{K}$ is a **partial isometry** if there is a closed subspace $M \subseteq \mathscr{H}$ such that $V|_M$ is an isometry and $V|_{M^\perp} = 0$. The space M is the initial space, and $V(M)$ is the final space.

Equivalently, V is a partial isometry iff V^*V is a projection iff VV^* is a projection.

Theorem 6.3.1 (Polar decomposition) Let $A : \mathscr{H} \to \mathscr{K}$ be a linear map between finite dimensional Hilbert spaces. Then

$$A = V|A|, \qquad |A| = (A^*A)^{1/2},$$

where V is a partial isometry with initial space $\overline{\operatorname{ran}|A|} = (\ker A)^\perp$ and final space $\overline{\operatorname{ran} A}$. This V is uniquely determined by these conditions.

Proof. Define V first on $\operatorname{ran}|A|$ by

$$V(|A|x) = Ax.$$

This is well-defined: if $|A|x = |A|y$, then $\|A(x-y)\|^2 = \langle x-y, A^*A(x-y) \rangle = \||A|(x-y)\|^2 = 0$. It is an isometry on $\operatorname{ran}|A|$ because

$$\|Ax\|^2 = \langle x, A^*Ax \rangle = \||A|x\|^2.$$

Extend V by zero on $(\operatorname{ran}|A|)^\perp = \ker A$. Then V is a partial isometry and $A = V|A|$. The initial and final space requirements force uniqueness. □

If A is invertible, then V is unitary. If A is normal, then V and $|A|$ commute.

6.4 Singular value decomposition

Definition 6.4.1 ► Singular values

The singular values of A are the eigenvalues of $|A| = (A^*A)^{1/2}$, listed decreasingly:

$$s_1(A) \geq s_2(A) \geq \cdots \geq s_n(A) \geq 0.$$

Theorem 6.4.1 (Singular value decomposition) For every $A \in M_{m,n}(\mathbb{C})$ there exist unitaries $U \in M_m(\mathbb{C})$ and $V \in M_n(\mathbb{C})$ such that

$$A = U\Sigma V^*,$$

where Σ is rectangular diagonal with diagonal entries $s_1(A), s_2(A), \ldots$. Equivalently,

$$A = \sum_{j=1}^{r} s_j |u_j\rangle\langle v_j|,$$

where $r = \operatorname{rank} A$, $s_j > 0$, $\{u_j\}$ is orthonormal in $\mathbb{C}^m$, and $\{v_j\}$ is orthonormal in $\mathbb{C}^n$.

Proof. Diagonalize A^*A as

$$A^*A = \sum_j s_j^2 |v_j\rangle\langle v_j|.$$

For $s_j > 0$, set $u_j = s_j^{-1} A v_j$. Then

$$\langle u_i, u_j\rangle = s_i^{-1} s_j^{-1} \langle Av_i, Av_j\rangle = s_i^{-1} s_j^{-1} \langle v_i, A^*Av_j\rangle = \delta_{ij}.$$

Extend the u_j's and v_j's to orthonormal bases. The displayed SVD follows. □

6.5 Variational and perturbation inequalities

The operator norm satisfies $\|A\| = s_1(A)$. For $1 \leq k \leq n$,

$$s_k(A) = \inf\{\|A(I-P)\| : P \text{ projection with } \operatorname{rank} P = k-1\}.$$

Indeed, in an SVD, the infimum is attained by projecting onto the span of the first $k-1$ right singular vectors, and the converse follows from the min-max principle for A^*A.

Proposition 6.5.1 (Basic singular value inequalities)**.** For matrices of compatible sizes:

i. $s_k(XA) \leq \|X\| s_k(A)$ and $s_k(AX) \leq \|X\| s_k(A)$.

ii. $s_{k+m-1}(A+B) \leq s_k(A) + s_m(B)$ whenever $k+m-1 \leq n$.

iii. $s_{k+m-1}(AB) \leq s_k(A) s_m(B)$ whenever $k+m-1 \leq n$.

iv. $|s_k(A) - s_k(B)| \leq \|A - B\|$.

Proof. (1) follows immediately from the variational formula. For (2), choose matrices X, Y of ranks $< k$ and $< m$ such that $\|A - X\|$ and $\|B - Y\|$ are close to $s_k(A)$ and $s_m(B)$. Then $\operatorname{rank}(X+Y) < k+m-1$ and

$$\|A + B - (X+Y)\| \leq \|A - X\| + \|B - Y\|.$$

Take infima. For (3), write

$$AB - XY = (A-X)B + X(B-Y)$$

with suitable rank choices and use the variational characterization; equivalently combine (1) and (2). Finally, (4) follows from (2) applied to $A = B + (A-B)$ and then interchanging A, B. □

6.6 Aluthge transform

Definition 6.6.1 ► Aluthge transform

If $A = U|A|$ is a polar decomposition, define

$$\Delta(A) = |A|^{1/2} U |A|^{1/2}.$$

Proposition 6.6.1. The Aluthge transform is independent of the choice of partial isometry U in the polar decomposition. Moreover:

i. If A is normal, then $\Delta(A) = A$.

ii. $\sigma(\Delta(A)) = \sigma(A)$.

Proof. Only the action of U on $\overline{\operatorname{ran}|A|}$ enters $|A|^{1/2}U|A|^{1/2}$, and this action is uniquely determined by A. If A is normal, then in the polar decomposition U commutes with $|A|$, so $\Delta(A) = U|A| = A$.
For the spectrum, write

$$A = (U|A|^{1/2})|A|^{1/2}, \qquad \Delta(A) = |A|^{1/2}(U|A|^{1/2}).$$

The matrices XY and YX have the same non-zero eigenvalues with the same algebraic multiplicities. The multiplicity of 0 is also the same because $\operatorname{rank} A = \operatorname{rank} \Delta(A)$. Hence the spectra agree. □

6.7 QR and Cholesky factorisations

Theorem 6.7.1 (QR decomposition) Let $X \in M_{m,n}(\mathbb{C})$ with $m \geq n$ and linearly independent columns. Then

$$X = QR,$$

where $Q \in M_{m,n}(\mathbb{C})$ has orthonormal columns and $R \in M_n(\mathbb{C})$ is upper triangular with positive diagonal entries. This decomposition is unique.

Proof. Apply Gram-Schmidt to the columns $x_1, \ldots, x_n$ of X, obtaining orthonormal columns $q_1, \ldots, q_n$. Each x_j lies in $\operatorname{span}(q_1, \ldots, q_j)$, so $X = QR$ with R upper triangular. Choosing positive diagonal entries fixes the phases and gives uniqueness. □

Theorem 6.7.2 (Cholesky factorisation) If $A \in M_n(\mathbb{C})$ is positive definite, then there is a unique upper triangular matrix T with positive diagonal entries such that

$$A = T^*T.$$

Proof. Let $B = A^{1/2}$, which is invertible. Apply the QR decomposition to B: $B = QT$ with Q unitary and T upper triangular with positive diagonal entries. Then

$$A = B^*B = T^*Q^*QT = T^*T.$$

Uniqueness follows from the uniqueness in QR. Indeed, if $T_1^*T_1 = T_2^*T_2$, then $T_2T_1^{-1}$ is unitary and upper triangular with positive diagonal; hence it is I. □

6.8 Further singular value properties

The notes use the following elementary identities repeatedly. For every matrix A,

$$s_k(A) = s_k(|A|) = s_k(A^*) = s_k(|A^*|),$$

where $|A| = (A^*A)^{1/2}$. The first equality is the definition, and the equality with A^* follows from the singular value decomposition: if

$$A = \sum_{j=1}^{r} s_j |u_j\rangle\langle v_j|,$$

then

$$A^* = \sum_{j=1}^{r} s_j |v_j\rangle\langle u_j|.$$

Theorem 6.8.1 (Eckart-Young variational formula) For $1 \le k \le \min(m,n)$,

$$s_k(A) = \inf\{\|A - X\| : \operatorname{rank} X < k\}.$$

Equivalently,

$$s_k(A) = \inf\{\|A(I - P)\| : P \text{ is a projection and } \operatorname{rank} P = k - 1\}.$$

Proof. Let

$$A = \sum_{j=1}^{r} s_j |u_j\rangle\langle v_j|, \qquad s_1 \ge s_2 \ge \cdots > 0,$$

be an SVD. Taking

$$X_{k-1} = \sum_{j=1}^{k-1} s_j |u_j\rangle\langle v_j|$$

gives $\operatorname{rank} X_{k-1} < k$ and $\|A - X_{k-1}\| = s_k(A)$, so the infimum is at most $s_k(A)$.
Conversely, if $\operatorname{rank} X < k$, then $\ker X$ has dimension at least $n-k+1$. Intersecting $\ker X$ with $\operatorname{span}\{v_1, \dots, v_k\}$ gives a non-zero vector $v = \sum_{j=1}^{k} c_j v_j$. Normalize v to have norm one. Then

$$\|(A - X)v\| = \|Av\| = \left(\sum_{j=1}^{k} s_j^2 |c_j|^2 \right)^{1/2} \ge s_k(A).$$

Thus $\|A - X\| \ge s_k(A)$ for every rank $< k$ matrix X.
The projection version follows by taking $X = AP$ and by choosing P to be the projection onto $\operatorname{span}\{v_1, \dots, v_{k-1}\}$.
□

Proposition 6.8.1 (Singular value inequalities)**.** For compatible matrices and $k, m \ge 1$:

i. $s_k(XAY) \le \|X\| \, \|Y\| s_k(A)$.

ii. If $k + m - 1 \le n$, then
$$s_{k+m-1}(A + B) \le s_k(A) + s_m(B).$$

iii. If $k + m - 1 \le n$, then
$$s_{k+m-1}(AB) \le s_k(A) s_m(B).$$

iv. For each k,
$$|s_k(A) - s_k(B)| \le \|A - B\|.$$

Proof. For (1), use the Eckart-Young formula. If $\operatorname{rank} R < k$, then $\operatorname{rank}(XRY) < k$ and

$$\|XAY - XRY\| \le \|X\| \, \|A - R\| \, \|Y\|.$$

Take the infimum over R.
For (2), choose R, S with $\operatorname{rank} R < k$, $\operatorname{rank} S < m$ and

$$\|A - R\| \le s_k(A) + \varepsilon, \qquad \|B - S\| \le s_m(B) + \varepsilon.$$

Then $\operatorname{rank}(R + S) < k + m - 1$, so

$$s_{k+m-1}(A + B) \le \|A + B - (R + S)\| \le s_k(A) + s_m(B) + 2\varepsilon.$$

Let $\varepsilon \downarrow 0$.
For (3), choose a subspace E of codimension at most $m-1$ on which $\|B|_E\| \le s_m(B)$, and a subspace F of codimension at most $k-1$ on which $\|A|_F\| \le s_k(A)$. Then $E \cap B^{-1}F$ has codimension at most $k+m-2$. On this subspace,

$$\|ABx\| \le s_k(A)s_m(B)\|x\|.$$

The min-max characterization gives the desired estimate. Finally, (4) follows from (2) with $m=1$:

$$s_k(A) = s_k(B+(A-B)) \le s_k(B) + \|A-B\|,$$

and then interchange A and B. □

6.9 A worked QR/Cholesky example

Consider

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Applying Gram-Schmidt to the columns gives

$$q_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \qquad q_2 = \frac{1}{\sqrt{6}}\begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}, \qquad q_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}.$$

Thus $X = QR$, where

$$Q = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix}, \qquad R = \begin{pmatrix} \sqrt{2} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{\sqrt{6}}{2} & \frac{2}{\sqrt{6}} \\ 0 & 0 & \frac{1}{\sqrt{3}} \end{pmatrix}.$$

Consequently

$$X^*X = R^*R$$

is the Cholesky factorization of X^*X.

6.10 Exercises

i. Prove that $s_k(A) = s_k(A^*) = s_k(|A|)$.

ii. Prove the Eckart-Young formula $s_k(A) = \inf_{\operatorname{rank} R<k} \|A-R\|$.

iii. Give an example where $A = V|A|$ has non-unique partial isometry if the initial space condition is not imposed.

iv. Compute the QR and Cholesky decompositions of

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

v. Show that if A is positive definite and tridiagonal, then its Cholesky factor is bidiagonal.

Chapter 7

Perron-Frobenius Theory and the Sensitivity Conjecture

This chapter records the Perron-Frobenius material from the notes and the final application to Huang's proof of the sensitivity conjecture.

7.1 Walks in a connected graph

Let G be a finite simple graph with vertex set $\{1,\dots,n\}$ and adjacency matrix $A=[a_{ij}]$. Thus $a_{ij}=1$ if $i\sim j$ and $a_{ij}=0$ otherwise. The graph is connected iff for every i,j there is a path from i to j.

Proposition 7.1.1. If G is connected, then

$$(I+A)^{n-1}>0$$

entrywise.

Proof. Expand

$$(I+A)^{n-1}=\sum_{k=0}^{n-1}\binom{n-1}{k}A^k.$$

The entry $(A^k)_{ij}$ is the number of walks of length k from i to j. Since G is connected, there is a path from i to j of length at most $n-1$. Hence at least one summand in the (i,j) entry is positive. □

Proposition 7.1.2. Let A be the adjacency matrix of a connected graph. If $x\geq 0$, $x\neq 0$, and $Ax=\lambda x$, then $x>0$ entrywise and $\lambda>0$.

Proof. Since $(I+A)^{n-1}>0$ and $x\geq 0$, $x\neq 0$, we have $(I+A)^{n-1}x>0$. But

$$(I+A)^{n-1}x=(1+\lambda)^{n-1}x,$$

so $x>0$. Since $Ax\geq 0$ and $x>0$, the equation $Ax=\lambda x$ gives $\lambda\geq 0$. A connected graph with at least two vertices has no isolated vertex, so Ax has positive entries; hence $\lambda>0$. □

7.2 Perron-Frobenius theorem for connected graphs

Let

$$\Delta^{n-1}=\{x\in\mathbb{R}^n : x_i\geq 0,\ \sum_i x_i=1\}$$

be the probability simplex.

Theorem 7.2.1 (Perron-Frobenius theorem for connected graphs) Let A be the adjacency matrix of a connected graph G. Then there is a number $\lambda > 0$ and a vector $x > 0$ such that

$$Ax = \lambda x.$$

Moreover:

i. if μ is any eigenvalue of A, then $|\mu| \leq \lambda$;

ii. if y is an eigenvector with eigenvalue λ, then $y = \alpha x$ for some $\alpha \in \mathbb{C}$.

Thus $\lambda = \rho(A)$ and the Perron eigenvector is unique up to scalar multiples.

Proof. Existence can be obtained from the Rayleigh quotient. Since $A = A^*$, let λ be the largest eigenvalue and let u be a unit eigenvector for λ. Replacing u by $|u|$ does not decrease the Rayleigh quotient, because $a_{ij} \geq 0$:

$$\langle |u|, A|u| \rangle = \sum_{i,j} a_{ij} |u_i||u_j| \geq \left| \sum_{i,j} a_{ij} \overline{u_i} u_j \right|.$$

Hence a maximizing eigenvector may be chosen non-negative. By the previous proposition it is strictly positive and its eigenvalue is positive. Denote this vector by $x > 0$ and its eigenvalue by $\lambda > 0$.
Let $Az = \mu z$. Define

$$\alpha = \max_i \frac{|z_i|}{x_i}.$$

Choose i_0 attaining the maximum. Then

$$|\mu|\,|z_{i_0}| = |(Az)_{i_0}| \leq \sum_j a_{i_0 j} |z_j| \leq \alpha \sum_j a_{i_0 j} x_j = \alpha \lambda x_{i_0} = \lambda |z_{i_0}|.$$

If $z \neq 0$, this gives $|\mu| \leq \lambda$.
Now suppose $Ay = \lambda y$. Let

$$\alpha = \max_i \frac{|y_i|}{x_i}.$$

The same chain of inequalities must be an equality at a maximizing index. Equality in the triangle inequality forces all non-zero neighboring terms to have the same complex phase. By connectedness, this phase propagates through the whole graph. Hence $y = \beta x$ for some $\beta \in \mathbb{C}$. □

Remark 7.2.1. The same proof, with directed paths in place of paths, gives the usual irreducible non-negative matrix version: if $A \geq 0$ is irreducible, then $\rho(A) > 0$ is an eigenvalue with a strictly positive eigenvector, unique among non-negative eigenvectors up to scalar multiples.

7.3 Cauchy's interlacing theorem

For a self-adjoint matrix A, write

$$\lambda_1^{\downarrow}(A) \geq \lambda_2^{\downarrow}(A) \geq \cdots$$

for its eigenvalues in decreasing order.

Theorem 7.3.1 (Cauchy's interlacing theorem) Let $A = A^*$ act on an n-dimensional Hilbert space $\mathcal{H}$, and let B be the compression of A to a subspace $\mathcal{N}$ of dimension $n-k$. Then

$$\lambda_j^{\downarrow}(A) \geq \lambda_j^{\downarrow}(B) \geq \lambda_{j+k}^{\downarrow}(A), \qquad 1 \leq j \leq n-k.$$

Proof. Use the Courant-Fischer min-max formula

$$\lambda_j^{\downarrow}(A) = \max_{\dim L = j} \min_{0 \neq x \in L} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \min_{\dim M = n-j+1} \max_{0 \neq x \in M} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}.$$

For the upper bound, the maximization defining $\lambda_j^{\downarrow}(B)$ is over j-dimensional subspaces contained in $\mathscr{N}$, a smaller class than all j-dimensional subspaces of $\mathscr{H}$. Hence

$$\lambda_j^{\downarrow}(B) \leq \lambda_j^{\downarrow}(A).$$

For the lower bound, note that $\dim \mathscr{N} = n - k$. Hence

$$\lambda_j^{\downarrow}(B) = \min_{\substack{M \subset \mathscr{N} \\ \dim M = (n-k)-j+1}} \max_{0 \neq x \in M} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}.$$

The minimization is over fewer subspaces than the minimization defining

$$\lambda_{j+k}^{\downarrow}(A) = \min_{\substack{M \subset \mathscr{H} \\ \dim M = n-(j+k)+1}} \max_{0 \neq x \in M} \frac{\langle x, Ax \rangle}{\langle x, x \rangle},$$

and the two displayed dimensions are equal. Therefore

$$\lambda_j^{\downarrow}(B) \geq \lambda_{j+k}^{\downarrow}(A).$$

□

7.4 Sensitivity of Boolean functions

Fix $n \in \mathbb{N}$ and let

$$Q_n = \{0,1\}^n$$

be the Boolean hypercube graph: two vertices are adjacent if they differ in exactly one coordinate. For a Boolean function $f : Q_n \to \{0,1\}$ and $x \in Q_n$, define the local sensitivity

$$S(f,x) = \#\{i : f(x^{(i)}) \neq f(x)\},$$

where $x^{(i)}$ is obtained from x by flipping the ith coordinate. The sensitivity of f is

$$s(f) = \max_{x \in Q_n} S(f,x).$$

The sensitivity conjecture asserts that sensitivity is polynomially related to other standard complexity measures of Boolean functions. The graph-theoretic result below is the key theorem in Huang's proof.

> **Theorem** 7.4.1 (Huang's induced subgraph theorem) Let H be an induced subgraph of Q_n with
>
> $$|V(H)| = 2^{n-1} + 1.$$
>
> Then
>
> $$\Delta(H) \geq \sqrt{n},$$
>
> where $\Delta(H)$ is the maximum degree of H.

Proof. We construct a signed adjacency matrix $\widetilde{A}_n$ for Q_n. Define

$$\widetilde{A}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and recursively

$$\widetilde{A}_n = \begin{pmatrix} \widetilde{A}_{n-1} & I \\ I & -\widetilde{A}_{n-1} \end{pmatrix}.$$

This matrix has the same zero pattern as the adjacency matrix of Q_n, except that the non-zero entries are signs ± 1. It is self-adjoint. By induction,

$$\widetilde{A}_n^2 = \begin{pmatrix} \widetilde{A}_{n-1}^2 + I & 0 \\ 0 & \widetilde{A}_{n-1}^2 + I \end{pmatrix} = nI.$$

Also $\mathrm{Tr}\big(\widetilde{A}_n\big) = 0$. Therefore the eigenvalues of $\widetilde{A}_n$ are

$$\sqrt{n}, \ldots, \sqrt{n}, -\sqrt{n}, \ldots, -\sqrt{n},$$

with each sign occurring 2^{n-1} times.
Let $\widetilde{A}_H$ be the principal submatrix corresponding to $V(H)$. Since $|V(H)| = 2^{n-1}+1$, Cauchy's interlacing gives

$$\lambda_1^{\downarrow}(\widetilde{A}_H) \geq \lambda_{2^{n-1}}^{\downarrow}(\widetilde{A}_n) = \sqrt{n}.$$

Thus $\|\widetilde{A}_H\| \geq \sqrt{n}$.
On the other hand, each row of $\widetilde{A}_H$ has at most $\Delta(H)$ non-zero entries, each of modulus 1. Hence

$$\|\widetilde{A}_H\|_2 \leq \sqrt{\|\widetilde{A}_H\|_1 \|\widetilde{A}_H\|_\infty} \leq \Delta(H).$$

Combining the two inequalities gives $\Delta(H) \geq \sqrt{n}$. □

Remark 7.4.1. Taking a Boolean function and looking at the larger of the two induced subgraphs $f^{-1}(0)$ and $f^{-1}(1)$ connects this theorem to sensitivity. The degree of a vertex in the induced subgraph measures the number of same-colored neighbors, while the number of edges leaving the subgraph measures local sensitivity. Huang's theorem supplies the lower bound that resolves the sensitivity conjecture after the standard reductions.

7.5 Exercises

i. Show directly that if G is disconnected, then its adjacency matrix can be permuted into block diagonal form.

ii. For the path graph on n vertices, find the Perron eigenvector explicitly.

iii. Prove the codimension-one case of Cauchy's interlacing theorem from the Rayleigh-Ritz formula.

iv. Verify explicitly that $\widetilde{A}_3^2 = 3I$ for Huang's signed adjacency matrix.

v. Show that the operator norm of any signed adjacency matrix of a graph H is at most $\Delta(H)$.

References

Bibliography

[1] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics 169, Springer, 1997.

[2] R. Bhatia, *Positive Definite Matrices*, Princeton University Press, 2007.

[3] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, 2012.

[4] A. W. Marshall, I. Olkin and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications*, 2nd ed., Springer, 2011.

[5] V. I. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge University Press, 2002.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed., Cambridge University Press, 2010.

[7] R. Pereira, *Differentiators and the geometry of polynomials*, J. Math. Anal. Appl. 285 (2003), 336–348.

[8] H. Huang, *Induced subgraphs of hypercubes and a proof of the Sensitivity Conjecture*, Ann. of Math. (2) 190 (2019), no. 3, 949–955.

Index