Introduction to linear algebra

Teo Banica

Real matrices, The determinant, Complex matrices, Calculus and applications, Infinite matrices, Special matrices

08/20

Foreword

These are slides written in the Fall 2020, on linear algebra. Presentations available at my Youtube channel.

Real matrices and their properties

Teo Banica

"Introduction to linear algebra", 1/6

08/20

Rotations 1/3

Problem: what's the formula of the rotation of angle t?

Rotations 2/3

The points in the plane $\mathbb{R}^2$ can be represented as vectors $\binom{x}{y}$. The 2×2 matrices "act" on such vectors, as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

Many simple transformations (symmetries, projections..) can be written in this form. What about the rotation of angle t?

Rotations 3/3

A quick picture shows that we must have:

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$$

Also, by paying attention to positives and negatives:

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin t \\ \cos t \end{pmatrix}$$

Thus, the matrix of our rotation can only be:

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

By "linear algebra'', this is the correct answer.

Linear maps 1/4

Theorem. The maps $f : \mathbb{R}^2 \to \mathbb{R}^2$ which are linear, in the sense that they map lines through 0 to lines through 0, are:

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

Remark. If we make the multiplication convention

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

the theorem says $f(v) = Av$, with A being a 2×2 matrix.

Linear maps 2/4

Examples. The identity and null maps are given by:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}\quad,\quad\begin{pmatrix}0&0\\0&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

The projections on the horizontal and vertical axes are given by:

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x\\0\end{pmatrix}\quad,\quad\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\y\end{pmatrix}$$

The symmetry with respect to the $x=y$ diagonal is given by:

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}y\\x\end{pmatrix}$$

We have as well the rotation of angle $t\in\mathbb{R}$, studied before.

Linear maps 3/4

Theorem. The maps $f : \mathbb{R}^N \to \mathbb{R}^N$ which are linear, in the sense that they map lines through 0 to lines through 0, are:

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1N}x_N \\ \vdots \\ a_{N1}x_1 + \ldots + a_{NN}x_N \end{pmatrix}$$

Remark. With the matrix multiplication convention

$$\begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \ldots & a_{NN} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1N}x_N \\ \vdots \\ a_{N1}x_1 + \ldots + a_{NN}x_N \end{pmatrix}$$

the theorem says $f(v) = Av$, with A being a $N \times N$ matrix.

Linear maps 4/4

Example. Consider the all-1 matrix. This acts as follows:

$$\begin{pmatrix}1&\ldots&1\\ \vdots&\ddots&\vdots\\ 1&\ldots&1\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_N\end{pmatrix}=\begin{pmatrix}x_1+\ldots+x_N\\ \vdots\\ x_1+\ldots+x_N\end{pmatrix}$$

But this formula can be written as follows:

$$\frac{1}{N}\begin{pmatrix}1&\ldots&1\\ \vdots&\ddots&\vdots\\ 1&\ldots&1\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_N\end{pmatrix}=\frac{x_1+\ldots+x_N}{N}\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$$

And this latter map is the projection on the all-1 vector.

Theory 1/4

<u>Definition</u>. We can multiply $M \times N$ matrices with $N \times K$ matrices,

$$\begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & & \vdots \\ a_{M1} & \ldots & a_{MN} \end{pmatrix} \begin{pmatrix} b_{11} & \ldots & b_{1K} \\ \vdots & & \vdots \\ b_{N1} & \ldots & b_{NK} \end{pmatrix}$$

the product being a $M \times K$ matrix, given by the formula

$$\begin{pmatrix} a_{11}b_{11} + \ldots + a_{1N}b_{N1} & \ldots\ldots & a_{11}b_{1K} + \ldots + a_{1N}b_{NK} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ a_{M1}b_{11} + \ldots + a_{MN}b_{N1} & \ldots\ldots & a_{M1}b_{1K} + \ldots + a_{MN}b_{NK} \end{pmatrix}$$

obtained via the rule "multiply rows by columns".

Theory 2/4

Better definition. The matrix multiplication is given by

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}$$

with A_{ij} being the entry on the i-th row and j-th column.

Theorem. The linear maps $f : \mathbb{R}^N \to \mathbb{R}^M$ are those of the form

$$f_A(v) = Av$$

with A being a $N \times M$ matrix.

Remark. Size check $(N \times 1) = (N \times M)(M \times 1)$, ok.

Theory 3/4

Theorem. With the above convention $f_A(v) = Av$, we have

$$f_A f_B = f_{AB}$$

"the product of matrices corresponds to the composition of maps".

Theorem. A linear map $f : \mathbb{R}^N \to \mathbb{R}^N$ is invertible when the matrix $A \in M_N(\mathbb{R})$ which produces it is invertible, and we have:

$$(f_A)^{-1} = f_{A^{-1}}$$

Theory 4/4

Theorem. The inverses of the 2×2 matrices are given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Proof. When $ad = bc$ the columns are proportional, so the matrix cannot be invertible. When $ad - bc \neq 0$, let us solve:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} * & * \\ * & * \end{pmatrix}$$

We must solve the following equations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} * & * \\ * & * \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix}$$

But this leads to the formula in the statement.

Eigenvectors 1/4

Definition. Let $A \in M_N(\mathbb{R})$ be a square matrix, and assume that A multiplies by $\lambda \in \mathbb{R}$ in the direction of a vector $v \in \mathbb{R}^N$:

$$Av = \lambda v$$

In this case, we say that:

(1) $v \in \mathbb{R}^N$ is an eigenvector of A.

(2) $\lambda \in \mathbb{R}$ is the corresponding eigenvalue.

Eigenvectors 2/4

Examples. The identity has all vectors as eigenvectors, with $\lambda = 1$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

The same goes for the null matrix, with $\lambda = 0$ this time:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

For the projection on the horizontal axis, $P\binom{x}{y} = \binom{x}{0}$, we have:

$$Pv = \lambda v \quad \iff \quad v = \begin{pmatrix} 0 \\ y \end{pmatrix}, \lambda = 0 \quad \text{or} \quad v = \begin{pmatrix} x \\ 0 \end{pmatrix}, \lambda = 1$$

A similar result holds for the projection on the vertical axis.

Eigenvectors 3/4

More examples. For the symmetry $S\binom{x}{y} = \binom{y}{x}$, we have:

$$Sv = \lambda v \iff v = \begin{pmatrix} x \\ x \end{pmatrix}, \lambda = 1 \text{ or } v = \begin{pmatrix} x \\ -x \end{pmatrix}, \lambda = -1$$

For the transformation $T\binom{x}{y} = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\binom{x}{y} = \binom{y}{0}$ we have:

$$Tv = \lambda v \quad \iff \quad v = \begin{pmatrix} x \\ 0 \end{pmatrix}, \lambda = 0$$

For the rotation of angle $t \neq 0$, we must have $v = 0, \lambda = 0$.

Eigenvectors 4/4

Definition. We say that a matrix $A \in M_N(\mathbb{R})$ is diagonalizable if it has N eigenvectors $v_1, \ldots, v_N$ which form a basis of $\mathbb{R}^N$.

Remark. When A is diagonalizable, in that basis we can write:

$$A = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$$

This means that we have $A = PDP^{-1}$, with D diagonal.

Problems. Which matrices are diagonalizable? And, how to diagonalize them?

The determinant of real matrices

Teo Banica

"Introduction to linear algebra", 2/6

08/20

Definition 1/3

Definition. Associated to any vectors $v_1, \ldots, v_N \in \mathbb{R}^N$ is the volume

$$\det^+(v_1 \ldots v_N) = vol < v_1, \ldots, v_N >$$

of the parallelepiped made by these vectors.

Remark. This notion is useful, for instance because $v_1, \ldots, v_N$ are linearly dependent precisely when $\det^+(v_1 \ldots v_N) = 0$.

Definition 2/3

Theorem. In 2 dimensions we have the formula

$$\det^+ \begin{pmatrix} a & b \\ c & d \end{pmatrix} = |ad - bc|$$

valid for any two vectors $\binom{a}{c}, \binom{b}{d} \in \mathbb{R}^2$.

Proof. We must show that the area of the parrallelogram formed by the vectors $\binom{a}{c}, \binom{b}{d}$ equals the quantity $|ad - bc|$.

But this latter quantity is a difference of areas of two rectangles, and this can be done in "puzzle" style.

Comment. This is nice, but with $ad - bc$ as "answer", which is linear in a, b, c, d, it would be even nicer.

Definition 3/3

Convention. A system of vectors $v_1, \ldots, v_N \in \mathbb{R}^N$ is called:

(1) Oriented (+), if one can pass from the standard basis to it.

(2) Unoriented (-), otherwise.

Definition. Associated to $v_1, \ldots, v_N \in \mathbb{R}^N$ is the signed volume

$$\det(v_1 \ldots v_N) = vol^{\pm} < v_1, \ldots, v_N >$$

of the parallelepiped made by these vectors.

Remark. We have $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$, which is nice.

Properties 1/4

Notation. Given a matrix $A \in M_N(\mathbb{R})$, we write $\det A$, or just $|A|$, for the determinant of the system of column vectors of A.

Notation. Given a linear map, written as $f(v) = Av$, we call the number $\det A$ the "inflation coefficient" of f.

Remark. The inflation coefficient of f is the signed volume of the image $f(\square_N)$ of the unit cube $\square_N \in \mathbb{R}^N$.

Properties 2/4

Theorem. The determinant $\det A$ of the matrices $A \in M_N(\mathbb{R})$ has the following properties:

(1) It is a linear function of the columns of A.

(2) We have $\det(AB) = \det A \cdot \det B$.

(3) We have $\det(AB) = \det(BA)$.

Proof. (1) By doing some geometry, we obtain indeed:

$$\det(u+v,\{w_i\}) = \det(u,\{w_i\}) + \det(v,\{w_i\})$$

$$\det(\lambda u,\{w_i\}) = \lambda \det(u,\{w_i\})$$

(2) This follows from $f_{AB} = f_A f_B$, by looking at "inflation".

(3) Follows from (2), both quantities being $\det A \cdot \det B$.

Properties 3/4

Theorem. Assuming that a matrix $A \in M_N(\mathbb{R})$ is diagonalizable, with eigenvalues $\lambda_1, \ldots, \lambda_N$, we have:

$$\det A = \lambda_1 \ldots \lambda_N$$

Proof. This is clear from the "inflation" viewpoint, because in the basis formed by the eigenvectors $v_1, \ldots, v_N$, we have:

$$f_A(v_i) = \lambda_i v_i$$

Alternatively, $A = PDP^{-1}$ with $D = diag(\lambda_1, \ldots, \lambda_N)$, so

$$\det(A) = \det(PDP^{-1}) = \det(DP^{-1} \cdot P) = \det(D)$$

and by linearity $\det(D) = \lambda_1 \ldots \lambda_N \cdot \det(1_N) = \lambda_1 \ldots \lambda_N$.

Properties 4/4

Theorem. We have the following formula, for any $\lambda \in \mathbb{R}$:

$$\det(u, v, \{w_i\}_i) = \det(u - \lambda v, v, \{w_i\}_i)$$

Theorem. For an upper triangular matrix we have

$$\begin{vmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_N \end{vmatrix} = \lambda_1 \ldots \lambda_N$$

and a similar result holds for the lower triangular matrices.

Proofs. The first theorem follows from linearity, because we have $\det(v, v, \{w_i\}_i) = 0$, and the second theorem follows from it.

Examples 1/4

Theorem. In 2 dimensions, the determinant is given by:

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

Proof. This is something that we already know, but that we can recover by using the general theory developed above:

$$\begin{aligned} \begin{vmatrix} a & b \\ c & d \end{vmatrix} &= \begin{vmatrix} a - b \cdot c/d & b \\ c - d \cdot c/d & d \end{vmatrix} \\ &= \begin{vmatrix} a - bc/d & b \\ 0 & d \end{vmatrix} \\ &= (a - bc/d)d \end{aligned}$$

Thus, we obtain the formula in the statement.

Examples 2/4

Theorem. In 3 dimensions, the determinant is given by

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - ceg - bdi - afh$$

and this can be memorized by using Sarrus' triangle method.

Proof. This follows a bit as in 2 dimensions, by using the "Gauss method". We will be back later with a more conceptual proof.

Examples 3/4

Theorem. The determinant of a projection is always 0, unless the projection is the identity, and the determinant is 1.

Proof. This is clear with the "inflation" viewpoint. Alternatively, P is diagonalizable, with 1 eigenvalues on the image, and 0 outside:

$$P \sim \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 0 \end{pmatrix}$$

By making the product we obtain $\det P = 1 \ldots 1 \cdot 0 \ldots 0$, with at least one 0 in the case $P \neq 1_N$, as claimed.

Examples 4/4

Example. For the symmetry with respect to $x = y$, we have:

$$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = 0 \cdot 0 - 1 \cdot 1 = -1$$

Example. For the rotation of angle $t \in \mathbb{R}$, we have:

$$\begin{vmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{vmatrix} = \cos^2 t + \sin^2 t = 1$$

These formulae follow as well without computations, by "inflation".

Remark. The "basic" matrices tend to have determinant $-1, 0, 1$.

Theory 1/4

Theorem. The determinant can be fully computed by using the Gauss method, namely:

(1) Multiplying row by scalars.

(2) Substracting rows.

Theorem. The determinant function

$$\det : \mathbb{R}^N \times \ldots \times \mathbb{R}^N \to \mathbb{R}$$

is multilinear, alternate and unital, and unique with these properties.

Proofs. The first theorem is something that we already know, and the second theorem follows from it, by uniqueness.

Theory 2/4

Definition. A permutation of $\{1, \ldots, N\}$ is a bijection, as follows:

$$\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$$

The set of such permutations is denoted S_N.

Theorem. There are $N! = 1.2.3 \ldots N$ such permutations.

Proof. We have N choices for $\sigma(1)$, then $N - 1$ choices for $\sigma(2)$, and so on, up to 1 choice for $\sigma(N)$.

Definition. The signature of a permutation $\varepsilon(\sigma) \in \{\pm 1\}$ is the number of inversions, $i < j$ with $\sigma(i) > \sigma(j)$.

Theory 3/4

Theorem. The determinant is given by the formula

$$\det A = \sum_{\sigma \in S_N} \varepsilon(\sigma) A_{1\sigma(1)} \ldots A_{N\sigma(N)}$$

with the signature function being the one introduced above.

Proof. This follows either by using the Gauss method, or by using the abstract characterization of the determinant.

Remark. At $N = 3$ we obtain in this way the Sarrus formula.

Theory 4/4

Theorem. The eigenvalues of a matrix $A \in M_N(\mathbb{R})$ must satisfy

$$P_A(\lambda) = 0$$

where $P_A = \det(A - \lambda 1_N)$ is the characteristic polynomial.

Proof. Given a vector $v \in \mathbb{R}^N$ and a number $\lambda \in \mathbb{R}$, we have:

$$Av = \lambda v \iff (A - \lambda 1_N)v = 0$$

But this latter equation has nonzero solutions when

$$B = \det(A - \lambda 1_N)$$

is not invertible, and so when $\det B = 0$.

Complex matrices and diagonalization

Teo Banica

"Introduction to linear algebra", 3/6

08/20

Complex numbers 1/3

The complex numbers are $z = a + ib$, with $i^2 = -1$.

They can be represented in the plane, with z being $\binom{a}{b}$.
We have $z = re^{it}$, with $r = \sqrt{a^2 + b^2}$, and $\tan t = b/a$.

The equation $x^2 = -1$ has two solutions, $x = \pm i$.
In fact, the equation $P(x) = 0$ has $N = \deg P$ solutions.

Also, complex numbers are important in quantum physics.

Complex numbers 2/3

Consider the rotation of angle $t \in \mathbb{R}$:

$$R_t = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$$

This rotation has 2 complex eigenvectors (!), because:

$$R_t \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} \cos t - i \sin t \\ \sin t + i \cos t \end{pmatrix} = e^{-it} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$R_t \begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} \cos t + i \sin t \\ \sin t - i \cos t \end{pmatrix} = e^{it} \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

Thus, good news, R_t is diagonalizable over $\mathbb{C}$.

Complex numbers 3/3

More magics. When identifying $\mathbb{R}^2$ with the complex plane $\mathbb{C}$, the rotation of angle $t \in \mathbb{R}$ becomes a 1×1 matrix (!):

$$R_t = (e^{it})$$

Thus, with complex numbers, this rotation R_t of angle $t \in \mathbb{R}$ in the plane is something completely trivial. Very nice.

Theory 1/4

The theory from the real case extends to this setting:

Theorem. Any linear map $f:\mathbb{C}^N\to\mathbb{C}^N$ is of the form $f(v)=Av$, with $A\in M_N(\mathbb{C})$.

Theorem. More generally, any linear map $f:\mathbb{C}^N\to\mathbb{C}^M$ is of the form $f(v)=Av$, with $A\in M_{M\times N}(\mathbb{C})$.

Theorem. With $f_A(v)=Av$, we have $f_{AB}=f_Af_B$. In particular f_A is invertible when A is invertible, and $f_A^{-1}=f_{A^{-1}}$.

Theory 2/4

The theory of the determinant extends as well:

Definition. The determinant of a matrix $A \in M_N(\mathbb{C})$ is

$$\det A = \sum_{\sigma \in S_N} \varepsilon(\sigma) A_{1\sigma(1)} \ldots A_{N\sigma(N)}$$

where $\varepsilon(\sigma) = (-1)^c$, c being the number of inversions.

Theorem. The determinant is subject to the following rules:

(1) $\det(\lambda u, \{w_i\}) = \lambda \det(u, \{w_i\})$.

(2) $\det(u, v, \{w_i\}) = \det(u - v, v, \{w_i\})$.

Also, we have $\det(AB) = \det A \cdot \det B$, $\det(A^t) = \det A$.

Theory 3/4

The theory of the eigenvalues extends as well:

Definition. Given $A \in M_N(\mathbb{C})$, if $v \in \mathbb{C}^N$ and $\lambda \in \mathbb{C}$ satisfy

$$Av = \lambda v$$

we say that v is an eigenvector of A, with eigenvalue λ.

Theorem. The eigenvalues are the roots of the polynomial

$$P(\lambda) = \det(A - \lambda 1_N)$$

called characteristic polynomial of the matrix.

Theory 4/4

Theorem. Consider a 2×2 real or complex matrix:

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

(1) The characteristic polynomial is $P(\lambda) = \lambda^2 - S\lambda + P$, with:

$$S = a + d \quad , \quad P = ad - bc$$

(2) We have two complex eigenvalues, given by:

$$\lambda_1 + \lambda_2 = S \quad , \quad \lambda_1 \lambda_2 = P$$

(3) Equivalently, we have the following formula:

$$\lambda_{1,2} = \frac{S \pm \sqrt{S^2 - 4P}}{2}$$

Diagonalization 1/4

Theorem. Given $A \in M_N(\mathbb{C})$, consider its characteristic polynomial $P(x) = \det(A - x1_N)$, and decompose it into factors:

$$P(x) = (-1)^N (x - \lambda_1) \ldots (x - \lambda_N)$$

For $\lambda \in \{\lambda_1, \ldots, \lambda_N\}$ consider the corresponding eigenspace:

$$E_\lambda = \left\{ v \in \mathbb{C}^N \Big| Av = \lambda v \right\}$$

We have then dimension inequalities as follows, for any λ,

$$1 \leq \dim(E_\lambda) \leq \#(\lambda \in \{\lambda_1, \ldots, \lambda_N\})$$

and A is diagonalizable precisely when we have equalities at right.

Diagonalization 2/4

In practice, the above result can be used as follows:

(1) Compute the characteristic polynomial $P(x) = \det(A - x1_N)$, and factorize it as $P(x) = (-1)^N (x - \lambda_1) \ldots (x - \lambda_N)$.

(2) Remark: if λ_i are distinct, A is certainly diagonalizable. Also, if $\lambda_i \notin \mathbb{R}$ for some i, A is not diagonalizable over $\mathbb{R}$.

(3) Solve $Av = \lambda_i v$ for any i. If a space of solutions E_{λ_i} satisfies $\dim(E_{\lambda_i}) < \#(\lambda \in \{\lambda_1, \ldots, \lambda_N\})$, A is not diagonalizable.

(4) Otherwise, find a basis of each of these spaces E_{λ_i}, and put all eigenvectors found into a matrix P (the "passage matrix").

(5) Put as well all eigenvalues found on the diagonal of a matrix D. Compute P^{-1}. We have then $A = PDP^{-1}$.

Diagonalization 3/4

Some tricks and tips:

(1) In 2 dimensions, where $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the eigenvalues are best computed by using $x + y = a + d$, $xy = ad - bc$.

(2) In fact, in N dimensions, it is known that the eigenvalues satisfy $\lambda_1 + \ldots + \lambda_N = Tr(A)$ and $\lambda_1 \ldots \lambda_N = \det A$.

(3) If P has integer coefficients, $P \in \mathbb{Z}[X]$, look first for integer roots, $\lambda \in \mathbb{Z}$. These must divide the coefficient of X^0.

Diagonalization 4/4

More tricks and tips:

(1) When computing eigenspaces E_{λ_i}, start with eigenvalues having big multiplicity, because the computation here might lead to the conclusion that A is not diagonalizable, and so you're done.

(2) Always check and doublecheck your computations. If your matrix depends on a parameter t, plug in $t = 0$ or so from time to time, in order to doublecheck. Good luck!

Advanced 1/4

Theorem. With respect to $< x, y >= \sum_i x_i \bar{y}_i$ we have

$$< Ax, y >=< x, A^* y >$$

with A^* being the adjoint matrix, given by $(A^*)_{ij} = \bar{A}_{ji}$.

Theorem. For a matrix $U \in M_N(A)$, the following are equivalent:

(1) U is a unitary, $< Ux, Uy >=< x, y >$.

(2) U satisfies the equation $U^* = U^{-1}$.

Proof. We have indeed $< Ux, Uy >=< x, U^* Uy >$, as desired.

Advanced 2/4

Theorem. The matrices which are normal, in the sense that

$$AA^* = A^*A$$

are diagonalizable.

Theorem. The matrices which are self-adjoint, in the sense that

$$A = A^*$$

are diagonalizable. Moreover, their eigenvalues are real.

Theorem. The matrices which are unitary, in the sense that

$$U^* = U^{-1}$$

are diagonalizable. Their eigenvalues are on the unit circle.

Advanced 3/4

<u>Theorem</u>. The following happen, inside $M_N(\mathbb{C})$:

(1) The matrices having distinct eigenvalues are dense.

(2) The diagonalizable matrices are dense.

<u>Proof</u>. Here (1) follows by using the resultant $R(P, P')$, because the equation $R = 0$ defines a hypersurface in $M_N(\mathbb{C})$, having dense complement. As for (2), this follows from (1).

<u>Comment</u>. This is interesting, because it tells us that "any formula which is true for diagonalizable matrices is true in general".

Advanced 4/4

Theorem. Any matrix $A \in M_N(\mathbb{C})$ can be put in Jordan form

$$A \sim \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_k \end{pmatrix}$$

with each Jordan block being of the following type,

$$J = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

with the numbers λ ranging over the eigenvalues of A.

Linear algebra and calculus questions

Teo Banica

"Introduction to linear algebra", 4/6

08/20

Systems 1/3

<u>Theorem</u>. Any linear system of equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1N}x_N = v_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N = v_2 \\ \qquad\qquad \vdots \\ a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NN}x_N = v_N \end{cases}$$

can be written in matrix form, as follows,

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1N} \\ a_{21} & a_{22} & \ldots & a_{2N} \\ \vdots & & & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NN} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix}$$

and when A is invertible, its solution is given by $x = A^{-1}v$.

Systems 2/3

Theorem. Any linear recurrence system

$$\begin{cases} x_{k+1} = a_{11}x_k + a_{12}y_k + a_{13}z_k + \ldots \\ y_{k+1} = a_{21}x_k + a_{22}y_k + a_{23}z_k + \ldots \\ z_{k+1} = a_{31}x_k + a_{32}y_k + a_{33}z_k + \ldots \\ \qquad\qquad \vdots \end{cases}$$

can be written in matrix form, as follows,

$$\begin{pmatrix} x_{k+1} \\ y_{k+1} \\ z_{k+1} \\ \vdots \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots \\ a_{21} & a_{22} & a_{23} & \ldots \\ a_{31} & a_{32} & a_{33} & \ldots \\ \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} x_k \\ y_k \\ z_k \\ \vdots \end{pmatrix}$$

and the solution is obtained by applying A^k to the inital data.

Systems 3/3

In order to compute A^k, we must diagonalize the matrix,

$$A = PDP^{-1}$$

and then the powers are given by the following formula:

$$A^k = PD^kP^{-1}$$

This formula holds in fact for any $k \in \mathbb{Z}$, or even $k \in \mathbb{R}$.

Calculus 1/4

Theorem. Any function can be locally approximated as

$$f(x+t) \simeq f(x) + at$$

where $a = f'(x)$ is the derivative of f at the point x.

Proof. Let us recall indeed the definition of the derivative:

$$f'(x) = \lim_{t \to 0} \frac{f(x+t) - f(x)}{t}$$

But this gives the formula in the statement.

Calculus 2/4

Theorem. Any function of several variables, written as

$$f = (f_1, \ldots, f_N)$$

can be locally approximated as follows,

$$f(x+t) \simeq f(x) + At$$

with A being the matrix of partial derivatives at x,

$$A = \left(\frac{\partial f_i}{\partial x_j}(x) \right)_{ij}$$

acting on the vectors t by usual multiplication.

Calculus 3/4

<u>Theorem</u>. We have the change of variable formula

$$\int_a^b f(x)dx = \int_c^d f(\varphi(t))\varphi'(t)dt$$

where $c = \varphi^{-1}(a)$ and $d = \varphi^{-1}(b)$.

<u>Proof</u>. This follows with $f = F'$ from the rule

$$(F\varphi)'(t) = F'(\varphi(t))\varphi'(t)$$

by integrating between c and d.

Calculus 4/4

Theorem. Given a transformation in several variables,

$$\varphi = (\varphi_1, \ldots, \varphi_N)$$

we have the following change of variable formula,

$$\int_E f(x)dx = \int_{\varphi^{-1}(E)} f(\varphi(t))J_\varphi(t)dt$$

with the J_φ quantity, called Jacobian, being given by:

$$J_\varphi(t) = \det\left[\left(\frac{\partial\varphi_i}{\partial x_j}(x)\right)_{ij}\right]$$

Polar coordinates 1/4

Theorem. We have polar coordinates in 2 dimensions,

$$\begin{cases} x = r\cos t \\ y = r\sin t \end{cases}$$

and the corresponding Jacobian is $J(r,t) = r$.

Proof. The Jacobian is by definition given by:

$$\begin{vmatrix} \cos t & -r\sin t \\ \sin t & r\cos t \end{vmatrix} = r$$

Thus, we have indeed the formula in the statement.

Polar coordinates 2/4

$$\int_{\mathbb{R}} e^{-x^2} dx = ?$$

Polar coordinates 3/4

Theorem. We have the following formula:

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

Proof. The square of the integral is given by:

$$\begin{aligned} I^2 &= \int_{\mathbb{R}} \int_{\mathbb{R}} e^{-x^2-y^2} dxdy \\ &= \int_0^{2\pi} \int_0^{\infty} re^{-r^2} drdt \\ &= \int_0^{2\pi} \left[-\frac{e^{-r^2}}{2} \right]_0^{\infty} dt \end{aligned}$$

We obtain $I^2 = (2\pi) \times \frac{1}{2} = \pi$, and so $I = \sqrt{\pi}$.

Polar coordinates 4/4

Definition. The normal law of parameter 1 is:

$$g_1 = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$$

More generally, the normal law of parameter $t > 0$ is:

$$g_t = \frac{1}{\sqrt{2\pi t}} e^{-x^2/2t} dx$$

Remark. The Gauss formula gives with $x = y/\sqrt{2t}$

$$\int_{\mathbb{R}} e^{-y^2/2t} dy = \sqrt{2\pi t}$$

so these laws have indeed mass 1.

Spheres 1/4

<u>Theorem</u>. We have spherical coordinates in 3 dimensions,

$$\begin{cases} x = r\cos s \\ y = r\sin s\cos t \\ z = r\sin s\sin t \end{cases}$$

and the corresponding Jacobian is $J(r,s,t) = r^2\sin s$.

<u>Proof</u>. The Jacobian is given by:

$$\begin{vmatrix} \cos s & -r\sin s & 0 \\ \sin s\cos t & r\cos s\cos t & -r\sin s\sin t \\ \sin s\sin t & r\cos s\sin t & r\sin s\cos t \end{vmatrix} = r^2\sin s$$

Thus, we have indeed the formula in the statement.

Spheres 2/4

Theorem. We have spherical coordinates in N dimensions,

$$\begin{cases} x_1 & = r\cos t_1 \\ x_2 & = r\sin t_1\cos t_2 \\ \vdots & \\ x_{N-1} & = r\sin t_1\ldots\sin t_{N-2}\cos t_{N-1} \\ x_N & = r\sin t_1\ldots\sin t_{N-2}\sin t_{N-1} \end{cases}$$

and the corresponding Jacobian is:

$$J(r,t) = r^{N-1}\sin^{N-2}t_1\sin^{N-3}t_2\ldots\sin^2 t_{N-3}\sin t_{N-2}$$

Remark. This generalizes the previous coordinates at $N = 2, 3$.

Spheres 3/4

<u>Theorem</u>. The volume of the sphere in $\mathbb{R}^N$ is given by

$$\frac{V}{2^N} = \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}$$

with $N!! = (N-1)(N-3)(N-5)\ldots$, stopping at 1 or 2.

(1) At $N = 1$ we obtain $V/2 = 1$, so $V = 2$.

(2) At $N = 2$ we obtain $V/4 = \pi/2 \cdot 1/2$, so $V = \pi$.

(3) At $N = 3$ we obtain $V/8 = \pi/2 \cdot 1/3$, so $V = 4\pi/3$.

(4) At $N = 4$ we obtain $V/16 = \pi^2/4 \cdot 1/8$, so $V = \pi^2/2$.

Spheres 4/4

Proof. By using spherical coordinates, and Fubini, we are left with computing integrals over the circle. But these are given by

$$\frac{2}{\pi}\int_0^{\pi/2} \cos^p t \sin^q t \, dt = \left(\frac{2}{\pi}\right)^{\delta(p,q)} \frac{p!!q!!}{(p+q+1)!!}$$

where $\delta(a,b) = 0$ if both a, b are even, and $\delta(a,b) = 1$ otherwise, and by plugging in these quantities, we obtain the result.

Infinite matrices and spectral theory

Teo Banica

"Introduction to linear algebra", 5/6

08/20

Linear spaces 1/3

Definition. A complex vector space is a set V with operations

$$(u, v) \to u + v \quad , \quad (\lambda, u) \to \lambda u$$

having the following properties:

(1) $u + v = v + u$.

(2) $(u + v) + w = u + (v + w)$.

(3) $(\lambda + \mu)u = \lambda u + \mu u$.

(4) $(\lambda\mu)u = \lambda(\mu u)$.

(5) $\lambda(u + v) = \lambda u + \lambda v$.

Examples. $\mathbb{C}^N$, $\mathbb{C}^\infty$, $M_N(\mathbb{C})$, $C[0, 1]$ and many other.

Linear spaces 2/3

Definition. A map $f : V \to W$ is called linear when:

(1) $f(u+v) = f(u) + f(v)$.

(2) $f(\lambda u) = \lambda f(u)$.

Theorem. Let $f : V \to W$ be a linear map.

(1) $\ker f = \{v \in V | f(v) = 0\}$ is a linear space.

(2) $\mathrm{Im}\, f = \{f(v) | v \in V\}$ is a linear space.

(3) $\dim \ker f + \dim \mathrm{Im}\, f = \dim V$.

Linear spaces 3/3

Theorem. In finite dimensions, any vector space V has a basis $\{e_i\}$, which is such that any $v \in V$ can be written, uniquely, as:

$$v = v_1 e_1 + \ldots + v_N e_N$$

Thus we have $V = \mathbb{C}^N$, the identification being given by:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix}$$

As a consequence, any linear map $f : V \to W$ between finite dimensional vector spaces corresponds to a matrix.

Hilbert spaces 1/4

Definition. A scalar product on a complex vector space H is an operation $(x, y) \to < x, y >$, satisfying:

(1) $< x, y >$ is linear in x, and antilinear in y.

(2) $\overline{< x, y >} = < y, x >$, for any x, y.

(3) $< x, x >> 0$, for any $x \neq 0$.

Theorem. If we set $||x|| = \sqrt{< x, x >}$ then:

(1) $| < x, y > | \leq ||x|| \cdot ||y||$.

(2) $||x + y|| \leq ||x|| + ||y||$.

(3) $d(x, y) = ||x - y||$ is a distance.

Proof. (1) follows from the fact that the degree 2 polynomial $f(t) = ||tx + y||^2$ is positive, and (1) $\implies$ (2) $\implies$ (3).

Hilbert spaces 2/4

Definition. A Hilbert space is a complex vector space H with a scalar product $< x, y >$, which is complete with respect to

$$||x|| = \sqrt{< x, x >}$$

in the sense that the Cauchy sequences with respect to the associated distance $d(x, y) = ||x - y||$ converge.

Examples.

(1) $H = \mathbb{C}^N$, with $< x, y >= \sum_i x_i \bar{y}_i$.

(2) $H = l^2(\mathbb{N})$, with $< x, y >= \sum_i x_i \bar{y}_i$.

(3) $H = L^2(X)$, with $< f, g >= \int_X f(x)\overline{g(x)}dx$.

Hilbert spaces 3/4

Theorem. Any Hilbert space H has an orthonormal basis $\{e_i\}_{i\in I}$, and so we have an indentification $H = l^2(I)$.

Proof. The basis can be constructed by starting with an "algebraic" basis, and using the Gram-Schmidt method.

Warning. For spaces like $H = L^2[0,1]$, this is something not trivial.

Theorem. Let H be a Hilbert space, with basis $\{e_i\}_{i\in I}$. We have

$$\mathcal{L}(H) \subset M_I(\mathbb{C})$$

with $T : H \to H$ linear corresponding to the following matrix:

$$M_{ij} =< Te_j, e_i >$$

In particular, when $\dim(H) = N < \infty$, we obtain $\mathcal{L}(H) \simeq M_N(\mathbb{C})$.

Hilbert spaces 4/4

Theorem. Given a Hilbert space H, the linear operators $T : H \to H$ which are bounded, in the sense that

$$||T|| = \sup_{||x|| \leq 1} ||Tx||$$

is finite, form a complex algebra with unit $B(H)$, which:

(1) is complete with respect to $||.||$ (Banach algebra).

(2) has an involution $T \to T^*$, $< Tx, y >=< x, T^*y >$.

The norm and involution are related by $||TT^*|| = ||T||^2$.

Proof. Here "complex algebra" is elementary, (1) follows by setting $Tx = \lim_{n\to\infty} T_n x$, (2) comes from the fact that $\varphi(x) =< Tx, y >$ is linear, and (3) can be proved by double inequality.

Spectral theory 1/4

Definition. A C^*-algebra is a complex algebra with unit A, with:

(1) A norm $a \to ||a||$, making it a Banach algebra.

(2) An involution $a \to a^*$, such that $||aa^*|| = ||a||^2$, $\forall a \in A$.

Definition. The spectrum of an element $a \in A$ is the set:

$$\sigma(a) = \left\{\lambda \in \mathbb{C}\Big|a - \lambda \notin A^{-1}\right\}$$

Theorem. $\sigma(ab) = \sigma(ba)$ outside $\{0\}$.

Proof. Indeed, $c = (1 - ab)^{-1} \implies 1 + cba = (1 - ba)^{-1}$.

Remark. In infinite dimensions, $S^*S = 1, SS^* \neq 1$ (shift).

Spectral theory 2/4

Theorem. We have the following formula, for any rational function $f \in \mathbb{C}(X)$ having its poles outside $\sigma(a)$:

$$\sigma(f(a)) = f(\sigma(a))$$

Proof. In the polynomial case, $f \in \mathbb{C}[X]$, we can factorize,

$$f(X) - \lambda = c(X - r_1) \ldots (X - r_n)$$

and the result can be proved as follows:

$$\begin{aligned} \lambda \notin \sigma(f(a)) &\iff a - r_1, \ldots, a - r_n \in A^{-1} \\ &\iff r_1, \ldots, r_n \notin \sigma(a) \\ &\iff \lambda \notin f(\sigma(a)) \end{aligned}$$

In the general case, $f = P/Q$, we can use $F = P - \lambda Q$.

Spectral theory 3/4

Definition. Given an element $a \in A$, its spectral radius $\rho(a)$ is the radius of the smallest disk centered at 0 containing $\sigma(a)$.

Theorem. Let A be a C^*-algebra.

(1) The spectrum of a norm 1 element is in the unit disk.

(2) The spectrum of a unitary ($a^* = a^{-1}$) is on the unit circle.

(3) The spectrum of a self-adjoint element ($a = a^*$) is real.

(4) ρ of a normal element ($aa^* = a^*a$) equals its norm.

Spectral theory 4/4

(1) Clear from $(1-a)^{-1} = 1 + a + a^2 + \ldots$ for $||a|| < 1$.

(2) Follows by using $f(z) = z^{-1}$. Indeed, we have:

$$\sigma(a)^{-1} = \sigma(a^{-1}) = \sigma(a^*) = \overline{\sigma(a)}$$

(3) Follows from (2), by using $f(z) = (z + it)/(z - it)$.

(4) By (1) we have $\rho(a) \leq ||a||$. Given $\rho > \rho(a)$, we have:

$$\int_{|z|=\rho} \frac{z^n}{z-a} \, dz = \sum_{k=0}^{\infty} \left(\int_{|z|=\rho} z^{n-k-1} dz \right) a^k = a^{n-1}$$

By applying the norm and taking n-th roots we obtain:

$$\rho \geq \lim_{n \to \infty} ||a^n||^{1/n}$$

If $a = a^*$ we are done. In general, we can use $||aa^*|| = ||a||^2$.

Advanced 1/4

Theorem. Given a compact space X, the complex algebra

$$C(X) = \{f : X \to \mathbb{C} \text{ continuous}\}$$

is a C^*-algebra, with norm and involution given by:

$$||f|| = \sup_{x \in X} |f(x)| \quad , \quad f^*(x) = \overline{f(x)}$$

This algebra is commutative, in the sense that $fg = gf$.

Proof. It is well-known that $C(X)$ is complete with respect to the sup norm, and the other conditions are trivially satisfied.

Advanced 2/4

Theorem. Any commutative C^*-algebra is the form $C(X)$, with its "spectrum" $X = Spec(A)$ consisting of the characters:

$$\chi : A \to \mathbb{C}$$

Proof. Set $X = Spec(A)$, with topology making continuous all the evaluation maps $ev_a : \chi \to \chi(a)$. Then X is a compact space, and $a \to ev_a$ is a morphism of algebras $ev : A \to C(X)$.

(1) ev involutive. Using real + imaginary parts, we must prove that $ev_{a^*} = ev_a^*$ when $a = a^*$. But this follows from $\sigma(a) \subset \mathbb{R}$.

(2) ev isometric. Follows from $||ev_a|| = \rho(a) = ||a||$.

(3) ev surjective. Follows from Stone-Weierstrass.

Advanced 3/4

Theorem. Assume that $a \in A$ is normal, and let $f \in C(\sigma(a))$.

(1) We can define $f(a) \in A$, with $f \to f(a)$ being a morphism.

(2) We have the formula $\sigma(f(a)) = f(\sigma(a))$.

Proof. Since a is normal, $B =< a >$ is commutative, and the Gelfand theorem gives $B = C(X)$, with $X = Spec(B)$.

The map $X \to \sigma(a)$ given by evaluation at a being bijective, we have $X = \sigma(a)$. Thus $B = C(\sigma(a))$, and we are done.

Advanced 4/4

Definition. Given an arbitrary C^*-algebra A, we can write

$$A = C(X)$$

and call X a "noncommutative compact space".

Special matrices and matrix tricks

Teo Banica

"Introduction to linear algebra", 6/6

08/20

Fourier 1/3

Theorem. We have the Vandermonde formula:

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_N \\ \vdots & \vdots & & \vdots \\ x_1^{N-1} & x_2^{N-1} & \ldots & x_N^{N-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

Proof. The determinant D is a polynomial in $x_1, \ldots, x_N$, of degree $N-1$ in each variable. Since $x_i = x_j$ makes $D = 0$, we obtain:

$$D = c\prod_{i>j}(x_i - x_j)$$

The constant $c \in \mathbb{R}$ can be computed by recurrence, we get $c = 1$.

Fourier 2/3

Definition. The Fourier matrix F_N is given by:

$$F_N = (w^{ij})_{ij} \quad , \quad w = e^{2\pi i/N}$$

With matrices indices $i, j = 0, 1, \ldots, N-1$, we have:

$$F_N = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & w & w^2 & \ldots & w^{N-1} \\ 1 & w^2 & w^4 & \ldots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{N-1} & w^{(2N-1)} & \ldots & w^{(N-1)^2} \end{pmatrix}$$

This is a Vandermonde matrix, with $x_i = w^i$.

Fourier 3/3

Theorem. The rescaled matrix $\mathcal{F}_N = \frac{1}{\sqrt{N}}(w^{ij})_{ij}$ is unitary.

Proof. We have the following computation:

$$\begin{aligned}
(F_N F_N^*)_{ij} &= \sum_k (F_N)_{ik}(\bar{F}_N)_{jk} \\
&= \sum_k w^{ik} \cdot w^{-jk} \\
&= \sum_k (w^{i-j})^k \\
&= N\delta_{ij}
\end{aligned}$$

Thus the rescaled matrix $\mathcal{F}_N = F_N/\sqrt{N}$ is unitary.

Special matrices 1/4

Theorem. For a matrix $H \in M_N(\mathbb{C})$, the following are equivalent,

(1) H is circulant, $H_{ij} = \xi_{j-i}$ for some $\xi \in \mathbb{C}^N$.

(2) H is Fourier-diagonal, $H = \mathcal{F} Q \mathcal{F}^*$ with Q diagonal.

where $\mathcal{F} = \mathcal{F}_N$. In addition, the first row vector of H is

$$\xi = \mathcal{F} q / \sqrt{N}$$

where $q_i = Q_{ii}$ is the vector formed by the diagonal entries of Q.

Special matrices 2/4

<u>Proof</u>. If $H_{ij} = \xi_{j-i}$ is circulant then $Q = \mathcal{F}^* H \mathcal{F}$ is diagonal:

$$Q_{ij} = \frac{1}{N} \sum_{kl} w^{jl-ik} \xi_{l-k} = \delta_{ij} \sum_{r} w^{jr} \xi_r$$

Also, if $Q = diag(q)$ is diagonal then $H = \mathcal{F} Q \mathcal{F}^*$ is circulant:

$$H_{ij} = \sum_{k} \mathcal{F}_{ik} Q_{kk} \bar{\mathcal{F}}_{jk} = \frac{1}{N} \sum_{k} w^{(i-j)k} q_k$$

This formula proves as well the last assertion, $\xi = \mathcal{F} q / \sqrt{N}$.

Special matrices 3/4

Theorem. The various sets of circulant matrices are as follows,

(1) $M_N(\mathbb{C})^{circ} = \{\mathcal{F}Q\mathcal{F}^* | q \in \mathbb{C}^N\}$.

(2) $U_N^{circ} = \{\mathcal{F}Q\mathcal{F}^* | q \in \mathbb{T}^N\}$.

(3) $O_N^{circ} = \{\mathcal{F}Q\mathcal{F}^* | q \in \mathbb{T}^N, \bar{q}_i = q_{-i}, \forall i\}$.

with the convention $Q = diag(q)$, for $q \in \mathbb{C}^N$.

Proof. (1) This is something that we already know.

(2) This is because the eigenvalues must be on the unit circle $\mathbb{T}$.

(3) For $q \in \mathbb{C}^N$ we have $\overline{\mathcal{F}q} = \mathcal{F}\tilde{q}$, with $\tilde{q}_i = \bar{q}_{-i}$, and so $\xi = \mathcal{F}q$ is real if and only if $\bar{q}_i = q_{-i}$ for any i. This gives the result.

Special matrices 4/4

Theorem. The groups $B_N \subset O_N$ and $C_N \subset U_N$ of bistochastic matrices (sum 1 on each row and column) are given by:

$$B_N \simeq O_{N-1} \quad , \quad C_N \simeq U_{N-1}$$

Proof. The all-1 vector ξ being equal to $\sqrt{N}\mathcal{F}e_0$, we have:

$$\begin{aligned} U\xi = \xi \quad &\iff \quad U\mathcal{F}e_0 = \mathcal{F}e_0 \\ &\iff \quad \mathcal{F}^*U\mathcal{F}e_0 = e_0 \\ &\iff \quad \mathcal{F}^*U\mathcal{F} = diag(1, w) \end{aligned}$$

Thus we have isomorphisms as in the statement.

Hadamard matrices 1/4

Definition. A complex Hadamard matrix is a square matrix

$$H \in M_N(\mathbb{C})$$

whose entries are on the unit circle, $H_{ij} \in \mathbb{T}$, and whose rows are pairwise orthogonal, with respect to the scalar product of $\mathbb{C}^N$.

Example. For the Fourier matrix, $F_N = (w^{ij})$ with $w = e^{2\pi i/N}$, the scalar products between rows are:

$$< R_a, R_b >= \sum_j w^{aj} w^{-bj} = \sum_j w^{(a-b)j} = N\delta_{ab}$$

Thus the Fourier matrix F_N is Hadamard.

Hadamard matrices 2/4

<u>Theorem</u>. Given a finite abelian group G, with group dual

$$\widehat{G} = \{\chi : G \to \mathbb{T}\}$$

consider the Fourier coupling $G \times \widehat{G} \to \mathbb{T}$:

$$(i, \chi) \to \chi(i)$$

(1) Via the standard isomorphism $G \simeq \widehat{G}$, this Fourier coupling is a square matrix, $F_G \in M_G(\mathbb{T})$, which is complex Hadamard.

(2) For a cyclic group $G = \mathbb{Z}_N$ we obtain in this way, via the standard identification $\mathbb{Z}_N = \{1, \ldots, N\}$, the Fourier matrix F_N.

(3) In general, when using a decomposition $G = \mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$, the corresponding Fourier matrix is $F_G = F_{N_1} \otimes \ldots \otimes F_{N_k}$.

Hadamard matrices 3/4

Examples. (1) For the cyclic group $\mathbb{Z}_2$ we obtain the Fourier matrix F_2, also denoted W_2, and called first Walsh matrix:

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

(2) For the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$ we obtain the tensor product $W_4 = W_2 \otimes W_2$, called second Walsh matrix:

$$W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

(3) In general, for the group $\mathbb{Z}_2^n$ we obtain the n-th Walsh matrix $W_N = W_2^{\otimes n}$, having size $N = 2^n$. Useful in radio, coding.

Hadamard matrices 4/4

Hadamard Conjecture. There is at least one real Hadamard matrix

$$H \in M_N(\pm 1)$$

for any integer $N \in 4\mathbb{N}$.

Comment. Verified so for up to $\mathfrak{N} = 666$.

Rotations 1/4

Theorem. For a matrix $U \in M_N(\mathbb{C})$, the following are equivalent:

(1) U preserves the scalar product, $< Ux, Uy >=< x, y >$.

(2) U preserves the norm, $||Ux|| = ||x||$, where $||x|| = \sqrt{< x, x >}$.

(3) U is unitary, in the sense that $U^* = U^{-1}$, where $(U^*)_{ij} = \bar{U}_{ji}$.

(4) U has its eigenvalues on the unit circle $\mathbb{T}$.

Proof. The equivalences (1) $\iff$ (2) $\iff$ (3) follow by using $< Mx, y >=< x, M^*y >$, and (4) is something that we know.

Rotations 2/4

<u>Theorem</u>. The unitaries in $M_2(\mathbb{C})$ of determinant 1 are

$$U = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

with $a, b \in \mathbb{C}$ satisfying $|a|^2 + |b|^2 = 1$.

<u>Proof</u>. For $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of determinant 1, $U^* = U^{-1}$ reads:

$$\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Thus $c = -\bar{b}, d = \bar{a}$. Finally, $\det U = 1$ gives $|a|^2 + |b|^2 = 1$.

Rotations 3/4

Theorem. The unitaries in $M_3(\mathbb{R})$ of determinant 1 are

$$O = \begin{pmatrix} x^2+y^2-z^2-t^2 & 2(yz-xt) & 2(xz+yt) \\ 2(xt+yz) & x^2+z^2-y^2-t^2 & 2(zt-xy) \\ 2(yt-xz) & 2(xy+zt) & x^2+t^2-y^2-z^2 \end{pmatrix}$$

with $x, y, z, t \in \mathbb{R}$ satisfying $x^2+y^2+z^2+t^2=1$.

Proof. With $a = x+iy$, $b = z+it$, the previous formula reads:

$$U = \begin{pmatrix} x+iy & z+it \\ -z+it & x-iy \end{pmatrix}$$

But we must have "$O+1 = ad(U)$", and this gives the result.

Rotations 4/4

Conclusion. We can now:

- do some serious engineering
- or write 3D games software.

References 1/2

[1] M.F. Atiyah and I.G. MacDonald, Introduction to commutative algebra, Addison-Wesley (1969).

[2] R. Brauer, On algebras which are connected with the semisimple continuous groups, *Ann. of Math.* **38** (1937), 857–872.

[3] P. Deligne, Catégories tannakiennes, in "Grothendieck Festchrift", Birkhauser (1990), 111–195.

[4] P. Diaconis and M. Shahshahani, On the eigenvalues of random matrices, *J. Applied Probab.* **31** (1994), 49–62.

[5] S. Doplicher and J. Roberts, A new duality theory for compact groups, *Invent. Math.* **98** (1989), 157–218.

[6] V.G. Drinfeld, Quantum groups, Proc. ICM Berkeley (1986), 798–820.

[7] R. Hartshorne, Algebraic geometry, Springer (1977).

[8] F. Klein, Vergleichende Betrachtungen über neuere geometrische Forschungen, *Math. Ann.* **43** (1893), 63–100.

References 2/2

[9] S. Lang, Algebra, Addison-Wesley (1993).

[10] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[11] J.P. Serre, Linear representations of finite groups, Springer (1977).

[12] I.R. Shafarevich, Basic algebraic geometry, Springer (1974).

[13] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.

[14] T. Tannaka, Über den Dualitätssatz der nichtkommutativen topologischen Gruppen, *Tôhoku Math. J.* **45** (1939), 1–12.

[15] H. Weyl, The classical groups: their invariants and representations, Princeton (1939).

[16] S.L. Woronowicz, Compact matrix pseudogroups, *Comm. Math. Phys.* **111** (1987), 613–665.