Linear algebra basics

Teo Banica

Linear algebra, Matrix groups

08/20

Foreword

These are slides written in the Fall 2020, on:

1. Linear algebra
2. Matrix groups

Presentations available at my Youtube channel.

Contents 1/2

Contents 2/2

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

Definition. 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 $T\binom{x}{y} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\binom{x}{y} = \binom{y}{0}$ 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

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

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

<u>Proof</u>. 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

<u>Theorem</u>. In 2 dimensions, the determinant is given by:

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

<u>Proof</u>. 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:

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

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

<u>Theorem</u>. The matrices which are normal, in the sense that

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

are diagonalizable.

<u>Theorem</u>. The matrices which are self-adjoint, in the sense that

$$A = A^*$$

are diagonalizable. Moreover, their eigenvalues are real.

<u>Theorem</u>. The matrices which are unitary, in the sense that

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

are diagonalizable. Their eigenvalues are on the unit circle.

Advanced 3/4

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

(1) The matrices having distinct eigenvalues are dense.

(2) The diagonalizable matrices are dense.

Proof. 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).

Comment. 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

Theorem. Any linear system of equations

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

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

Theorem. 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 $d = \varphi^{-1}(b)$.

Proof. 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

Theorem. 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:

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

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

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

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

<u>Proof</u>. 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

Proof. 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

Theorem. 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

Theorem. 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 $|a|^2 + |b|^2 = 1$.

Proof. 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.

Groups of unitary matrices

Teo Banica

"Introduction to matrix groups", 1/6

08/20

Groups 1/3

Definition. A group is a set G with a multiplication operation

$$(g, h) \to gh$$

satisfying the following conditions:

(1) Associativity: $(gh)k = g(hk)$.

(2) Unit: $\exists 1 \in G$, $g1 = 1g = g$.

(3) Inverses: $\forall g, \exists g^{-1}$, $gg^{-1} = g^{-1}g = 1$.

Groups 2/3

Examples.

(1) $\mathbb{R}$ with the addition operation $x + y$. Here the unit is 0 (!) and the inverses are $-x$.

(2) $\mathbb{R}^*$ with the multiplication operation xy. Here the unit is 1 and the inverses are x^{-1}.

(3) $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ with the addition operation $x + y$, and $\mathbb{Q}^*, \mathbb{C}^*$ with the multiplication operation xy.

Note that $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ and $(\mathbb{Z}^*, \cdot)$ are not groups, because here we have no inverses.

Groups 3/3

More examples.

(1) The group S_N of permutations $\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$. Note that we have $\sigma\tau \neq \tau\sigma$ in general, in this group.

(2) The groups $GL_N(\mathbb{Q})$, $GL_N(\mathbb{R})$, $GL_N(\mathbb{C})$ of invertible $N \times N$ matrices over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Here $gh = hg$ fails too, in general.

Conventions.

– When $ab = ba$ we say that the group is abelian.

– We usually denote the operation of an abelian group by a sum, $g + h$, the unit element by 0, and the inverses by $-g$.

– This is not a general rule. What is true, however, is that if a group is denoted $(G, +)$, then the group must be abelian.

Orthogonal groups 1/4

Notations. We use the usual scalar product and norm on $\mathbb{R}^N$:

$$< x, y >= \sum_i x_i y_i \quad , \quad ||x|| = \sqrt{< x, x >}$$

Theorem. For a matrix $U \in M_N(\mathbb{R})$, the following are equivalent, and if they are satisfied, we say that U is orthogonal:

(1) $< Ux, Uy >=< x, y >$.

(2) $||Ux|| = ||x||$.

(3) $U^t = U^{-1}$, where $(U^t)_{ij} = U_{ji}$.

(4) The rows of U form an orthonormal basis of $\mathbb{R}^N$.

(5) The columns of U form an orthonormal basis of $\mathbb{R}^N$.

Proof. All this follows from $< Ux, y >=< x, U^t y >$.

Orthogonal groups 2/4

Theorem. The set formed by the orthogonal matrices

$$O_N=\left\{U\in M_N(\mathbb R)\Big|U^t=U^{-1}\right\}$$

is a group, with the usual multiplication of the matrices.

Proof. Assuming $U,V\in O_N$, we have $UV\in O_N$, because:

$$(UV)^t=V^tU^t=V^{-1}U^{-1}=(UV)^{-1}$$

Also, $1_N\in O_N$, and $U\in O_N\implies U^{-1}\in O_N$.

Orthogonal groups 3/4

Theorem. The elements of O_2 fall into two classes:

(1) Rotations. The rotation of angle $t \in \mathbb{R}$ is given by the following formula:

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

The rotations are exactly the elements of O_2 having determinant 1, and they form a group, denoted SO_2.

(2) Symmetries. The symmetry with respect to the Ox axis rotated by $t/2 \in \mathbb{R}$ is given by the following formula:

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

The symmetries are exactly the elements of O_2 having determinant -1, and they do not form a group.

Orthogonal groups 4/4

Theorem. The elements of O_N fall into two classes:

(1) Those of determinant 1, which form a group, denoted SO_N:

$$SO_N = \left\{ U \in O_N \middle| \det U = 1 \right\}$$

(2) Those of determinant -1, which do not form a group.

Proofs. For $U \in O_N$ we have $\det(UU^t) = 1$, so $\det U = \pm 1$.

The set SO_N is a group, because $\det(UV) = \det U \det V$, and its complement is not a group, because $\det(1_N) = 1$.

Finally, the various 2D formulae are well-known, and elementary.

Unitary groups 1/4

<u>Notations</u>. We use the usual scalar product and norm on $\mathbb{C}^N$:

$$< x, y >= \sum_i x_i \bar{y}_i \quad , \quad ||x|| = \sqrt{< x, x >}$$

<u>Theorem</u>. For a matrix $U \in M_N(\mathbb{C})$, the following are equivalent, and if they are satisfied, we say that U is unitary:

(1) $< Ux, Uy >=< x, y >$.

(2) $||Ux|| = ||x||$.

(3) $U^* = U^{-1}$, where $(U^*)_{ij} = \bar{U}_{ji}$.

(4) The rows of U form an orthonormal basis of $\mathbb{C}^N$.

(5) The columns of U form an orthonormal basis of $\mathbb{C}^N$.

<u>Proof</u>. All this follows from $< Ux, y >=< x, U^* y >$.

Unitary groups 2/4

Theorem. The set formed by the unitary matrices

$$U_N = \left\{ U \in M_N(\mathbb{C}) \middle| U^* = U^{-1} \right\}$$

is a group, with the usual multiplication of the matrices.

Proof. Assuming $U, V \in U_N$, we have $UV \in U_N$, because:

$$(UV)^* = V^* U^* = V^{-1} U^{-1} = (UV)^{-1}$$

Also, $1_N \in U_N$, and $U \in U_N \implies U^{-1} \in U_N$.

Unitary groups 3/4

Theorem. The determinant of a unitary matrix $U \in U_N$ must be a number on the unit circle:

$$\det U \in \mathbb{T}$$

The unitary matrices $N \times N$ having determinant 1 form a group, denoted SU_N:

$$SU_N = \left\{ U \in U_N \middle| \det U = 1 \right\}$$

Any matrix $U \in U_N$ is proportional to a matrix in SU_N, the proportionality factor being a number $d \in \mathbb{T}$.

Proof. For $U \in U_N$ we have $\det(UU^*) = 1$, so $|\det U| = 1$.

The second assertion is clear from $\det(UV) = \det U \det V$.

The third assertion follows by dividing by $d = (\det U)^{1/N}$.

Unitary groups 4/4

Theorem. We have the following formula,

$$SU_2 = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \Big| \, |a|^2 + |b|^2 = 1 \right\}$$

as well as the following formula:

$$U_2 = \left\{ d \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \Big| \, |a|^2 + |b|^2 = 1, |d| = 1 \right\}$$

Proof. 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 $|a|^2 + |b|^2 = 1$.

Subgroups 1/4

The groups that we considered so far are as follows:

$$\begin{array}{ccc} O_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ SO_N & \longrightarrow & SU_N \end{array}$$

It is possible to construct more groups along these lines:

(1) By multiplying by $\mathbb{Z}_r = \{w \in \mathbb{C} | w^r = 1\}$.

(2) By imposing the condition $(\det U)^s = 1$.

We can equally talk about the symplectic groups $Sp_N \subset U_N$.

Subgroups 2/4

Another big class of groups of matrices comes by looking at

$$U_N^{diag} = \mathbb{T}^N$$

and its subgroups. We have for instance the groups

$$\mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_N}$$

for any choice of numbers $r_1, \ldots, r_N \in \mathbb{N} \cup \{\infty\}$.

Subgroups 3/4

Importantly, the permutation groups S_N appear as well as groups of unitary matrices,

$$S_N \subset O_N \subset U_N$$

by making each $\sigma \in S_N$ act on the coordinate axes of $\mathbb{R}^N$. Indeed, this action is clearly isometric, so $S_N \subset O_N$.

Subgroups 4/4

In fact, any finite group G appears as a group of unitary matrices. Indeed, we can make act G on itself, by left multiplication,

$$G \subset S_G \quad , \quad \sigma_g(h) = gh$$

and so with $N = |G|$ we have embeddings as follows:

$$G \subset S_N \subset O_N \subset U_N$$

However, groups such as $D_N \subset O_N$ show that each finite group G has its own "privileged" embedding $G \subset U_N$.

Symmetry and reflection groups

Teo Banica

"Introduction to matrix groups", 2/6

08/20

Finite groups 1/3

Theorem. Any finite group is a permutation group.

Proof. Given a finite group G, we have an embedding as follows:

$$G \subset S_G \quad , \quad \sigma_g(h) = gh$$

In other words, we have $G \subset S_N$, with $N = |G|$.

Finite groups 2/3

Theorem. Any finite group appears as group of orthogonal matrices.

Proof. This is true for S_N, which can be regarded as being the permutation group of the N coordinate axes of $\mathbb{R}^N$:

$$S_N \subset O_N$$

Thus, given a group G of finite order $N < \infty$, we have:

$$G \subset S_N \subset O_N$$

Finite groups 3/3

Conclusion. The following are the same thing:

(1) The finite groups.

(2) The subgroups $G \subset S_N$.

(3) The finite subgroups $G \subset O_N$.

(4) The finite subgroups $G \subset U_N$.

Problem. Given a finite group G, what is the "best" embedding of type $G \subset U_N$, say with $N \in \mathbb{N}$ being smallest possible?

Comment. This is a "representation theory" problem.

Dihedral groups 1/4

Theorem. Consider the cyclic group $\mathbb{Z}_N$.

(1) We have an embedding $\mathbb{Z}_N \subset O_2$, given by:

$$k \to \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \quad , \quad t = \frac{2k\pi}{N}$$

(2) We have an embedding $\mathbb{Z}_N \subset O_N$, given by:

$$k \to [e_i \to e_{i+k}]$$

(3) We have an embedding $\mathbb{Z}_N \subset U_1$, given by:

$$k \to (w^k) \quad , \quad w = e^{2\pi i/N}$$

Comment. (2) is nicer than (1), and (3) beats everything.

Dihedral groups 2/4

Definition. The dihedral group D_N is the group of symmetries of a regular N-gon.

Examples.

(1) At $N = 3$ we have 3 symmetries, with respect to the 3 medians of $\triangle$, as well as 3 rotations, of angles $0^\circ, 120^\circ, 240^\circ$.

(2) At $N = 4$ we have 4 symmetries, with respect to Ox, Oy and the diagonals of $\square$, and 4 rotations, of angles $0^\circ, 90^\circ, 180^\circ, 270^\circ$.

Dihedral groups 3/4

Theorem. The dihedral group D_N has $2N$ elements, as follows:

(1) N rotations, of angles $2k\pi/N$, with $k = 0, 1, \ldots, N-1$. These form a copy $\mathbb{Z}_N \subset D_N$ of the cyclic group $\mathbb{Z}_N$.

(2) N symmetries, with respect to the N medians when N is odd, and to the $N/2 + N/2$ symmetry axes, when N is even.

In addition, we have a formula of type $D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$.

Proof. (1) and (2) are clear. Regarding the last part, D_N has the same number of elements as $\mathbb{Z}_N \times \mathbb{Z}_2$, but is not abelian. Thus, we must "twist" the product of $\mathbb{Z}_N \times \mathbb{Z}_2$ in order to obtain D_N.

Dihedral groups 4/4

Theorem. Consider the dihedral group D_N.

(1) We have an embedding $D_N \subset O_2$, given by the usual rotation and symmetry matrices:

$$R_k \to \begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix} \quad , \quad t = \frac{2k\pi}{N}$$

$$S_k \to \begin{pmatrix}\cos t & \sin t\\ \sin t & -\cos t\end{pmatrix} \quad , \quad t = \frac{2k\pi}{N}$$

(2) We have an embedding $D_N \subset O_N$, obtained by permuting the N-gon on the coordinate axes of $\mathbb{R}^N$, at distance 1 from 0:

$$\sigma \to [e_i \to e_{\sigma(i)}]$$

(3) We cannot have an embedding $D_N \subset U_1$, because the group U_1 is abelian, and D_N is not abelian.

Symmetric groups 1/4

Theorem. The permutation group S_N has $N!$ elements.

Proof. In order to construct a permutation $\sigma \in S_N$, we must:

(1) Choose $\sigma(1)$, and there are N choices here.

(2) Choose $\sigma(2)$, and there are $N-1$ choices left.

$\vdots$

$\vdots$

(N) Choose $\sigma(N)$, and there is 1 choice left.

Thus, we have a total of $N(N-1)\ldots 1 = N!$ choices.

Symmetric groups 2/4

Theorem. We have an embedding $S_N \subset O_N$, given by:

$$\sigma \to [e_i \to e_{\sigma(i)}]$$

By using the standard $e_{ij} : e_j \to e_i$ notation, the formula is:

$$\sigma \to \sum_i e_{\sigma(i)i}$$

In matrix notation, and with Kronecker symbols, the formula is:

$$\sigma \to [\delta_{i\sigma(j)}]_{ij}$$

Proof. The first assertion is clear, because the transformations $e_i \to e_{\sigma(i)}$ are isometries of $\mathbb{R}^N$, and the rest is clear too.

Symmetric groups 3/4

Theorem. The permutation matrices $S_N \subset O_N$ are precisely the 0-1 matrices having a 1 entry on each row and column.

Theorem. The trace of a permutation matrix $\sigma \in S_N \subset O_N$ is the number of its fixed points.

Proofs. Both these results are clear from definitions.

Symmetric groups 4/4

Theorem. The determinant of the permutation matrices

$$\det(\sigma) \in \{\pm 1\}$$

coinsides with the signature of the permutations,

$$\varepsilon(\sigma) = (-1)^c$$

where c is the number of inversions.

Proof. This is clear with any of the definitions of det.

Comment. Thus, $S_N \cap SO_N = A_N$, the alternating group.

Reflection groups 1/4

Definition. The hyperoctahedral group H_N is the symmetry group of the hypercube $\square_N \subset \mathbb{R}^N$.

Comment. Thus, we have by definition $H_N \subset S_{2^N}$.

Example. We have $H_2 = D_4$.

Problem. $|H_N| = ?$

Reflection groups 2/4

<u>Theorem</u>. The group H_N appears as well as the group of signed permutations of the coordinate axes of $\mathbb{R}^N$, so we have

$$H_N \subset O_N$$

with the image consisting of the $-1, 0, 1$ matrices having exactly one ± 1 entry on each row and each column. Thus we have:

$$|H_N| = 2^N N!$$

<u>Comment</u>. One can prove that $H_N = S_N \rtimes \mathbb{Z}_2^N$, which is also written as $H_N = \mathbb{Z}_2 \wr S_N$, wreath product.

Reflection groups 3/4

Definition. The reflection group H_N^s, depending on parameters

$$N\in\mathbb N\quad,\quad s\in\mathbb N\cup\{\infty\}$$

is the group of $N\times N$ matrices having entries in

$$\mathbb Z_s\cup\{0\}$$

having exactly one nonzero entry on each row and each column.

Examples. At $s=1$ we obtain S_N, and at $s=2$ we obtain H_N.
In general, at $s<\infty$, we have a certain finite group $H_N^s\subset U_N$.
At $s=\infty$ we have a group $K_N\subset U_N$, which is no longer finite.

Reflection groups 4/4

One can prove that the "complex reflection groups" are:

– The above groups $H_N^s = S_N \wr \mathbb{Z}_s$.

– Their subgroups H_N^{sd} given by $\det^d = 1$.

– And some exceptional examples.

Symmetric groups and Poisson laws

Teo Banica

"Introduction to matrix groups", 3/6

08/20

Characters 1/3

Definition. A representation of a finite group G is a morphism

$$\pi : G \to U_N$$

and the character of this representation is the map

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

obtained by taking the trace of the images of group elements:

$$\chi(g) = Tr(\pi(g))$$

When G comes as $G \subset_\pi U_N$, we call χ the "main character".

Characters 2/3

Remark. The characters are central functions on the group, in the sense that they satisfy the following condition:

$$\chi(gh) = \chi(hg)$$

We will see later that any central function on the group is a linear combination of characters. This is something non-trivial.

Remark. We can talk, more generally, about representations and characters of compact groups, with the representations

$$\pi : G \to U_N$$

being assumed to be continuous. We will do this later on.

Characters 3/3

Problem. Given $\pi : G \to U_N$, we want to compute the law of:

$$\chi = Tr \circ \pi : G \to \mathbb{C}$$

That is, we would like to compute the following probabilities,

$$P(\chi = k) \in [0,1] \quad , \quad k \in \mathbb{C}$$

and then the complex discrete measure encoding them:

$$\mu = \sum_{k \in \mathbb{C}} P(\chi = k)\delta_k$$

There are many motivations for this question. Details later.

Fixed points 1/4

Theorem. For the symmetric group S_N, regarded as subgroup

$$S_N \subset O_N$$

permuting the coordinate axes of $\mathbb{R}^N$, the main character is

$$\chi(\sigma) = \#\left\{i \Big| \sigma(i) = i\right\}$$

and its law is a discrete probability measure, supported by $\mathbb{N}$.

Proof. Each $\sigma \in S_N \subset O_N$ is a 0-1 matrix, whose trace $Tr(\chi)$ counts the 1 diagonal entries, corresponding to fixed points.

Fixed points 2/4

Theorem. The probability for a permutation $\sigma \in S_N$ to be a derangement is, in the $N \to \infty$ limit:

$$P_0 \simeq \frac{1}{e}$$

Proof. We must be outside the union $F = \bigcup_i F_i$, where:

$$F_i = \left\{ \sigma \in S_N \middle| \sigma(i) = i \right\}$$

The inclusion-exclusion principle gives:

$$F^c = N! - \sum_i |F_i| + \sum_{i<j} |F_i \cap F_j| - \sum_{i<j<k} |F_i \cap F_j \cap F_k| + \ldots$$

We obtain $P_0 = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots \simeq \frac{1}{e}$, as claimed.

Fixed points 3/4

Theorem. The probability for a permutation $\sigma \in S_N$ to have exactly $k \in \mathbb{N}$ fixed points is

$$P_k \simeq \frac{1}{e} \cdot \frac{1}{k!}$$

once again in the $N \to \infty$ limit.

Proof. We already know that the result holds at $k = 0$. In general the proof is similar, by using the inclusion-exclusion principle.

Fixed points 4/4

Theorem. The character of the standard representation

$$S_N \subset O_N$$

obtained by permuting the coordinate axes of $\mathbb{R}^N$ is given by

$$\chi(\sigma) = \#\left\{i \middle| \sigma(i) = i\right\}$$

and follows with $N \to \infty$ the following law:

$$p_1 = \frac{1}{e}\sum_k \frac{\delta_k}{k!}$$

Proof. This follows by putting together the above results.

Poisson laws 1/4

Definition. The Poisson law of parameter 1 is:

$$p_1 = \frac{1}{e} \sum_k \frac{\delta_k}{k!}$$

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

$$p_t = e^{-t} \sum_k \frac{t^k}{k!} \, \delta_k$$

Remark. These laws have indeed mass 1.

Poisson laws 2/4

Theorem. We have the following formula, for any $s, t > 0$:

$$p_s * p_t = p_{s+t}$$

Proof. By using $\delta_k * \delta_l = \delta_{k+l}$ and the binomial formula:

$$\begin{aligned} p_s * p_t &= e^{-s}\sum_k \frac{s^k}{k!}\,\delta_k * e^{-t}\sum_l \frac{t^l}{l!}\,\delta_l \\ &= e^{-s-t}\sum_n \delta_n \sum_{k+l=n} \frac{s^k t^l}{k!\,l!} \\ &= e^{-s-t}\sum_n \frac{(s+t)^n}{n!}\,\delta_n \end{aligned}$$

Thus, we obtain the Poisson law p_{s+t}, as claimed.

Poisson laws 3/4

Theorem. The Fourier transform of p_t is given by:

$$F_{p_t}(x) = \exp\left((e^{ix} - 1)t\right)$$

Proof. By using $F_f(x) = \mathbb{E}(e^{ixf})$, we obtain:

$$\begin{aligned} F_{p_t}(x) &= e^{-t} \sum_k \frac{t^k}{k!} e^{ikx} \\ &= e^{-t} \sum_k \frac{(e^{ix}t)^k}{k!} \\ &= \exp(-t) \exp(e^{ix}t) \end{aligned}$$

Thus, we obtain the formula in the statement.

Poisson laws 4/4

Theorem. We have the following convergence, in moments:

$$\left(\left(1-\frac{t}{n}\right)\delta_0+\frac{t}{n}\delta_1\right)^{*n}\to p_t$$

Proof. We have the following computation:

$$\begin{aligned}
F_{\delta_t}(x)=e^{itx} &\implies F_{\mu_n}(x)=\left(1-\frac{t}{n}\right)+\frac{t}{n}e^{ix}\\
&\implies F_{\mu_n^{*n}}(x)=\left(\left(1-\frac{t}{n}\right)+\frac{t}{n}e^{ix}\right)^n\\
&\implies F_{\mu_n^{*n}}(x)=\left(1+\frac{(e^{ix}-1)t}{n}\right)^n\\
&\implies F(x)=\exp\left((e^{ix}-1)t\right)
\end{aligned}$$

Thus, we obtain the Fourier transform of p_t.

Truncation 1/4

Problem. We know that for $S_N \subset O_N$ with $N \to \infty$, the main character follows the Poisson law p_1.

What about the general Poisson law p_t, of parameter $t > 0$? Can we obtain this law in the representation theory context?

Truncation 2/4

<u>Definition</u>. Given a group representation $\pi : G \to U_N$, its truncated character with respect to a parameter $t \in (0,1]$,

$$\chi_t : G \to \mathbb{C}$$

is the map given by the following formula:

$$\chi_t(g) = \sum_{i=1}^{[tN]} \pi(g)_{ii}$$

When G comes as a group of matrices, $G \subset_\pi U_N$, we call this map χ_t the "main truncated character" of the group.

Truncation 3/4

Theorem. The main truncated character of the symmetric group

$$S_N \subset O_N$$

which permutes the coordinate axes of $\mathbb{R}^N$, is given by

$$\chi_t(\sigma) = \#\left\{ i \in \{1, \ldots, [tN]\} \Big| \sigma(i) = i \right\}$$

and follows with $N \to \infty$ the Poisson law of parameter t,

$$p_t = e^{-t} \sum_k \frac{t^k}{k!} \delta_k$$

for any value of the parameter $t \in (0, 1]$.

Truncation 4/4

Proof. We already know that the formula holds at $t = 1$. The same method, inclusion-exclusion, gives, more generally:

$$\lim_{N \to \infty} P(\chi = k) = \frac{1}{e^t} \cdot \frac{t^k}{k!}$$

Thus, we obtain with $N \to \infty$ the Poisson law p_t, as claimed.

Comment. We will see later extensions and interpretations of all this, in the advanced representation theory context.

Complex reflections and Bessel laws

Teo Banica

"Introduction to matrix groups", 4/6

08/20

Reflection groups 1/3

Definition. The reflection group H_N^s, depending on parameters

$$N \in \mathbb{N} \quad , \quad s \in \mathbb{N} \cup \{\infty\}$$

is the group of $N \times N$ matrices with entries in

$$\mathbb{Z}_s \cup \{0\}$$

having one nonzero entry on each row and each column.

Examples. At $s = 1$ we have the symmetric group $S_N \subset O_N$.
At $s = 2$ we have the hyperoctahedral group $H_N \subset O_N$.
At $s = 3, 4, \ldots$ we have a certain finite subgroup $H_N^s \subset U_N$.
At $s = \infty$ we have a certain infinite subgroup $K_N \subset U_N$.

Reflection groups 2/3

Theorem. We have $H_N^s=\mathbb{Z}_s\wr S_N$, wreath product decomposition.

Proof. This basically says that the elements $g\in H_N^s$ appear as permutations $\sigma\in S_N$ "decorated" with signs $\varepsilon\in\mathbb{Z}_s^N$, which is something that we already know, from the matrix picture.

Theorem. The irreducible complex reflection groups are

$$H_N^{sd}=\{U\in H_N^s|\det U\in\mathbb{Z}_d\}$$

along with 34 exceptional examples.

Proof. This is something complicated, due to Shephard and Todd.

Reflection groups 3/3

Theorem. The groups H_N^s are easy, in the sense that

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

are Brauer type algebras, spanned by diagrams.

Proof. This holds indeed, with $D_{kl} \subset \mathcal{P}(k, l)$ being defined by the condition $\# \circ = \# \bullet (s)$, weighted count, in each block.

Problem. What is the law of the main character χ for H_N^s? And, what about the laws of truncated characters χ_t?

Comment. At $s = 1$, where the group is S_N, we have $\chi \sim p_1$, and more generally $\chi_t \sim p_t$, Poisson laws, with $N \to \infty$.

Real reflections 1/4

Definition. The hyperoctahedral group $H_N \subset O_N$ is:

(1) The symmetry group of the unit hypercube $\square_N \subset \mathbb{R}^N$.

(2) The group of symmetries of the N coordinate axes of $\mathbb{R}^N$.

(3) The group of permutation-like matrices with ± 1 entries.

Theory. We have $H_N = \mathbb{Z}_2 \wr S_N$, the reflection subgroups reduce to $SH_N = H_N \cap SO_N$, and we have easiness, with $D = P_{even}$.

Real reflections 2/4

Theorem. The laws of truncated characters for H_N are

$$\mathrm{law}(\chi_t) \simeq e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \sum_{p=0}^{\infty} \frac{(t/2)^{|k|+2p}}{(|k|+p)!p!}$$

for any $t \in (0,1]$, in the $N \to \infty$ limit.

Proof. Inclusion-exclusion principle, exactly as for S_N, but this time with the permutations $\sigma \in S_N$ being decorated by signs $\varepsilon \in \mathbb{Z}_2^N$.

Real reflections 3/4

Remark. The limiting truncated character law for H_N is

$$b_t = e^{-t} \sum_{k\in\mathbb{Z}} \delta_k \, f_k(t/2)$$

where f_k is the Bessel function of the first kind:

$$f_k(t) = \sum_{p=0}^{\infty} \frac{t^{|k|+2p}}{(|k|+p)!p!}$$

Due to this fact, we call b_t Bessel law, of parameter t.

Real reflections 4/4

Theorem. The Bessel laws b_t have the semigroup property

$$b_s * b_t = b_{s+t}$$

with respect to the usual convolution of real measures.

Theorem. The Bessel laws are compound Poisson laws,

$$b_t = \mathrm{law}(a - b)$$

with a, b being independent, both following the Poisson law p_t.

Proofs. Similar to the proofs for S_N, using the Fourier transform.

Bessel laws 1/4

Theorem. Given a compactly supported positive measure ν on $\mathbb{R}$, having mass $t = mass(\nu)$, the following limit converges,

$$p_\nu = \lim_{n\to\infty}\left(\left(1-\frac{t}{n}\right)\delta_0 + \frac{1}{n}\nu\right)^{*n}$$

and the measure p_ν is called compound Poisson law. For

$$\nu = \sum_{i=1}^s t_i\delta_{z_i}$$

with $t_i > 0$ and $z_i \in \mathbb{R}$, we have the formula

$$p_\nu = \mathrm{law}\left(\sum_{i=1}^s z_i\alpha_i\right)$$

whenever the variables α_i are Poisson (t_i), independent.

Bessel laws 2/4

Definition. The higher Bessel laws are the compound Poisson laws

$$b_t^s = p_{t\varepsilon_s}$$

with ε_s being the uniform measure on the s-roots of unity.

Comments. By the above, this means that we have:

$$b_t^s = \lim_{n\to\infty}\left(\left(1-\frac{t}{n}\right)\delta_0 + \frac{t}{n}\varepsilon_s\right)^{*n}$$

Equivalently, we have the following formula,

$$b_t^s = \mathrm{law}\left(\sum_{r=1}^{s} w^r \alpha_i\right)$$

where $w = e^{2\pi i/s}$, and where $\alpha_i \sim p_t$, independent.

Bessel laws 3/4

Examples.

(1) At $s = 1$ we obtain the Poisson laws p_t.

(2) At $s = 2$ we obtain the Bessel laws b_t.

(3) At $s = 3, 4, \ldots$ we obtain certain discrete complex measures.

(4) At $s = \infty$ we obtain certain complex measures B_t.

Bessel laws 4/4

Theorem. The Fourier transform of b_t^s is given by:

$$F_{b_t^s}(y) = \exp\left(t\sum_{r=1}^{s}(e^{iw^r y} - 1)\right)$$

Theorem. The Bessel laws for a convolution semigroup:

$$b_t^s * b_{t'}^s = b_{t+t'}^s$$

Proofs. The first formula is clear from the $b_t^s = \mathrm{law}\left(\sum_{r=1}^s w^r \alpha_i\right)$ interpretation, and the second formula follows from it.

Complex reflections 1/4

Definition. The reflection group H_N^s, depending on parameters

$$N\in\mathbb N\quad,\quad s\in\mathbb N\cup\{\infty\}$$

is the group of $N\times N$ matrices with entries in

$$\mathbb Z_s\cup\{0\}$$

having one nonzero entry on each row and each column.

Examples. At $s=1$ we have the symmetric group $S_N\subset O_N$.
At $s=2$ we have the hyperoctahedral group $H_N\subset O_N$.
At $s=3,4,\ldots$ we have a certain finite subgroup $H_N^s\subset U_N$.
At $s=\infty$ we have a certain infinite subgroup $K_N\subset U_N$.

Complex reflections 2/4

Theorem. The laws of truncated characters for H_N^s are

$$\mathrm{law}(\chi_t) \simeq b_t^s$$

for any $t \in (0,1]$, in the $N \to \infty$ limit.

Proof. Inclusion-exclusion principle, exactly as for S_N, but this time with the permutations $\sigma \in S_N$ being decorated by signs $\varepsilon \in \mathbb{Z}_s^N$.

Remark. This extends and unifies all our previous results.

Complex reflections 3/4

In the order to further extend all this, a first idea would be to look at the general series of complex reflection groups:

$$H_N^{sd} = \left\{ U \in H_N^s \middle| \det U \in \mathbb{Z}_d \right\}$$

However, this does not seem to bring new laws, at least at order 0. The study of the fluctuations is an interesting problem.

Complex reflections 4/4

Another type of extension comes by staying with H_N^s, but looking at the fluctuations of the characters

$$g \to Tr(g)$$

or of the truncated characters

$$g \to \sum_{i=1}^{[tN]} g_{ii} \quad , \quad t \in (0,1]$$

or of the Diaconis-Shahshahani variables

$$g \to Tr(g^k) \quad , \quad k \in \mathbb{N}$$

and so on. Things here are quite well understood at $s = 1, 2$.

Representations of compact groups

Teo Banica

"Introduction to matrix groups", 5/6

08/20

Representations 1/3

Definition. Given a closed subgroup $G \subset U_N$, its representations are the continuous morphisms into unitary groups:

$$\rho : G \to U_n$$

As a basic example, we have the embedding $G \subset U_N$, called fundamental representation, and denoted π.

Comment. We will assume that our representations are "smooth", in the sense that their coefficients are polynomials of g_{ij}.

Representations 2/3

Definition. The representations of G are subject to:

(1) Making sums: $\rho+\nu:g\to diag(\rho(g),\nu(g))$.

(2) Making products: $\rho\otimes\nu:g\to\rho(g)\otimes\nu(g)$.

(3) Taking conjugates: $\bar{\rho}:g\to\overline{\rho(g)}$.

Definition. Given $G\subset_\pi U_N$, its Peter-Weyl representations

$$\pi^{\otimes k}\quad,\quad k=\circ\bullet\bullet\circ\ldots$$

are the representations obtained by tensoring $\pi,\bar{\pi}$.

Representations 3/3

Definition. Given $\rho : G \to U_n$ and $\nu : G \to U_m$, we set:

$$Hom(\rho, \nu) = \left\{ T \in M_{m\times n}(\mathbb{C}) \middle| T\rho(g) = \nu(g)T \right\}$$

and we use the following conventions:

(1) $Fix(\rho) = Hom(1, \rho)$ and $End(\rho) = Hom(\rho, \rho)$.

(2) $\rho \sim \nu$ when $Hom(\rho, \nu)$ contains an invertible element.

(3) ρ is called irreducible, $\rho \in Irr(G)$, when $End(\rho) = \mathbb{C}1$.

Definition. Given $G \subset_\pi U_N$, the collection of vector spaces

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

with $k, l = \circ \bullet \bullet \circ \ldots$ is called Tannakian category of G.

Peter-Weyl 1/7

Theorem (PW1). Any representation $\rho : G \to U_n$ decomposes as

$$\rho = \rho_1 + \ldots + \rho_k$$

direct sum of irreducible representations.

Proof. Consider the intertwiner algebra of our representation:

$$A = End(\rho) \subset M_n(\mathbb{C})$$

By writing its unit as $1 = q_1 + \ldots + q_k$, with q_i being minimal projections, we obtain a decomposition as follows:

$$A = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$$

We can now define a subrepresentation ρ_i by restricting ρ to the space $Im(q_i)$, which is invariant, and the result follows.

Peter-Weyl 2/7

Theorem (PW2). Any irreducible representation $\rho : G \to U_n$ appears inside a certain Peter-Weyl representation $\pi^{\otimes k}$.

Proof. Given a representation $\rho : G \to U_n$, consider its space of coefficients, $C_\rho = span(g \to \rho(g)_{ij})$. Then $\rho \to C_\rho$ is functorial, mapping subrepresentations into subspaces. We have:

$$< C_\pi >= \sum_k C_{\pi^{\otimes k}}$$

By smoothness, $C_\rho \subset < C_\pi >$, for certain exponents $k_1, \ldots, k_p$:

$$C_\rho \subset C_{\pi^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}}$$

Thus we have $\rho \subset \pi^{\otimes k_1} \oplus \ldots \oplus \pi^{\otimes k_p}$, and PW1 gives the result.

Peter-Weyl 3/7

Theorem. Any closed subgroup $G \subset U_N$ has a Haar measure

$$\mu(gE) = \mu(Eg) = \mu(E)$$

which can be constructed by starting with any probability measure ν, and taking the following Cesàro limit:

$$\mu = \lim_{r\to\infty} \frac{1}{r}\sum_{k=1}^{r} \nu^{*k}$$

Moreover, for any representation $\rho : G \to U_n$, the matrix

$$P = \left(\int_G \rho(g)_{ij}\, dg\right)_{ij}$$

is the projection onto $Fix(\rho) = \{\xi \in \mathbb{C}^n | \rho(g)\xi = \xi\}$.

Peter-Weyl 4/7

Proof. Our first claim is that given any positive mass 1 measure ν on our group G, not necessarily strictly positive, the limit

$$\int_G^\nu f = \lim_{r\to\infty}\frac{1}{r}\sum_{k=1}^r\int_G f(g)d\nu^{*k}(g)$$

exists, and for any representation $\rho : G \to U_n$, the matrix

$$P = \left(\int_G^\nu \rho(g)_{ij}\, dg\right)_{ij}$$

is the projection onto the 1-eigenspace of the matrix:

$$M = \left(\int_G \rho(g)_{ij} d\nu(g)\right)_{ij}$$

This is indeed standard algebra, on the coefficient space C_ρ.

Peter-Weyl 5/7

End of proof. Assuming now that ν is strictly positive, we must prove that $M\xi = \xi$ implies $\xi \in Fix(\rho)$. Let us set:

$$f(g) = \sum_i \left(\sum_j \rho(g)_{ij}\xi_j - \xi_i \right) \overline{\left(\sum_k \rho(g)_{ik}\xi_k - \xi_i \right)}$$

We must prove that $f = 0$. Since $\rho(g)$ is unitary, we obtain:

$$f(g) = 2\Big(||\xi||^2 - Re(< \rho(g)\xi, \xi >) \Big)$$

By using now $M\xi = \xi$, we obtain from this, by integrating:

$$\int_G f(g) d\nu(g) = 0$$

Thus we have $f = 0$, and so $\xi \in Fix(\rho)$, as desired.

Peter-Weyl 6/7

Theorem (PW3). The space $\mathcal{C}(G) = < C_\pi >$ decomposes as

$$\mathcal{C}(G) = \bigoplus_{\rho \in Irr(A)} M_{\dim(\rho)}(\mathbb{C})$$

the summands being pairwise orthogonal with respect to $\int_G$.

Proof. We must prove that for $\rho, \nu \in Irr(G)$ we have:

$$\rho \not\sim \nu \implies C_\rho \perp C_\nu$$

The matrix P given by $P_{ia,jb} = \int_G \rho_{ij} \bar{\nu}_{ab}$ is the projection onto:

$$Fix(\rho \otimes \bar{\nu}) \simeq Hom(\rho, \nu) = \{0\}$$

Thus we have $P = 0$, and this gives the result.

Peter-Weyl 7/7

Theorem (PW4). The characters of irreducible representations

$$\chi_\rho : G \to \mathbb{C} \quad , \quad g \to Tr(\rho(g))$$

belong to the algebra of "smooth central functions"

$$\mathcal{C}(G)_{central} = \left\{ f \in \mathcal{C}(G) \Big| f(gh) = f(hg) \right\}$$

and form an orthonormal basis of it.

Proof. The only tricky assertion is the norm 1 one. But:

$$\int_G \chi_\rho \bar{\chi}_\rho = \sum_{ij} \int_G \rho_{ii} \bar{\rho}_{jj} = \sum_i \frac{1}{N} = 1$$

Here we have used the fact that the integrals $\int_G \rho_{ij} \bar{\rho}_{kl}$ form the orthogonal projection onto $Fix(\rho \otimes \bar{\rho}) \simeq End(\rho) = \mathbb{C}1$.

Easiness 1/3

Theorem. The closed subgroups $G \subset U_N$ are in correspondence with the Tannakian categories $C = (C_{kl})$, via the construction

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

in one sense, and via the construction

$$G = \left\{ g \in U_N \middle| Tg^{\otimes k} = g^{\otimes l} T, \forall T \in C \right\}$$

in the other sense.

Proof. This is something quite technical, basically due to Tannaka and Krein, and heavily using the Peter-Weyl theory.

Easiness 2/3

<u>Definition</u>. A collection of subsets $D(k,l) \subset P(k,l)$ is called a category of partitions when it satisfies:

(1) Stability under the horizontal concatenation, $(\pi, \sigma) \to [\pi\sigma]$.

(2) Stability under vertical concatenation $(\pi, \sigma) \to [^{\sigma}_{\pi}]$ (matching).

(3) Stability under the upside-down turning $*$, with $\circ \leftrightarrow \bullet$.

(4) Each $P(k,k)$ contains the identity partition $|| \ldots ||$.

(5) Both $P(\emptyset, \circ\bullet)$ and $P(\emptyset, \bullet\circ)$ contain the semicircle $\cap$.

Easiness 3/3

Definition. A closed subgroup $G \subset U_N$ is called easy when

$$Hom(\pi^{\otimes k}, \pi^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for a certain category of partitions $D \subset P$, where

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

with $\delta_\pi \in \{0,1\}$ depending on whether the indices fit or not.

Examples 1/2

Theorem. The basic unitary and reflection groups, namely

$$\begin{matrix} O_N & \longrightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \longrightarrow & K_N \end{matrix}$$

are all easy, coming from the following categories of partitions:

$$\begin{matrix} P_2 & \longleftarrow & \mathcal{P}_2 \\ \downarrow & & \downarrow \\ P_{even} & \longleftarrow & \mathcal{P}_{even} \end{matrix}$$

Proof. This result, due to Brauer, and also known as Schur-Weyl duality, comes from Tannaka, by working out the details.

Examples 2/2

In addition to the above, it is known that:

(1) In the continuous case, the bistochastic groups $B_N \subset O_N$ and $C_N \subset U_N$ are easy as well, coming from $P_{12}, \mathcal{P}_{12}$.

(2) In the discrete case, S_N is easy as well, coming from P itself. In fact, the reflection groups H_N^s are all easy, coming from P^s.

(3) Back to the continuous case, SU_2, SO_3 and $Sp_N \subset U_N$ are not easy. However, they are "super-easy" in a suitable sense.

(4) However, the general SO_N, SU_N, and other groups constructed using det, such as H_N^{sd}, are definitely not easy.

Probability on compact groups

Teo Banica

"Introduction to matrix groups", 6/6

08/20

Characters 1/3

Problem. Given a closed subgroup $G \subset U_N$, what is the law of

$$\chi : G \to \mathbb{C} \quad , \quad g \to Tr(g)$$

with respect to the uniform integration over G?

Characters 2/3

<u>Motivation</u>. The moments of χ are the dimensions

$$M_k = \dim(Fix(\pi^{\otimes k}))$$

of the fixed point spaces of tensor powers of $\pi : G \subset U_N$.

<u>Comment</u>. We are mostly interested in the Tannakian category

$$C_{kl} = Hom(\pi^{\otimes k}, \pi^{\otimes l})$$

and by Frobenius, we have identifications as follows:

$$Hom(\pi^{\otimes k}, \pi^{\otimes l}) = Fix(\pi^{\otimes \bar{k}l})$$

Thus, the moments of χ count the dimensions $\dim(C_{kl})$.

Characters 3/3

Version. More generally, we are interested in the truncations

$$\chi_t : G \to \mathbb{C} \quad , \quad g \to \sum_{i=1}^{[tN]} g_{ii}$$

with $t \in (0,1]$ of the main character $\chi = \chi_1$.

Example. For the symmetric group $S_N \subset O_N$ we have

$$\chi \sim p_1$$

Poisson, and more generally $\chi_t \sim p_t$ for any t, with $N \to \infty$.

Finite groups 1/4

Theorem. For the cyclic group $\mathbb{Z}_N \subset O_N$ we have

$$\chi(g) = N\delta_{g0}$$

and the corresponding distribution is a Bernoulli law:

$$law(\chi) = \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\delta_N$$

Proof. The cyclic matrices have 0 on the diagonal, and so trace 0, expect for the identity, having 1 on the diagonal, and trace N.

Remark. The truncated characters and the asymptotics are not interesting. We do not have convolution semigroups.

Finite groups 2/4

Theorem. For the dihedral group $D_N \subset S_N$ we have:

$$law(\chi) = \begin{cases} \left(\frac{3}{4} - \frac{1}{2N}\right)\delta_0 + \frac{1}{4}\delta_2 + \frac{1}{2N}\delta_N & (N\ even) \\ \\ \left(\frac{1}{2} - \frac{1}{2N}\right)\delta_0 + \frac{1}{2}\delta_1 + \frac{1}{2N}\delta_N & (N\ odd) \end{cases}$$

Proof. The dihedral group D_N consists of:

(1) N symmetries, having 1 fixed point when N is odd, and having 0 or 2 fixed points, $50-50$, when N is even.

(2) N rotations, having 0 fixed points, except for the identity, which has N fixed points.

Remark. The truncations and asymptotics are not interesting.

Finite groups 3/4

Theorem. For the symmetric group $S_N \subset O_N$ we have

$$\chi_t(\sigma) = \left\{ i \in \{1, \ldots, [tN]\} \middle| \sigma(i) = i \right\}$$

and we have $law(\chi_t) \simeq p_t$, Poisson laws, with $N \to \infty$.

Proof. By using the inclusion-exclusion principle, we have:

$$P(\chi = 0) = 1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + \frac{(-1)^N}{N!} \simeq \frac{1}{e}$$

The same method gives succesively, by generalizing,

$$P(\chi = k) \simeq \frac{1}{e} \cdot \frac{1}{k!} \quad , \quad P(\chi_t = k) \simeq \frac{1}{e^t} \cdot \frac{t^k}{k!}$$

so we obtain in the $N \to \infty$ limit the Poisson laws p_t.

Finite groups 4/4

Theorem. For the complex reflection groups

$$H_N^s = \mathbb{Z}_s \wr S_N$$

we have $law(\chi_t) \simeq b_t^s$, Bessel laws, with $N \to \infty$.

Proof. The elements of H_N^s being usual permutations $\sigma \in S_N$ "decorated" with signs $\varepsilon \in \mathbb{Z}_s^N$, we can use the same method as before, inclusion-exclusion, and with $N \to \infty$ we are led to

$$b_t^s = \pi_{t\varepsilon_s}$$

compound Poisson laws, with ε_s being the uniform measure on $\mathbb{Z}_s$, which are called Bessel laws, due to the fact that at $s = 2$ the density is the Bessel function of the first kind.

Lie groups 1/4

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:

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

These laws appear via the Central Limit Theorem (CLT).

Lie groups 2/4

Theorem. The moments of the normal laws are

$$M_k(g_t) = t^{k/2} \times k!!$$

where $k!! = 1.3.5\ldots(k-1)$, with $k!! = 0$ when k is odd.

Proof. We have the following computation:

$$\begin{aligned} M_k &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} x^k e^{-x^2/2t}dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (tx^{k-1})\left(-e^{-x^2/2t}\right)' dx \\ &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} t(k-1)x^{k-2}e^{-x^2/2t}dx \end{aligned}$$

We obtain $M_k = t(k-1)M_{k-2}$, which gives the result.

Lie groups 3/4

Theorem. For the orthogonal group O_N we have

$$law(\chi) \simeq g_1$$

with $N \to \infty$.

Proof. By using the Brauer easiness result, we have:

$$\begin{aligned} M_k(\chi) &= \dim(Fix(\pi^{\otimes k})) \\ &= \dim(span(T_\pi | \pi \in P_2(k))) \\ &\simeq |P_2(k)| \\ &= k!! \end{aligned}$$

Thus, the main character χ has the same moments as g_1.

Lie groups 4/4

The other classical Lie groups can be investigated by using the same method, and the asymptotic law of χ is as follows:

(1) For U_N we obtain the complex Gaussian law G_1. The proof is similar, by using $M_k(G_1) = |\mathcal{P}_2(k)|$.

(2) For the bistochastic groups $B_N \subset O_N$ and $C_N \subset U_N$ we obtain shifted versions of g_1, G_1.

(3) The symplectic group $Sp_N \subset U_N$ is not exactly easy, but rather "super-easy", and we obtain the Gaussian law g_1.

Truncation 1/4

Theorem. The Haar integration over $G \subset_\pi U_N$ is given by

$$\int_G g_{i_1 j_1}^{s_1} \ldots g_{i_k j_k}^{s_k} dg = \sum_{\sigma, \tau \in D_k} \delta_\sigma(i) \delta_\tau(j) W_k(\sigma, \tau)$$

where D_k is a basis of $Fix(\pi^{\otimes k})$, $\delta_\sigma(i) = < \sigma, e_{i_1} \otimes \ldots \otimes e_{i_k} >$, and $W_k = G_k^{-1}$ is the inverse of $G_k(\sigma, \tau) = < \sigma, \tau >$.

Proof. The integrals in the statement form the projection P onto $Fix(\pi^{\otimes k}) = span(D_k)$. Consider the following linear map:

$$E(x) = \sum_{\sigma \in D_k} < x, \sigma > \sigma$$

By linear algebra we have $P = WE$, where W is the inverse on $span(D_k)$ of the restriction of E, and this gives the result.

Truncation 2/4

Theorem. For an easy group $G_N \subset U_N$, coming from a category of partitions $D = (D(k,l))$, we have

$$\int_{G_N} g_{i_1 j_1}^{s_1} \ldots g_{i_k j_k}^{s_k} dg = \sum_{\sigma,\tau \in D(k)} \delta_\sigma(i)\delta_\tau(j) W_{kN}(\sigma,\tau)$$

where $D(k) = D(\emptyset, k)$, δ are usual Kronecker symbols, and $W_{kN} = G_{kN}^{-1}$ is the inverse of $G_{kN}(\sigma,\tau) = N^{|\sigma \vee \tau|}$.

Proof. The vectors associated to partitions are given by:

$$T_\sigma(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\sigma \begin{pmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_l \end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

Thus the Gram matrix and Kronecker symbols are those above.

Truncation 3/4

Application. We have the following computation,

$$\begin{aligned}
&\int_{G_N}(g_{11}+\ldots+g_{ss})^k\,dg\\
=&\sum_{i_1=1}^s\ldots\sum_{i_k=1}^s\int_{G_N}g_{i_1i_1}\ldots g_{i_ki_k}\,dg\\
=&\sum_{\sigma,\tau\in D(k)}W_{kN}(\sigma,\tau)\sum_{i_1=1}^s\ldots\sum_{i_k=1}^s\delta_\sigma(i)\delta_\tau(i)\\
=&\sum_{\sigma,\tau\in D(k)}W_{kN}(\sigma,\tau)G_{ks}(\tau,\sigma)\\
=&\,Tr(W_{kN}G_{ks})
\end{aligned}$$

and the $s=[tN]\to\infty$ asymptotics can be worked out.

Truncation 4/4

Theorem. The truncated characters χ_t for the main unitary and reflection groups are as follows, in the $N \to \infty$ limit,

$$\begin{array}{ccc} O_N & \rightarrow & U_N \\ \uparrow & & \uparrow \\ H_N & \rightarrow & K_N \end{array} \qquad \sim \qquad \begin{array}{ccc} g_t & \cdots & G_t \\ \vdots & & \vdots \\ b_t & \cdots & B_t \end{array}$$

and we have independence results as well, with $N \to \infty$.

Proof. In the discrete case, this is something that we already know. In general, this follows by using the above results.

References 1/4

[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.

References 2/4

[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 3/4

[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).

References 4/4

[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.