Numerical experiments and random matrices

Francesco Mezzadri

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK

There are two types of random matrices that one might be interested in generating:

1. Matrices from the gaussian ensembles: GUE, GOE, GSE, etc.)
2. Matrices from the circular ensembles and the classical compact groups: $\mathrm{U}(N)$, $\mathrm{O}(N)$, $\mathrm{Sp}(2N)$, COE ($\mathrm{U}(N)/\mathrm{O}(N)$), CSE ($\mathrm{U}(N)/\mathrm{Sp}(2N)$).

1. Gaussian ensembles: independent matrix elements are statistically uncorrelated. The rest are determined by simple relations like $h_{jk} = \overline{h}_{kj}$.
2. Circular ensembles are more subtle: the correlations among matrix elements are complicated.

First question: How do we generate a random unitary with probability distribution given by Haar Measure on $\mathrm{U}(N)$?

Recipe:

1. Take an $N \times N$ complex matrix $Z = (z_{jk})$ whose entries are *complex standard normal random variables:*

$$\operatorname{Re} z_{jk} \sim N(0, 1/2) \quad \text{and} \quad \operatorname{Im} z_{jk} \sim N(0, 1/2).$$

2. Apply Gram-Schmidt's decomposition to the column of Z.

3. The resulting matrix U is unitary by definition:

$$\sum_{j=1}^{N} \overline{u}_{jk} u_{jl} = \delta_{kl}.$$

4. Theorem: *U is distributed according to Haar measure on $\mathrm{U}(N)$.*

Problem: Gram-Schimdt's algorithm is numerically poorly stable.

Gram-Schmidt's algorithm:

$$\mathbf{u}_1 = \mathbf{z}_1$$

$$\mathbf{u}_2 = \mathbf{z}_2 - \frac{(\mathbf{u}_1, \mathbf{z}_2)}{(\mathbf{u}_1, \mathbf{u}_1)}\mathbf{u}_1$$

$$\vdots$$

$$\mathbf{u}_n = \mathbf{z}_n - \sum_{j=1}^{n-1} \frac{(\mathbf{u}_j, \mathbf{z}_n)}{(\mathbf{u}_j, \mathbf{u}_j)}\mathbf{u}_j$$

$$\vdots$$

$$\mathbf{e}_1 = \frac{\mathbf{u}_1}{\|\mathbf{u}_1\|}, \quad \mathbf{e}_2 = \frac{\mathbf{u}_2}{\|\mathbf{u}_2\|}, \ldots, \quad \mathbf{e}_n = \frac{\mathbf{u}_n}{\|\mathbf{u}_n\|}, \ldots$$

Gram-Schmidt is a way of realizing the QR *decomposition.*

Exsercise: Prove the following

Theorem. *If $X = (x_{jk})$ is an $m \times n$ matrix (real or complex) whose n columns are linearly independent (i.e. its rank is n), it is always possible to factorize it into the product*

$$X = QR,$$

where $Q = (q_{jk})$ is an $m \times n$ matrix whose columns are n orthonormal vectors and R is invertible and upper-triangular, i.e.

$$R = \begin{pmatrix} r_{11} & r_{12} & r_{13} & \cdots & r_{1n} \\ 0 & r_{22} & r_{23} & \cdots & r_{2n} \\ 0 & 0 & r_{33} & \cdots & r_{3n} \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r_{nn} \end{pmatrix}$$

with $\det(R) \neq 0$.

Every computer linear algebra package has a routine that implements the QR factorization (Householder reflections).

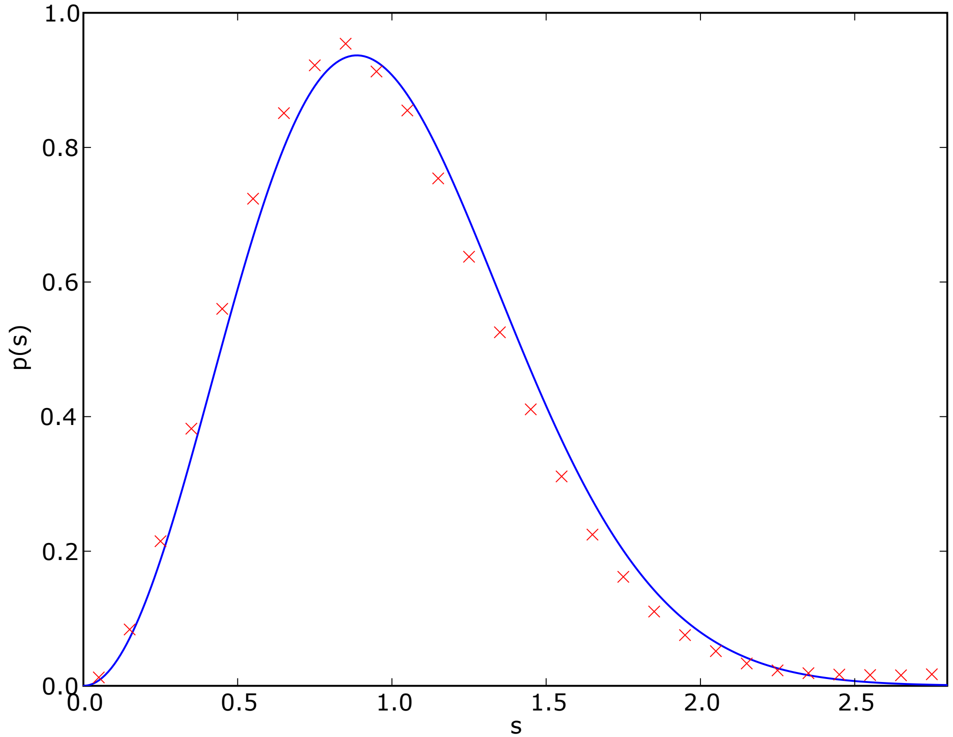

Figure 1: Spacing distribution of 10^5 50×50 random unitary matrices obtained using the 'wrong' QR factorization.

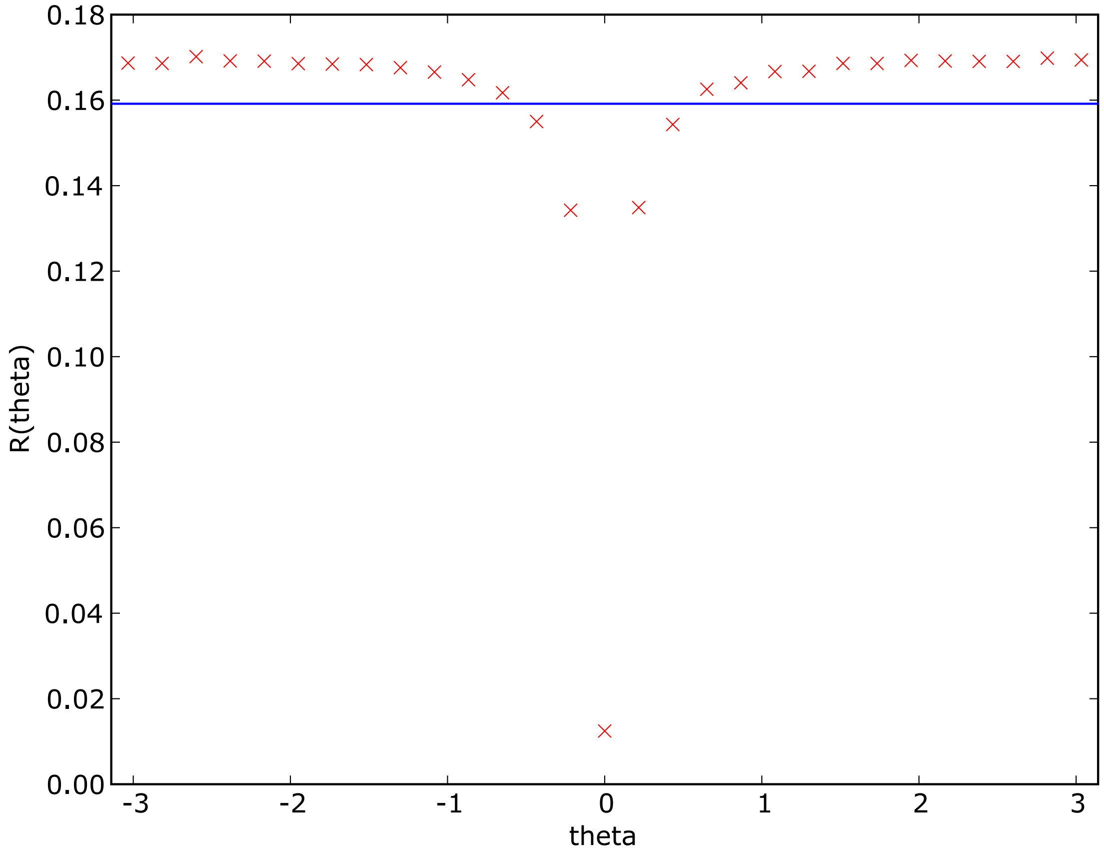

Figure 2: One-level density of 10^5 50×50 random unitary matrices obtained using the 'wrong' QR factorization.

Two possibilities:

1. Applying Gram-Schmidt's decomposition to a complex matrix whose elements are complex standard normal random variables does not yield a random matrix whose distribution is given by Haar measure.
2. There is something wrong in applying the black box routine of the QR decomposition that standard linear algebra packages have.

- The first statement is wrong.
- The second one is correct.

Theorem 1. *Let $Z = (z_{jk})$ a complex matrix whose elements are i.i.d. complex standard normal random variables. The probability distribution of the unitary matrix obtained by applying Gram-Schmidt's orthonormalization to the columns of Z is Haar measure on $\mathrm{U}(N)$.*

Proof. The p.d.f. of a single matrix entry is

$$p(z_{jk}) = \frac{1}{\pi} e^{-|z_{jk}|^2}.$$

Thus, the j.p.d.f for the matrix elements of Z is

$$P(Z) = \frac{1}{\pi^{N^2}} \prod_{j,k=1}^{N} e^{-|z_{jk}|^2} = \frac{1}{\pi^{N^2}} \exp\left(- \sum_{j,k=1}^{N} |z_{jk}|^2 \right)$$

$$= \boxed{\frac{1}{\pi^{N^2}} \exp\left(\operatorname{Tr} Z Z^*\right).}$$

Let us denote

$$dZ = \prod_{j,k=1}^{N} d\,\mathrm{Re}\,(z_{jk})\,d\,\mathrm{Im}\,(z_{jk}) \quad \text{and} \quad d\mu(Z) = P(Z)dZ.$$

Let $U \in \mathrm{U}(N)$. We have

$$d\mu(UZ) = d\mu(Z).$$

It is trivial that

$$P(UZ) = \frac{1}{\pi^{N^2}} \exp\left(-\,\mathrm{Tr}\,UZZ^*U^*\right) = \frac{1}{\pi^{N^2}} \exp\left(-\,\mathrm{Tr}\,ZZ^*\right).$$

Furthermore, the Jacobian of

$$Z \mapsto UZ$$

is one. **Exercise:** Prove this statement.

Exercise. Let $X \in \mathbb{C}^{m\times n}$. Prove that the Jacobian of the transformation

$$X \mapsto AXB,$$

where $A \in \mathbb{C}^{m\times m}$ and $B \in \mathbb{C}^{n\times n}$ is

$$\left|\det(A)^n \det(B)^m\right|^2 .$$

Hint. You first need to show that

$$\det(A \otimes B) = \det(A)^n \det(B)^m$$

by proving that

$$(A \otimes D) \cdot (C \otimes B) = (A \cdot C) \otimes (D \cdot B)\,,$$

where $A, C \in \mathbb{C}^{m\times m}$ and $B, D \in \mathbb{C}^{n\times n}$. Then set $D = I_n$ and $C = I_m$.

Main steps:

1. $d\mu(UZ) = d\mu(Z)$.

2. Grahm-Schmidt's orthonormalization defines a single-valued map $\mathrm{G}(N, \mathbb{C}) \longrightarrow \mathrm{U}(N) \times \mathrm{T}(N)$ defined by

$$Z = QR. \tag{1}$$

3. Thus we have

$$\boxed{d\mu(Z) = d\tilde{\mu}(Q, R).}$$

where $d\tilde{\mu}$ is a measure on some subset of $\mathrm{U}(N) \times \mathrm{T}(N)$, $\mathrm{T}(N)$ being the group of invertible upper triangular matrices.

4. Since $(U\mathbf{u}_j, U\mathbf{z}_j) = (\mathbf{u}_j, \mathbf{z}_j)$ applying Gram-Schmidt to UZ gives

$$UZ = UQR$$

with the same R as in (1).

Step 4 is crucial:

(a) The map $\mathrm{G}(N, \mathbb{C}) \longrightarrow \mathrm{U}(N) \times \mathrm{T}(N)$ is surjective onto $\mathrm{U}(N)$.

(b) We have

$$d\mu(UZ) \stackrel{1}{=} d\mu(Z) \stackrel{3}{=} d\tilde{\mu}(Q, R) \boxed{\stackrel{4}{=} d\tilde{\mu}(UQ, R) = d\mu_{\mathrm{Haar}}(Q) d\mu(R).}$$

The last passage follows from the uniqueness of Haar measure

- ***The QR factorization is not unique:*** given $Z \in \mathrm{GL}(N, \mathbb{C})$ there are an infinite number of pairs $(Q, R) \in \mathrm{U}(N) \times \mathrm{T}(N)$ such that $Z = QR$.
- An arbitrary factorization algorithm that factorizes Z as QR may not factorize UZ as $UZ = UQR$ with the same R.

This is what goes wrong with standard QR routines (Householder reflections algorithm): step 1–3 hold ***but not 4.***

Problem:

- Gram-Schmidt's orthonormalization is not numerically stable.
- QR factorization routines in standard linear algebra packages do not produce matrices distributed with Haar measure.

Let $\Lambda(N) = \mathrm{U}(1) \times \cdots \times \mathrm{U}(1)$ the maximal torus of $\mathrm{U}(N)$.

$\Lambda(N)$ is the set of all the matrices

$$D = \begin{pmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_N} \end{pmatrix}$$

If $Q' = QD$ and $R' = D^{-1}R$ then

$$Z = QR = Q'R'.$$

Let $\Gamma(N) = T(N)/\Lambda(N)$, that is $\Gamma(N)$ is the set of all the equivalence classes $[R]$ defined by

$$R \sim R' \quad \text{if } R' = DR \text{ for some } D \in \Lambda(N).$$

Exercise: Prove the following

Corollary. *The QR factorization defines a bijective map*

$$\mathrm{QR} : \mathrm{GL}(N, \mathbb{C}) \longrightarrow \mathrm{U}(N) \times \Gamma(N).$$

Thus, we have

$$d\mu(Z) = d\mu_{\mathrm{U}(N)\times\Gamma(N)}(Q, \gamma),$$

for $Q \in \mathrm{U}(N)$ and $\gamma \in \Gamma(N)$.

Then, step 4 in Theorem 1 holds if we chose a set of representatives of $\Gamma(N)$ such that if

$$Z \mapsto (Q, R) \quad \text{then} \quad UZ \mapsto (UQ, R)$$

with the same R for both Z and UZ.

One possible choice of such set of representatives is given by the set of all upper-triangular matrices whose elements on the main diagonal ***are all real and strictly positive.***

Exercise: Prove the statement in the blue box.

New recipe:

1. Take an $N \times N$ complex matrix $Z = (z_{jk})$ whose entries are complex standard normal random variables.

2. Feed Z into ***any*** QR factorization routine and let the pair $Q = (q_{jk})$ and $R = (r_{jk})$ be the output, i.e. $Z = QR$

3. Create the following diagonal matrix

$$D = \begin{pmatrix} \frac{r_{11}}{|r_{11}|} & & \\ & \ddots & \\ & & \frac{r_{NN}}{|r_{NN}|} \end{pmatrix},$$

4. ***The probability distribution of the unitary matrix $Q' = QD$ is Haar measure.***

The QR decomposition to choose is $Z = Q'R'$, where $R' = D^{-1}R$ belongs to the correct set of representatives of $\Gamma(N)$.

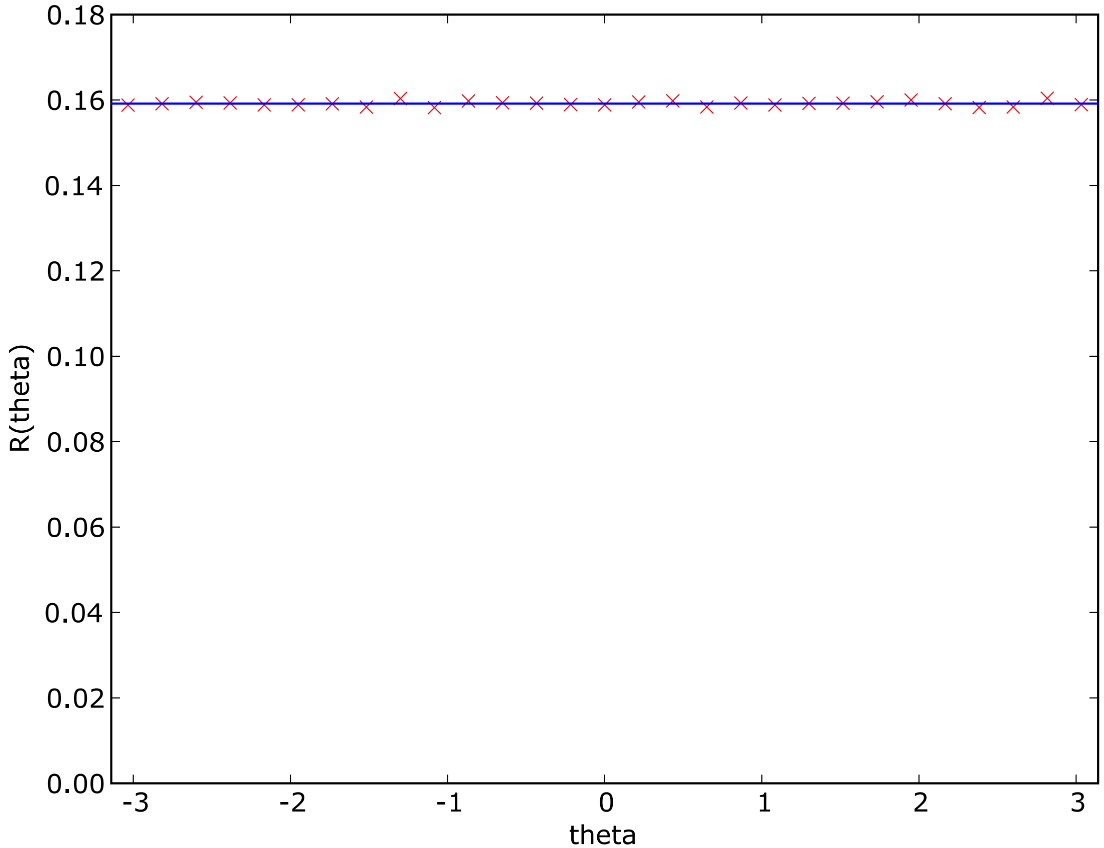

Figure 3: One-level density of 10^5 50×50 random unitary matrices obtained using the 'right' QR factorization.

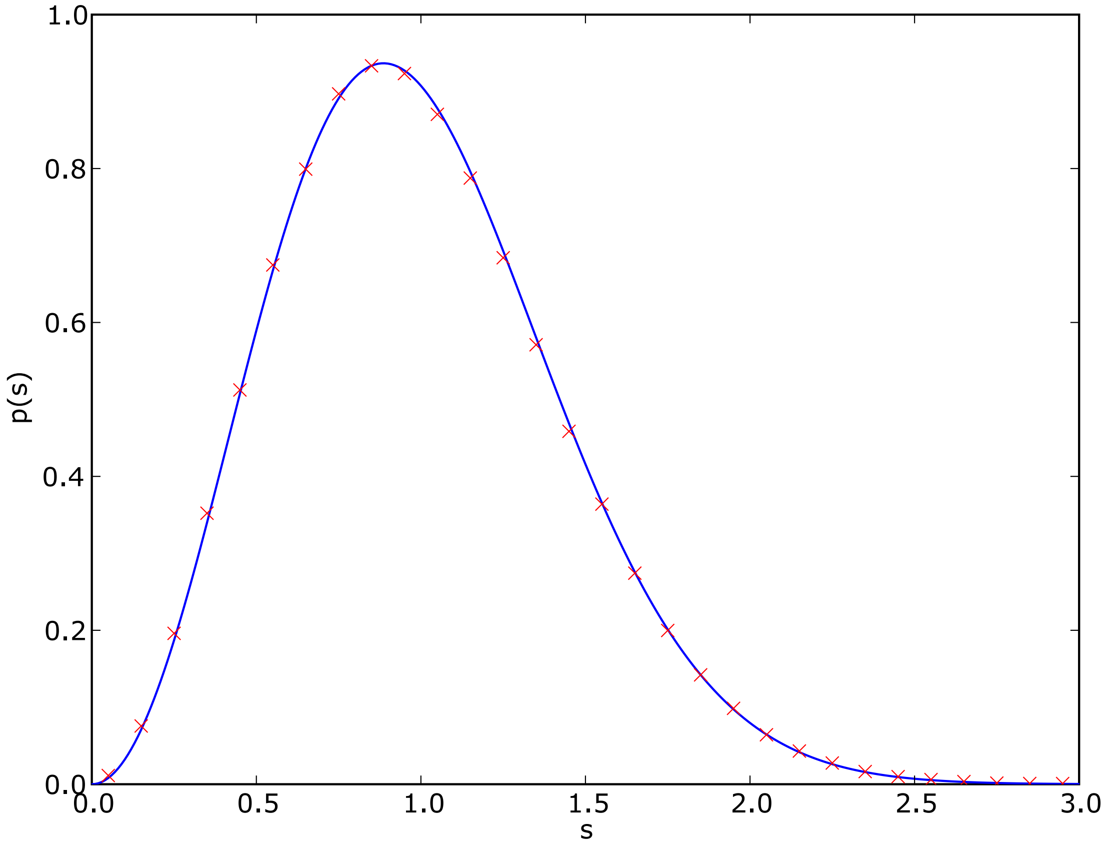

Figure 4: Spacing distribution of 10^5 50×50 random unitary matrices obtained using the 'right' QR factorization.

Exercise:

Take your favorite computer linear algebra package and write a code to generate random matrices distributed with Haar measure.

PS. If it is longer than ten lines, you are doing something wrong.

> The recipe for generating random orthogonal matrices with distribution given by Haar measure on $\mathrm{O}(N)$ is identical, except that you start by generating matrices in $\mathrm{GL}(N,\mathbb{R})$ whose elements are *real* standard normal random variables.

Generating random matrices in Sp($2N$)

- The group Sp($2N$) is the subgroup of U($2N$) whose elements satisfy the relation
$$SJS^t = J,$$
where J is the matrix
$$J = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}.$$

- It is often convenient to express their properties using the algebra of *Hamilton's quaternions, denoted by* $\mathbb{H}$.

- A quaternion q is a linear combination

$$q = a1 + bi + cj + dk,$$

where $a, b, c, d \in \mathbb{R}$ and

$$i^2 = j^2 = k^2 = ijk = -1.$$

- The conjugate $\overline{q}$ of q is

$$\overline{q} = a1 - bi - cj - dk.$$

- The norm of a quaternion is

$$\|q\|^2 = q\overline{q} = a^2 + b^2 + c^2 + d^2.$$

- Note that in general if $p \neq q$,

$$\overline{pq} = \overline{q}\,\overline{p}.$$

- The smallest irreducible representation of the quaternion units is

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

- By setting $z = a + ib$ and $w = c + id$

$$q \mapsto \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \quad \text{and} \quad \overline{q} \mapsto \begin{pmatrix} \overline{z} & -w \\ \overline{w} & z \end{pmatrix}$$

- Any element in $\mathrm{GL}(N, \mathbb{H})$ has a matrix representation in $\mathrm{GL}(2N, \mathbb{C})$.

- If $S \in \mathrm{GL}(N, \mathbb{H})$ we define the conjugate transpose $S^* = (s^*_{jk})$ by

$$s^*_{jk} = \overline{s}_{kj}.$$

Exercise:

Let $A \in \mathrm{GL}(2N, \mathbb{C})$ be the representation of $S \in \mathrm{GL}(N, \mathbb{H})$. Show that the relation

$$SS^* = I_N$$

is equivalent to

$$AJA^t = J.$$

Let $\mathbf{v} = (v_1, \ldots, v_N)$ a vector of quaternions. Define a bilinear map (scalar product) $\mathbb{H}^N \times \mathbb{H}^N \longrightarrow \mathbb{H}$ by

$$\langle v, w \rangle = \sum_{j=1}^{N} \overline{v}_j \, w_j$$

Exercise:

Show that

1. $\langle \mathbf{v}, \mathbf{w} \rangle = \overline{\langle \mathbf{w}, \mathbf{v} \rangle}$;
2. $\langle \mathbf{v}, \mathbf{w} + \mathbf{z} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{z} \rangle$;
3. $\langle \mathbf{v}, \mathbf{v} \rangle \in \mathbb{R}$ and $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$, where the equality holds if and only if $\mathbf{v} = \mathbf{0}$.

The symplectic group $\mathrm{Sp}(2N)$ is the group of isometries in $\mathbb{H}^N$. In other words

$$\langle Sv, Sw \rangle = \langle v, w \rangle \, .$$

Gram-Schmidt can be generalized to quaternion matrices:

$$\mathbf{u}_1 = \mathbf{z}_1$$

$$\mathbf{u}_2 = \mathbf{z}_2 - \mathbf{u}_1 \frac{\langle \mathbf{u}_1, \mathbf{z}_2 \rangle}{\langle \mathbf{u}_1, \mathbf{u}_1 \rangle}$$

$$\vdots$$

$$\mathbf{u}_n = \mathbf{z}_n - \sum_{j=1}^{n-1} \mathbf{u}_j \frac{\langle \mathbf{u}_j, \mathbf{z}_n \rangle}{\langle \mathbf{u}_j, \mathbf{u}_j \rangle}$$

$$\vdots$$

$$\langle \mathbf{u}_1, \mathbf{u}_2 \rangle = \left\langle \mathbf{u}_1, \mathbf{z}_2 - \mathbf{u}_1 \frac{\langle \mathbf{u}_1, \mathbf{z}_2 \rangle}{\langle \mathbf{u}_1, \mathbf{u}_1 \rangle} \right\rangle = \langle \mathbf{u}_1, \mathbf{z}_2 \rangle - \langle \mathbf{u}_1, \mathbf{u}_1 \rangle \frac{\langle \mathbf{u}_1, \mathbf{z}_2 \rangle}{\langle \mathbf{u}_1, \mathbf{u}_1 \rangle}$$
$$= \langle \mathbf{u}_1, \mathbf{z}_2 \rangle - \langle \mathbf{u}_1, \mathbf{z}_2 \rangle = 0.$$

The COE ensemble

The COE is the ensemble of **unitary symmetric matrices** *whose probability distribution is invariant under the transformation* $S \mapsto USU^t$ *for any* $U \in \mathrm{U}(N)$.

An alternative definition is the following:

The COE ensemble is the symmetric space $\mathrm{U}(N)/\mathrm{O}(N)$ *with probability measure induced by Haar measure on* $\mathrm{U}(N)$.

Exercise:

Prove that the two definitions of the COE ensemble are equivalent.

Hint. You need to use the fact that that every unitary symmetric matrix can be written as $S = UU^t$ for $U \in \mathrm{U}(N)$.

Recipe to generate random matrices in the COE:

- Generate a unitary matrix U distributed with Haar measure.
- Compute $S = UU^t$.

The CSE ensemble

- Let us consider *complex* quaternions:

$$q = a1 + bi + cj + dk,$$

where now $a, b, c, d \in \mathbb{C}$.

- There is a one-to-one correspondence between $2N \times 2N$ complex matrices and $N \times N$ complex quaternion matrices.
- A quaternion matrix S is *self-dual* if

$$S = S^*$$

- Let A the $2N \times 2N$ matrix representation of S. If S is self-dual we call A self-dual too and obeys the relation

$$A = -JA^tJ,$$

where $J = \left(\begin{smallmatrix} 0 & I_N \\ -I_N & 0 \end{smallmatrix} \right)$.

Let S and T denote the quaternion representations of $U, W \in \mathrm{U}(2N)$.

The CSE is the ensemble of **self-dual unitary matrices** *whose distribution is invariant under the transformation* $S \mapsto TST^*$.

An alternative definition is the following:

The CSE ensemble is the symmetric space $\mathrm{U}(2N)/\mathrm{Sp}(2N)$ *with probability measure induced by Haar measure on* $\mathrm{U}(N)$.

Exercise:

Prove that the two definitions of the CSE ensemble are equivalent.

Hint. You need to use the fact that that every unitary self-dual matrix S can be written as $S = TT^*$ where T is unitary.

Recipe to generate random matrices in the CSE:

- Generate a $2N \times 2N$ unitary matrix U distributed with Haar measure.
- Compute its dual: $V = -JUJ$
- Compute $A = UV$.