UNIVERSITY OF ILLINOIS
URBANA-CHAMPAIGN

Math 595 Representation-theoretic methods in QIT

How to sample from the Haar measure

Felix Leditzky

Fall term 2025

Last update: November 20, 2025

Sampling algorithm

For more details, see [Mez07; Ozo09].

Algorithm to sample a Haar-random unitary $U \in \mathcal{U}_d$.

(i) Let Z be a $(d \times d)$-matrix whose entries are independent complex standard normal random variables: $Z_{ij} \sim (N(0,1) + iN(0,1))/\sqrt{2}$.

(ii) Compute a QR decomposition (Q, R) of Z with Q unitary, R upper-triangular and $Z = QR$.

(iii) Define the matrix $\Lambda = \operatorname{diag}(R_{11}/|R_{11}|, \dots, R_{dd}/|R_{dd}|)$.

(iv) Set $U = Q\Lambda$, which is distributed with Haar measure.

Ginibre ensemble

Ginibre ensemble: complex $(d \times d)$-matrices whose coordinates Z_{ij} are independent and identically distributed (i.i.d.) standard normal complex random variables.

Probability density function of a coordinate: $f(Z_{ij}) = \pi^{-1}\exp(-|Z_{ij}|^2)$.

Joint probability density:

$$f_G(Z) = \prod_{i,j} f(Z_{ij}) = \frac{1}{\pi^{d^2}}\exp\left(\sum_{i,j} |Z_{ij}|^2\right) = \frac{1}{\pi^{d^2}}\exp(-\mathrm{tr}(Z^\dagger Z))$$

$f_G(Z)$ is left- and right-invariant under unitaries:

$$f_G(UZ) = \frac{1}{\pi^{d^2}}\exp(-\mathrm{tr}((UZ)^\dagger(UZ))) = \frac{1}{\pi^{d^2}}\exp(-\mathrm{tr}(Z^\dagger U^\dagger UZ)) = \frac{1}{\pi^{d^2}}\exp(-\mathrm{tr}(Z^\dagger Z))$$

Since $\det(Z \mapsto UZ) = 1$, the measure $\mathrm{d}\mu_G(Z) := f(Z)dZ$ is also U-invariant.

Orthogonalizing a Ginibre matrix

Observation: Singular matrices have measure zero with respect to the Ginibre measure $d\mu_G(Z) := f(Z)dZ$, so $Z \sim d\mu_G(Z)$ is invertible almost surely.

Hence, in the QR decomposition (Q, R) the matrix $R = Q^{-1}Z$ is upper-triangular and invertible. In particular, $R_{ii} \neq 0$.

QR decomposition is not unique, since for any diagonal unitary $\Lambda \in \mathcal{U}_d$ we have $Z = QR = (Q\Lambda)(\Lambda^\dagger R)$, where $Q\Lambda$ is unitary and $\Lambda^\dagger R$ is upper-triangular.

One can **make the QR decomposition unique** by requiring R to have strictly positive (real) diagonal elements, hence multiplying Q by $\Lambda = \mathrm{diag}(R_{11}/|R_{11}|, \ldots, R_{dd}/|R_{dd}|)$ yields a unique QR decomposition.

This process induces a probability measure on unitary matrices that is still left- and right-invariant (see [Ozo09]), and hence equal to the Haar measure.

Unitary designs

Problem in applications: Sampling from the Haar measure is inefficient (in terms of circuit complexity).

Fortunately, we often only need random unitary ensembles whose **first k moments match** those of the Haar measure:

$$\sum_{i=1}^{M} p_i U_i^{\otimes k} X (U_i^\dagger)^{\otimes k} = \int_{\mathcal{U}_d} \mathrm{d}U \, U^{\otimes k} X (U^\dagger)^{\otimes k} \qquad \text{for all } X \in \mathcal{L}(\mathcal{H}). \qquad (*)$$

Such an ensemble of unitaries $(p_i, U_i)_{i=1}^{M}$ is called a **unitary k-design**.

If the relation $(*)$ is only satisfied approximately up to some error ε, then the ensemble is called an **ε-approximate unitary k-design.**

See the presentation on Dec 11!

References

[Mez07] Francesco Mezzadri. **“How to generate random matrices from the classical compact groups”.** English. *Notices of the American Mathematical Society* 54.5 (May 2007), pp. 592–604. arXiv: `math-ph/0609050`.

[Ozo09] Maris Ozols. **“How to generate a random unitary matrix”.** *Unpublished essay* (2009). Available at: `http://home.lu.lv/~sd20008/papers/essays/Random%20unitary%20[paper].pdf`.