Decomposition of measure in RMT applied to integral geometry and number theory

Peter Forrester,

M&S, University of Melbourne

Outline

- Random determinants and volumes of pinned polytopes
- Volumes of affine random simplices
- Blaschke–Petkantschin decomposition of measure
- Random lattices, and lattice reduction

Determinants of non-hermitian random matrices

Method I: Singular values

Introducing the singular value decomposition $X = Q_1 \mathrm{diag}\,(\tau_1, \ldots, \tau_N) Q_2$, where $\{\tau_l\}$ denotes the singular values of X, we have

$$|\det X| = \prod_{l=1}^{N} \tau_l.$$

In the Gaussian case, $X = [\mathrm{N}\,[0,1]]_{N\times N}$, $\{\lambda_l = \tau_l^2\}$ — eigenvalues of $X^T X$ — have joint PDF prop. to

$$\prod_{l=1}^{N} \lambda_l^{-1/2} e^{-\lambda_l/2} \prod_{1\le j<k\le N} |\lambda_k - \lambda_k|, \qquad \lambda_l > 0.$$

Moments of the determinant

Can study the distribution of $\prod_l \lambda_l$ through its moments $\langle \prod_{l=1}^N \lambda_l^s \rangle$. In the Gaussian case, need then to compute the multi-dimensional integral

$$\int_0^\infty d\lambda_1 \cdots \int_0^\infty d\lambda_N \prod_{l=1}^N \lambda_l^{-1/2+s} e^{-\lambda_l} \prod_{1 \le j < k \le N} |\lambda_k - \lambda_j|$$

This is a particular Selberg integral, and so can be evaluated as a product of gamma functions

$$\Big\langle \prod_{l=1}^N \lambda_l^s \Big\rangle = \prod_{j=1}^N \frac{\Gamma(s+j/2)}{\Gamma(j/2)}$$

Let χ_j^2 denote the chi-square distribution with j degrees of freedom. We read off that

$$\Big\langle \prod_{l=1}^N \lambda_l^s \Big\rangle = \prod_{j=1}^N \Big\langle \lambda_j^s \Big\rangle_{\chi_j^2} \quad \iff \quad |\det X|^2 \overset{\mathrm{d}}{=} \prod_{j=1}^N \chi_j^2 .$$

Distribution the determinant

Explanation. Method II: Gram-Schmidt

Write $X = QR$, where R is upper triangular with positive real entries on the diagonal, e.g. $N = 3$, $R = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ 0 & r_{22} & r_{23} \\ 0 & 0 & r_{33} \end{bmatrix}$

We have the change of variables formula

$$(dX) = \prod_{l=1}^{N} r_{ll}^{N-l} (dR)(Q^T dQ)$$

Also

$$e^{-\frac{1}{2}\mathrm{Tr}\, X^T X} = \prod_{1 \le j < k \le N} e^{-\frac{1}{2} r_{jk}^2}, \quad \det X^T X = \prod_{j=1}^{N} r_{jj}^2.$$

Conclusion. Each variable r_{jj}^2 has distribution χ_{N-j+1}^2. Hence

$$|\det X|^2 \stackrel{\mathrm{d}}{=} \prod_{j=1}^{N} \chi_j^2.$$

Volume of a Gaussian random polytope pinned to the origin

In $\mathbb{R}^N$, choose N point from N standard Gaussian vectors $\mathbf{x}_j$. The simplex formed by the convex hull of these points and the origin is a Gaussian random polytope pinned to the origin.

Multiplying this volume by $N!$ gives the volume of a Gaussian random parallelotope Δ (in 2d, parallelogram) formed by the N vectors. We know

$$\mathrm{vol.}\, \Delta = \Big| \det[\mathbf{x}_j]_{j=1}^N \Big| \quad \text{and hence} \quad \Big(\mathrm{vol.}\, \Delta\Big)^2 \overset{\mathrm{d}}{=} \prod_{j=1}^N \chi_j^2.$$

The (Hausdorff) volume of the parallelotope Δ_M formed by $M < N$ vectors in $\mathbb{R}^N$ (e.g. the area of the parallelogram formed by $\mathbf{x}_1$ and $\mathbf{x}_2$ in $\mathbb{R}^3$) is equal to $(\det(X_{N\times M})^T X_{N\times M})^{1/2}$. In the Gaussian case the Gram-Schmidt decomposition gives

$$\Big(\mathrm{vol.}\, \Delta_M\Big)^2 \overset{\mathrm{d}}{=} \prod_{j=1}^M \chi_{N-j+1}^2.$$

Application: Computation of Lypanunov spectrum for Gaussian random matrices

Define the random product matrix $P_m = X_1 X_2 \cdots X_m$ where each X_i is an $N \times N$ matrix independently distributed from a common distribution.

According to the multiplicative ergodic theorem of Oseledec, the limiting matrix $\lim_{m\to\infty}(P^T P)^{1/(2m)}$ is well defined and non-random. Parameterising the eigenvalues as $e^{\mu_1} > \cdots > e^{\mu_N}$, one refers to $\{\mu_j\}$ as the Lyapunov exponents, and Oseledec showed

$$\mu_1 + \cdots + \mu_k = \sup \lim_{m\to\infty} \frac{1}{m} \log \mathrm{vol}_k \{y_1(m), \ldots, y_k(m)\} \quad (k = 1, \ldots, N),$$

where $y_j(m) := P_m y_j(0)$ and the sup operation is over all sets of linearly independent vectors $\{y_j(0)\}$.

For $X_j = \Sigma^{1/2} G_j$, G_j standard Gaussian matrix

$$\mu_1 + \cdots + \mu_k = \Big\langle \log\det\Big((G_{N\times k})^T \Sigma G_{N\times k}\Big)^{1/2} \Big\rangle.$$

Differentiate s-th moment on RHS w.r.t. s, set $s = 0$, to get log.

Beyond the Gaussian case — isotropic ensembles

For isotropic ensembles the distribution of each row of the matrix is dependent on its length only, thus unchanged by rotations.

For example, suppose the random matrix X is formed by choosing each row uniformly from the unit $(N-1)$-sphere. Always, by Gram-Schmidt $(dX) = \prod_{l=1}^{N} r_{ll}^{N-l}(dR)(Q^T dQ)$. The Gram-Schmidt vectors are now uniformly distributed on the unit $(l-1)$-sphere $(l = 1, \ldots, N)$, so each r_{ll}^2 has distribution proportional to $\mathrm{Beta}[1/2, (l-1)/2]$, implying that

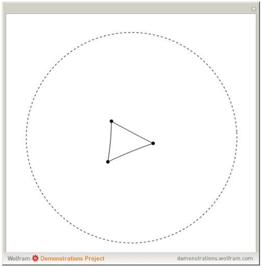
$$|\det X|^2 \overset{\mathrm{d}}{=} \prod_{l=1}^{N} \mathrm{Beta}\left[(N-l+1)/2, (l-1)/2\right].$$

Largest Lyapunov exponent: Sum of squares of r.v. with PDF $\propto (1-x^2)^{(N-3)/2}$. Geometric interpretation for $N = 3$: volume of intersection unit cube and sphere.

$$2\mu_1 = \frac{\pi}{4}\int_0^1 s^{1/2}\log s\,\mathrm{d}s + \frac{\pi}{4}\int_1^2 (3-2s^{1/2})\log s\,\mathrm{d}s + \int_2^3 f_{3,2}(s)\log s\,\mathrm{d}s$$
$$\approx -0.187705.$$

Expected volume of a uniformly random simplex Δ ($N+1$ points in $\mathbb{R}^N$) in a unit ball B_N

E.g. $N = 2$. What is the mean area of a random triangle in the unit disk? Relates to Sylvester's problem: when is the convex hull of 4 points a triangle?



Kingman (1969) gives

$$\frac{1}{\mathrm{vol}\, B_N}\left\langle \mathrm{vol}\, \Delta \right\rangle = 2^{-N}\binom{(N+1)}{(N+1)/2}^{N+1} \Big/ \binom{(N+1)^2}{(N+1)^2/2},$$

For $N = 2$, evaluates to $\frac{35}{48\pi^2}$. Question: What underlies this?

Polar decomposition

E.g. real case. Begin with singular value decomposition

$$\begin{aligned} M_{n\times N} &= U_{n\times N}\mathrm{diag}\,(s_1,\ldots,s_N)V^T_{N\times N} \\ &= UV^T(V\mathrm{diag}\,(s_1,\ldots,s_N)V^T \\ &= QP \end{aligned}$$

where $P = V\mathrm{diag}\,(s_1,\ldots,s_N)V^T = W^{1/2}$, $W = M^TM$ is symmetric.

We have the change of variables formula (from classical RMT)

$$(\mathrm{d}M) = 2^{-N}(\det W)^{\beta(n-N+1)/2-1}\,(\mathrm{d}W)\,\left(Q^\dagger\mathrm{d}Q\right).$$

Polar integration formula (Moghadasi [Bull. Aust. Math. Soc. 2012]

Corollary of the above decomposition of measure:

$$\int_{\mathcal{M}_{n\times N}} g(M)\,\mathrm{d}M = 2^{-N}\int_{\mathcal{V}_{N,n}} \left(Q^\dagger \mathrm{d}Q\right) \int_{W>0} (\mathrm{d}W)\,(\det W)^{\beta(n-N+1)/2-1} \times g(QW^{1/2})$$

Choose $g(M) = f(M^\dagger M)$. RHS integration over W independent of Q. Use the case $n = N$ to now rewrite integration over W. Inserting value of $\int_{\mathcal{V}_{N,n}} \left(Q^\dagger \mathrm{d}Q\right)$ gives

$$\int_{\mathcal{M}^\beta_{n\times N}} f(M^\dagger M)\,(\mathrm{d}M) = \prod_{i=1}^{N} \frac{\sigma_{\beta(n-i+1)}}{\sigma_{\beta(N-i+1)}} \int_{\mathcal{M}^\beta_{N\times N}} f(M^\dagger M)\,\left(\det M^\dagger M\right)^{\beta(n-N)/2}(\mathrm{d}M).$$

(σ_l equals surface area of unit ball in $\mathbb{R}^l$)

Remark: This allows for a "different" computation of the moments of $\det M$ for M Gaussian.

Blaschke-Petkantschin decomposition of measure (Miles version)

Factor

$$Q_{n\times N} = A_{n\times N}\tilde{Q}_{N\times N}$$

Here $A_{n\times N}$ specifies a "reference basis" — an element of the Grassmanian $G_{N,n}$, which is the set of N-dimensional subspaces in $\mathbb{F}^n$. Denote the corresponding invariant measure by $d\omega_{N,n}$.

The polar integration formula (again used twice) implies

$$\int_{M\in\mathcal{M}^{\beta}_{N,n}} g(M)\,(\mathrm{d}M) = \int_{A\in G_{N,n}} \mathrm{d}\omega_{N,n} \int_{M\in\mathcal{M}^{\beta}_{N,N}} (\mathrm{d}M)\, g(AM)\, \left(\det M^{\dagger}M\right)^{\beta(n-N)/2}.$$

Equivalently

$$\prod_{k=1}^{N} \mathrm{d}\mathbf{v}_k^n = \left|\det[\mathbf{v}_k^N]_{k=1}^N\right|^{\beta(n-N)} \prod_{k=1}^{N} \mathrm{d}\mathbf{v}_k^N \mathrm{d}\omega_{N,n}$$

Here $\mathbf{v}_k^N \in (\mathbb{F}_\beta)^N$ is the co-ordinate for $\mathbf{v}_k^n$ in a particular basis.

Affine Blaschke-Petkantschin

Introduce

$$\mathbf{z}_k^n = \mathbf{v}_k^n - \mathbf{v}_0^n$$
$$\mathbf{z}_k^n = B_{n\times N}\mathbf{z}_k^N$$
$$\mathbf{z}_k^N = \mathbf{v}_k^N - \mathbf{v}_0^N$$
$$\mathbf{v}_0^n = B_{n\times N}\mathbf{v}_0^N + \mathbf{r}$$

Here $\mathbf{r}$ is an element of the orthogonal complement of the column space of B, with corresponding volume element $dS_{n-N}^{\perp}$.

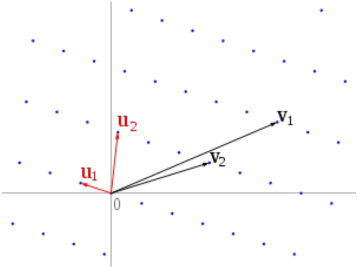
Conclude

$$\prod_{k=0}^{N} \mathrm{d}\mathbf{v}_k^n = \left| \det[\mathbf{v}_k^N - \mathbf{v}_0^N]_{k=1}^N \right|^{\beta(n-N)} \prod_{k=0}^{N} \mathrm{d}\mathbf{v}_k^N \, \mathrm{d}\omega_{N,n}^{\beta} \, \mathrm{d}S_{n-N}^{\perp,\beta}$$

For $\beta = 1$ (real case) Miles used this to generalise the result of Kingman, evaluating, for example, all the moments of vol Δ.

Statistical properties of random lattices (problem in the geometry of numbers)

For $M \in SL_2(\mathbb{R})$ denote the columns by $\vec{v}_1, \vec{v}_2$. They define a basis of $\mathbb{R}^2$. Associated with this basis is the lattice $\left\{\vec{y} : \vec{y} = n_1\mathbf{v}_1 + n_2\mathbf{v}_2, \;\; n_1, n_2 \in \mathbb{Z}\right\}$. Note that a unit cell in the lattice has volume 1.



Question: Let $\vec{v}_1, \vec{v}_2$ be chosen with invariant measure. What are the statistical properties of the reduced basis? What about general dimension d? What can be said about the complex case $M \in SL_2(\mathbb{C})$ with (say) the Gaussian or Eisenstein integers?

Invariant measure for $GL_N(\mathbb{R})$ and $SL_N(\mathbb{R})$

Work of Siegel on the geometry of numbers lead him to consider the invariant measure on $GL_N(\mathbb{R})$,

$$d\mu(M) = \frac{(dM)}{|\det M|^N}$$

Here $(dM) = \prod_{i,j=1}^{N} dM_{i,j}$.

For matrices $A \in SL_N(\mathbb{R})$, Siegel defines the cone λA, $0 < \lambda < 1$, $\lambda A \in GL_N(\mathbb{R})$. From above, the latter has invariant measure equal to the Lebesgue measure (dA). Equivalently, the invariant measure for matrices in $SL_N(\mathbb{R})$ is equal to

$$\delta\Big(1 - \det M\Big)(dM)$$

for $M \in GL_N(\mathbb{R})$.

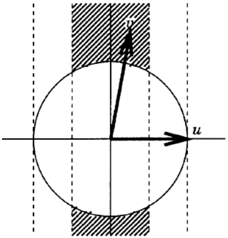
Shortest lattice vector

Basis vectors $\vec{m}_1, \dots, \vec{m}_n$. Want to choose $(n_1, \dots, n_N) \neq \vec{0}$ and $\in \mathbb{Z}^N$ such that $\left| \sum_{j=1}^{N} n_j \vec{m}_j \right|$ is minimum.

Question: What is the distribution of the shortest lattice vector when the basis vectors are chosen with invariant measure?

Can answer this question for $N = 2$.

For $N = 2$ it is easy to show that the shortest vector $\mathbf{u}$ and the second shortest, linearly independent vector $\mathbf{v}$ are characterised by the inequalities $||\mathbf{v}|| \geq ||\mathbf{u}||$, $2|\mathbf{u} \cdot \mathbf{v}| \leq ||\mathbf{u}||^2$, the second being equivalent to $||\mathbf{v} + n\mathbf{u}|| \geq ||\mathbf{v}||$ for all $n \in \mathbb{Z}$.



QR (Gram-Schmidt) decomposition

To align the shortest vector along the x-axis we use the QR decomposition: for $N = 2$

$$\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} \\ 0 & r_{22} \end{bmatrix}$$

with $r_{11} > 0$ and $r_{22} = 1/r_{11}$. Hence $\mathbf{u} = (r_{11}, 0)$ and $\mathbf{v} = (r_{12}, r_{22})$.

Invariant measure factorises according to

$$d\mu(M) = \delta(1 - \prod_{l=1}^{N} r_{ll}) \prod_{l=1}^{N} r_{ll}^{N-l} (dR)(Q^T dQ).$$

For $N = 2$, integrate over r_{22}, and $(Q^T dQ)$. Leaves $2\pi dr_{11} d_{12}$ — flat measure. Inequalities for a reduced lattice read $r_{12}^2 + r_{22}^2 \geq r_{11}^2$, $2|r_{12}| \leq r_{11}$.

The coordinate r_{11} corresponds to the length of the shortest basis vector. Integrating out r_{12} gives its distribution.

Complex case

There are multiple choices for the meaning of integers, e.g. Gaussian, Eisenstein integers.

In the real case, the inequality $2|r_{12}| \leq r_{11}$, rewritten

$$-\frac{1}{2} \leq \frac{r_{12}}{r_{11}} \leq \frac{1}{2}$$

can be interpreted as the values r_{12}/r_{11} closest to the origin in $\mathbb{Z}$. In the complex case, the reduced basis in Gram-Schmidt coordinates requires

$$\mathcal{D}_{\mathbb{Z}[\omega]}\left(\frac{r_{12}^{\mathrm{r}} + i r_{12}^{\mathrm{i}}}{r_{11}}\right) = 0,$$

where $\mathcal{D}_{\mathbb{Z}[\omega]}$ is the so-called lattice quantiser for $\mathbb{Z}[\omega]$, giving the set of values closest to the origin in $Z[\omega]$.

For the Gaussian integers, $|r_{12}^{\mathrm{r}}/r_{11}| \leq 1/2$, $|r_{12}^{\mathrm{i}}/r_{11}| \leq 1/2$. With $x_1 = r_{12}^{\mathrm{r}}/r_{11}$, $x_2 = r_{12}^{\mathrm{i}}/r_{11}$, $x_3 = 1/t_{11}^2$, invariant measure reads

$$\pi^2 \chi_{x_1^2+x_2^2+x_3^2>1} \chi_{|x_1|\leq 1/2} \chi_{|x_2|\leq 1/2} \chi_{x_3>0} \frac{dx_1 dx_2 dx_3}{x_3^3}.$$

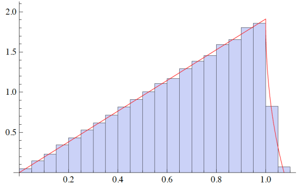
Realisation

For 2d real case, integration over the fundamental domain gives for the PDF of the shortest vector

$$\frac{12}{\pi}\left(\frac{s}{2} - \chi_{s>1}(s^2 - 1/s^2)^{1/2}\right), \qquad 0 < s < (4/3)^{1/4}.$$

Can be illustrated by the following numerical procedure:

1. Generate random matrices M from $\mathrm{SL}_2(\mathbb{R})$ with invariant measure, constrained so that $||M||_{\mathrm{Op}} \leq R$ for some (large) R. For this use the singular value decomposition and the associated decomposition of measure.
2. Apply Lagrange–Gauss lattice reduction to the columns of M, giving the reduced basis.

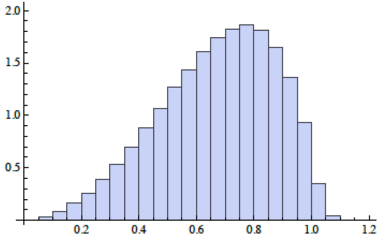


Small distance distribution of shortest lattice vectors for general d

Let $C = \frac{d}{2\zeta(d)} \mathrm{Vol}\,(B_R)\Big|_{R=1}$. To leading order, the Siegel mean value theorem implies the PDF for the length of the shortest lattice vector has leading small s behaviour

$$P(s) = Cs^{d-1}.$$

E.g. $d = 3$, using exact lattice reduction



References

PJF, Lyapunov exponents for products of complex Gaussian matrices, J. Stat. Phys. (2013)

PJF and J. Zhang, 'Lyapunov exponents for some isotropic random matrix ensembles', arXiv:1805.05529

PJF, 'Matrix polar decomposition and generalisations of the Blaschke–Petkantschin formula in integral geometry', arXiv:1701.04505

PJF, 'Volumes for $SL_N(\mathbb{R})$, the Selberg integral and random lattices', Found. Comp. Math. (2018)

PJF and J. Zhang, 'Volumes and distributions for random complex and quaternion lattices' J. Number Th. (2018).