THE CHARACTERISTIC POLYNOMIAL ON COMPACT GROUPS WITH HAAR MEASURE:
SOME EQUALITIES IN LAW

P. BOURGADE, A. NIKEGHBALI, AND A. ROUAULT

Presented by Marc Yor.

Abstract. This note presents some equalities in law for \( Z_N := \det(\text{Id} - G) \), where \( G \) is an element of a subgroup of the set of unitary matrices of size \( N \), endowed with its unique probability Haar measure. Indeed, under some general conditions, \( Z_N \) can be decomposed as a product of independent random variables, whose laws are explicitly known. Our results can be obtained in two ways: either by a recursive decomposition of the Haar measure (Section 1) or by previous results by Killip and Nenciu ([3]) on orthogonal polynomials with respect to some measure on the unit circle (Section 2). This latter method leads naturally to a study of determinants of a class of principal submatrices.

Résumé. Cette note présente quelques égalités en loi pour \( Z_N := \det(\text{Id} - G) \), où \( G \) est un sous-groupe de l’ensemble des matrices unitaires de taille \( N \), muni de son unique mesure de Haar normalisée. En effet, sous des conditions assez générales, \( Z_N \) peut être décomposé comme le produit de variables aléatoires indépendantes, dont on connaît la loi explicitement. Notre résultat peut être obtenu de deux manières : soit par une décomposition récursive de la mesure de Haar (Partie 1) soit en utilisant un résultat de Killip et Nenciu ([3]) à propos des polynômes orthogonaux relativement à une certaine mesure sur le cercle unité (Partie 2). Cette dernière méthode nous conduit naturellement à l’étude des déterminants de certaines sous-matrices.

In this note, \( \langle a, b \rangle \) denotes the Hermitian product of two elements \( a \) and \( b \) in \( \mathbb{C}^N \) (the dimension is implicit).

1. A recursive decomposition, consequences

1.1. The general equality in law. Let \( G \) be a subgroup of \( U(N) \), the group of unitary matrices of size \( N \). Let \( (e_1, \ldots, e_N) \) be an orthonormal basis of \( \mathbb{C}^N \) and \( \mathcal{H} := \{ H \in G \mid H(e_1) = e_1 \} \), the subgroup of \( G \) which
stabilizes $e_1$. For a generic compact group $\mathcal{A}$, we write $\mu_\mathcal{A}$ for the unique Haar probability measure on $\mathcal{A}$. Then we have the following Theorem.

**Theorem 1.1.** Let $M$ and $H$ be independent matrices, $M \in \mathcal{G}$ and $H \in \mathcal{H}$ with distribution $\mu_\mathcal{H}$. Then $MH \sim \mu_\mathcal{G}$ if and only if $M(e_1) \sim f(\mu_\mathcal{G})$, where $f$ is the map $f : G \mapsto G(e_1)$.

Let $\mathcal{M}$ be the set of elements of $\mathcal{G}$ which are reflections with respect to a hyperplane of $\mathbb{C}^N$. Define also

$$g : \begin{cases} \mathcal{H} & \mapsto U(N-1) \\ H & \mapsto H_{\text{span}(e_2, \ldots, e_N)} \end{cases},$$

where $H_{\text{span}(e_2, \ldots, e_N)}$ is the restriction of $H$ to span$(e_2, \ldots, e_N)$. Now suppose that $\{G(e) \mid G \in \mathcal{G}\} = \{M(e) \mid M \in \mathcal{M}\}$. Under this additional condition the following Theorem can be proven, using Theorem 1.1 and elementary manipulations of determinants.

**Theorem 1.2.** Let $G \sim \mu_\mathcal{G}$, $G' \sim \mu_\mathcal{G}$ and $H \sim g(\mu_\mathcal{H})$ be independent. Then

$$\det(\text{Id}_N - G) \overset{\text{law}}{=} (1 - \langle e_1, G'(e_1) \rangle) \det(\text{Id}_{N-1} - H).$$

1.2. Examples : the unitary group, the group of permutations. Take $G = U(N)$. As all reflections with respect to a hyperplane of $\mathbb{C}^N$ are elements of $G$, one can apply Theorem 1.2. The corresponding measures are the following.

1. The distribution $g(\mu_\mathcal{H})$ is clearly $\mu_{U(N-1)}$.
2. $\langle e_1, G(e_1) \rangle$ is distributed as the first coordinate of a vector of the $N$-dimensional unit complex sphere with uniform measure: $\langle e_1, G(e_1) \rangle \sim e^{i\theta_N} \sqrt{\beta_{1,N-1}}$ with $\theta_n$ uniform on $(0, 2\pi)$ and independent of $\beta_{1,N-1}$, a beta variable with parameters 1 and $N - 1$.

Thus iterations of Theorem 1.2 lead to the following Corollary.

**Corollary 1.3.** (2) Let $G \in U(N)$ be $\mu_{U(N)}$ distributed. Then

$$\det(\text{Id}_N - G) \overset{\text{law}}{=} \prod_{k=1}^{N} \left(1 - e^{i\theta_k} \sqrt{\beta_{1,k-1}}\right),$$

with $\theta_1, \ldots, \theta_N, \beta_{1,0}, \ldots, \beta_{1,N-1}$ independent random variables, the $\theta_k$’s uniformly distributed on $(0, 2\pi)$ and the $\beta_{1,j}$’s $(0 \leq j \leq N - 1)$ being beta distributed with parameters 1 and $j$ (by convention, $\beta_{1,0}$ is the Dirac distribution at 1).

The group $S_N$ of permutations of size $N$ gives another possible application. Identify an element $\sigma \in S_N$ with the matrix $(\delta^{ij}_{\sigma(i)})_{1 \leq i, j \leq N}$ ($\delta$ is Kronecker’s symbol). As $\det(\text{Id}_N - \sigma)$ is equal to 0, we prefer to deal with the group $\tilde{S}_N$ of matrices $(e^{i\theta} \delta^{ij}_{\sigma(i)})_{1 \leq i, j \leq N}$, with $\sigma \in S_N$ and $\theta_1, \ldots, \theta_N$ independent uniform random variables on $(0, 2\pi)$. Then the measures corresponding to Theorem 1.2 are the following.
(1) The distribution $g(\mu_{\tilde{S}_N})$ is $\mu_{\tilde{S}_{N-1}}$.

(2) $\langle e_1, G(e_1) \rangle$ is 0 with probability $1-1/N$ and $e^{i\theta}$ ($\theta$ uniform on $(0,2\pi)$) with probability $1/N$.

As previously, iterations of Theorem 1.2 give the following result.

**Corollary 1.4.** Let $S_N \in \tilde{S}_N$ be $\mu_{\tilde{S}_N}$ distributed. Then

$$\det(\text{Id}_N - S_N) \overset{\text{law}}{=} \prod_{k=1}^{N} \left( 1 - e^{i\theta_k} X_k \right),$$

with $\theta_1, \ldots, \theta_N, X_1, \ldots, X_N$ independent random variables, the $\theta_k$’s uniformly distributed on $(0,2\pi)$ and the $X_k$’s Bernoulli variables: $\mathbb{P}(X_k = 1) = 1/k$, $\mathbb{P}(X_k = 0) = 1-1/k$.

**Remark.** Let $k_\sigma$ be the number of cycles of a random permutation of size $N$, with respect to the (probability) Haar measure. Corollary 1.4 allows us to recover the following celebrated result about the law of $k_\sigma$:

$$k_\sigma \overset{\text{law}}{=} X_1 + \cdots + X_N,$$

with the previous notations. Indeed, if a permutation $\sigma \in S_N$ has $k_\sigma$ cycles with lengths $l_1, \ldots, l_{k_\sigma}$ ($\sum l_k = N$), then it is easy to see that under the Haar measure

$$\det(x \text{Id} - \tilde{S}_N) \overset{\text{law}}{=} \prod_{k=1}^{k_\sigma} (x^{l_k} - e^{i\alpha_k})$$

with the $\alpha_k$’s independent and uniform on $(0,2\pi)$. Using the previous relation and the result of Corollary 1.4 we get

$$\prod_{k=1}^{N} \left( 1 - e^{i\theta_k} X_k \right) \overset{\text{law}}{=} \prod_{k=1}^{k_\sigma} (1 - e^{i\alpha_k}).$$

The equality of the Mellin transforms of the modulus of the above members easily implies the expected result: $k_\sigma \overset{\text{law}}{=} X_1 + \cdots + X_N$. Our discussion on the permutation group is closely related to the so-called Chinese restaurant process and the Feller decomposition of the symmetric group (see, e.g. [1]).

## 2. Characteristic Polynomials as Orthogonal Polynomials

We now show how Corollary 1.3 can be obtained as a consequence of a result by Killip and Nenciu ([3]).

### 2.1. A result by Killip and Nenciu.

Let $\mathbb{D}$ be the open unit disk $\{z \in \mathbb{C} : |z| < 1\}$ and $\partial \mathbb{D}$ the unit circle. Let $(e_1, \ldots, e_N)$ be the canonical basis of $\mathbb{C}^N$. If $G \in U(N)$, and if $e_1$ is cyclic for $G$, the spectral measure for the pair $(G, e_1)$ is the unique probability $\nu$ on $\partial \mathbb{D}$ such that, for every integer $k \geq 0$

$$\langle e_1, G^k e_1 \rangle = \int_{\partial \mathbb{D}} z^k d\nu(z). \quad (2.1)$$
In fact, we have the expression
\[ \nu = \sum_{j=1}^{N} \pi_j \delta_{e^{i\zeta_j}} \]
where \((e^{i\zeta_j}, j = 1, \ldots, N)\) are the eigenvalues of \(G\) and where \(\pi_j = |\langle e_1, \Pi e_j \rangle|^2\) with \(\Pi\) a unitary matrix diagonalizing \(G\).

The relation (2.1) allows to define an isometry from \(\mathbb{C}^N\) equipped with the basis \((e_1, Ge_1, \ldots, G^{N-1}e_1)\) into the subspace of \(L^2(\partial \mathbb{D}; d\nu)\) spanned by the family \((1, z, \ldots, z^N)\). The endomorphism \(G\) is then a representation of the multiplication by \(z\).

From the linearly independent family of monomials \(\{1, z, z^2, \ldots, z^{N-1}\}\) in \(L^2(\partial \mathbb{D}, \nu)\), we construct an orthogonal basis \(\Phi_0, \ldots, \Phi_{N-1}\) of monic polynomials by the Gram-Schmidt procedure. The \(N^{th}\) degree polynomial obtained this way is
\[ \Phi_N(z) = \prod_{j=1}^{N} (z - e^{i\zeta_j}), \]

i.e. the characteristic polynomial of \(G\). The \(\Phi_k\)'s \((k = 0, \ldots, N)\) obey the Szegö recursion relation:
\[ \Phi_{j+1}(z) = z\Phi_j(z) - \bar{\alpha}_j \Phi^*_j(z) \]
where \(\Phi^*_j(z) = z^j \overline{\Phi_j(z)}(\overline{z}^{-1})\). The coefficients \(\alpha_j\)'s \((j \geq 0)\) are called Schur or Verblunsky coefficients and satisfy the condition \(\alpha_0, \ldots, \alpha_{N-2} \in \mathbb{D}\) and \(\alpha_{N-1} \in \partial \mathbb{D}\). There is a bijection between this set of coefficients and the set of spectral probability measures \(\nu\) (Verblunsky’s theorem). If \(G \sim \mu_{U(N)}\), then we know the exact distribution of the Verblunsky coefficients:

**Theorem 2.1.** (Killip and Nenciu [3]) Let \(G \in U(N)\) be \(\mu_{U(N)}\) distributed. The Verblunsky parameters \(\alpha_0, \ldots, \alpha_{N-2}, \alpha_{N-1}\) are independent and the density of \(\alpha_j\) for \(j \leq N-1\) is
\[ \frac{N-j-1}{\pi} \left(1 - |z|^2\right)^{N-j-2} \mathbb{I}_\mathbb{D}(z) \]
(for \(j = N-1\) by convention this is the uniform measure on the unit circle).

2.2. **Recovering Corollary 1.3.** For \(z = 1\), Szegö’s recursion (2.2) can be written
\[ \Phi_{j+1}(1) = \Phi_j(1) - \overline{\alpha}_j \Phi^*_j(1). \]

Under the Haar measure for \(G\), as \(\alpha_j\) is independent of \(\Phi_j(1)\) and its distribution is invariant by rotation, (2.3) easily yields
\[ \Phi_{j+1}(1) \xrightarrow{\text{law}} (1 - \alpha_j) \Phi_j(1). \]

In particular, for \(j = N-1\) we get by induction
\[ \det(\text{Id} - G) \xrightarrow{\text{law}} \prod_{k=0}^{N-1} (1 - \alpha_j). \]
From the density for $\alpha_j$ given in Theorem 2.1 one can see that this is exactly the same result as Corollary 1.3.

Remark. A similar result holds for $SO(2N)$, and can be shown using either the method of Section 1 or the one in Section 2, with the corresponding result by Killip and Nenciu for the Verblunsky coefficients on the orthogonal group $[3]$.

2.3. Extension. We now consider the whole sequence of polynomials $\Phi_j, j \leq N$ for $j \leq N$ as a sequence of characteristic polynomials. For this purpose, we apply the Gram-Schmidt procedure to $1, z, z^{-1}, z^2, \ldots, z^{p-1}, z^{-p}, z^p$ if $N = 2p$ and to $1, z, z^{-1}, z^2, \ldots, z^p, z^{-p}$ if $N = 2p + 1$ in $L^2(\partial D; d\nu)$. In the resulting basis, the mapping $f(z) \mapsto zf(z)$ is represented by a so-called CMV matrix (see [3] Appendix B, [5]) denoted by $C_N(G)$. It is five-diagonal and conjugate to $G$. For $1 \leq j \leq N$ let $C_N^{(j)}(G)$ the principal submatrix of order $j$ of $C_N(G)$. It is known (see for instance Proposition 3.1 in [5]) that

$$\Phi_j(z) = \det\left(zId_j - C_N^{(j)}(G)\right).$$

From the recursion (2.3) and looking at the invariance of conditional distributions, we see that

$$\left(\det\left(Id_j - C_N^{(j)}(G)\right)\right)_{1 \leq j \leq N} = \left(\Phi_j(1)\right)_{1 \leq j \leq N} \xrightarrow{\text{law}} \left(\prod_{l=0}^{j}(1 - \alpha_l)\right)_{0 \leq j \leq N-1} \quad (2.5)$$

It allows a study of the process $(\log \Phi_{\lfloor Nt \rfloor}(1), t \in [0, 1])$ as a triangular array of (complex) independent random variables. For $t = 1$ the asymptotic behavior is presented in [2] (see (2.7) below). It is remarkable that for $t < 1$, we do not need any normalization for the CLT.

Theorem 2.2. (1) As $N \to \infty$

$$(\log \det(Id_j - C_N^{(j)}(G)); t \in [0, 1]) \Rightarrow (B_{-\frac{1}{2}\log(1-t)}; t \in [0, 1]), \quad (2.6)$$

where $B$ is a standard complex Brownian motion and $\Rightarrow$ stands for the weak convergence of distributions in the set of càdlàg functions on $[0, 1)$, starting from 0, endowed with the Skorokhod topology.

(2) As $N \to \infty$,

$$\frac{\log \det(Id_N - G)}{\sqrt{2\log N}} \Rightarrow \mathcal{N}_1 + i\mathcal{N}_2 \quad (2.7)$$

where $\mathcal{N}_1$ and $\mathcal{N}_2$ are independent standard normal and independent of $B$, and $\Rightarrow$ stands for the weak convergence of distributions in $\mathbb{C}$.

This theorem can be proved using the Mellin-Fourier transform of the $1 - \alpha_j$’s and independence. This method may also be used to prove large deviations. It is the topic of a companion paper. These results occur in similar way for other random determinants (see [3]).
REFERENCES

[1] R. Arratia, A.D. Barbour, S. Tavaré, Logarithmic Combinatorial Structures: A Probabilistic Approach. 352 pp, 2003. EMS Monographs in Mathematics, 1. European Mathematical Society Publishing House, Zürich.

[2] P. Bourgade, C.P. Hughes, A. Nikeghbali, M. Yor, The characteristic polynomial of a random unitary matrix: a probabilistic approach, arXiv math.PR/0706.0333, 2007.

[3] R. Killip and I. Nenciu, Matrix models for circular ensembles, International Mathematics Research Notices, vol. 2004, no. 50, pp. 2665-2701, 2004.

[4] A. Rouault, Asymptotic behavior of random determinants in the Laguerre, Gram and Jacobi ensembles, arXiv math.PR/0607767, 2007.

[5] B. Simon, CMV matrices: Five years after, arXiv math.SP/0603093, 2006.

Laboratoire de Probabilités et Modèles Aléatoires, Université Pierre et Marie Curie, et C.N.R.S. UMR 7599, 175, rue du Chevaleret, F-75013 Paris, France

E-mail address: bourgade@enst.fr

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland

E-mail address: ashkan.nikeghbali@math.unizh.ch

Université Versailles-Saint Quentin, LMV, Bâtiment Fermat, 45 avenue des Etats-Unis, 78035 Versailles Cedex

E-mail address: rouault@fermat.math.uvsq.fr