

Some results on random circulant matrices

Mark W. Meckes¹

Case Western Reserve University

Abstract: This paper considers random (non-Hermitian) circulant matrices, and proves several results analogous to recent theorems on non-Hermitian random matrices with independent entries. In particular, the limiting spectral distribution of a random circulant matrix is shown to be complex normal, and bounds are given for the probability that a circulant sign matrix is singular.

1. Introduction

Given a sequence X_0, X_1, \dots of independent complex random variables, denote by \mathcal{C}_n the $n \times n$ random circulant matrix with first row X_0, \dots, X_{n-1} :

$$\mathcal{C}_n = \begin{bmatrix} X_0 & X_1 & \cdots & \cdots & X_{n-2} & X_{n-1} \\ X_{n-1} & X_0 & X_1 & & & X_{n-2} \\ \vdots & X_{n-1} & X_0 & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ X_2 & & & & X_0 & X_1 \\ X_1 & X_2 & \cdots & \cdots & X_{n-1} & X_0 \end{bmatrix}.$$

It is well-known (and easy to verify) that the eigenvalues of \mathcal{C}_n are

$$\sum_{j=0}^{n-1} \omega_n^{jk} X_j, \quad k = 0, \dots, n-1,$$

where $\omega_n = e^{2\pi i/n}$. The eigenvalues of random circulant matrices have only recently been studied explicitly in the literature, e.g. in [5, 6, 20], which consider real symmetric circulant matrices and variants of them. Other models of random matrices lying in some linear subspace of matrix space have also been studied recently in [5, 6, 8, 10, 14, 20], among others. These papers mainly prove results analogous to classical theorems for Wigner-type random matrices, i.e. symmetric (or Hermitian) random matrices whose entries are all independent except for the symmetry constraint.

This paper mainly considers the eigenvalues of the random circulant matrices \mathcal{C}_n with no symmetry constraint, and prove results analogous to recent theorems about random matrices with all independent entries. In Section 2 we investigate

¹Department of Mathematics, Case Western Reserve University, Cleveland, Ohio 44106, USA, e-mail: mark.meckes@case.edu

Keywords and phrases: random matrix, circulant matrix, eigenvalues.

AMS 2000 subject classifications: Primary 15A52; secondary 60F05.

the limiting spectral distribution of large-dimensional random circulant matrices. In Section 3 we consider the joint distribution of eigenvalues of circulant matrices with Gaussian entries and observe some consequences, especially for the distributions of extreme eigenvalues. Finally, in Section 4 we investigate the probability that a circulant matrix with ± 1 Bernoulli entries is singular.

2. Limiting spectral distribution

We denote by

$$(2.1) \quad \lambda_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega_n^{jk} X_j$$

for $k = 0, \dots, n-1$ the eigenvalues of $n^{-1/2}\mathcal{C}_n$, and by

$$\mu_n = \frac{1}{n} \sum_{k=0}^{n-1} \delta_{\lambda_k}$$

the empirical spectral measure of $n^{-1/2}\mathcal{C}_n$. Theorems 1 and 2 show that as $n \rightarrow \infty$, μ_n converges to a universal limiting measure, namely the standard complex Gaussian measure $\gamma_{\mathbb{C}}$ with density $\frac{1}{\pi}e^{-|z|^2}$ with respect to Lebesgue measure on \mathbb{C} . Theorem 1 shows that this convergence holds in probability under very weak assumptions on the random variables X_j (including in particular the case of i.i.d. random variables with finite variance); Theorem 2 strengthens this to almost sure convergence under much stronger assumptions.

Theorems 1 and 2 are analogues for circulant matrices of the circular law for eigenvalues of random matrices with independent entries, which was recently proved by Tao and Vu in [27] in the almost sure sense for i.i.d. entries with finite variance. It is possible that the conclusion of Theorem 2 also holds in this level of generality; in any case it certainly holds under weaker conditions than those given below. However, the result of [27] and other results leading up to it were made possible by recent advances in controlling how close a random matrix with i.i.d. entries is to being singular. As discussed in Section 4 below, random circulant matrices are frequently much more likely to be singular; thus it may be difficult to prove the optimal result for circulant matrices. (On the other hand, the fact that circulant matrices are normal may make such a result approachable via the classical moment method used extensively for Hermitian random matrices.)

Theorem 1. *Suppose that the X_j satisfy*

$$(2.2) \quad \mathbb{E}X_j = 0, \quad \mathbb{E}X_j^2 = \alpha, \quad \mathbb{E}|X_j|^2 = 1,$$

for some $\alpha \in \mathbb{C}$ and

$$(2.3) \quad \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=0}^{n-1} \mathbb{E}(|X_j|^2 1_{|X_j| > \varepsilon \sqrt{n}}) = 0$$

for every $\varepsilon > 0$. Then μ_n converges in expectation and weak-* in probability to $\gamma_{\mathbb{C}}$, the standard complex Gaussian measure on \mathbb{C} .

Observe that the hypotheses cover the case of i.i.d. complex random variables with finite variance, as well as real random variables and rotationally invariant distributions satisfying the Lindeberg condition (2.3).

Proof. Without loss of generality we may assume $\alpha \in \mathbb{R}$. Observe that for a measurable set $A \subseteq \mathbb{C}$,

$$\mathbb{E}\mu_n(A) = \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{P}[\lambda_k \in A] = \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{P} \left[\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega_n^{jk} X_j \in A \right].$$

We consider λ_k as a sum of independent random vectors in $\mathbb{R}^2 \cong \mathbb{C}$, so we will need

$$\text{Cov}(\omega_n^{jk} X_j) = \begin{pmatrix} \mathbb{E}(\text{Re } \omega_n^{jk} X_j)^2 & \mathbb{E}(\text{Re } \omega_n^{jk} X_j)(\text{Im } \omega_n^{jk} X_j) \\ \mathbb{E}(\text{Re } \omega_n^{jk} X_j)(\text{Im } \omega_n^{jk} X_j) & \mathbb{E}(\text{Im } \omega_n^{jk} X_j)^2 \end{pmatrix}.$$

The identities

$$(2.4) \quad \begin{aligned} \frac{1}{2}(w + \bar{w})z &= (\text{Re } w)(\text{Re } z) + i(\text{Re } w)(\text{Im } z), \\ \frac{1}{2}(w - \bar{w})z &= -(\text{Im } w)(\text{Im } z) + i(\text{Re } w)(\text{Im } z). \end{aligned}$$

for $w, z \in \mathbb{C}$ are useful. Letting $w = z = \omega_n^{jk} X_j$,

$$\sum_{j=0}^{n-1} \mathbb{E}(\text{Re } \omega_n^{jk} X_j)^2 = \frac{1}{2} \text{Re} \sum_{j=0}^{n-1} \mathbb{E}(\omega_n^{2jk} X_j^2 + |X_j|^2) = \frac{1}{2} \text{Re} \sum_{j=0}^{n-1} (\alpha \omega_n^{2jk} + 1).$$

Since ω_n^{2k} is an n th root of unity, $\sum_{j=0}^{n-1} \omega_n^{2jk} = 0$ unless $\omega_n^{2k} = 1$, which is the case only if $k = 0$ or $k = n/2$. Thus unless $k = 0$ or $n/2$,

$$\frac{1}{n} \sum_{j=0}^{n-1} \mathbb{E}(\text{Re } \omega_n^{jk})^2 = \frac{1}{2}.$$

The other covariances are computed similarly and it follows that for $k \neq 0, n/2$

$$\frac{1}{n} \sum_{j=0}^{n-1} \text{Cov}(\omega_n^{jk} X_j) = \frac{1}{2} I_2.$$

Since $|\omega_n^{jk} X_j| = |X_j|$, by (2.3) we can now apply a quantitative two-dimensional version of Lindeberg's central limit theorem to the complex random variables $\{\omega_n^{jk} X_j \mid 0 \leq j \leq n-1\}$. Let $A \subseteq \mathbb{C}$ be measurable and convex and assume $k \neq 0, n/2$. By the proof of [4, Corollary 18.2]), there is a function $h(n)$ with $\lim_{n \rightarrow \infty} h(n) = 0$, which depends on A and the rate of convergence in (2.3) but is independent of k , such that

$$\left| \mathbb{P} \left[\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega_n^{jk} X_j \in A \right] - \gamma_{\mathbb{C}}(A) \right| \leq h(n).$$

Therefore

(2.5)

$$|\mathbb{E}\mu_n(A) - \gamma_{\mathbb{C}}(A)| \leq \frac{1}{n} \sum_{k=0}^{n-1} |\mathbb{P}[\lambda_k \in A] - \gamma_{\mathbb{C}}(A)| \leq \frac{2 + (n-2)h(n)}{n} \xrightarrow{n \rightarrow \infty} 0.$$

Thus the claimed convergence holds in expectation.

Next observe that

$$\mathbb{E}\mu_n(A)^2 = \mathbb{E} \left[\frac{1}{n^2} \sum_{k,\ell=0}^{n-1} 1_{\lambda_k \in A} 1_{\lambda_\ell \in A} \right] = \frac{1}{n^2} \sum_{k,\ell=0}^{n-1} \mathbb{P}[(\lambda_k, \lambda_\ell) \in A \times A].$$

As before, we can compute the sums of the relevant covariance matrices using (2.4), in this case with $w = \omega_n^{jk} X_j$ and $z = \omega_n^{j\ell} X_j$. We obtain

$$\frac{1}{n} \sum_{j=0}^{n-1} \text{Cov}(\omega_n^{jk} X_j, \omega_n^{j\ell} X_j) = \frac{1}{2} I_4$$

except when $k = 0$ or $n/2$, $\ell = 0$ or $n/2$, $k + \ell = 0$ or n , or $k = \ell$. These exceptional cases account for fewer than $6n$ of the n^2 possible values of (k, ℓ) . Applying the four-dimensional case of Lindeberg’s theorem similarly to above, we have

$$(2.6) \quad |\mathbb{E}\mu_n(A)^2 - \gamma_{\mathbb{C}}(A)^2| \leq \frac{1}{n^2} \sum_{k,\ell=0}^{n-1} |\mathbb{P}[(\lambda_k, \lambda_\ell) \in A \times A] - \gamma_{\mathbb{C}}(A)^2| \xrightarrow{n \rightarrow \infty} 0.$$

We are of course using here that standard Gaussian measure on \mathbb{C}^2 is the two-fold product of $\gamma_{\mathbb{C}}$.

From (2.5) and (2.6) it follows that

$$\mathbb{E}[\mu_n(A) - \gamma_{\mathbb{C}}(A)]^2 = [\mathbb{E}\mu_n(A)^2 - \gamma_{\mathbb{C}}(A)^2] - 2\gamma_{\mathbb{C}}(A)[\mathbb{E}\mu_n(A) - \gamma_{\mathbb{C}}(A)] \xrightarrow{n \rightarrow \infty} 0.$$

Thus for every convex measurable $A \subset \mathbb{C}$, the random variable $\mu_n(A)$ converges to $\gamma_{\mathbb{C}}(A)$ in L^2 and hence in probability. \square

Bose and Mitra [5] proved earlier a result analogous to Theorem 1 for real symmetric circulant matrices, which is a circulant matrix analogue of Wigner’s semicircle law; the limiting distribution in this case is a real Gaussian measure. This result was strengthened from convergence in probability to almost sure convergence (under the assumption of i.i.d. entries with finite third moments) by Bercu and Bryc [3]; see also [20]. The main result of [5] is a similar result for circulant Hankel matrices, which amounts to studying the singular values instead of eigenvalues of \mathcal{C}_n (see [8, Remark 1.2] about the relationship between Hankel and Toeplitz matrices). Since circulant matrices are normal, their singular values are simply the moduli of their eigenvalues; thus this latter result is essentially a corollary of Theorem 1. The proof of Theorem 1 follows the basic outline of the proofs of [5], which assume the X_j are i.i.d. with finite third absolute moments; the greater generality of Theorem 1 is achieved by applying Lindeberg’s theorem, instead of the Berry-Esseen theorem as in [5].

The statement of Theorem 1 assumes that the same sequence of random variables X_j is used to construct \mathcal{C}_n for every n . The proof shows however that the result generalizes directly to circulant matrices constructed from a triangular array of random variables. The same comment applies to Theorem 2 below.

Theorem 2. *Suppose that, in addition to (2.2) one of the following holds.*

1. *There exists a $K > 0$ such that for each j , $|X_j| \leq K$ almost surely.*
2. *There exists a $K > 0$ such that for each j , the distribution of X_j satisfies a quadratic transportation cost inequality with constant K (see below for the meaning of this).*

Then μ_n converges weak-* to $\gamma_{\mathbb{C}}$ almost surely.

Recall that a probability measure μ on \mathbb{R}^d is said to satisfy a quadratic transportation cost inequality with constant $K > 0$ if

$$\inf_{\pi \in \Pi(\mu, \nu)} \int \int |x - y|^2 d\pi(x, y) \leq \sqrt{2KH(\mu|\nu)}$$

for every probability measure ν on \mathbb{R}^d . Here $\Pi(\mu, \nu)$ is the class of probability measures on $\mathbb{R}^d \times \mathbb{R}^d$ with marginals μ and ν respectively, and $H(\mu|\nu)$ is relative entropy. Such an inequality is satisfied in particular if μ satisfies a logarithmic Sobolev inequality. See [19, Chapter 6] for background and references.

Proof. We begin with the assumption that a quadratic transportation cost inequality is satisfied. This assumption implies (and is essentially equivalent to, see [13]) the following concentration inequality for Lipschitz functions of (X_1, \dots, X_n) . Let $F : \mathbb{C}^n \rightarrow \mathbb{R}$ have Lipschitz constant $|F|_{\text{Lip}} = L$. Then

$$(2.7) \quad \mathbb{P}[|F(X_1, \dots, X_n) - \mathbb{E}F(X_1, \dots, X_n)| \geq t] \leq Ce^{-ct^2/K^2L^2}$$

for every $t > 0$, where $c, C > 0$ are absolute constants. Now for a compactly supported smooth function $f : \mathbb{C} \rightarrow \mathbb{R}$, define

$$F(x_1, \dots, x_n) = \frac{1}{n} \sum_{j=1}^n f(x_j),$$

so that $F(X_1, \dots, X_n) = \int_{\mathbb{C}} f d\mu_n$. Then

$$|F(x_1, \dots, x_n) - F(y_1, \dots, y_n)| \leq \frac{|f|_{\text{Lip}}}{n} \sum_{j=1}^n |x_j - y_j| \leq \frac{|f|_{\text{Lip}}}{\sqrt{n}} \sqrt{\sum_{j=1}^n |x_j - y_j|^2},$$

so $|F|_{\text{Lip}} \leq n^{-1/2}|f|_{\text{Lip}}$. Combining Theorem 1, (2.7), and the Borel-Cantelli lemma, we obtain that for each compactly supported smooth function $f : \mathbb{C} \rightarrow \mathbb{R}$,

$$\int_{\mathbb{C}} f d\mu_n \xrightarrow{n \rightarrow \infty} \int_{\mathbb{C}} f d\gamma_{\mathbb{C}}$$

almost surely. Applying this for a countable dense family of such f proves the theorem.

The case of bounded entries is treated similarly using Talagrand’s famous concentration inequality for convex Lipschitz functions of bounded random variables [26] (also see [19, Section 4.2]); in this case an extra step is required to handle non-convex test functions $f : \mathbb{C} \rightarrow \mathbb{R}$.

As above, let $f : \mathbb{C} \rightarrow \mathbb{R}$ be compactly supported and smooth. Let $R > 0$ be such that $f(x) = 0$ for $|x| \geq R$ and let $\lambda \geq 0$ be such that the eigenvalues of the Hessian D^2f are bounded below by $-\lambda$. For $x \in \mathbb{C}$ define

$$g(x) = \begin{cases} \frac{\lambda}{2}|x|^2 & \text{if } |x| \leq R, \\ \lambda R(|x| - \frac{R}{2}) & \text{if } |x| \geq R. \end{cases}$$

Then $|g|_{\text{Lip}} = \lambda R$ and so $|f + g|_{\text{Lip}} \leq |f|_{\text{Lip}} + \lambda R$. Furthermore, since $D^2(f + g) \geq 0$, both g and $f + g$ are convex. Applying the above argument to $f + g$ and

g using Talagrand’s concentration inequality in place of (2.7) implies that with probability 1,

$$\int_{\mathbb{C}} (f + g) d\mu_n \xrightarrow{n \rightarrow \infty} \int_{\mathbb{C}} (f + g) d\gamma_{\mathbb{C}} \quad \text{and} \quad \int_{\mathbb{C}} g d\mu_n \xrightarrow{n \rightarrow \infty} \int_{\mathbb{C}} g d\gamma_{\mathbb{C}}$$

and hence

$$\int_{\mathbb{C}} f d\mu_n \xrightarrow{n \rightarrow \infty} \int_{\mathbb{C}} f d\gamma_{\mathbb{C}}.$$

(For an explicit statement of a version of Talagrand’s concentration inequality which may be applied directly to complex random variables X_j , see e.g. [21, Corollary 4].)

Again, applying this for a countable dense family of such f proves the theorem. □

We remark that a slight generalization of the argument in the last paragraph shows that convex Lipschitz functions on \mathbb{R}^d form a convergence-determining class for the family of probability measures on \mathbb{R}^d with respect to which such functions are integrable. This fact is presumably well-known to experts but we could not find a statement of it in the literature.

3. Gaussian circulant matrices and extreme eigenvalues

The following result is a circulant analogue of classical formulas (found, e.g., in [23]) for the joint distribution of eigenvalues of random matrices with independent complex Gaussian entries.

Proposition 3. *Let each X_j have the standard complex normal distribution. Then the sequence $\lambda_0, \dots, \lambda_{n-1}$ of eigenvalues of $n^{-1/2}\mathcal{C}_n$ is distributed as n independent standard complex normal random variables.*

Proof. The map $(X_0, \dots, X_{n-1}) \mapsto (\lambda_0, \dots, \lambda_{n-1})$ defined by (2.1) is easily checked to be a unitary transformation of \mathbb{C}^n , so it preserves the standard Gaussian measure on \mathbb{C}^n . □

An easy consequence of Proposition 3 is that in this setting, $\mathbb{E}\mu_n = \gamma_{\mathbb{C}}$ for every n , and not only in the limit $n \rightarrow \infty$ as guaranteed by Theorem 1.

If each X_j is a standard real normal random variable, then the same observation implies that the sequence of eigenvalues $\lambda_0, \dots, \lambda_{n-1}$ are jointly Gaussian random variables, but with singular covariance since this sequence will lie in an n -dimensional real subspace of the $2n$ -dimensional space \mathbb{C}^n . On the other hand, Proposition 3 does have the following simple analogue for complex Hermitian circulant matrices with Gaussian entries.

Corollary 4. *Let \mathcal{C}_n^H be a Hermitian random circulant matrix*

$$\mathcal{C}_n^H = \begin{bmatrix} Y_0 & Y_1 & \cdots & \cdots & Y_{n-2} & Y_{n-1} \\ \overline{Y_{n-1}} & Y_0 & Y_1 & & & Y_{n-2} \\ \vdots & \overline{Y_{n-1}} & Y_0 & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ \overline{Y_2} & & & & Y_0 & Y_1 \\ \overline{Y_1} & \overline{Y_2} & \cdots & \cdots & \overline{Y_{n-1}} & Y_0 \end{bmatrix},$$

where $Y_0, \dots, Y_{\lfloor n/2 \rfloor}$ are independent, $Y_j = Y_{n-j}$ for $j > n/2$, Y_0 and $Y_{n/2}$ (if n is even) have the standard real normal distribution, and Y_j has the standard complex normal distribution for $1 \leq j < n/2$. Then the eigenvalues of $n^{-1/2} \mathcal{C}_n^H$ are distributed as n independent standard real normal random variables.

Proof. If \mathcal{C}_n is as in Proposition 3, then \mathcal{C}_n^H has the same distribution as $\frac{1}{\sqrt{2}}(\mathcal{C}_n + \mathcal{C}_n^*)$. Because \mathcal{C}_n is normal, the eigenvalues of $n^{-1/2} \mathcal{C}_n^H$ are

$$\frac{1}{\sqrt{2}}(\lambda_k + \overline{\lambda_k}) = \sqrt{2} \operatorname{Re} \lambda_k$$

for $k = 0, \dots, n-1$, which by Proposition 3 are independent standard real normal random variables. \square

The Gaussian Hermitian circulant matrix \mathcal{C}_n^H of Corollary 4 should be thought of as a circulant analogue of the Gaussian Unitary Ensemble, which (up to a choice of normalization) is defined as $\frac{1}{\sqrt{2}}(G + G^*)$, where G is an $n \times n$ random matrix whose entries are independent standard complex normal random variables.

Corollary 5. *Let \mathcal{C}_n and \mathcal{C}_n^H be as in Proposition 3 and Corollary 4. Let $\alpha_1 \geq \dots \geq \alpha_n \geq 0$ be the eigenvalues of $n^{-1} \mathcal{C}_n \mathcal{C}_n^*$ and let $\beta_1 \geq \dots \geq \beta_n$ be the eigenvalues of $n^{-1/2} \mathcal{C}_n^H$. Then α_n has an exponential distribution with mean $1/n$, and*

$$\alpha_1 - \log n$$

and

$$\sqrt{2 \log n} \left(\beta_1 - \sqrt{2 \log n} - \frac{\log \log n + \log 4\pi}{2\sqrt{2 \log n}} \right)$$

both converge in distribution as $n \rightarrow \infty$ to the Gumbel distribution with cumulative distribution function $e^{-e^{-x}}$.

Proof. Observe that since \mathcal{C}_n is normal, the eigenvalues of $n^{-1} \mathcal{C}_n \mathcal{C}_n^*$ are $|\lambda_k|^2$ (though not usually in the same order), which by Proposition 3 are distributed as independent exponential random variables. The corollary follows by combining this fact and Corollary 4 with classical theorems of extreme value theory (see [18, Chapter 1]). \square

The asymptotic distributions of β_1 and α_1 are circulant matrix analogues of famous results of Tracy and Widom [28] and Johnstone [16], respectively. Davis and Mikosch [11], who did not consider random circulant matrices explicitly, proved (with slight modifications) what amounts to a universality result for α_1 , which shows the conclusion follows for quite general distributions of the X_j . Following their method Bryc and Sethuraman [9] proved an explicitly stated universality result for β_1 ; these are then the circulant matrix analogues of the results of Soshnikov in [25, 24] respectively. The rough orders of magnitude of α_1 and β_1 follow in even greater generality from work of the author [22] and Adamczak [1] (see the remarks in [22, Section 3.1]).

4. Singularity of circulant sign matrices

In this section we specialize to the case in which $\mathbb{P}[X_j = -1] = \mathbb{P}[X_j = 1] = 1/2$ for every j and consider the probability that \mathcal{C}_n is singular. The corresponding problem

for random $n \times n$ matrices M_n with independent ± 1 entries has a long history. An old conjecture (see [17]) claims that

$$\mathbb{P}[M_n \text{ is singular}] = \left(\frac{1}{2} + o(1)\right)^n,$$

which is asymptotically the probability that two rows of M_n are equal up to sign. The best result currently known, proved by Bourgain, Vu, and Wood in [7], is

$$\mathbb{P}[M_n \text{ is singular}] \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

By contrast, the following result shows that the singularity probability of an $n \times n$ random circulant matrix with ± 1 entries depends strongly on the number-theoretic properties of n .

Theorem 6. *Let $\mathbb{P}[X_j = -1] = \mathbb{P}[X_j = 1] = 1/2$ for each j . If n is even, then*

$$(4.1) \quad \frac{c_1}{\sqrt{n}} \leq \mathbb{P}[\mathcal{C}_n \text{ is singular}] \leq \frac{c_2}{\sqrt{n}},$$

where $c_1, c_2 > 0$ are absolute constants. If $n \geq 3$ is odd, then

$$(4.2) \quad \mathbb{P}[\mathcal{C}_n \text{ is singular}] \leq \min \left\{ c_3 \frac{d(n)}{n}, \sum_{\substack{1 < m \leq n \\ m|n}} 2^{-\varphi(m)} \right\},$$

where $c_3 > 0$ is an absolute constant, $d(n)$ is the number of divisors of n , and $\varphi(m)$ is the number of positive integers less than m which are relatively prime with m .

The lower bound in (4.1) shows that if n is even, then an $n \times n$ circulant sign matrix is much more likely to be singular than a sign matrix with independent entries. The first upper bound in (4.2) implies that the singularity probability is rather lower if n is odd; it is known that

$$(4.3) \quad d(n) \leq n^{c/\log \log n},$$

for every n , see [2, Theorem 13.12]. The bound is of course smaller if n has few divisors; for example if $n = p^k$ for an odd prime p then $d(n) = k+1 = \log_p n + 1$. The second upper bound in (4.2) implies that the singularity probability is extremely small if n has no small prime factors. In particular, if $n \geq 3$ is prime then

$$\mathbb{P}[\mathcal{C}_n \text{ is singular}] = 2^{-n+1}$$

since this is the probability that all the entries of \mathcal{C}_n are equal. It would be nice to have a more complete description of the dependence of the singularity probability on the prime factorization of n . As observed by an anonymous referee, it would be still more interesting to obtain estimates on the condition number or smallest singular value of \mathcal{C}_n .

Proof. Begin by defining the random polynomial

$$f(t) = \sum_{j=0}^{n-1} X_j t^j,$$

so that the eigenvalues of \mathcal{C}_n are $f(\omega_n^k)$ for $k = 0, \dots, n - 1$. Observe first that $f(1)$ and $f(-1)$ are identically distributed and

$$(4.4) \quad \mathbb{P}[f(1) = 0] = \mathbb{P}[f(-1) = 0] = \begin{cases} 2^{-n} \binom{n}{n/2} & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

which implies the lower bound in (4.1) by Stirling’s formula.

For each $k > 0$, ω_n^k is a primitive root of unity of order n/m , where $m = \gcd(k, n)$. The minimal polynomial of ω_n^k over the rational numbers is thus the cyclotomic polynomial $\Phi_{n/m}$, so $f(\omega_n^k) = 0$ if and only if $\Phi_{n/m}$ is a factor of f . (See e.g. [15, Section V.8] for background on cyclotomic polynomials.) Therefore we need only consider the cases when k is a divisor of n , and

$$(4.5) \quad \mathbb{P}[\mathcal{C}_n \text{ is singular}] \leq \mathbb{P}[f(1) = 0] + \sum_{\substack{1 \leq k < n \\ k|n}} \mathbb{P}[f(\omega_n^k) = 0].$$

A straightforward application of the multidimensional inverse Littlewood-Offord theorem proved by Friedland and Sodin [12] yields that

$$(4.6) \quad \mathbb{P}[f(\omega_n^k) = 0] \leq \frac{c}{n}$$

for some $c > 0$ when $k \neq 0, n/2$; the calculations involved in applying the result of [12] are similar to those in the proof of Theorem 1. The upper bound of (4.1) and the first upper bound of (4.2) follow by combining (4.5), (4.4), and (4.6). To bound the number of terms in (4.5) in the even case it is enough to use the trivial estimate $d(n) < 2\sqrt{n}$ (divisors of n occur in pairs $k, n/k$ with $k \leq \sqrt{n}$) rather than the much more delicate result (4.3).

For $n \geq 3$ and $d \geq 2$ let $P_{n,m}$ be the set of polynomials g with rational coefficients of degree at most $n - 1$ such that Φ_m is a factor of g . With the substitution $m = n/k$, (4.5) becomes

$$\mathbb{P}[\mathcal{C}_n \text{ is singular}] \leq \sum_{\substack{1 < d \leq n \\ d|n}} \mathbb{P}[f \in P_{n,m}].$$

Since Φ_m has degree $\varphi(m)$, $P_{n,m}$ is an $(n - \varphi(m))$ -dimensional subspace of the (rational) vector space of polynomials of degree at most $n - 1$. Therefore some set of $n - \varphi(m)$ coefficients of a polynomial g suffice to determine whether $g \in P_{n,m}$, and so

$$\mathbb{P}[f \in P_{n,m}] \leq 2^{-\varphi(m)},$$

which proves the second upper bound in (4.2). □

Acknowledgements

The author thanks Włodek Bryc and Elizabeth Meckes for helpful discussions, and the referee for pointing out reference [3].

References

[1] ADAMCZAK, R. (2009). A few remarks on the operator norm of random Toeplitz matrices. *J. Theoret. Probab.* To appear.

- [2] APOSTOL, T. M. (1976). *Introduction to Analytic Number Theory*. Springer-Verlag, New York. Undergraduate Texts in Mathematics.
- [3] BERCU, B. AND BRYC, W. (2007). Asymptotic results for empirical measures of weighted sums of independent random variables. *Electron. Comm. Probab.* **12** 184–198 (electronic).
- [4] BHATTACHARYA, R. N. AND RANGA RAO, R. (1986). *Normal Approximation and Asymptotic Expansions*. Robert E. Krieger Publishing Co. Inc., Melbourne, FL. Reprint of the 1976 original.
- [5] BOSE, A. AND MITRA, J. (2002). Limiting spectral distribution of a special circulant. *Statist. Probab. Lett.* **60**(1) 111–120.
- [6] BOSE, A. AND SEN, A. (2008). Another look at the moment method for large dimensional random matrices. *Electron. J. Probab.* **13**(21) 588–628.
- [7] BOURGAIN, J., VU, V. AND WOOD, P. (2009). On the singularity probability of discretely random complex matrices. Preprint. Available at <http://arxiv.org/abs/0905.0461>.
- [8] BRYC, W., DEMBO, A. AND JIANG, T. (2006). Spectral measure of large random Hankel, Markov and Toeplitz matrices. *Ann. Probab.* **34**(1) 1–38.
- [9] BRYC, W. AND SETHURAMAN, S. (2009). On the maximum eigenvalue for circulant matrices. *IMS Coll.* **5** 179–184.
- [10] CHATTERJEE, S. (2009). Fluctuations of eigenvalues and second order Poincaré inequalities. *Probab. Theory Related Fields* **143**(1,2) 1–40.
- [11] DAVIS, R. A. AND MIKOSCH, T. (1999). The maximum of the periodogram of a non-Gaussian sequence. *Ann. Probab.* **27**(1) 522–536.
- [12] FRIEDLAND, O. AND SODIN, S. (2007). Bounds on the concentration function in terms of the Diophantine approximation. *C. R. Math. Acad. Sci. Paris* **345**(9) 513–518.
- [13] GOZLAN, N. (2009). A characterization of dimension free concentration in terms of transportation inequalities. Preprint. Available at <http://arxiv.org/abs/0804.3089>.
- [14] HAMMOND, C. AND MILLER, S. J. (2005). Distribution of eigenvalues for the ensemble of real symmetric Toeplitz matrices. *J. Theoret. Probab.* **18**(3) 537–566.
- [15] HUNGERFORD, T. W. (1980). *Algebra. Graduate Texts in Mathematics* **73**. Springer-Verlag, New York. Reprint of the 1974 original.
- [16] JOHNSTONE, I. M. (2001). On the distribution of the largest eigenvalue in principal components analysis. *Ann. Statist.* **29**(2) 295–327.
- [17] KAHN, J., KOMLÓS, J. AND SZEMERÉDI, E. (1995). On the probability that a random ± 1 -matrix is singular. *J. Amer. Math. Soc.* **8**(1) 223–240.
- [18] LEADBETTER, M. R., LINDGREN, G. AND ROOTZÉN, H. (1983). *Extremes and Related Properties of Random Sequences and Processes. Springer Series in Statistics*. Springer-Verlag, New York.
- [19] LEDOUX, M. (2001). *The Concentration of Measure Phenomenon. Mathematical Surveys and Monographs* **89**. American Mathematical Society, Providence, RI.
- [20] MASSEY, A., MILLER, S. J. AND SINSHEIMER, J. (2007). Distribution of eigenvalues of real symmetric palindromic Toeplitz matrices and circulant matrices. *J. Theoret. Probab.* **20**(3) 637–662.
- [21] MECKES, M. W. (2004). Concentration of norms and eigenvalues of random matrices. *J. Funct. Anal.* **211**(2) 508–524.
- [22] MECKES, M. W. (2007). On the spectral norm of a random Toeplitz matrix. *Electron. Comm. Probab.* **12** 315–325 (electronic).

- [23] MEHTA, M. L. (2004). *Random Matrices*, 3rd ed. *Pure and Applied Mathematics (Amsterdam)* **142**. Elsevier/Academic Press, Amsterdam.
- [24] SOSHIKOV, A. (1999). Universality at the edge of the spectrum in Wigner random matrices. *Comm. Math. Phys.* **207**(3) 697–733.
- [25] SOSHIKOV, A. (2002). A note on universality of the distribution of the largest eigenvalues in certain sample covariance matrices. *J. Statist. Phys.* **108**(5,6) 1033–1056. Dedicated to David Ruelle and Yasha Sinai on the occasion of their 65th birthdays.
- [26] TALAGRAND, M. (1995). Concentration of measure and isoperimetric inequalities in product spaces. *Inst. Hautes Études Sci. Publ. Math.* (81) 73–205.
- [27] TAO, T. AND VU, V. (2009). Random matrices: Universality of ESDs and the circular law. Preprint. Available at <http://arxiv.org/abs/0807.4898>. With an appendix by M. Krishnapur.
- [28] TRACY, C. A. AND WIDOM, H. (1994). Level-spacing distributions and the Airy kernel. *Comm. Math. Phys.* **159**(1) 151–174.