# RANDOM CIRCULANT DETERMINANTS

SEAN EBERHARD AND PADRAIG Ó CATHÁIN

Abstract. We show that asymptotically almost all $n \times n$ circulant matrices with $\pm 1$ entries have determinant $\pm e^{-(\gamma + o(1))n/2} n^{n/2}$. A similar result is also proved for $G$-invariant $\pm 1$ matrices of order $n$ for any abelian group $G$ of order $n$.



## 1. Introduction

Let $M$ be an $n \times n$ matrix with entries $\pm 1$. By the well-known Hadamard bound, $\det(M)^2 \le n^n$. Matrices achieving equality are called *Hadamard matrices*. It was first observed by Turán that, if $M$ is chosen uniformly at random, $\mathbf{E}\left[\det(M)^2\right] = n!$ [Tur40]. By Stirling's approximation $n! = e^{-n+o(n)} n^n$, which implies that random matrices are generally far from Hadamard. More recently it was shown by Tao and Vu that $\det(M)^2 = n! e^{o(n)}$ with high probability [TV06].

Now consider a random *circulant* matrix with $\pm 1$ entries, i.e., a matrix $M$ of the form

$$M = (a_{i-j})_{i,j \in \mathbf{Z}/n\mathbf{Z}} \qquad (a_0, \dots, a_{n-1} = \pm 1).$$

For matrices of this form we show that the typical determinant is actually much larger than $n!^{1/2}$, though still much less than $n^{n/2}$, and the precise estimate involves an (initially) surprising appearance of the Euler–Mascheroni constant.

**Theorem 1.1.** *Asymptotically almost all $n \times n$ circulant matrices satisfy*

$$\det(M)^2 = e^{-\gamma n + o(n)} n^n,$$

*where $\gamma = 0.577\dots$ is the Euler–Mascheroni constant.*

**Remark 1.2** (Symmetry)**.** The distribution of $\det(M)$ is symmetric about zero. Indeed, if $P$ is the permutation matrix representing an $n$-cycle then the map $M \mapsto -PM$ is an involution of the set of $n \times n$ circulant matrices with $\pm 1$ entries such that $\det(-PM) = -\det(M)$ for all $M$.

**Remark 1.3** (Even moments)**.** The even moments of $\det(M)$ are heavily skewed by extreme values. Since the sample space has cardinality only $2^n$, if there is even a single circulant Hadamard matrix of order $n$ then

$$\mathbf{E}\left[\det(M)^4\right] \ge 2^{-n} n^{2n}.$$

---

SE is supported by the Royal Society.

There are no circulant Hadamard matrices for $4 < n < 4 \cdot 10^{33}$ [LS16], but there are circulant matrices which come within a linear factor of the Hadamard bound. For example, if $n$ is prime and $M = (a_{i-j})_{i,j \in \mathbf{Z}/n\mathbf{Z}}$ with $a_x = \left(\frac{x}{n}\right)$ for $x \neq 0$ and $a_0 = 1$ then $\det(M)^2 = (n \pm 1)^{n-1} \asymp n^{n-1}$. Moreover, computational evidence suggests that large determinants are not restricted to prime orders [BY18]. Based on this observation it seems likely that the even moments of $\det(M)$ are asymptotically given by

$$\mathbf{E}\left[\det(M)^{2k}\right] = \begin{cases} e^{-\gamma n + o(n)} n^n & : k = 1, \\ 2^{-n+o(n)} n^{kn} & : k \geq 2. \end{cases}$$

Note that Theorem 1.1 in particular asserts that asymptotically almost all $n \times n$ circulant matrices are nonsingular. Estimates for the singularity probability for circulant matrices were given by Meckes [Mec09, Theorem 6], and an asymptotic formula was recently given by Miller [Mil24].

Theorem 1.1 is a special case of a more general result about random $G$-invariant matrices, where $G$ is an arbitrary abelian group of order $n$ (written additively). Let $\mathrm{Mat}(G)$ denote the set of $G^2$-indexed $G$-invariant matrices with $\pm 1$ entries, i.e., matrices of the form

$$M = (a_{x-y})_{x,y \in G}, \qquad (a_x = \pm 1 \text{ for } x \in G).$$

We study the asymptotic proportion of nonsingular matrices in $\mathrm{Mat}(G)$ as well as the typical determinant of a nonsingular matrix. Recall that the Vinogradov notation $f \ll g$ means $f \leq O(g)$.

**Theorem 1.4.** *Let $G$ be an abelian group of order $n$, where $n \to \infty$. Let $n_d$ be the number of elements of order $d$ in $G$ for $d \in \{2, 3, 4, 6\}$.*

*(1) Asymptotically almost all nonsingular matrices in $\mathrm{Mat}(G)$ satisfy*

$$\det(M)^2 = e^{-\gamma n + o(n)} 2^{-n_2} n^n.$$

*(2) The proportion of nonsingular matrices in $\mathrm{Mat}(G)$ is bounded away from zero, and tends to 1 unless $n_2 \gg n^{1/2}$ or $n_3 + n_4 + n_6 \gg n$.*

*(3) Assume either $\min(n_2, n_3) \to \infty$ or $n_6 = n_2 n_3 = o(n)$. Then the proportion of nonsingular matrices in $\mathrm{Mat}(G)$ is*

$$\frac{1}{6}(1 + e^{-\lambda_2 n_2 / n^{1/2} - \lambda_4 n_4 / n})(2 + e^{-\lambda_3 n_3 / n}) e^{-\lambda_6 n_6 / n} + o(1),$$

*where*

$$\lambda_2 = 2\sqrt{2/\pi}, \qquad \lambda_3 = 3\sqrt{3}/\pi, \qquad \lambda_4 = 4/\pi, \qquad \lambda_6 = \sqrt{3}/\pi.$$

To illustrate the nonsingularity formula, consider the case of $G = C_d^m$ where $d \geq 2$ is fixed and $m \to \infty$. Then Theorem 1.4 asserts that the proportion of nonsingular matrices in $\mathrm{Mat}(C_d^m)$ tends to the constant

$$\begin{cases} 1/2 & : d = 2, \\ (2 + e^{-\lambda_3})/3 = 0.730\ldots & : d = 3, \\ (1 + e^{-\lambda_2 - \lambda_4})/2 = 0.528\ldots & : d = 4, \\ e^{-\lambda_6} = 0.576\ldots & : d = 6, \\ 1 & : \text{otherwise.} \end{cases}$$

Moreover, the nonsingularity formula is minimized with value $e^{-\lambda_6}/2 = 0.288\ldots$ when $n_2/n^{1/2} \to \infty$ and $n_6/n \to 1$, for example for the sequence $G = C_2^m \times C_6^m$,

The technical condition in part (3) is necessary. We are not certain of the asymptotic singularity probability for groups such as $G = C_2^m \times C_3$ or $G = C_2 \times C_3^m$, but we guess the following is true. If $n_2 \ll 1$, the nonsingularity probability is

$$\left(\frac{2 + e^{-3\lambda_6 n_3/n}}{3}\right)^{1+n_2} + o(1).$$

If $n_3 \ll 1$, the nonsingularity probability is

$$\frac{1}{2}(1 + e^{-\lambda_2 n_2/n^{1/2} - \lambda_4 n_4/n})\left(\frac{3 + e^{-8\lambda_6 n_2/n}}{4}\right)^{n_3/2} + o(1).$$

One can check that these formulas tend towards agreement with Theorem 1.4 as $n_2, n_3 \to \infty$.

## 2. Notation

If $G$ is an abelian group we write $\hat{G}$ for the group of characters $\chi : G \to \mathbf{C}^\times$. When $G$ is finite of order $n$ we elect to use the counting measure on $G$ and the uniform measure on $\hat{G}$. Thus, for $f \in L^2(G)$, our convention is that

$$\hat{f}(\chi) = \sum_{x \in G} f(x)\chi(-x), \qquad f(x) = \frac{1}{n}\sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).$$

We will also use Fourier analysis on various Euclidean spaces and we will be explicit about our normalization in due course.

We use standard asymptotic notation including big-$O$ and little-$o$. The notation $O_k(\cdot)$ indicates that the implicit constant may depend on the parameter $k$. As mentioned previously, the Vinogradov notation $f \ll g$ means $f \le O(g)$, $f \asymp g$ means $f \ll g$ and $f \gg g$, and $f \sim g$ means $f/g \to 1$.

The notation $[E]$ is used for the indicator of an event $E$. To avoid unwieldy superscripts, $e^{2\pi i x}$ is abbreviated in places to $e(x)$.

## 3. Idea

Let $M \in \mathrm{Mat}(G)$. Define $f : G \to \{\pm 1\}$ to be a function equal to the first row of $M$. Then $f$ is a uniformly random $\pm 1$ function on $G$, and $M$ represents the linear map of $L^2(G)$ defined by convolution with $f$, so the eigenvalues of $M$ are just the Fourier coefficients of $f$. In particular

$$\det(M) = \prod_{\chi \in \hat{G}} \hat{f}(\chi).$$

Thus $M$ is nonsingular if and only if $\hat{f}(\chi) \neq 0$ for all $\chi \in \hat{G}$. In view of Remark 1.3 it is clear that $\det(M)$ has super-exponential growth, and the key question is to estimate its decay from the Hadamard bound, so we consider

$$\log(\det(M)^2/n^n)/n = \frac{1}{n} \sum_{\chi \in \hat{G}} \log\left(|\hat{f}(\chi)|^2/n\right).$$

Letting $\mu_f$ denote the law of the discrete random variable $\chi \mapsto |\hat{f}(\chi)|^2/n$ (where $\chi \in \hat{G}$), we can express this equivalently as

$$\log(\det(M)^2/n^n)/n = \int \log x \, d\mu_f.$$

We will prove Theorem 1.1 and Theorem 1.4(1) by justifying a natural limit law for $\mu_f$ as $|G| \to \infty$. Let $Z \sim N_{\mathbf{C}}(0,1)$ be a stanard complex Gaussian random variable, which has density function $e^{-|z|^2}/\pi$. Let $\mu_{\mathbf{C}}$ denote the law of $|Z|^2$. In the case $G = C_n$ we will show that $\mu_f$ converges weakly to $\mu_{\mathbf{C}}$, and thus (ignoring for the moment the issue at zero) Theorem 1.1 will follow by recalling the identity

$$\mathbf{E}\left[\log\left(|Z|^2\right)\right] = \int_0^\infty e^{-t} \log t \, dt = \Gamma'(1) = -\gamma. \tag{3.1}$$

In the case of an arbitrary abelian group $G$ we must revise this model slightly. Let $r = n/(n_2+1)$ be the index of the 2-torsion subgroup $G[2] = \{g \in G : 2g = 0\}$. Then a proportion $1/r$ of the characters $\chi$ are real, and we should rather compare this part of the spectrum with a real Gaussian $X \sim N_{\mathbf{R}}(0,1)$, for which by contrast

$$\mathbf{E}\left[\log(|X|^2)\right] = \frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-t/2} t^{-1/2} \log t \, dt = -\gamma - \log 2. \tag{3.2}$$

Let $\mu_{\mathbf{R}}$ denote the law of $|X|^2$ where $X \sim N_{\mathbf{R}}(0,1)$. In general we will show, using the method of moments, that

$$\mu_f \approx (1 - r^{-1})\mu_{\mathbf{C}} + r^{-1}\mu_{\mathbf{R}}.$$

Theorem 1.4(1) will follow from this, but since $\log x$ is not a bounded function we must take special care with the extreme values of $|\hat{f}|$. For example, if there is any $\chi$ for which $\hat{f}(\chi) = 0$ then obviously $\det(M) = 0$. To finish the proof of part (1) of Theorem 1.4 we must show that the nonzero extreme values do not contribute significantly. This is the more difficult part of the proof. We also show that with high probability there are no zero Fourier coefficients unless $n_2 \gg n^{1/2}$ or $n_3 + n_4 + n_6 \gg n$, so in particular this will complete the proof of Theorem 1.1.

To prove part (2) of Theorem 1.4 we will establish a conditional Poisson model for the number of characters $\chi \in \hat{G}$ such that $\hat{f}(\chi) = 0$. It is easy to prove that only the characters of order $d \in \{2, 3, 4, 6\}$ are important here, so we may restrict to these characters. Now for any fixed character $\chi$ of order 2, the Fourier coefficient $\hat{f}(\chi)$ is just the result of a random walk of length $n$ in $\mathbf{Z}$ with $\pm 1$ steps, so by Stirling's approximation

$$\mathbf{P}\left[\hat{f}(\chi) = 0\right] = 2^{-n}\binom{n}{n/2} \sim (2/\pi)^{1/2} n^{-1/2}.$$

Similarly, for characters of order $d = 3, 4, 6$, one can compare $\hat{f}(\chi)$ with a random walk on a square or triangular lattice in the plane, and this leads to the approximation

$$\mathbf{P}\left[\hat{f}(\chi) = 0\right] \sim \begin{cases} (4/\pi) n^{-1} & : d = 4, \\ (2\sqrt{3}/\pi) n^{-1} & : d = 3, 6. \end{cases}$$

These approximations immediately suggest a rare-events-type model for the number of characters $\chi$ such that $\hat{f}(\chi) = 0$. However, there are two important obstructions to bear in mind. Let $H$ be the number of $x \in G$ such that $f(x) = 1$. If $\hat{f}(\chi) = 0$ for some character $\chi$ of order 2 or 4 then $H$ must be even. Similarly, if $\hat{f}(\chi) = 0$ and $\chi$ has order 3 then $H$ must be divisible by 3 (while if $\chi$ has order 6 there is no divisibility obstruction). Furthermore, since $f$ is real-valued, $\hat{f}(\bar{\chi}) = 0$ if and only if $\hat{f}(\chi) = 0$. Taking account of these corrections, it is reasonable to guess that the number of conjugate pairs of characters $\chi \in \hat{G}$ such that $\hat{f}(\chi) = 0$ converges to the model

$$\mathrm{Pois}(\lambda_2 n_2/n^{1/2} + \lambda_4 n_4/n)[2 \mid H] + \mathrm{Pois}(\lambda_3 n_3/n)[3 \mid H] + \mathrm{Pois}(\lambda_6 n_6/n),$$

where $\lambda_2, \lambda_3, \lambda_4, \lambda_6$ are the constants defined in the introduction, and this is indeed what we prove.

Unfortunately we must exclude the cases in which $\min(n_2, n_3) \ll 1$ and $n_6 \gg n$. In these cases the characters of order 6 do not behave sufficiently independently.

Finally, as a technical point, note that to prove Theorem 1.4 it suffices to show that an arbitrary sequence of abelian groups $G = G_i$ of order $n = n_i$ tending to infinity has a subsequence satisfying the conclusion of the theorem. This basic observation simplifies matters by allowing us to assume by compactness that various quantities converge. For example we may assume $n_d/n$ converges (necessarily to a point of $\{1, 1/2, 1/3, \dots\} \cup \{0\}$) for each $d \in \{2, 3, 4, 6\}$.

## 4. Bulk

The following calculation may be largely familiar to experts in additive combinatorics or harmonic analysis. See, e.g., [Gre01, Section 4.5].

**Lemma 4.1.** *Let $G$ be an abelian group of order $n$ and let $r$ be the index of $G[2] = \{g \in G : 2g = 0\}$. Let $f : G \to \{\pm 1\}$ be uniformly random. For any nonnegative integer $k$, let*

$$m_{2k} = \frac{1}{n} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^{2k}.$$

*Then*

*(1)* $\mathbf{E}\,[m_{2k}]/n^k = (1 - r^{-1})k! + r^{-1}\frac{(2k)!}{2^k k!} + O_k(n^{-1})$,

*(2)* $\mathbf{Var}\,[m_{2k}]/n^{2k} \le \frac{(4k)!}{2^{2k}(2k)!} n^{-1}$.

*Proof.* By expanding the definition of the Fourier transform,

$$\begin{aligned} |\hat{f}(\chi)|^{2k} &= \hat{f}(\chi)^k \overline{\hat{f}(\chi)^k} \\ &= \sum_{x_1, \dots, x_{2k} \in G} f(x_1) \cdots f(x_{2k}) \chi(x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k}). \end{aligned}$$

Recalling that $\sum_{\chi \in \hat{G}} \chi(x)$ vanishes unless $x = 0$, in which case the value is $n$, it follows that

$$m_{2k} = \frac{1}{n} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^{2k} = \sum_{\substack{x_1, \dots, x_{2k} \in G \\ \ell(x) = 0}} f(x_1) \cdots f(x_{2k}),$$

where

$$\ell(x) = x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k}.$$

Say a $2k$-tuple $(x_1, \dots, x_{2k})$ is *paired* its entries can be arranged into $k$ pairs of equal elements. The expectation of $f(x_1) \cdots f(x_{2k})$ is 1 if $(x_1, \dots, x_{2k})$ is paired and zero otherwise. Therefore $\mathbf{E}\,[m_{2k}]$ is exactly the number of paired $2k$-tuples $x \in G^{2k}$ such that $\ell(x) = 0$.

A *pairing* is a partition of $\{1, \dots, 2k\}$ into $k$ pairs. Call a pairing *good* if each pair contains one element of $\{1, \dots, k\}$ and one element of $\{k+1, \dots, 2k\}$, and *bad* otherwise. The number of pairings is $(2k)!/(2^k k!)$, of which $k!$ are good. If $x \in G^{2k}$ is paired by a good pairing then $\ell(x) = 0$ automatically. On the other hand, if $x$ is paired by a bad pairing $p$, say with $2t > 0$ pairs not crossing the partition, then $\ell(x) = 0$ reduces to an equation of the form

$$2(x_1 + \cdots + x_t - x_{t+1} - \cdots - x_{2t}) = 0,$$

i.e.,

$$x_1 + \cdots + x_t - x_{t+1} - \cdots - x_{2t} \in G[2].$$

It follows by choosing $x_1$ last that the number of $2k$-tuples paired by $p$ and satisfying $\ell(x) = 0$ is $n^k/r$. Finally, for any two pairings $p \neq q$, the number of $2k$-tuples paired by both $p$ and $q$ is $O(n^{k-1})$. We therefore have

$$\mathbf{E}\,[m_{2k}] = \Big(k! + r^{-1}((2k)!/(2^k k!) - k!)\Big)n^k + O_k(n^{k-1}).$$

This proves (1).

Next,

$$m_{2k} - \mathbf{E}\,[m_{2k}] = \sum_{\substack{x\in G^{2k}\\ \text{unpaired}\\ \ell(x)=0}} f(x_1)\cdots f(x_{2k}),$$

so

$$(m_{2k} - \mathbf{E}\,[m_{2k}])^2 = \sum_{\substack{x,y\in G^{2k}\\ \text{unpaired}\\ \ell(x)=\ell(y)=0}} f(x_1)\cdots f(x_{2k}) f(y_1)\cdots f(y_{2k}).$$

Again, each term in the sum above is either identically 1 or of mean zero, and the former holds if and only if the $4k$-tuple $(x_1,\dots,x_{2k},y_1,\dots,y_{2k})$ is paired. The variance $\mathbf{Var}\,[m_{2k}]$ is therefore exactly the number of paired $4k$-tuples $(x,y)$ such that $x$ and $y$ are unpaired and $\ell(x)=\ell(y)=0$. The number of pairings of $\{1,\dots,4k\}$ is $(4k)!/2^{2k}(2k)!$. Of these, we can ignore those that restrict to pairings on $\{1,\dots,2k\}$ and $\{2k+1,\dots,4k\}$. For any other pairing $p$, when we count the $4k$-tuples paired by $p$ and satisfying $\ell(x)=\ell(y)=0$, there is some variable $x_i$ paired with some variable $y_j$. The number of possible values of all the other variables is at most $n^{2k-1}$, after which the linear relation $\ell(x)=0$ determines $x_i=y_j$. Thus there are at most $n^{2k-1}$ $4k$-tuples paired by $p$ and satisfying $\ell(x)=\ell(y)=0$. This proves part (2). □

**Proposition 4.2.** *Let $(G_n)_{n\in I}$ be a sequence of abelian groups such that $|G_n| = n$ and $r_n = [G_n : G_n[2]]$ converges to $r \in \mathbf{Z}^+\cup\{\infty\}$. Let $f_n$ be a random $\pm1$ function on $G_n$. As in the previous section let $\mu_f$ denote the law of the random variable $\chi \mapsto |\hat{f}(\chi)|^2/n$ and let $\mu = (1-r^{-1})\mu_{\mathbf{C}} + r^{-1}\mu_{\mathbf{R}}$. Then there is a subsequence $(G_n)_{n\in I'}$ such that $\mu_{f_n}$ converges weakly to $\mu$ almost surely.*

*Proof.* By a standard exercise in integration by parts,

$$\int x^k\,d\mu_{\mathbf{C}} = k!, \qquad \int x^k\,d\mu_{\mathbf{R}} = \frac{(2k)!}{2^k k!}.$$

Therefore the $k$th moment of $\mu$ is $c_k = (1-r^{-1})k! + r^{-1}(2k)!/(2^k k!)$. By [Bil95, Theorem 30.1], $\mu$ is determined by its moments. On the other hand the $k$th moment of $\mu_{f_n}$ is $m_{2k}/n^k$, which by the prevous lemma and Chebyshev's inequality converges to $c_k$ in probability. By passing to a subsequence we may assume $m_{2k}/n^k \to c_k$ almost surely for all $k \ge 0$. Now applying [Bil95, Theorem 30.2], it follows that $\mu_{f_n}$ converges weakly to $\mu$ almost surely. □

**Remark 4.3.** Instead of using the method of moments directly, it is also possible to proceed using quantitative versions of the central limit theorem. See the results of Meckes [Mec09, Mec12]. In particular Proposition 4.2 is actually a special case of [Mec12, Theorem 4.1]. The above proof is included in the present paper because it is comparatively short.

## 5. Tails

The following lemma may be of independent interest.

**Lemma 5.1.** *Let $\zeta$ be a primitive $d$th root of unity. Let $n$ be a multiple of $d$ and let*

$$Z = \sum_{i=0}^{d-1} X_i \zeta^i,$$

*where $X_0, \dots, X_{d-1}$ are independent random walks in $\mathbf{Z}$ of length $n/d$ with $\pm 1$ steps. Then, for $t \geq 0$,*

$$\mathbf{P}\left[|Z|^2 \leq tn\right] \ll \begin{cases} t^{1/2} + n^{-1/2} & : d \leq 2, \\ t + d^{-2} n^{-1} \log n & : d \geq 3. \end{cases}$$

*Proof.* First assume $d \leq 2$. Then $Z$ is just a standard $\pm 1$ random walk in $\mathbf{Z}$ with $n$ steps, in particular integer-valued, and

$$\mathbf{P}\left[Z = 2k - n\right] = 2^{-n} \binom{n}{k} \ll n^{-1/2}.$$

It follows immediately that

$$\mathbf{P}\left[|Z| \leq (tn)^{1/2}\right] \leq (2(tn)^{1/2} + 1) n^{-1/2} \ll t^{1/2} + n^{-1/2}.$$

Now assume $d \geq 3$. We use a Fourier-analytic approach in the spirit of [TV10, Section 7.2]. Let $\mu$ be the law of $Z$. Then the Fourier transform (or characteristic function) of $\mu$ is

$$\hat{\mu}(w) = \mathbf{E}\left[e(-\langle w, Z\rangle)\right] = \prod_{i=0}^{d-1} \cos(2\pi \langle w, \zeta^i \rangle)^{n/d}. \tag{5.1}$$

Here $\langle w, z\rangle = \Re(\bar{w} z)$.

First consider (5.1) for $w$ close to 0. Using the approximation

$$\log \cos(2\pi x) = -2\pi^2 x^2 + O(x^4) \qquad (|x| \leq 1/5), \tag{5.2}$$

we have

$$\hat{\mu}(w) = \exp\left(-2\pi^2 \frac{n}{d} \sum_{i=0}^{d-1} \langle w, \zeta^i\rangle^2 + O(n|w|^4)\right) \qquad (|w| \leq 1/5).$$

Since $d \geq 3$,

$$\sum_{i=0}^{d-1} \langle w, \zeta^i \rangle^2 = \sum_{i=0}^{d-1} \frac{1}{4}\left(\bar{w}^2 \zeta^{2i} + 2w\bar{w} + w^2 \zeta^{-2i}\right) = d|w|^2/2.$$

Thus
$$\hat{\mu}(w) = \exp\left(-\pi^2 n|w|^2 + O(n|w|^4)\right) \qquad (|w| \le 1/5).$$
We therefore have an estimate of the form
$$0 < \hat{\mu}(w) \le e^{-c_1 n|w|^2} \qquad (|w| \le c_1),$$
for some constant $c_1 > 0$.

Now consider the range $c_1 \le |w| \le c_2 d$, where $c_2 = \min(c_1/10, (8\pi)^{-1})$. This range is empty if $d \le 10$, so we may assume $d > 10$. Assuming $\zeta = e(1/d)$ without loss of generality, we have $|\Re(\bar{w}\zeta^{i+1}) - \Re(\bar{w}\zeta^i)| \le 2\pi|w|/d$ for all $i$. It follows that every subinterval of $[0,|w|]$ of length at least $2\pi|w|/d$ contains at least one value of $\Re(\bar{w}\zeta^i)$. If $|w| \le 1/2$, we deduce that there are $\gg d$ values of $i$ such that $\Re(\bar{w}\zeta^i)/|w| \in [1/4, 3/4]$, which implies that $\Re(\bar{w}\zeta^i) \in [c_1/4, 3/8]$. If $|w| > 1/2$, there are $\gg |w|$ subintervals of $[0,|w|]$ of the form $[1/8, 3/8] + m$ ($m \in \mathbf{Z}$), and each of these contains $\gg d/|w|$ disjoint subintervals of length at least $2\pi|w|/d$ (since $2\pi|w|/d \le 1/4$). Thus there are $\gg d$ indices $i$ such that $\Re(\bar{w}\zeta^i)$ has fractional part in $[1/8, 3/8]$. Thus, in either case, from (5.1) we have an estimate of the form
$$|\hat{\mu}(w)| \le e^{-c_3 n} \qquad (c_1 \le |w| \le c_2 d).$$

Now, since[1]
$$\left[|z|^2 \le R\right] \le e^{\pi - \pi|z|^2/R},$$
we have
$$\mathbf{P}\left[|Z|^2 \le R\right] \le e^{\pi} \int e^{-\pi|z|^2/R}\, d\mu.$$
Recalling that $e^{-\pi|z|^2/R}$ has Fourier transform $Re^{-\pi R|w|^2}$, by Plancherel's identity we have
$$\int e^{-\pi|z|^2/R}\, d\mu = R\int_{\mathbf{C}} e^{-\pi R|w|^2}\hat{\mu}(w)\, dw.$$
We can bound the integral using our bounds for $\hat{\mu}$. The integral over the range $|w| \le c_1$ is bounded by
$$\int_{\mathbf{C}} e^{-c_1 n|w|^2}\, dw \asymp 1/n.$$
The integral over the range $c_1 \le |w| \le c_2 d$ is bounded by
$$\int_{\mathbf{C}} e^{-\pi R|w|^2 - c_3 n}\, dw \asymp e^{-c_3 n}/R.$$
Finally, since $|\hat{\mu}(w)| \le 1$ the integral over the range $|w| \ge c_2 d$ is bounded by
$$\int_{|w|\ge c_2 d} e^{-\pi R|w|^2}\, dw = R^{-1}\int_{|w|\ge c_2 R^{1/2} d} e^{-\pi|w|^2}\, dw \ll e^{-c_2 R d^2} d/R^{1/2}.$$

[1]Recall that we use the Iverson bracket notation $[P]$, which is defined to be 1 if $P$ is true and 0 otherwise. Here, this is the characteristic function of the disk of radius $\sqrt{R}$, and the inequality is to be understood pointwise.

If $R \geq 10c_2^{-1}(\log n)/d^2 \gg 1/n^2$, this last quantity is no larger than $n^{-10}dn^1 \leq n^{-8}$. Thus, provided $R \geq 10c_2^{-1}(\log n)/d^2$, the integral is bounded by

$$O(1/n + e^{-c_3 n}/R + e^{-c_2 R d^2} d/R^{1/2}) = O(1/n),$$

and we have $\mathbf{P}\left[|Z|^2 \leq R\right] \ll R/n$. Set $R = tn + C(\log n)/d^2$ to get the result. $\square$

**Lemma 5.2.** *Let $Z$ be as in the previous lemma. Then*

$$\mathbf{P}[Z = 0] \leq \min(O(d/n)^{1/2}, 1/2)^{\varphi(d)} \ll \begin{cases} n^{-1/2} & : d \in \{1,2\}, \\ n^{-1} & : d \in \{3,4,6\}, \\ n^{-2} & : \textit{otherwise}. \end{cases}$$

*Moreover if $Z \neq 0$ then*

$$n^{1-\varphi(d)} \leq |Z| \leq n.$$

*Proof.* Let $L : \mathbf{Q}^d \to \mathbf{Q}[\zeta] \cong \mathbf{Q}^{\varphi(d)}$ be the linear map defined by

$$L(x) = \sum_{i=0}^{d-1} x_i \zeta^i.$$

By Gaussian elimination there is a set $S \subset \{0, \dots, d-1\}$ of cardinality $\varphi(d)$ such that if $L(x) = 0$ then the variables $(x_i)_{i \in S}$ are determined (linearly) by the others. By conditioning on the values of $(X_i)_{i \notin S}$, it follows that

$$\begin{aligned} \mathbf{P}[Z = 0] = \mathbf{P}[L(X_0, \dots, X_{d-1}) = 0] &\leq \prod_{i \in S} \max_y \mathbf{P}[X_i = y] \\ &\leq \min(O(d/n)^{1/2}, 1/2)^{\varphi(d)}. \end{aligned}$$

This proves the first inequality. The second inequality is clear for $d \leq 12$. If $13 \leq d \leq n^{1/3}$ then $\phi(d) \geq 6$, so we get $O(n^{-1/3})^6 \ll n^{-2}$. Finally, if $d \geq n^{1/3}$ then since $\phi(d) \gg d/\log\log d$ we get the much stronger bound $\exp(-cn^{1/3}/\log\log n)$.

For the last part, obviously $|Z| \leq n$. By applying this bound to the Galois conjugates of $Z$ it follows that

$$|\mathcal{N}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(Z)| \leq |Z| n^{\varphi(d)-1}.$$

On the other hand $Z$ is an algebraic integer, so its norm is a nonzero integer if $Z \neq 0$ and it follows that $|Z| \geq n^{1-\varphi(d)}$. $\square$

**Proposition 5.3.** *Let $T \geq 1$ be a parameter. Let $G$ be an abelian group of order $n$ and let $f : G \to \{\pm 1\}$ be a uniformly random function. Let $S$ be the event that $\hat{f}(\chi) = 0$ for some $\chi \in \hat{G}$.*

*(0)* $\mathbf{P}[S] \ll (1 + n_2)/n^{1/2} + (n_3 + n_4 + n_6)/n$.
*(1)* $\mathbf{P}[\mu_f((0,\delta)) > 0] \ll (\log n)^{-1}$ *where* $\delta = n^{-2\log n}$.
*(2)* $\mathbf{E}\left[\int_\delta^{1/T} |\log x| \, d\mu_f\right] \ll T^{-1/2} \log T$.
*(3)* $\mathbf{E}\left[\int_T^\infty |\log x| \, d\mu_f\right] \ll e^{-cT}$.

*(4)* $\mathbf{P}\left[S^c \wedge \int_{[1/T,T]^c} |\log x| \, d\mu_f > T^{-1/4}\right] \ll T^{-1/4} \log T + (\log n)^{-1}$.

*Proof.* (0) This follows immediately from the previous lemma and a union bound:

$$\mathbf{P}[S] \le \sum_{\chi \in \hat{G}} \mathbf{P}\left[\hat{f}(\chi) = 0\right] \ll (n_1 + n_2)/n^{1/2} + (n_3 + n_4 + n_6)/n + 1/n.$$

(1) Let $\chi \in \hat{f}(\chi)$ be a character of order $d$. If $d \le \log n$ then $n^{-2\log(n)} < n^{1-\phi(d)}$ and by Lemma 5.2, it follows that $|\hat{f}(\chi)|^2/n \notin (0, \delta)$. On the other hand if $d \ge \log n$ then by Lemma 5.1 we have

$$\mathbf{P}\left[|\hat{f}(\chi)|^2/n \le \delta\right] \ll \delta + d^{-2} n^{-1} \log n \ll (n \log n)^{-1}.$$

The result follows from a union bound over the characters of $G$.

(2) Let $F(x) = |\log(x)|[\delta \le x \le 1/T]$. By summing over dyadic intervals and applying Lemma 5.1, noting that the bound for real characters is strictly larger than for $d \ge 3$ in this parameter range,

$$\begin{aligned} \mathbf{E}\left[F(|\hat{f}(\chi)|^2/n)\right] &\le \sum_{\substack{\delta \le t \le 1/T \\ \text{dyadic}}} |\log(t/2)| \, \mathbf{P}\left[|\hat{f}(\omega)|^2/n \in [t/2, t]\right] \\ &\ll \sum_{\substack{\delta \le t \le 1/T \\ \text{dyadic}}} |\log(t/2)| \left(t^{1/2} + n^{-1/2}\right) \\ &\ll T^{-1/2} \log T + n^{-1/2} (\log n)^5. \end{aligned}$$

The second term is $o(1)$, so this is $O(T^{-1/2} \log T)$. Averaging over $\chi \in \hat{G}$ gives the claim.

(3) Let $F(x) = (\log x)[x \ge T]$. By Hoeffding's inequality (e.g., [TV10, (1.3.5)]) applied to the real and imaginary parts separately, for any fixed $\chi \in \hat{G}$ and real number $t > 0$ we have

$$\mathbf{P}\left[|\hat{f}(\chi)|^2 \ge tn\right] \ll e^{-t/4}.$$

By summing over dyadic intervals it follows that

$$\begin{aligned} \mathbf{E}\left[F(|\hat{f}(\chi)|^2/n)\right] &\le \sum_{\substack{t \ge T \\ \text{dyadic}}} \log(2t) \, \mathbf{P}\left[\frac{|\hat{f}(\omega)|^2}{n} \in [t, 2t]\right] \\ &\ll \sum_{\substack{t \ge T \\ \text{dyadic}}} \log(2t) e^{-t/4} = O(e^{-cT}). \end{aligned}$$

Averaging over $\chi \in \hat{G}$ gives $\mathbf{E}\left[\int F \, d\mu_f\right] = O(e^{-cT})$.

(4) Combine (1)–(3) and Markov's inequality. $\square$

## 6. Determinant

Let $G_n$ be an abelian group of order $n$ and let $M_n \in \mathrm{Mat}(G_n)$ be uniformly random. Let $f : G_n \to \{\pm 1\}$ be given by the first row of $M_n$. Let $r_n$ be the index of $G_n[2]$ in $G_n$. Let $S_n$ be the event that $\hat{f}(\chi) = 0$ for some $\chi \in \hat{G}$. Where $S_n^c$ holds let

$$L_n = \log(\det(M_n)^2/n^n)/n = \int \log(x)\, d\mu_f.$$

Theorem 1.4(1) is equivalent to the assertion that, for every $\epsilon > 0$,

$$\limsup_{n\to\infty} \mathbf{P}\left[S_n^c \wedge |L_n + \gamma + (\log 2)/r_n| \geq \epsilon\right] \leq \epsilon. \tag{6.1}$$

Theorem 1.1 is the special case that $G$ is cyclic, in which case $S_n^c$ tends to 1 and $r_n \geq n/2$. Pass to a subsequence realizing the limsup. Passing to a further subsequence, we may assume $r_n$ converges to some $r \in \mathbf{Z}^+ \cup \{\infty\}$ and, by Proposition 4.2, we may also assume that $\mu_f$ converges weakly to $\mu = (1 - r^{-1})\mu_{\mathbf{C}} + r^{-1}\mu_{\mathbf{R}}$ almost surely.

Let $T \geq 1$ be a parameter and let

$$F(x) = \max(-\log T, \min(\log T, \log x)).$$

Then $F$ is a bounded continous function on $[0, \infty)$ such that

$$|F(x) - \log x| \leq |\log x|([x < 1/T] + [x > T]).$$

Therefore

$$\begin{aligned}\left|\int \log x\, d(\mu_f - \mu)\right| &= \left|\int F\, d(\mu_f - \mu) + \int (\log x - F)\, d(\mu_f - \mu)\right| \\ &\leq \left|\int F\, d(\mu_f - \mu)\right| + \int_{[1/T,T]^c} |\log x| d(\mu_f + \mu).\end{aligned}$$

Note that

$$\begin{aligned}\int_{[1/T,T]^c} |\log x|\, d\mu &\ll \left(\int_0^{1/T} + \int_T^\infty\right)\left(e^{-t}\log t + e^{-t/2}t^{-1/2}\log t\right) dt \\ &\ll T^{-1/2}\log T + e^{-T/2}\log T.\end{aligned}$$

Therefore if $T$ is large enough then $\int_{[1/T,T^c]} |\log x|\, d\mu \leq \epsilon/4$. It follows that

$$\mathbf{P}\left[S_n^c \wedge \left|\int \log x\, d(\mu_f - \mu)\right| \geq \epsilon/2\right] \leq P_1 + P_2,$$

where

$$\begin{aligned}P_1 &= \mathbf{P}\left[\left|\int F\, d(\mu_f - \mu)\right| \geq \epsilon/8\right], \\ P_2 &= \mathbf{P}\left[S_n^c \wedge \int_{[1/T,T]^c} |\log x|\, d\mu_f \geq \epsilon/8\right].\end{aligned}$$

By Proposition 5.3(4),

$$P_2 \ll T^{-1/4} \log T + (\log n)^{-1},$$

so if $T$ is a large enough constant and $n$ is large enough we have $P_2 \le \epsilon$. Finally, if $T$ is fixed and $n \to \infty$ then $P_1 \to 0$ since $\mu_f \to \mu$ weakly almost surely. Thus

$$\limsup \mathbf{P}\left[S_n^c \wedge \left|\int \log x \, d(\mu_f - \mu)\right| \ge \epsilon/2\right] \le \epsilon.$$

By (3.1)–(3.2) we have

$$\int \log x \, d(\mu_f - \mu) = L_n + \gamma + (\log 2)/r.$$

Since $r_n \to r$, (6.1) follows. This completes the proofs of Theorem 1.4(1) and Theorem 1.1.

## 7. Singularity

In this final section we study $\mathbf{P}[\det(M) = 0]$. By Proposition 5.3(0), $\mathbf{P}[\det(M) = 0]$ tends to zero unless $n_2 \gg n^{1/2}$ or $n_3 + n_4 + n_6 \gg n$. The following key calculation will enable us to complete the proof of Theorem 1.4 in full generality.

If $\chi \in \hat{G}$, the character $\chi^{-1}$ is defined by $\chi^{-1}(g) = \chi(-g) = \overline{\chi(g)}$. We say $\chi_1, \dots, \chi_k \in \hat{G}$ are *independent* if

$$G/\bigcap_{i=1}^{k} \ker \chi_i \cong \prod_{i=1}^{k} G/\ker \chi_i.$$

**Proposition 7.1.** *Let $G$ be an abelian group of order $n$ and let $f : G \to \{\pm 1\}$ be a uniformly random function. Let*

$$H = \sum_{g \in G} \frac{f(g) + 1}{2} \bmod 6.$$

*Let $\chi_1, \dots, \chi_k \in \hat{G}$ be a collection of $k = k_2 + k_3 + k_4 + k_6$ characters, of which $k_d$ have order $d$ for $d = 2, 3, 4, 6$. Let*

$$Z = (\hat{f}(\chi_1), \dots, \hat{f}(\chi_k)).$$

*(0) If $k_2 + k_4 > 0$ and $h$ is odd or $k_3 > 0$ and $h$ is not divisible by 3 then*

$$\mathbf{P}[H = h, Z = 0] = 0.$$

*(1) Assume $\chi_i \ne \chi_j^{\pm 1}$ for $i \ne j$. Then*

$$\mathbf{P}[H = h, Z = 0] \ll_k \frac{1}{n^{k_2/2 + k_3 + k_4 + k_6}}.$$

(2) *Assume $\chi_1, \dots, \chi_k$ are independent. If $k_2 + k_4 > 0$ assume $h$ is even. If $k_3 > 0$ assume $h$ is divisible by 3. Then for $k$ fixed and $n \to \infty$ we have*

$$\mathbf{P}\left[H = h, Z = 0\right] \sim \frac{1}{6} \frac{\lambda_2^{k_2}(2\lambda_3)^{k_3}(2\lambda_4)^{k_4}(2\lambda_6)^{k_6}}{n^{k_2/2+k_3+k_4+k_6}}.$$

*Proof.* Part (0) is easy to check. If $\hat{f}(\chi) = 0$ where $\chi$ has order 2 then the ones of $f$ must be evenly divided between $\chi(g) = 1$ and $\chi(g) = -1$, so $H$ must be even. Similarly if $\chi$ has order 4 then there must be equally many ones on $\chi(g) = 1$ as $\chi(g) = -1$ as well as equally many ones on $\chi(g) = i$ as $\chi(g) = -i$. Finally, if $\chi$ has order 3 and $\hat{f}(\chi) = 0$ then we have

$$\sum_{\chi(g)=1} f(g) = \sum_{\chi(g)=\omega} f(g) = \sum_{\chi(g)=\omega^2} f(g),$$

which implies that $\sum_{g\in G} f(g) = 2H - n$ is divisible by 3. Since $n$ also must be divisible by 3 in this case, this implies that $H$ is divisible by 3.

Now consider parts (1) and (2). Observe that $(H, Z)$ takes values in the lattice

$$L = \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}^{k_2} \times \mathbf{Z}[\omega]^{k_3} \times \mathbf{Z}[i]^{k_4} \times \mathbf{Z}[\omega]^{k_6}$$

of

$$V = \mathbf{Z}/6\mathbf{Z} \times \mathbf{R}^{k_2} \times \mathbf{C}^{k_3+k_4+k_6},$$

where $\omega = (-1 + \sqrt{-3})/2$. Let $\mu$ be the law of $(H, Z)$. Then the Fourier transform $\hat{\mu} : V \to \mathbf{C}$ is given by

$$\begin{aligned}
\hat{\mu}(v) &= \mathbf{E}\left[e\left(-\frac{v_0}{6}\sum_{g\in G}\frac{f(g)+1}{2} - \sum_{i=1}^{k}\langle v_i, \hat{f}(\chi_i)\rangle\right)\right] \\
&= \mathbf{E}\left[e\left(-v_0 n/12 - \sum_{g\in G} f(g)\left(v_0/12 + \sum_{i=1}^{k}\langle v_i, \chi_i(-g)\rangle\right)\right)\right] \\
&= F(v)^{n/m},
\end{aligned}$$

where $m$ is the order of $\bar{G} = G/\bigcap_{i=1}^{k}\ker\chi_i$ and

$$F(v) = e(-v_0 m/12)\prod_{g\in\bar{G}}\cos\left(2\pi\left(v_0/12 + \sum_{i=1}^{k}\langle v_i, \chi_i(g)\rangle\right)\right). \tag{7.1}$$

Note that $F$ is $L^\perp$-periodic. By integrating over a fundamental domain for $L^\perp$ we get the Fourier inversion formula

$$\mathbf{P}\left[H = h, Z = 0\right] = \frac{1}{\mathrm{vol}(V/L^\perp)}\int_{V/L^\perp} e(v_0 h/6)F(v)^{n/m}\,dv. \tag{7.2}$$

Here we normalize the measure on $V$ so that $\mathrm{vol}(V/\mathbf{Z}^k) = 6$.

Our first step is to study $F(v)$ in a neighbourhood of zero. Let $I_d$ be the set of indices $i$ such that $\chi_i$ has order $d$ for $d \in \{2,3,4,6\}$. For $v \in V$ define

$$\|v\|^2 = \sum_{i \in I_2} |v_i|^2 + \sum_{i \in I_3 \cup I_4 \cup I_6} |v_i|^2/2.$$

Let $B = \{v \in V : v_0 = 0, \|v\| \le 1/(10k)\}$. By (5.2), (7.1), and orthogonality of $\chi_1^{\pm 1}, \dots, \chi_k^{\pm 1}$ we have

$$\begin{aligned} F(v) &= \exp\left(-2\pi^2 \sum_{g \in \bar{G}} \left(\sum_{i=1}^k \langle v_i, \chi_i(g)\rangle\right)^2 + O_k(\|v\|^4)\right) \qquad (v \in B) \\ &= \exp\left(-2\pi^2 m \|v\|^2 + O_k(\|v\|^4)\right). \end{aligned}$$

It follows by a scalar change of variables that

$$\begin{aligned} \int_B F(v)^{n/m}\, dv &= \int_B e^{-2\pi^2 n\|v\|^2 + O_k(n\|v\|^4)}\, dv \\ &= n^{-k_2/2 - k_3 - k_4 - k_6} \int_{n^{1/2}B} e^{-2\pi^2\|v\|^2 + O_k(n^{-1}\|v\|^4)}\, dv. \end{aligned}$$

By the dominated convergence theorem, the last integral converges to

$$\begin{aligned} \int_V e^{-2\pi^2\|v\|^2}\, dv &= \left(\int_{\mathbf{R}} e^{-2\pi^2 x^2}\, dx\right)^{k_2} \left(\int_{\mathbf{C}} e^{-\pi^2|z|^2}\, dz\right)^{k_3+k_4+k_6} \\ &= (2\pi)^{-k_2/2}\pi^{-k_3-k_4-k_6}. \end{aligned}$$

Thus

$$\int_B F(v)^{n/m}\, dv \sim \frac{(2\pi)^{-k_2/2}\pi^{-k_3-k_4-k_6}}{n^{k_2/2+k_3+k_4+k_6}}. \tag{7.3}$$

Next, consider the subgroup $\Lambda \le V$ defined by $|F(v)| = 1$, namely

$$\Lambda = \left\{ v \in V : v_0/12 + \sum_{i=1}^k \langle v_i, \chi_i(g)\rangle \in \frac{1}{2}\mathbf{Z} \text{ for all } g \in \bar{G} \right\}.$$

Since $\Lambda \ge L^\perp$ and $|F(v)| < 1$ for $0 \ne v \in B$, it is clear that $\Lambda$ is cocompact and discrete, i.e., a lattice in $V$. We claim that $F$ is actually $\Lambda$-periodic. Since $\cos(2\pi(x+1/2)) = -\cos(2\pi x)$ it is clear that $|F(u+v)| = |F(u)|$ for $u \in V$ and $v \in \Lambda$, and in fact the overall modulation is

$$e(-v_0 m/12) \prod_{g \in \bar{G}} e\left(v_0/12 + \sum_{i=1}^k \langle v_i, \chi_i(g)\rangle\right) = 1.$$

Thus we can simplify the formula (7.2). If $e(v_0 h/6)$ is a nontrivial character on $\Lambda$ the result is $\mathbf{P}[H = h, Z = 0] = 0$, and otherwise we get

$$\mathbf{P}[H = h, Z = 0] = \frac{1}{\mathrm{vol}(V/\Lambda)} \int_{V/\Lambda} e(v_0 h/6) F(v)^{n/m}\, dv.$$

Since $\Lambda$ depends only on $F$ (and therefore on $\chi_1, \dots, \chi_k$ but not on $n$) and $|F(v)| < 1$ for $0 \neq v \in V/\Lambda$, it follows from (7.3) that

$$\mathbf{P}\left[H = h, Z = 0\right] \sim \frac{\mathrm{vol}(V/\Lambda)^{-1}(2\pi)^{-k_2/2}\pi^{-k_3-k_4-k_6}}{n^{k_2/2+k_3+k_4+k_6}}. \tag{7.4}$$

Since $\mathrm{vol}(V/\Lambda) \asymp_k 1$, part (1) follows immediately.

Now assume that $\bar{G} \cong C_2^{k_2} \times C_3^{k_3} \times C_4^{k_4} \times C_6^{k_6}$. Then $v \in \Lambda$ if and only if

$$v_0/12 + \sum_{i \in I_2} (-1)^{e_i} v_i + \sum_{i \in I_3} \langle \omega^{e_i}, v_i \rangle + \sum_{i \in I_4} \langle i^{e_i}, v_i \rangle + \sum_{i \in I_6} \langle (-\omega)^{e_i}, v_i \rangle \in \frac{1}{2}\mathbf{Z},$$

for all integers $e_1, \dots, e_k$. By considering individual changes in $e_1, \dots, e_k$ we find that $v \in \Lambda$ if and only if

$$\begin{aligned}
&v_i \in \frac{1}{4}\mathbf{Z} && (i \in I_2),\\
&v_i \in \frac{1}{3}\mathbf{Z}[\omega] && (i \in I_3),\\
&v_i \in \frac{1}{2}\mathbf{Z}[i] + \{0, (1+i)/4\} && (i \in I_4),\\
&v_i \in \mathbf{Z}[\omega] + \{0, \pm(1+2\omega)/3\} && (i \in I_6),
\end{aligned}$$

and

$$v_0/12 + \sum_{i=1}^{k} \Re(v_i) \in \frac{1}{2}\mathbf{Z}.$$

Since $v_0 \in \mathbf{Z}/6\mathbf{Z}$, the last condition is equivalent to

$$v_0 = -12 \sum_{i=1}^{k} \Re(v_i).$$

Thus

$$\mathrm{vol}(V/\Lambda) = 6 \cdot 4^{-k_2} (6\sqrt{3})^{-k_3} 8^{-k_4} (2\sqrt{3})^{-k_6}.$$

Moreover for $v \in \Lambda$ we have

$$e(v_0 h/6) = e\left(-2h \sum_{i=1}^{k} \Re(v_i)\right).$$

Since

$$\begin{aligned}
&2\Re\left(\frac{1}{4}\mathbf{Z}\right) &&= \frac{1}{2}\mathbf{Z},\\
&2\Re\left(\frac{1}{3}\mathbf{Z}[\omega]\right) &&= \frac{1}{3}\mathbf{Z},\\
&2\Re\left(\frac{1}{2}\mathbf{Z}[i] + \{0, (1+i)/4\}\right) &&= \frac{1}{2}\mathbf{Z},\\
&2\Re(\mathbf{Z}[\omega] + \{0, \pm(1+2\omega)/3\}) &&= \mathbf{Z},
\end{aligned}$$

we find that $e(v_0h/6)$ defines a nontrivial character on $\Lambda$ if and only if $k_2 + k_4 > 0$ and $h$ is odd or $k_3 > 0$ and $h$ is not divisible by 3. By combining with (7.4) we deduce (2). $\square$

We can now complete the proof of Theorem 1.4(2). Consider a sequence of abelian groups $G$ of order $n$ tending to infinity. By passing to a subsequence we may assume $\lambda_2 n_2/n^{1/2} \to x_2 \in [0, \infty]$ and $\lambda_d n_d/n \to x_d \in [0, 1]$ for $d \in \{3, 4, 6\}$. Let $f : G \to \{\pm 1\}$ be a random function. As in Proposition 7.1 let $H$ be the number of ones modulo 6, and note that $H$ tends to the uniform distribution on $\mathbf{Z}/6\mathbf{Z}$.

By the proof of Proposition 5.3(0), with probability $1 - O(1/n^{1/2})$ there are no characters such that $\hat{f}(\chi) = 0$ apart from characters of order $2, 3, 4, 6$. Let $X_2$ be the set of $n_2$ characters $\chi \in \hat{G}$ of order 2 and for $d = 3, 4, 6$ let $X_d \subset \hat{G}$ be a set of cardinality $n_d/2$ containing one of each conjugate pair of characters of order $d$. Let $N_d$ be the number of characters $\chi \in X_d$ such that $\hat{f}(\chi) = 0$ and let $N = N_2 + N_3 + N_4 + N_6$.

First we argue that the $\mathbf{P}[N = 0]$ is bounded away from zero. Since $\mathbf{P}[H = \pm 1] \sim 1/3$, it suffices to condition on this event, which implies $N_2 = N_3 = N_4 = 0$, so $N = N_6$. Now by Proposition 7.1(2) with $(k_2, k_3, k_4, k_6) = (0, 0, 0, 1)$ we have

$$\mathbf{P}[N_6 > 0 \mid H = \pm 1] \le \mathbf{E}[N_6 \mid H = \pm 1] \to x_6 \le \lambda_6.$$

Thus

$$\mathbf{P}[N = 0] \ge \frac{1}{3}\mathbf{P}[N_6 = 0 \mid H = 1] - o(1) \ge (1 - \lambda_6)/3 - o(1).$$

Note that $(1 - \lambda_6)/3 = 0.149\ldots > 0$.

Next, with the exception of the cases in which $\min(n_2, n_3) \ll 1$ and $n_6 = n_2 n_3 \gg n$, we claim that

$$\mathbf{P}[N = 0 \mid H = h] \to \begin{cases} e^{-x_2 - x_3 - x_4 - x_6} & : h = 0, \\ e^{-x_2 - x_4 - x_6} & : h = 2, 4, \\ e^{-x_3 - x_6} & : h = 3, \\ e^{-x_6} & : h = 1, 5. \end{cases} \tag{7.5}$$

First consider the case in which $x_2 < \infty$. For any integers $k_2, k_3, k_4, k_6 \ge 0$, consider the mixed moment

$$\mathbf{E}\left[\binom{N_2}{k_2}\binom{N_3}{k_3}\binom{N_4}{k_4}\binom{N_6}{k_6} \mid H = h\right] = \sum_{\chi_1, \ldots, \chi_k} \mathbf{P}\left[\bigcap (\hat{f}(\chi_i) = 0) \mid H = h\right],$$

where the sum is taken over all $k$-tuples

$$(\chi_1, \ldots, \chi_k) \in \binom{X_2}{k_2} \times \binom{X_3}{k_3} \times \binom{X_4}{k_4} \times \binom{X_6}{k_6}.$$

The number of such tuples is

$$\binom{n_2}{k_2}\binom{n_3/2}{k_3}\binom{n_4/2}{k_4}\binom{n_6/2}{k_6} \sim \frac{n_2^{k_2}(n_3/2)^{k_3}(n_4/2)^{k_4}(n_6/2)^{k_6}}{k_2! k_3! k_4! k_6!}.$$

If $k_2 + k_4 > 0$ assume $h$ is even, and if $k_3 > 0$ assume $h$ is divisible by 3 (otherwise the moment is trivially zero). We claim that Proposition 7.1 implies that

$$\mathbf{E}\left[\binom{N_2}{k_2}\binom{N_3}{k_3}\binom{N_4}{k_4}\binom{N_6}{k_6} \mid H = h\right] \to \frac{x_2^{k_2} x_3^{k_3} x_4^{k_4} x_6^{k_6}}{k_2! k_3! k_4! k_6!}. \tag{7.6}$$

If $x_2^{k_2} x_3^{k_3} x_4^{k_4} x_6^{k_6} = 0$ then this follows from part (1), so assume $x_d > 0$ for each $d$ such that $k_d > 0$. Then almost all of the given $k$-tuples $(\chi_1, \dots, \chi_k)$ are independent. Indeed, otherwise there is some nontrivial relation

$$\chi_1^{e_1} \cdots \chi_k^{e_k} = 1.$$

There are only $O_k(1)$ possible relations, so it suffices to consider each one individually. Suppose say $\chi_i$ has order $d$ and $e = e_i$ is not divisible by $d$. Note then $x_d > 0$. We may assume $e$ is a proper divisor of $d$. Then $\chi_i^e$ is determined by the other $\chi_j$, and the number of choices for $\chi_i$ given $\chi_i^e$ is at most $n_e$. We are done if $e = 1$ since $n_1 = 1$. If $d = 4$ and $e = 2$ then since $n_2 \le n_4^{1/2}$ we get the bound $n_d^{-1/2}$, which tends to zero. Finally, if $d = 6$ and $e \in \{2, 3\}$ then we get the bound $(n_2 + n_3)/n_6$, which tends to zero by our technical hypothesis. Therefore, applying part (2) of Proposition 7.1 for the independent $k$-tuples and part (1) for the others, we get the claimed limit (7.6).

Since the Poisson distribution is determined by its moments, it follows that $(N \mid H = h)$ converges in distribution to

$$\mathrm{Pois}(x_2 + x_4)[2 \mid h] + \mathrm{Pois}(x_3)[3 \mid h] + \mathrm{Pois}(x_6),$$

and this implies (7.5). Alternatively, more directly, one can use the Bonferroni inequalities

$$\sum_{k=0}^{K} (-1)^k \binom{N}{k} \le [N = 0] \le \sum_{k=0}^{K+1} (-1)^k \binom{N}{k} \qquad (K \text{ odd}),$$

estimating $\mathbf{E}\left[\binom{N}{k} \mid H = h\right]$ using (7.6) and the binomial theorem.

Now assume $x_2 = \infty$. The same analysis as above demonstrates that $(N \mid H = h)$ converges in distribution to $\mathrm{Pois}(x_3)[3 \mid h] + \mathrm{Pois}(x_6)$ when $h$ is odd. Assume $h$ is even. Then from Proposition 7.1 we have

$$\mathbf{E}\left[N_2 \mid H = h\right] \sim \lambda_2 n_2 / n^{1/2} \to \infty$$

and

$$\mathbf{E}\left[N_2(N_2 - 1) \mid H = h\right] \sim \lambda_2^2 n_2 (n_2 - 1)/n \sim \mathbf{E}\left[N_2 \mid H = h\right]^2,$$

so by Chebyshev's inquality

$$\begin{aligned} \mathbf{P}\left[N_2 = 0 \mid H = h\right] &\le \frac{\mathbf{E}\left[N_2^2 \mid H = h\right] - \mathbf{E}\left[N_2 \mid H = h\right]^2}{\mathbf{E}\left[N_2 \mid H = h\right]^2} \\ &= \frac{1}{\mathbf{E}\left[N_2 \mid H = h\right]} + \frac{\mathbf{E}\left[N_2(N_2 - 1) \mid H = h\right]}{\mathbf{E}\left[N_2 \mid H = h\right]^2} - 1 \to 0. \end{aligned}$$

Thus $N$ is positive with probability $1 - o(1)$ whenever $H$ is even. This completes the proof.

## References


[Bil95] P. Billingsley, *Probability and measure*, Third, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995. A Wiley-Interscience Publication. MR1324786 ↑4

[BY18] R. P. Brent and A. B. Yedidia, *Computation of maximal determinants of binary circulant matrices*, J. Integer Seq. **21** (2018), no. 5, article 18.5.6, 19 (English). ↑1.3

[Gre01] B. Green, *Some applications of harmonic analysis to arithmetic combinatorics* (2001). Smith-Knight Prize essay, Cambridge University. ↑4

[LS16] K. H. Leung and B. Schmidt, *The anti-field-descent method*, J. Comb. Theory, Ser. A **139** (2016), 87–131 (English). ↑1.3

[Mec09] M. W. Meckes, *Some results on random circulant matrices*, High dimensional probability V: the Luminy volume, 2009, pp. 213–223. MR2797949 ↑1, 4.3

[Mec12] ———, *The spectra of random abelian G-circulant matrices*, ALEA Lat. Am. J. Probab. Math. Stat. **9** (2012), no. 2, 435–450. MR3069372 ↑4.3

[Mil24] N. Miller, *On the singularity probability of random circulant Bernoulli matrices*, arXiv e-prints (Nov. 2024), arXiv:2411.17577, available at `https://arxiv.org/abs/2411.17577`. ↑1

[Tur40] P. Turán, *On extremal problems concerning determinants*, Math. Naturwiss. Anz. Ungar. Akad. Wiss. **59** (1940), 95–105. MR4215 ↑1

[TV06] T. Tao and V. Vu, *On random* $\pm 1$ *matrices: singularity and determinant*, Random Structures Algorithms **28** (2006), no. 1, 1–23. MR2187480 ↑1

[TV10] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2010. Paperback edition [of MR2289012]. MR2573797 ↑5, 5



Sean Eberhard, Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK

*Email address*: `sean.eberhard@warwick.ac.uk`

Padraig Ó Catháin, Fiontar agus Scoil na Gaeilge, Dublin City University, Dublin D09 N920, Ireland

*Email address*: `padraig.ocathain@dcu.ie`