A NOTE ON THE SINGULARITY PROBABILITY OF RANDOM DIRECTED d-REGULAR GRAPHS

HOI H. NGUYEN AND AMANDA PAN

Abstract. In this note we show that the singular probability of the adjacency matrix of a random d-regular graph on n vertices, where d is fixed and $n \to \infty$, is bounded by $n^{-1/3+o(1)}$. This improves a recent bound by Huang in [15]. Our method is based on the study of the singularity problem modulo a prime developed in [15] (and also partially in [24, 27]), together with an inverse-type result on the decay of the characteristic function. The latter is related to the inverse Kneser's problem in combinatorics.

1. Introduction

The singularity problem in combinatorial random matrix theory states that if a square matrix A_n of size n is "sufficiently random", then A_n is non-singular asymptotically almost surely as n tends to infinity, in other words p_n, the probability of A_n being singular, tends to zero. This problem has a rich history, which we now mention briefly. In the early 60s Komlós [19] showed that if the entries of A_n take values $\{0, 1\}$ independently with probability 1/2 then $p_n = O(n^{-1/2})$. This bound was significantly improved to exponential bounds of type $(1-\varepsilon)^n$ by Kahn, Komlós and Szemerédi [18] in 1995, by Tao and Vu [30] in 2007, by Rudelson and Vershynin [28] in 2008, and by Bourgain, Vu and Wood [7] in 2010. More recently, Tikhomirov [32] has obtained a nearly optimal bound $p_n = (\frac{1}{2} + o(1))^n$. The methods of these results also give exponential bounds for other more general iid ensembles. Since then, there have been subsequent papers addressing the sparse cases, such as [34], [3], [16], [8], [22], [17]. We refer the reader to these papers and the references therein to various extension and application of the singularity problem for the iid models.

In another direction, there have been results regarding the singularity problem for matrices with various dependency conditions on the entries. For instance in [26] the first author studied random doubly stochastic matrices, or in [1] Adamczak, Chafai and Wolff studied random matrices with exchangeable entries. More relatedly, Cook [9] studied the singularity of $A_{n,d}$, the adjacency matrix of a random directed d-regular graph, where he showed that $p_n = d^{-\Omega(1)}$ as long as $\min(d, n-d) \ge C \log^2 n$ for some absolute constant C. A similar result was also established by Basak, Cook and Zeitouni [2] for sum of d random permutation matrices as long as $d \ge \log^{12-o(1)} n$. While these results are highly non-trivial, the random matrices are still relatively dense. For smaller d, the recent work by Litvak, Lytova, Tikhomirov, Tomczak-Jaegermann and Youssef in [20] shows that $p_n \le \frac{C \log^3 d}{\sqrt{d}}$ as long as $C \le d \le cn/\ln^2 n$ for some constants c, C. As a consequence, this bound implies that $p_n \to 0$ if $d \to \infty$. Through a more involved study of the structure of the eigenvectors of matrices of $A_{n,d}$, it has been shown by the same group of authors in [21] that asymptotically almost surely the rank of $A_{n,d}$ is at least $n-1$ as long as $d > C$ for sufficiently large constant C. Finally, very recently Huang [15], Mészáros [24] (see also [27]) confirmed the conjecture by Vu [33] that $p_n \to 0$ as $n \to \infty$ for the $A_{n,d}$ model with fixed d.[1] The following quantitative result was shown in [15, Theorem 1.3].

Theorem 1.1. *Let $d \ge 3$ be a fixed integer. Then if n sufficiently large, for a random d-regular directed graph on n vertices, the probability p_n that its adjacency matrix $A_{n,d}$ is singular is*

$$p_n \le n^{-\min\{1/4,(d-2)/(2d)\}}.$$

The authors are supported by the NSF CAREER grant DMS-1752345.

[1] We also refer the reader to [8, 12] for results regarding other models of extremely sparse graphs.

In particular, when $d = 3$ the above gives $O(n^{-1/6})$.

The papers [15, 24, 27] also addressed the symmetric case, which is more complicated and is not the main focus of our current paper. As the reader can see, although there have been massive contributions on the quantitative aspect of the singularity bound for various (not very sparse) random matrix models, the above paper [15] is the only reference that produces a quantitative estimate for p_n of $A_{n,d}$. In the current note we further explore this quantitative direction by showing

Theorem 1.2 (Main result)**.** *Let $\varepsilon > 0$ be given. Let $d \geq 3$ be fixed. Then for sufficiently large n, for a random d-regular directed graph on n vertices, the probability that $A_{n,d}$ is singular is bounded by*

$$p_n \leq n^{-1/3+\varepsilon}.$$

Hence with respect to the model $A_{n,d}$, our result improves over the $n^{-1/4}$ barrier from Theorem 1.1 for all $d \geq 2$. With a more careful analysis, we can also replace the bound $n^{-1/3+\varepsilon}$ by $Cn^{-1/3}$ for some sufficiently large constant C, but our bounds are still far from being best possible, where it seems the bound for p_n should be of order $1/n^{d-2}$, which would mean that the singularity event is mainly from the cases of having two identical rows or two identical columns (see Figure [1]). It is desirable to establish similar probability bound for the least singular value of $A_{n,d}$, for which the current approach does not seem to work.

Our approach mainly follows the method of [15] which studies the singularity of the matrix $A_{n,d}$ over $\mathbb{Z}/p\mathbb{Z}$ for some large p. In this approach we will consider $\mathbb{P}(A_{n,d}\mathbf{v} = 0)$ for each fixed non-zero $\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^n$. We hope that the probability is still small after taking union bound over all non-zero choices of $\mathbf{v}$ (modulo its direction). A somewhat similar strategy was also carried out in [24, 27] for the cokernel statistics of $A_{n,d}$ as an integral matrix. Our new contribution shows an interesting relation between the decay of the characteristic functions of a special family of random walks arises from the configuration model of $A_{n,d}$ and an inverse-type Kneser problem in combinatorics (Theorem 3.3). More specifically, we extend the treatment of [15] on the central limit theorem (Proposition 2.5) and on the tail bound estimate (Proposition 2.4) to a broader range $p \leq n^{1/3-o(1)}$. Least but not last, it is an interesting problem to extend the treatments to larger p, a problem which is directly related to the upper bound of p_n, but is also useful toward the study of $\mathbb{Z}$-statistics of the cokernels of $A_{n,d}$.

Notations. We say that $X \asymp Y$ if $X = O(Y)$ and $Y = O(X)$. We say that $X = \Omega(Y)$ if $X \geq CY$ for some absolute positive constant C. Given a parameter α, we say that $X = O_\alpha(Y)$, or $X \ll_\alpha Y$, if $X \leq CY$ and C is allowed to depend on α.

For any $x \in \mathbb{R}$, we define $\|x\| := \|x\|_{\mathbb{R}/\mathbb{Z}}$ to be the distance of x to the nearest integer.

Finally, if not specified otherwise, the parameter n in this note is assumed to be sufficiently large.

2. Some formulas and the proof method

As mentioned, the singularity problem views the M as matrices over $\mathbb{R}$, but if the entries are integers they could also be viewed as elements of the field $\mathbb{Z}/p\mathbb{Z}$ for any prime p. A matrix is singular mod p exactly when its determinant is 0 mod p, and so heuristically, one expects this to happen about $1/p$ of the time instead of 0% of the time. This was the motivation for the treatments of [15, 24, 27]. In what follows we closely follow the approach of [15].

We first use work of Bollobás [4], to replace $A_{n,d}$ with a random multi-graph $A^*_{n,d}$ given as follows (see [5, Corollary 2.18]). We associate to each vertex $k \in \{1, \dots, n\}$ a fiber F_k of d points and select a permutation $\mathcal{P}$ of the nd points uniformly at random. Then for each vertex $k \in \{1, \dots, n\}$ and point $k' \in F_k$ we add a directed edge from k to vertex ℓ if the points $\mathcal{P}(k')$ belongs to the fiber $\mathcal{F}_\ell$. By [4], for any fixed d the probability that $A^*_{n,d}$ has a loop or multiple edge is bounded away from 1. Hence it suffices to prove the

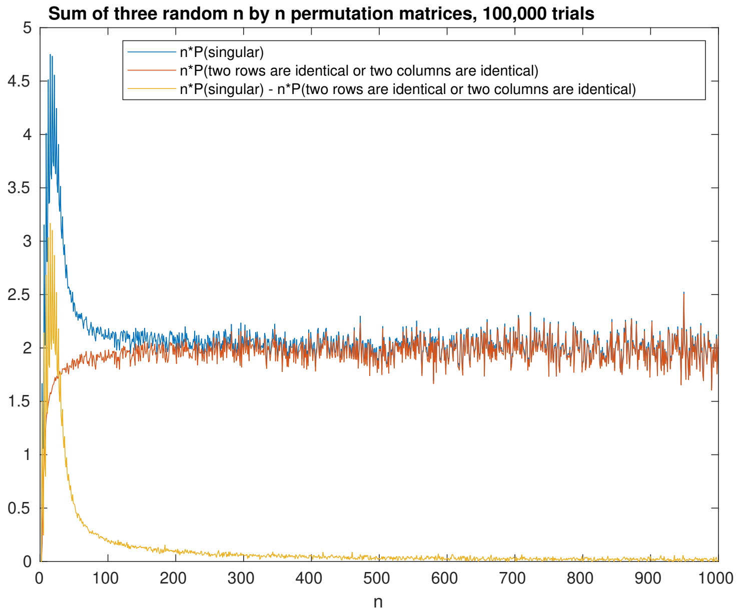

FIGURE 1. Sum of three random permutation matrices

theorem with $A^*_{n,d}$ replaced by $A_{n,d}$. Without loss of generality, in what follows by the configuration model $A_{n,d}$ we mean the model $A^*_{n,d}$.

For a vector $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{F}_p^d$ with n_j components x_i of value j, we define

$$\Phi(\mathbf{x}) := (n_0, \dots, n_{p-1}).$$

Thus we have

$$\sum_j n_j = d \text{ and } \sum_j jn_j = x_1 + \dots + x_d.$$

Given $n_0, \dots, n_{p-1}$ where $\sum_i n_i = n$ we denote by $S_{n_0,\dots,n_{p-1}}$ the set of vectors $\mathbf{v} = (v_1, \dots, v_n)$ where for each $i = 0, \dots, p-1$ there are exactly n_i entries i in $(v_1, \dots, v_n)$; so there are $\binom{n}{n_0,\dots,n_{p-1}}$ such vectors.

Let $\mathcal{U}_{d,p}$ be the multi-set

$$\mathcal{U}_{d,p} := \Big\{\Phi(\mathbf{x}) : \mathbf{x} \in \mathbb{F}_p^d, \sum_{i=1}^d x_i = 0\Big\}.$$

Hence $|\mathcal{U}_{d,p}| = p^{d-1}$. For instance, when $d = 3$ the vectors $(3, 0, \dots, 0)$, $(1, 1, 0, \dots, 0, 1)$, and $(1, 0, 1, 0, \dots, 0, 1, 0)$ all belong to $\mathcal{U}_{3,p}$.

We have the following beautiful random walk interpretation (see [15, Proposition 2.1]).

Claim 2.1. *Given $n_0, \dots, n_{p-1}$, and given $\mathbf{v} \in S_{n_0,\dots,n_{p-1}}$, for the configuration model $A_{n,d}$ on random d-regular directed graphs we have*

$$\Big|\{M \in A_{n,d} : M\mathbf{v} = 0\}\Big| = \prod_{j=0}^{p-1} (dn_j)! \Big|\{(\mathbf{u}_1, \dots, \mathbf{u}_n) \in \mathcal{U}_{d,p}^n : \mathbf{u}_1 + \dots + \mathbf{u}_n = d(n_0, \dots, n_{p-1})\}\Big|$$

$$= \prod_{j=0}^{p-1} (dn_j)! p^{(d-1)n} \mathbb{P}(X_1 + \dots + X_n = (dn_0, \dots, dn_{p-1})),$$

where $X_1, \dots, X_n$ are independent copies of X, which is uniformly distributed over $\mathcal{U}_{d,p}$.

2.2. **Proof methods.** As shown by the above interpretation, it boils down to understanding the random variable X. It is elementary to show

$$\boldsymbol{\mu} = \mathbb{E}X = (d/p, \dots, d/p)$$

and

$$\boldsymbol{\Sigma} = \mathbb{E}((X-\boldsymbol{\mu})(X-\boldsymbol{\mu})^t) = \frac{d}{p}I - \frac{d}{p^2}\mathbf{1}\mathbf{1}^t.$$

Also, the characteristic function of X and $X-\mu$ are defined as

$$\phi_X(\mathbf{s}) = \frac{1}{p^{d-1}} \sum_{\mathbf{w}\in\mathcal{U}_{d,p}} e^{i\mathbf{s}\cdot\mathbf{w}}$$

and

$$\phi_{X-\boldsymbol{\mu}}(\mathbf{s}) = \mathbb{E}\exp(i\mathbf{t}\cdot(X-\boldsymbol{\mu})) = \exp(-i\mathbf{t}\cdot\boldsymbol{\mu})\phi_X(\mathbf{s}), \mathbf{s}\in\mathbb{R}^p.$$

For instance when $d=3$, we have

$$\phi_X(\mathbf{s}) = \frac{1}{p^2}\sum_{a,b\in\mathbb{Z}/p\mathbb{Z}} e^{i(s_a+s_b+s_{-a-b})}.$$

Because of Claim 2.1 and because $|A_{n,d}| = (nd)!$, in order to prove the singularity probability to be small we aim to show that

$$\sum_{\substack{(n_0,\dots,n_{p-1})\in\mathbb{Z}_{\ge 0}, n_0<n \\ \sum_i n_i = n}} \binom{n}{n_0,\dots,n_{p-1}} \frac{p^{(d-1)n}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!}\mathbb{P}(X_1+\dots+X_n = (dn_0,\dots,dn_{p-1})). \tag{1}$$

is small.

Definition 2.3. Let $b>0$ be chosen to be sufficiently large, and let $\mathcal{E}=\mathcal{E}_b$ be the set of vectors satisfying

$$\sum_{j=0}^{p-1}(\frac{n_j}{n}-\frac{1}{p})^2 \le \frac{b\log n}{n}. \tag{2}$$

We will call such vectors *equidistributed*.

Let $\mathcal{N}$ be the set of p-tuples $(n_0,\dots,n_{p-1})$ which are not $(n,0,\dots,0)$ and *not* equidistributed. Our main result can be deduced from the following two key propositions.

Proposition 2.4 (Deviation estimate for the error term)**.** *The contribution in (1) from $\mathcal{N}$ is bounded by $o(1)$ as long as $p \le n^{1/3-\varepsilon}$.*

Note that this result improves upon [15, Proposition 3.2] where a similar statement was proved for $p \le n^{(d-2)/2d}$. As a consequence, to justify Theorem 1.2 it suffices to work with equidistributed vectors. For this we show

Proposition 2.5 (Local limit theorem for the main term)**.** *The contribution in (1) from equidistributed vectors is at most $1+o(1)$ as long as $p\le n^{1/3-\varepsilon}$.*

We note that with some extra work it might be possible to actually prove that the contribution is $1+o(1)$, see Remark **??**. The above result slightly improves [15, Proposition 3.1] where the author there worked with $p \le n^{1/4}$.

We will prove Proposition 2.4 in Section 5 and Proposition 2.5 in Section 3, in what follows we deduce our main result.

Proof. (of Theorem 1.2) Note that if $M \in A_{n,d}$ is singular then there exists a non-zero vector $\mathbf{v}$ so that $M\mathbf{v} = 0$ (and hence $M(t\mathbf{v}) = 0$ for $t = 1, \dots, p-1$). We thus have

$$
\begin{aligned}
(p-1)\mathbb{P}(M \in A_{n,d} \text{ is singular}) &\le \frac{1}{(nd)!}\sum_{M\in A_{n,d}}\sum_{\mathbf{v}\neq 0}\mathbf{1}_{M\mathbf{v}=0} = \sum_{\mathbf{v}\neq 0}\Big|\{M \in A_{n,d} : M\mathbf{v} = 0\}\Big| \\
&= \sum_{\substack{(n_0,\dots,n_{p-1})\in\mathbb{Z}_{\ge 0}, n_0<n \\ \sum_i n_i = n}} \binom{n}{n_0,\dots,n_{p-1}} \frac{p^{(d-1)n}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!}\mathbb{P}(X_1+\dots+X_n = (dn_0,\dots,dn_{p-1})) \\
&= \sum_{(n_0,\dots,n_{p-1})\notin\mathcal{E}} \dots + \sum_{(n_0,\dots,n_{p-1})\in\mathcal{E}} \dots \\
&\le o(1) + 1 + o(1) = 1 + o(1).
\end{aligned}
$$

Hence

$$\mathbb{P}(M \in A_{n,d} \text{ is singular}) \le \frac{1+o(1)}{p-1} = O(n^{-1/3+\varepsilon}).$$

□

Choices of p, δ. Here and later, ε is a sufficiently small positive constant. If not specified otherwise we will assume

$$\delta = p^{-(1+3\varepsilon)} \text{ and } p^{3(1+2\varepsilon)} \asymp n. \tag{3}$$

3. Treatment over equidistributed vectors: proof of Proposition 2.5

There are two factors of the terms of (1) to analyze, we will give some preliminary discussion on each separately: (i) Stirling formulas for the factor $\binom{n}{n_0,\dots,n_{p-1}}\frac{p^{(d-1)n}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!}$ and (ii) Fourier analysis for the factor $\mathbb{P}(X_1+\dots+X_n = (dn_0,\dots,dn_{p-1}))$. We then combine these estimates in Section 3.6.

3.1. Stirling formulas.

We first recall the following Stirling bound by Robbins for all positive integers l,

$$\sqrt{2\pi l}(l/e)^l e^{\frac{1}{12l+1}} < l! < \sqrt{2\pi l}(l/e)^l e^{\frac{1}{12l}}. \tag{4}$$

So $l! = \sqrt{2\pi l}(l/e)^l e^{O(1/l)}$ and therefore (see also [15, Eqn (3.4)])

$$
\begin{aligned}
\binom{n}{n_0,\dots,n_{p-1}}\frac{p^{(d-1)n}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!} &= p^{(d-1)n}\frac{n!}{\prod_j n_j!}\frac{\prod_{j=0}^{p-1}(dn_j)!}{(dn)!} \\
&= p^{(d-1)n}\frac{\sqrt{2\pi n}(n/e)^n e^{O(1/n)}}{\prod\sqrt{2\pi n_j}(n_j/e)^{n_j}e^{O(1/n_j)}}\frac{\prod\sqrt{2\pi dn_j}(dn_j/e)^{dn_j}e^{O(1/n_j)}}{\sqrt{2\pi dn}(dn/e)^{dn}e^{O(1/n)}} \\
&= e^{O(1/n)} \times (\sqrt{d})^{p-1} \times \frac{\prod n_j^{(d-1)n_j}}{(\frac{n}{p})^{(d-1)n}} \\
&= (1+o(1)) \times (\sqrt{d})^{p-1} \times [\prod_{j=0}^{p-1}(\frac{n_j}{n/p})^{n_j}]^{d-1} \\
&= \Big(1+o(1)\Big)d^{(p-1)/2}\exp\Big((d-1)n\sum_j(\frac{n_j}{n}\log\frac{n_j}{n} + \log p)\Big).
\end{aligned}
$$

Recall that

$$\sum_{j=0}^{p-1}(\frac{n_j}{n} - \frac{1}{p})^2 \le \frac{b\log n}{n}.$$

Hence trivially

$$|\frac{n_j}{n}-\frac{1}{p}| = O(\sqrt{\log n}/\sqrt{n}), |\frac{pn_j}{n}-1| = O(p\sqrt{\log n}/\sqrt{n}) = o(1).$$

Hence

$$\sum_j 1/n_j = O(p^2/n) = o(1).$$

Note that Taylor expansion for $|h|<1$ shows

$$(h+1)\log(h+1) = h + h^2/2 - h^3(1/2-1/3) + h^4(1/3-1/4) + \cdots .$$

Hence, because $|(pn_j/n)-1| = o(1)$

$$\begin{aligned} n_j \log((n_j/n)/(1/p)) = n_j \log[(pn_j/n-1)+1] &= (n/p) \times (pn_j/n-1+1)\log[(pn_j/n-1)+1] \\ &= (n/p)[(pn_j/n-1) + (pn_j/n-1)^2/2 + \sum_{k=3}^{\infty} \frac{(-1)^k}{(k-1)k}(pn_j/n-1)^k]. \end{aligned}$$

So

$$\sum_j n_j \log((n_j/n)/(1/p)) = (n/p)[\sum_j (pn_j/n-1)^2/2 + \sum_{k=3}^{\infty} \frac{(-1)^k}{(k-1)k}(pn_j/n-1)^k].$$

We will use the above expansion for $\sum_j \mathfrak{n}_j \log \mathfrak{n}_j$. One can see that for equidistributed vectors the terms $\sum_j (pn_j/n-1)^2$ and $n(d-1)\sum_j (pn_j/n-1)^3$ are the main contributions, while the contributions from higher order terms are bounded by $O(\sum_j (pn_j/n-1)^4)$, which is in turn bounded trivially by

$$(\sum_j (pn_j/n-1)^2)^2 = O(\frac{p^2 b \log n}{n}\sum_j (pn_j/n-1)^2) = O(p^{-1-\varepsilon/4}\sum_j (pn_j/n-1)^2),$$

and hence are negligible when $p \le n^{1/3(1+2\varepsilon)}$ (see also (7)). So we obtain

$$\binom{n}{n_0,\dots,n_{p-1}} \frac{p^{(d-1)n}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!} = (1+o(1))d^{(p-1)/2}\exp\Big(\frac{(d-1)pn}{2}\sum_j (\frac{n_j}{n}-\frac{1}{p})^2 - \frac{(d-1)p^2 n}{6}(\frac{n_j}{n}-\frac{1}{p})^3\Big). \tag{5}$$

3.2. **Treatment of the characteristic function.** We notice that $|\phi_{X-\boldsymbol{\mu}}(\mathbf{s})| = 1$ iff

$$\mathbf{s} \in 2\pi\mathbb{Z}^p + 2\pi(0,1/p,\dots,(p-1)/p)\mathbb{Z} + (1,\dots,1)\mathbb{R}.$$

For $\kappa>0$, for $j=0,\dots,p-1$ we define the domains

$$B_j(\kappa) = 2\pi j(0,1/p,\dots,(p-1)/p) + Q(\{\mathbf{x}\in\mathbb{R}^{p-1} : \|\mathbf{x}\|^2 \le \kappa\} \times [0, 2\sqrt{p}\pi]),$$

where Q is an orthogonal transform of the form $Q = [O, \mathbf{1}/\sqrt{p}]$ and O is an orthogonal transform in the space $\mathbf{1}^{\perp}$.

Suppose that $\mathbf{s}\in B_j(\kappa)$ for some j, and $d=3$. Then $\mathbf{s} = 2\pi j(0,1/p,\dots,(p-1)/p) + O\mathbf{x} + y\mathbf{1}$ for some $\|\mathbf{x}\|^2 \le \kappa$ and $y\in[0,2\pi]$. Let $s' = Ox$.

$$\begin{aligned} |\phi_X(\mathbf{s})| &= |\frac{1}{p^2}\sum_{a,b} e^{i(s'_a+s'_b+s'_{-(a+b)})}| \\ &= \frac{1}{p^2}\sum_{a,b} e^{i(s'_a+s'_b+s'_{-(a+b)})} = 1 - O(\frac{1}{p^2}\sum_{a,b}\|\frac{s'_a+s'_b+s'_{-(a+b)}}{2\pi}\|^2_{\mathbb{R}/\mathbb{Z}}) \\ &= 1 - O(\frac{1}{p^2}p\sum_a \|\frac{s'_a}{2\pi}\|^2_{\mathbb{R}/\mathbb{Z}}) = 1 - O(\kappa/p). \end{aligned}$$

Our main result says the converse.

Theorem 3.3 (Inverse result for fixed d)**.** *Assume that for* $\mathbf{s} \in 2\pi\mathbb{R}^p/\mathbb{Z}^p$

$$|\phi_{X-\boldsymbol{\mu}}(\mathbf{s})| \geq 1 - \alpha p^{-2}$$

where α is a small constant. Then there exists j such that $\mathbf{s} \in B_j(\kappa)$ for some $\kappa \leq Ap^{-1}$, where A is a sufficiently large constant depending on α, d.

This is an improvement of [15, Proposition 2.3] as there the right hand side is replaced by $1 - O(p^{-3})$. Compared to [15], our proof for this new setting is more complicated, but we believe that this is a delicate matter. In application, κ is set to be δ.

3.4. **Fourier analysis.** For equidistributed $(n_0, \dots, n_{p-1})$ we first write

$$\begin{aligned}\mathbb{P}(X_1 + \cdots + X_n = (dn_0, \dots, dn_{p-1})) &= \frac{1}{(2\pi)^p}\int_{2\pi\mathbb{R}^p/\mathbb{Z}^p} \phi^n_{X-\boldsymbol{\mu}}(\mathbf{x}) e^{-i\langle \mathbf{x}, d\mathbf{n} - n\boldsymbol{\mu}\rangle} d\mathbf{x} \\ &= \frac{p^{3/2}}{(2\pi)^{p-1}} \int_{\mathbf{x}\in\mathbb{R}^{p-1}: \|\mathbf{x}\|_2^2 \leq \delta} \phi^n_{X-\boldsymbol{\mu}}(O\mathbf{x}) e^{-i\langle O\mathbf{x}, d\mathbf{n} - n\boldsymbol{\mu}\rangle} d\mathbf{x} + O(e^{-\alpha n/p^2}).\end{aligned} \tag{6}$$

where α is a small constant and the error term $O(e^{-\alpha n/p^2})$ comes from $|\phi_{X-\boldsymbol{\mu}}(\mathbf{x})| \leq 1 - \alpha/p^2$ and Theorem 3.3.

We write

$$\phi_{X-\boldsymbol{\mu}}(O\mathbf{x}) = \mathbb{E}(1 + i\langle O\mathbf{x}, X - \boldsymbol{\mu}\rangle - \frac{1}{2}\langle O\mathbf{x}, X - \boldsymbol{\mu}\rangle^2 - \frac{i}{6}\langle O\mathbf{x}, X - \boldsymbol{\mu}\rangle^3 + O(\langle O\mathbf{x}, X - \boldsymbol{\mu}\rangle^4)).$$

Let

$$\mathbf{s} := O\mathbf{x}.$$

Then clearly $\|\mathbf{s}\|_2 = \|\mathbf{x}\|_2$. Because the columns of O are orthogonal to $\mathbf{1}$, we have $\sum_i s_i = 0$. For $\Phi(\mathbf{a}) \in \mathcal{U}_{d,p}$

$$\langle \mathbf{s}, \Phi(\mathbf{a}) - \boldsymbol{\mu}\rangle = s_{a_1} + \cdots + s_{a_{d-1}} + s_{-\sum a_i}.$$

From the above discussion it suffices to work with

$$\|s\|_2^2 \leq \delta.$$

The first moment is zero as $\sum_i s_i = 0$,

$$\mathbb{E}\langle \mathbf{s}, X - \boldsymbol{\mu}\rangle = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_{d-1}} (\sum_i s_{a_i} + s_{-\sum_i a_i}) = 0.$$

For the second moment,

$$\mathbb{E}\langle \mathbf{s}, X - \boldsymbol{\mu}\rangle^2 = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_{d-1},a_d,\sum_i a_i = 0} (\sum_i s_{a_i})^2 = \frac{1}{p^{d-1}} p^{d-2} \times d \sum_a s_a^2 = (d/p)\|\mathbf{s}\|_2^2 = (d/p)\|\mathbf{x}\|_2^2.$$

For the third moment, we see that the sum is a multiple of $\frac{1}{p^{d-1}} p^{d-2} \sum_a (s_a/p)^3$.

$$\mathbb{E}\langle \mathbf{x}, O^t(X - \boldsymbol{\mu})\rangle^3 = \mathbb{E}\langle \mathbf{x}, O^t(X)\rangle^3 = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_d,\sum_i a_i = 0} (\sum_i s_{a_i})^3 = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_d,\sum_i a_i = 0} \sum_{1 \leq i_1, i_2, i_3 \leq d} s_{a_{i_1}} s_{a_{i_2}} s_{a_{i_3}}$$

$$\mathbb{E}\langle \mathbf{s}, X - \boldsymbol{\mu}\rangle^3 = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_d,\sum_i a_i = 0} (\sum_i s_{a_i})^3 = \frac{1}{p^{d-1}} \sum_{a_1,\dots,a_d,\sum_i a_i = 0} \sum_{1 \leq i_1, i_2, i_3 \leq d} s_{a_{i_1}} s_{a_{i_2}} s_{a_{i_3}}$$

$$= \frac{1}{p^{d-1}}[\sum_a s_a^3 dp^{d-2}(1+\frac{d(d-1)}{p}+\frac{d(d-1)(d-2)}{p^2})+\sum_{a\neq b} s_a^2 s_b 3d(d-1)p^{d-3}(1+\frac{d-3}{p})+\sum_{a<b<c} s_a s_b s_c 6\binom{d}{3}p^{d-4}].$$

By passing the sum $\sum_{a<b<c} s_a s_b s_c$ to $(\sum_a s_b)^3$ and $\sum_{a<b} s_a^2 s_b$ to $(\sum_a s_a^2)(\sum_a s_a)$, we arrive at

$$\mathbb{E}\langle \mathbf{s}, X-\boldsymbol{\mu}\rangle^3 = (\frac{d}{p}+\frac{c'}{p^2}+\frac{c''}{p^3})\sum_j s_a^3 =: \frac{C_p}{p}\sum_j s_a^3$$

for absolute constants c', c'', where

$$C_p := d + c'/p + c''/p^2.$$

Notice that we can bound $\sum_a |s_a|^3$ from above by $(\sum_a s_a^2)^{3/2}$, but this does not give us a desirable bound.

For the fourth moment,

$$\begin{aligned}\frac{1}{p^{d-1}}\sum_{a_1,\dots,a_d,\sum_i a_i=0}(\sum_i s_{a_i})^4 &= C_d\frac{1}{p^{d-1}}p^{d-3}\sum_{a,b}s_a^2 s_b^2 + (d/p)\sum_a (s_a)^4\\ &= (C_d/p^2)\|\mathbf{s}\|_2^4 + (d/p)\sum_a (s_a)^4.\end{aligned}$$

Hence if $\|\mathbf{s}\|_2^2 \le \delta$ then

$$n\|\mathbf{s}\|_2^4/p^2 \le n\delta^2/p^2 \le p^{-1-\varepsilon/4}.$$

Also

$$\sum_a (s_a)^4 \le (\sum_a s_a^2)^2 \le \delta\sum_a s_a^2 \le p^{-1-\varepsilon/4}\sum_a s_a^2.$$

Note that

$$(1+O(1/p^{1+\varepsilon/4}))^p = 1+o(1). \tag{7}$$

Hence for (6) it boils down to considering (where for short we write $d\mathbf{s}$ for $ds_1\dots ds_{p-1}$)

$$\Big|(1+o(1))\frac{p^{3/2}}{(2\pi)^{p-1}}\int_{\mathbf{s}\in\mathbb{R}^p:\|\mathbf{s}\|_2^2\le\delta,\sum_a s_a=0} e^{-\frac{dn}{2p}\|\mathbf{s}\|_2^2}e^{-i\langle \mathbf{s}, d\mathbf{n}-b\boldsymbol{\mu}\rangle + i\frac{C_p n}{p}\sum_a s_a^3}d\mathbf{s}\Big|.$$

In fact, we can extend the integral to all $\mathbf{s}\in\mathbb{R}^p$ with $\sum_a s_a = 0$ excluding $B_2(\delta) = \{\mathbf{s} : \sum_a s_a^2 \le \delta\}$ above because

$$\begin{aligned}&|(1+o(1))\frac{p^{3/2}}{(2\pi)^{p-1}}\int_{\mathbf{s}\in\mathbb{R}^p\setminus B_2(\delta),\sum_a s_a=0} e^{-\frac{dn}{2p}\|\mathbf{s}\|_2^2}e^{-i\langle \mathbf{s}, d\mathbf{n}-\boldsymbol{\mu}\rangle + i\frac{C_p n}{p}\sum_a s_a^3}d\mathbf{s}|\\ &\le (1+o(1))\frac{p^{3/2}}{(2\pi)^{p-1}}\int_{\|\mathbf{s}\|_2^2\ge\delta,\sum_a s_a=0} e^{-\frac{dn}{4p}\|\mathbf{s}\|_2^2}d\mathbf{s} \le e^{-n\delta/8p} \le e^{-p^{1+\varepsilon}}.\end{aligned}$$

Hence we can pass to consider

$$|(1+o(1))\frac{p^{3/2}}{(2\pi)^{p-1}}\int_{\mathbf{s}\in\mathbb{R}^p,\sum_a s_a=0} e^{-\frac{dn}{2p}\|\mathbf{s}\|_2^2}e^{-i\langle \mathbf{s}, d\mathbf{n}-b\boldsymbol{\mu}\rangle + i\frac{C_p n}{p}\sum_a s_a^3}d\mathbf{s}|.$$

For short (with j playing to role of a), let

$$t_j := (d\frac{\mathbf{n}}{n}-\boldsymbol{\mu})_j. \tag{8}$$

We will show the following estimate.

Lemma 3.5. *We have*

$$|\int_{\mathbf{s}\in\mathbb{R}^p,\sum_j s_j=0} e^{-\frac{dn}{2p}\|\mathbf{s}\|_2^2}e^{-i\langle \mathbf{s}, d\mathbf{n}-b\boldsymbol{\mu}\rangle + i\frac{C_p n}{p}\sum_j s_j^3}d\mathbf{s}| \le (1+o(1))(\sqrt{2\pi})^{p-1}(\sqrt{\frac{p}{dn}})^{p-1}e^{-\frac{np}{2d}\sum_j t_j^2 + C_p(\sqrt{\frac{p}{n}})\frac{1}{d^{3/2}}(\sqrt{\frac{np}{d}})^3 t_j^3}.$$

Proof. We notice that

$$\sum_j t_j = 0 \text{ and } \sum_j t_j^2 = \|d\frac{\mathbf{n}}{n} - \boldsymbol{\mu}\|_2^2 \le \frac{b\log n}{n}.$$

By the change of variable $y_j = \sqrt{\frac{dn}{p}} s_j$ (and with $d\mathbf{y} = dy_1 \dots dy_{p-1}$), we can rewrite the left hand side of Lemma 3.5 as

$$(\sqrt{\frac{p}{dn}})^{p-1} \int_{\mathbf{y}\in\mathbb{R}^p, \sum y_j = 0} e^{\sum_j -\frac{1}{2}y_j^2 - it_j\sqrt{\frac{np}{d}}y_j + iC_p(\sqrt{\frac{p}{n}})\frac{1}{d^{3/2}}y_j^3} d\mathbf{y}.$$

To simplify furthermore, with $r_j = t_j\sqrt{\frac{np}{d}}$ and $\alpha_0 = C_p(\sqrt{\frac{p}{n}})\frac{1}{d^{3/2}}$, we have

$$\begin{aligned}
&\int_{y_j\in\mathbb{R},\sum y_j=0} e^{\sum_j -\frac{1}{2}y_j^2 - ir_jy_j + i\alpha_0 y_j^3} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}r_j^2} \int_{y_j\in\mathbb{R},\sum y_j=0} e^{\sum_j -\frac{1}{2}(y+ir_j)^2 + i\alpha_0 y_j^3} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}r_j^2} \int_{y_j\in\mathbb{R},\sum y_j=0; z_j = y_j + ir_j} e^{\sum -\frac{1}{2}z_j^2 + i\alpha_0(z_j - ir_j)^3} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}(r_j^2 - \alpha_0 r_j^3)} \int_{y_j\in\mathbb{R},\sum y_j=0; z_j = y_j + ir_j} e^{\sum -\frac{1}{2}z_j^2 + i\alpha_0(z_j^3 - 3z_j^2(ir_j) + 3z_j(ir_j)^2)} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}(r_j^2 - \alpha_0 r_j^3)} \int_{y_j\in\mathbb{R},\sum y_j=0; z_j = y_j + ir_j} e^{\sum -\frac{1}{2}z_j^2 + i\alpha_0 z_j^3 + 3\alpha_0 z_j^2 r_j - 3i\alpha_0 z_j r_j^2} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}(r_j^2 - \alpha_0 r_j^3)} \int_{y_j\in\mathbb{R},\sum y_j=0; z_j = y_j + ir_j} e^{\sum -(\frac{1}{2} - 3\alpha_0 r_j)z_j^2 + i(\alpha_0 z_j^3 - 3\alpha_0 r_j^2 z_j)} d\mathbf{y}\\
&= \prod_j e^{-\frac{1}{2}(r_j^2 - \alpha_0 r_j^3)} \int_{y_j\in\mathbb{R},\sum y_j=0} e^{\sum -(\frac{1}{2} - 3\alpha_0 r_j)y_j^2 + i(\alpha_0 y_j^3 - 3\alpha_0 r_j^2 y_j)} d\mathbf{y}
\end{aligned}$$

by contour integral. (Indeed, to see the last identity, by substituting $y_p = -\sum_{j=1}^{p-1} y_j$ into the exponent we can rewrite the integral as

$$\begin{aligned}
&\int_{y_1,\dots,y_{p-1}\in\mathbb{R}} e^{\sum_{j=1}^{p-1} -(\frac{1}{2}-3\alpha_0 r_j)y_j^2 + i(\alpha_0 y_j^3 - 3\alpha_0 r_j^2 y_j) - (\frac{1}{2} - 3\alpha_0 r_p)(\sum_{j=1}^{p-1} y_j)^2 - i(\alpha_0(\sum_{j=1}^{p-1} y_j)^3 - 3\alpha_0 r_p^2(\sum_{j=1}^{p-1} y_j))} dy_1 \dots dy_{p-1}\\
&= \int_{y_2,\dots,y_{p-1}\in\mathbb{R}} e^{\sum_{j=2}^{p-1}\cdots} \Big(\int_{y_1\in\mathbb{R}} e^{-(\frac{1}{2}-3\alpha_0 r_1)y_1^2 + i(\alpha_0 y_1^3 - 3\alpha_0 r_1^2 y_1) - (\frac{1}{2} - 3\alpha_0 r_p)(\sum_{j=1}^{p-1} y_j)^2 - i(\alpha_0(\sum_{j=1}^{p-1} y_j)^3 - 3\alpha_0 r_p^2(\sum_{j=1}^{p-1} y_j))} dy_1 \Big) dy_2 \dots dy_p
\end{aligned}$$

By using the fact that $e^{-(a+ib)^2} \to 0$ as $a \to \infty$ for any fixed b and the integrand is holomorphic in y_1 for any given $y_2, \dots, y_{p-1}$, we can replace the inner integral from $y_1 \in \mathbb{R}$ to $y_1 \in \mathbb{R} + ir_1$. Keep iterating the process until y_{p-1}, noting that $\sum_{j=1}^p r_j = 0$, we obtain as claimed.)

Next, because $\alpha_0|t_j| = o(1)$, the integral $|\int_{y_j\in\mathbb{R},\sum y_j=0} e^{\sum -(\frac{1}{2}-3\alpha_0 r_j)y_j^2 + i(\alpha_0 y_j^3 - 3\alpha_0 r_j^2 y_j)} d\mathbf{y}|$ can be bounded by $(\sqrt{2\pi})^{p-1}\prod\sqrt{1+O(\alpha_0 r_j)} \le (\sqrt{2\pi})^{p-1}\prod e^{O(\alpha_0|r_j|)}$. Hence we have

$$|\int_{y_j\in\mathbb{R},\sum y_j=0} e^{-\sum_j \frac{1}{2}y_j^2 - ir_jy_j + i\alpha_0 y_j^3} d\mathbf{y}| \le (\sqrt{2\pi})^{p-1}\prod_j e^{-\frac{1}{2}(r_j^2 - \alpha_0 r_j^3) + O(\alpha_0|r_j|)}.$$

Notice that with the choice of p from (3)

$$e^{\alpha_0\sum_j |r_j|} \le e^{\alpha_0\sqrt{p}\sqrt{\sum_j r_j^2}} \le e^{\alpha_0 p\sqrt{\frac{b\log n}{d}}} = o(1).$$

Putting these bounds together,

$$|\int_{y_j\in\mathbb{R},\sum y_j=0} e^{-\sum_j \frac{1}{2}y_j^2} e^{-ir_jy_j + i\alpha_0 y_j^3} d\mathbf{y}| \le (1+o(1))(\sqrt{2\pi})^{p-1} e^{-\frac{np}{2d}\sum_j t_j^2 + C_p(\sqrt{\frac{p}{n}})\frac{1}{d^{3/2}}(\sqrt{\frac{np}{d}})^3 t_j^3}.$$

□

As a consequence of (6) and Lemma 3.5, we thus obtain

$$P(X_1+\cdots+X_n=(dn_0,\dots,dn_{p-1}))\le(1+o(1))p^{3/2}(\frac{p}{2\pi dn})^{\frac{p-1}{2}}e^{-\frac{np}{2d}\sum_j t_j^2+C_pnp^2\frac{1}{d^3}t_j^3}, \tag{9}$$

where t_j are defined in (8).

3.6. **Completion of proof of Proposition 2.5.** First recall that

$$\sum_{\mathbf{v}\in S_{n_0,\dots,n_{p-1}}}\mathbb{P}(A_{n,d}\mathbf{v}=0)=\binom{n}{n_0,\dots,n_{p-1}}\frac{p^{n(d-1)}\prod_{j=0}^{p-1}(dn_j)!}{(dn)!}\times\mathbb{P}(X_1+\cdots+X_n=(dn_0,\dots,dn_{p-1})).$$

Recalling the first factor from (5) and the second factor from (9), after cancellation we obtain

$$(1+o(1))p^{3/2}(p/2\pi n)^{(p-1)/2}e^{-(pn/2)\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-[\frac{(d-1)}{6}-\frac{C_p}{d^3}]np^2(\frac{n_j}{n}-\frac{1}{p})^3}.$$

Our main goal in this part is the following (where $D_p=\frac{(d-1)}{6}-\frac{C_p}{d^3}$)

Lemma 3.7. *We have*

$$\sum_{(n_0,\dots,n_{p-1})\in\mathcal{E},\sum_j jn_j\equiv 0 \pmod p}(1+o(1))p^{3/2}(p/2\pi n)^{(p-1)/2}e^{-(pn/2)\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-D_pp^2n(\frac{n_j}{n}-\frac{1}{p})^3}=1+o(1).$$

It is clear that Proposition 2.5 then follows. For Lemma 3.7, we first show that one can pass from $\sum jn_j\equiv 0 \pmod p$ to general $(n_0,\dots,n_{p-1})\in\mathcal{E}$.

Claim 3.8. *We have*

$$\begin{aligned}&\sum_{(n_0,\dots,n_{p-1})\in\mathcal{E},\sum_j jn_j\equiv 0 \pmod p}p^{3/2}(p/2\pi n)^{(p-1)/2}e^{-(pn/2)\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-D_pp^2n(\frac{n_j}{n}-\frac{1}{p})^3}\\&=(1+o(1))\sum_{(n_0,\dots,n_{p-1})\in\mathcal{E}}p^{1/2}(p/2\pi n)^{(p-1)/2}e^{-(pn/2)\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-D_pp^2n(\frac{n_j}{n}-\frac{1}{p})^3}.\end{aligned}$$

Proof. First, it is clear from [15, Eqn (3.14), (3.15)] that

$$e^{-(pn/2)\|(\frac{\mathbf{n}+\mathbf{e}_k-\mathbf{e}_0}{n}-\frac{\boldsymbol{\mu}}{d})\|_2^2}=(1+O(p\log^{1/2}n/n^{1/2}))e^{-(pn/2)\|(\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})\|_2^2}.$$

Note that

$$((\frac{\mathbf{n}+\mathbf{e}_k-\mathbf{e}_0}{n}-\frac{\boldsymbol{\mu}}{d})_j)^3=((\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})_j+(\frac{\mathbf{e}_k-\mathbf{e}_0}{n})_j)^3=((\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})_j)^3+O(((\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})_j)^2/n)+|(\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})_j|/n^2+O(1/n^3)$$

and clearly $p^2\sum_j((\frac{\mathbf{n}}{n}-\frac{\boldsymbol{\mu}}{d})_j)^2\le p^2\log n/n$, Hence we see that

$$\begin{aligned}e^{-(pn/2)\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-D_pp^2n(\frac{n_j}{n}-\frac{1}{p})^3}&=(1+O(p\log^{1/2}n/n^{1/2}+(p^2\log n)/n)\times\\&\times e^{-(pn/2)\sum_j((\frac{\mathbf{n}+\mathbf{e}_k-\mathbf{e}_0}{n}-\frac{\boldsymbol{\mu}}{d})_j)^2-D_pp^2n\sum_j((\frac{\mathbf{n}+\mathbf{e}_k-\mathbf{e}_0}{n}-\frac{\boldsymbol{\mu}}{d})_j)^3}.\end{aligned}$$

Summing over j and taking the average we obtain the claim. □

We then claim that

$$\sum_{(n_0,\dots,n_{p-1})\in\mathcal{E}}p^{1/2}(p/2\pi n)^{(p-1)/2}e^{-\frac{pn}{2}\sum_j(\frac{n_j}{n}-\frac{1}{p})^2-D_pp^2n(\frac{n_j}{n}-\frac{1}{p})^3}=1+o(1).$$

Replacing this Riemann sum by its integral, it suffices to show that

Lemma 3.9. *With the choices of parameters as in* (3),

$$\int_{\|\mathbf{y}\|_2^2 \le p\log n} (1/\sqrt{2\pi})^p e^{-\sum_j y_j^2/2 + D_p\sqrt{p/n}\sum_j y_j^3} dy_1 \dots dy_p \le 1 + o(1).$$

Proof. For each positive R such that $R^2 \le p\log n$ we consider $\sum_i y_i^2 = R^2$ and write

$$\int_{\|\mathbf{y}\|_2^2 = R^2} e^{-R^2/2 + D_p\sqrt{p/n}\sum_j y_j^3} dy_1 \dots dy_p = e^{-R^2/2} R^p \int_{\|\mathbf{x}\|_2 = 1} e^{D_p\sqrt{p/n}R^3\sum_j x_j^3} dx_1 \dots dx_p.$$

It is well known that the uniform measure $\frac{1}{\mathrm{Vol}(S_p)} dx_1 \dots dx_p$ over the unit sphere can be replaced by $x_j = \xi_i/\sqrt{\sum_i \xi_i^2}$ where $\xi_1, \dots, \xi_p$ are iid standard Gaussian. As such, our first goal is to show that for $R^2 \le p\log n$, with respect to the random Gaussian variables $\xi_1, \dots, \xi_p$

$$\mathbb{E} e^{D_p\sqrt{p/n}R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3} = 1 + o(1). \tag{10}$$

First, as $R^3 \le (p\log n)^{3/2}$ and clearly $e^{-cp}e^{D_p\sqrt{p/n}R^3} = o(1)$ if $p \ll n^{1/3}$, by large deviation of $\sum_j \xi_j^2$ (that $\mathbb{P}(\sum_i \xi_i^2 < p/4 \text{ or } \sum_i \xi_i^2 > 4p) \le e^{-cp}$ for some absolute constant c), the contribution in the expectation when $\sum_i \xi_i^2 < p/4$ or $\sum_i \xi_i^2 > 4p$ is $o(1)$. Let $\mathcal{E}_b$ denote the event $p/4 \le \sum_i \xi_i^2 \le 4p$.

Second, on the event $R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3 \le p$, as $\sqrt{p/n} \le 1/p^{1+\varepsilon/8}$ we must have $e^{D_p\sqrt{p/n}R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3} = e^{o(1)} = 1 + o(1)$. Hence it remains to focus on the events $p^{1+\varepsilon/8} \le R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3$ and the event $\mathcal{E}_b$ that $\sum_i \xi_i^2$ has order p.

Claim 3.10. *For $p^{1+\varepsilon/8} \le t \le R^3$ we have*

$$\mathbb{P}\Big(R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3 \ge t \wedge \mathcal{E}_b\Big) \le e^{-ct^{2/3}p/R^2},$$

for some absolute constant c.

Proof. For short, let $\alpha := tp^{3/2}/R^3$. As $\mathbb{P}(\xi_i^3 \ge x) = \mathbb{P}(\xi \ge x^{1/3}) = O(e^{-x^{2/3}/2})$ if x is large, by a result of Nagaev (see for instance [13, Eqn. (1.2) and Theorem 1]) we have

$$\mathbb{P}(\sum_{i=1}^p \xi_i^3 \ge \alpha) = \mathbb{P}(\sum_i \xi_i^3/p \ge \alpha/p) \le e^{-cp^{2/3}(\alpha/p)^{2/3}} = e^{-c\alpha^{2/3}},$$

for some absolute constant c. □

Back to our proof, with $X = R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3$,

$$\mathbb{E} e^{D_p\sqrt{p/n}R^2 X} 1_{p^{1+\varepsilon/8} \le X \le R^3 \wedge \mathcal{E}_b} \le \int_{p^{1+\varepsilon/8}}^{R^3} \sqrt{p/n} e^{D_p\sqrt{p/n}t} \mathbb{P}(X > t \wedge \mathcal{E}_b) dt$$

$$\le \int_{p^{1+\varepsilon/8}}^{R^3} \sqrt{p/n} R^2 e^{D_p\sqrt{p/n}t - ct^{2/3}p/R^2} \le \int_{p^{1+\varepsilon/8}}^{R^3} \sqrt{p/n} e^{-(c/2)\ t^{2/3}p/R^2} = o(1)$$

where in the second to last bound we used the fact that $t \le R^3$ and $R^2 \le p\log n$ and the choices of parameters from (3) (where we note that our bounds are slightly better than needed). With this we are done with proving (10). □

We have shown that for each R so that $R^2 \le p\log n$

$$\int_{\|\mathbf{y}\|_2^2=R^2} e^{-R^2/2+D_p\sqrt{p/n}\sum_j y_j^3} dy_1\dots dy_p = e^{-R^2/2}R^p\int_{\|\mathbf{x}\|_2=1} e^{D_p\sqrt{p/n}R^3\sum_j x_j^3}dx_1\dots dx_p$$
$$= e^{-R^2/2}R^p\mathrm{Vol}(S_p)\mathbb{E}e^{D_p\sqrt{p/n}R^3\sum_i(\xi_i/\sqrt{\sum_i \xi_i^2})^3}$$
$$= (1+o(1))e^{-R^2/2}R^p\mathrm{Vol}(S_p).$$

Hence

$$\int_{\|\mathbf{y}\|_2^2\le p\log n}(1/\sqrt{2\pi})^p e^{-\sum_j y_j^2/2+D_p\sqrt{p/n}\sum_j y_j^3}dy_1\dots dy_p = (1+o(1))\int_{R\le\sqrt{p\log n}}(1/\sqrt{2\pi})^p e^{-R^2/2}R^p\mathrm{Vol}(S_p)dR$$
$$= 1+o(1),$$

completing the proof of Lemma 3.9.

4. Proof of Theorem 3.3

We will choose η so that

$$\eta^2 p = \alpha p^{-1}$$

and assume that

$$|\frac{1}{p^{d-1}}\sum_{a_1,\dots,a_{d-1}}\exp(i(s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}))| \ge 1-\eta^2.$$

In other words, if $\psi = -\arg\phi_X(\mathbf{s})$ then

$$\frac{1}{p^{d-1}}\sum_{a_1,\dots,a_{d-1}}\mathrm{Re}(\exp(i(s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi))) \ge 1-\eta^2. \quad (11)$$

By shifting every s_a by a constant, we can assume

$$s_0 = 0.$$

Note that $|\sin(x)| \ge 2\|x/\pi\|_{\mathbb{R}/\mathbb{Z}}$ (which we replace by $\|\cdot\|$ for short),

$$\mathrm{Re}(\exp(i(s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi))) = \cos(s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi)$$
$$= 1-2\sin^2(\frac{s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi}{2}) \le 1-8\|\frac{s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi}{2\pi}\|^2.$$

Hence the assumption of Theorem 3.3 (or more specifically (11)) implies

$$\sum_{a_1,\dots,a_{d-1}}\|\frac{s_{a_1}+\dots+s_{a_{d-1}}+s_{-\sum_i a_i}+\psi}{2\pi}\|^2 \le \eta^2 p^{d-1}/8. \quad (12)$$

Macroscopic analysis. Our first goal is the following

Lemma 4.1. *There exists $d_0 \in \{0,\dots,p-1\}$ such that for all a*

$$\|\frac{s_a}{2\pi}-\frac{d_0 a}{p}\| \ll \sqrt{\eta^2 p}.$$

For this, we first show the following

Claim 4.2. *We have*

(1)

$$\|\frac{\psi}{2\pi}\| \ll_d \sqrt{\eta^2 p}. \quad (13)$$

(2) Also, for all $a_1, \dots, a_{d-1}$

$$\|\frac{s_{a_1} + \dots + s_{a_{d-1}} + s_{-a_1 - \dots - a_{d-1}}}{2\pi}\| \ll_d \sqrt{\eta^2 p}.$$

Note that the proof of this result is similar to the first part of the proof of [15, Proposition 2.3].

Proof. We have learned that

$$\sum_{\mathbf{a}} \|\frac{\langle \mathbf{s}, \mathbf{a}\rangle + \psi}{2\pi}\|^2 \leq \eta^2 p^{d-1}/8.$$

Let $\varepsilon_0 < 4/d$. Let $\mathcal{G}$ be the set of $\mathbf{a}$ (such that $\sum_i a_i = 0$) where $\|\frac{\langle \mathbf{s},\mathbf{a}\rangle+\psi}{2\pi}\| \leq \sqrt{\varepsilon_0^{-1}\eta^2 p}$, then we have that the size of the set complement $\bar{\mathcal{G}}$ is at most

$$|\bar{\mathcal{G}}| \leq \varepsilon_0 p^{d-2}/8.$$

Fix $\mathbf{a}_1 = \mathbf{a} = (a_1, \dots, a_d)$ with $\sum_i a_i = 0$, and let $\mathbf{w} = \Phi(\mathbf{a}_1)$. The total number of zero sum $d \times d$ matrices (of zero column and row sums) with the first row $\mathbf{a}_1$ is $p^{(d-1)(d-2)}$. For any $\mathbf{b}$, the number of such matrices with first row $\mathbf{a}_1$ and some other row $\mathbf{b}$ is at most $(d-1)p^{(d-3)(d-1)}$, and the number with first row $\mathbf{a}_1$ and some other column $\mathbf{b}$ is at most $dp^{(d-2)(d-2)}$. So the number of zero sum $d \times d$ matrices with the first row $\mathbf{a}_1$ and at least one row or column belonging to $\bar{\mathcal{G}}$ is bounded by $((d-1)p^{(d-3)(d-1)} + dp^{(d-2)(d-2)})|\bar{\mathcal{G}}| < 2dp^{(d-2)(d-2)}\varepsilon_0 p^{d-2}/8 < p^{(d-2)(d-1)}$. It thus follows that there exists a zero sum $d \times d$ matrix with the first row $\mathbf{a}_1$ and all other rows $\mathbf{a}_2, \dots, \mathbf{a}_d$ and columns $\mathbf{b}_1, \dots, \mathbf{b}_d$ belonging to $\mathcal{G}$. By the triangle inequality,

$$\|\frac{\langle \mathbf{s}, \mathbf{a}\rangle + \psi}{2\pi}\| = \|\frac{\sum_{i=1}^n (\langle \mathbf{s}, \mathbf{b}_i\rangle + \psi) - \sum_{j=2}^n (\langle \mathbf{s}, \mathbf{a}_j\rangle + \psi)}{2\pi}\| \leq (2d-1)\sqrt{\varepsilon_0^{-1}\eta^2 p}.$$

□

Choosing $a_1 = a, a_2 = -a, a_3 = \dots = a_{d-1} = 0$, we obtain that

$$\|\frac{s_a + s_{-a}}{2\pi}\| \ll \sqrt{\eta^2 p}.$$

Hence without loss of generality we can assume that $s_{-a} = -s_a$.

Proof. (of Lemma 4.1) For short we let

$$q := \lceil p\sqrt{\eta^2 p}\rceil.$$

Note that by definition q is much smaller than p. By Claim 4.2, given that α is sufficiently small, we have that

$$\|\frac{s_{a_1} + \dots + s_{a_{d-1}} + s_{-a_1 - \dots - a_{d-1}}}{2\pi}\| < \sqrt{\eta^2 p}, \forall a_1, \dots, a_{d-1}.$$

It suffices to assume $s_a \in [-\pi, \pi]$ for all a. We first choose $k_a \in \mathbb{Z}$ such that

$$|\frac{k_a}{p} - \frac{s_a}{2\pi}| \leq \frac{1}{2p}$$

and $k_{-a} = -k_a$. Let K be a sufficiently large even constant (and recall that p is sufficiently large). Our goal is to show that there exists an integer d_0 such that

$$k_a \equiv d_0 a + [-5Kq, 5Kq] \pmod{p}, \text{ for all } a. \tag{14}$$

(Here we can replace 5 by 2 but it will not yield any significant improvement in application.) Lemma 4.1 would then follow because

$$\|\frac{s_a}{2\pi} - \frac{d_0 a}{p}\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{10Kq+1}{2p} \ll \sqrt{\eta^2 p}.$$

In what follows we show (14). Consider intervals (arcs) I_a in $\mathbb{Z}/p\mathbb{Z}$ of length Kq centered at k_a,

$$I_a = [k_a - Kq/2, k_a + Kq/2] \subset \mathbb{Z}/p\mathbb{Z}.$$

Note that $I_0 = [-Kq/2, Kq/2]$. Let B be the set of the following points in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$,

$$B = \{(a, l), a \in \mathbb{Z}/p\mathbb{Z}, l \in I_a\}.$$

For each $k \geq 1$, we will be interested in the set $kB := \{b_1 + \cdots + b_k, b_i \in B\}$. In particular,

$$(d-1)B = \bigcup_{a_1,\dots,a_{d-1}} \{a_1 + \cdots + a_{d-1}\} \times (I_{a_1} + \cdots + I_{a_{d-1}}).$$

For this set, on one hand,

$$I_{a_1} + \cdots + I_{a_{d-1}} = [\sum_i k_{a_i} - Kq(d-1)/2, \sum_i k_{a_i} + Kq(d-1)/2].$$

On the other hand, by definition, $\|\frac{s_{a_1}+\cdots+s_{a_{d-1}}+s_{-a_1-\cdots-a_{d-1}}}{2\pi}\| \leq \sqrt{\eta^2 p}$, and so by the triangle inequality

$$|\frac{k_{a_1} + \cdots + k_{a_{d-1}} + k_{-(a_1+\cdots+a_{d-1})}}{p}| \leq \|\frac{s_{a_1} + \cdots + s_{a_{d-1}} + s_{-a_1-\cdots-a_{d-1}}}{2\pi}\| + \frac{d}{2p} \leq \sqrt{\eta^2 p} + \frac{d}{2p}.$$

Hence (noting the choice of η) we have

$$|k_{a_1} + \cdots + k_{a_{d-1}} + k_{-(a_1+\cdots+a_{d-1})}| \leq 2p\sqrt{\eta^2 p} \leq 2q,$$

and for any $m \leq d-1$, by choosing $k_{a_{m+1}} = \cdots = k_{a_{d-1}} = 0$,

$$|k_{a_1} + \cdots + k_{a_m} + k_{-(a_1+\cdots+a_m)}| \leq 2q.$$

It can be shown by induction that for any $m \geq 0$

$$|k_{a_1} + \cdots + k_{a_m} + k_{-(a_1+\cdots+a_m)}| \leq 6q\frac{m-1}{d-2}.$$

Indeed, for $m = 2$, from $|l(k_a + k_b + k_{-(a+b)})| \leq 2q$ with $l = \lfloor d/3 \rfloor$ we have $|k_a + k_b + k_{-a-b}| \leq \frac{2q}{l} \leq \frac{6q}{d-2}$. If the above is true up to $m-1$, then

$$|k_{a_1}+\cdots+k_{a_m}+k_{-(a_1+\cdots+a_m)}| \leq |k_{a_1}+\cdots+k_{a_{m-2}}+k_{a_{m-1}+a_m}+k_{-(a_1+\cdots+a_m)}|+|k_{a_{m-1}+a_m}-k_{a_{m-1}}-k_{a_m}| \leq 6q\frac{m-1}{d-2}.$$

Therefore with $c = -(a_1 + \cdots + a_m)$, over $\mathbb{Z}/p\mathbb{Z}$

$$\begin{aligned} I_{a_1} + \cdots + I_{a_m} &= [\sum_i k_{a_i} - Kqm/2, \sum_i k_{a_i} + Kqm/2] \\ &\subset [-k_c - Kqm/2 - 6q\frac{m-1}{d-2}, -k_c + Kqm/2 + 6q\frac{m-1}{d-2}]. \end{aligned} \tag{15}$$

Notice that the set B has size $p(Kq+1)$, while the union of the sets $\{c\} \times [-k_c - \frac{Kqm}{2} - 6q\frac{m-1}{d-2}, -k_c + \frac{Kqm}{2} + 6q\frac{m-1}{d-2}]$ has size $p(Kqm + 12q\frac{m-1}{d-2} + 1)$. Thus we have

$$|mB| \leq pKqm + p + 12pq\frac{m-1}{d-2} \leq m|B| + 12pq\frac{m-1}{d-2}. \tag{16}$$

When $d = 3$. We have

$$|2B| \leq 2|B| + 12pq.$$

Note that when K is large, $12pq$ is small compared to $|B|$. This is similar to Freiman's $(3n-3)$-theorem [31] except that our setting is not torsion-free. We then use a very recent result by Lev [23, Theorem 1], which says that if B is not contained in the union of fewer than ℓ cosets of a subgroup of $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and if $|2B| \leq 3(1 - 1/\ell)|B|$, then there exists an arithmetic progression $P \subset G$ of size $|P| \geq 3$ and a subgroup G' of G such that

$$|P + G'| = |P||G'|, B \subset P + G', \text{ and } (|P| - 1)|G'| \leq |2B| - |B|. \tag{17}$$

For short, we call such a structure $P+G'$ a *coset progression (of rank one)*. We will choose $\ell = 4$. Consider the case that B is contained in 3 cosets of a subgroup G' of G. By definition, G' must be $\mathbb{Z}/p\mathbb{Z} \times \{0\}$. However this is impossible because $|I_a| = Kq+1 > 3$ (for any a) as K is large.

Hence B cannot be contained in 3 cosets, as $|B+B| < 3(1-1/4)|B|$, we see that there is some subgroup G' and some arithmetic progression $P \subset G$ such that

$$B \subset P + G'.$$

We then divide into several subcases.

(i) $G' = \{0\} \times \mathbb{Z}/p\mathbb{Z}$, as I_a is a proper subset of $\mathbb{Z}/p\mathbb{Z}$, this is impossible.

(ii) $G' = \{0\} \times \{0\}$, we then see that $B \subset P$ and $|P|$ has size at most $|2B| - |B| + 1 \leq |B| + 12pq + 1 < (K+13)pq$. As P is an arithmetic progression, it can be written as $P = \{(p_0, q_0) + i(x,y), 0 \leq i \leq |P|-1\}$ for some (p_0,q_0) and (x,y) in G, where it is clear that $x \neq 0$. For each a, consider $S_a = \{0 \leq i \leq |P|-1, p_0 + ix = a\}$. Each $i \in S_a$ has the form $i = i_a + lp$ for some representative i_a. So $I_a \subset \{q_0 + (i_a + lp)y\} = \{q_0 + i_a y\}$. However, this is impossible as I_a has length $Kq+1$, which is sufficiently large.

(iii) G' is a cyclic proper subgroup of form $\{i(g,h), 0 \leq i \leq p-1\}$, for some $(g,h) \neq (0,0)$ in G. We see that $(|P|-1)p \leq (K+13)pq$, and so $|P| \leq (K+13)q$. Write $P = \{(p_0,q_0) + j(x,y), 0 \leq j \leq |P|-1 \leq (K+13)q\}$. For each a we let S_a be the set of pairs (i,j) such that $p_0 + ig + jx = a$. Then it is clear that $g \neq 0$, $I_a \subset \{q_0 + ih + jy, (i,j) \in S_a\}$, and

$$i = g^{-1}(a - p_0) - jg^{-1}x.$$

So we have

$$\begin{aligned} I_a &\subset \{q_0 + (g^{-1}(a-p_0) - jg^{-1}x)h + jy, 0 \leq j \leq (K+13)q\} \\ &= \{q_0 + g^{-1}h(a-p_0) - j(g^{-1}xh - y), 0 \leq j \leq (K+13)q\}. \end{aligned}$$

Hence either $g^{-1}xh - y = -1$ or $g^{-1}xh - y = 1$. Without loss of generality we assume the latter. Note that as $I_0 \subset \{q_0 - g^{-1}hp_0 - j(g^{-1}xh - y), 0 \leq j \leq (K+13)\sqrt{\eta^2 p}\}$, we must have (with some room to spare)

$$q_0 - g^{-1}hp_0 \in [-2Kq, 2Kq].$$

Putting this together,

$$\begin{aligned} I_a = [k_a - Kq/2, k_a + Kq/2] &\subset \{q_0 - g^{-1}hp_0 - j(g^{-1}xh - y) + g^{-1}ha, 0 \leq j \leq (K+13)q\} \\ &\subset [-4Kq + g^{-1}ha, 4Kq + g^{-1}ha]. \end{aligned}$$

We thus conclude that for all a we have $k_a \in [g^{-1}ha - 5Kq, g^{-1}ha + 5Kq]$, confirming (14).

From the proof, we can actually obtain (14) from a slightly more general result (when we applied [23] for $\ell = 4$ as above)

Lemma 4.3. *Assume that $B = \{(a,l), a \in \mathbb{Z}/p\mathbb{Z}, l \in I_a\}$, where I_a are intervals of length $K+1$ for sufficiently large K as above, and $K \ll p$. Then if $|B+B| < 9|B|/4$, the set B can be contained in a coset progression of rank one $P+G'$ as in (17).*

Corollary 4.4. *Assume that for some positive integer h of order $O(1)$ we have*

$$|2^h B| < 2.25^h |B|.$$

Then there exists a coset progression of rank one $P+G'$ of size $O_h(|B|)$ as in (17) such that $B \subset P+G'$.

It is important to note that if there exists such $P+G'$, we can argue as (iii) in the above proof to then arrive at (14) (with H depending on h.)

Proof. By assumption, there exists $0 \le h' \le h-1$ so that

$$|2^{h'+1}B| \le 2.25|2^{h'}B|.$$

We will then apply Lemma 4.3 to contain the set $2^{h'}B$ in a coset progression $P+G'$ of size at most $2|2^{h'}B| \le 2.25^h|B|$. Now as $B \subset 2^{h'}B$ (as B contains $\{0\}$ [2]), we hence have a similar containment for B. □

General d. From (16), we have

$$|mB| \le m|B| + 6pq\frac{m-1}{d-2} \le m|B| + 6pqm \le m(1+\frac{6}{K})|B|$$

Choosing $m = 2^h$ and K to be sufficiently large we can apply Corollary 4.4.

□

4.5. **Microscopic analysis.** With the help of Lemma 4.1, by replacing s_a by $s_a - 2\pi(d_0 a/p)$ for all a, we are thus free to replace $\|\cdot\|$ (that is $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$) by $|\cdot|$ as all the numbers are sufficiently small. In the next step we establish the following key estimate.

Lemma 4.6 (structure of triple)**.** *Assume that for all a*

$$|\frac{s_a}{2\pi}| = o(1)$$

$$|\frac{s_{a_1} + \dots + s_{a_{d-1}} + s_{-a_1-\dots-a_{d-1}} + \psi}{2\pi}|^2 \le \eta^2 p.$$

Then there exists an absolute constant A such that

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} |\frac{s_a}{2\pi}|^2 \le A\eta^2 p.$$

Proof. (of Lemma 4.6) By shifting each s_a by ψ/d (in $2\pi\mathbb{R}/\mathbb{Z}$), we can assume $\psi = 0$. (Since $\psi = o(1)$, we still have $|\frac{s_a}{2\pi}| = o(1)$.) In what follows $\varepsilon_0 > 0$ is a sufficiently small constant, which can change depending on the situation.

For transparency, we again consider the simple case first.

When $d = 3$. Let $\mathcal{B}$ be the collection of (a,b) where

$$|\frac{s_a + s_b + s_{-a-b}}{2\pi}| + |\frac{s_{-a} + s_{-b} + s_{a+b}}{2\pi}| \ge \eta\varepsilon_0^{-1}.$$

By assumption,

$$|\mathcal{B}| \le \varepsilon_0^2 p^2.$$

Let $\mathcal{G}$ be the complement of $\mathcal{B}$ in $(\mathbb{Z}/p\mathbb{Z})^2$. Hence for all $(a,b) \in \mathcal{G}$ (and at the same time $(-a,-b) \in \mathcal{G}$ and $(a,-a-b),(b,-a-b) \in \mathcal{G}$) we have that

$$|\frac{s_a + s_b + s_{-a-b}}{2\pi}|, |\frac{s_{-a} + s_{-b} + s_{a+b}}{2\pi}| < \varepsilon_0^{-1}\eta =: \eta'. \tag{18}$$

Let η' be of order p^{-1}. As before, for each a we let $k_a \in \mathbb{Z}$ be such that $-p/2 < k_a < p/2$ and that $|\frac{s_a}{2\pi} - \frac{k_a}{p}| \le \frac{1}{2p}$. Then by the assumption of Lemma 4.6, $k_a = o(p)$, and also by (18), as long as $(a,b) \in \mathcal{G}$ we have

$$k_a + k_b + k_{-a-b} \in \{-3,\dots,3\}.$$

Indeed, this is because

$$\|\frac{k_a + k_b + k_{-a-b}}{p}\| \le \|\frac{s_{-a} + s_{-b} + s_{a+b}}{2\pi}\| + \frac{3}{2p} \le \frac{3}{p}.$$

[2] This assumption is not needed, as $2^{h'}B$ contains a translation of B.

As this holds for all $(a,b) \in \mathcal{G}$ (which consist most of the pairs (a,b)), we guess that k_a must be linear in a. This is very similar to our situation in the previous section, except that here we are working over $\mathbb{Z}$, and not all but almost all pairs (a,b) have this property. To confirm this we prove

Claim 4.7. *$|k_a|$ is at most $O(1)$ for all but $O(\varepsilon_0 p)$ indices $a \in \{0,\dots,p-1\}$.*

Proof. We say that a is *good* if the number of pairs $(b,c) \in \mathcal{G}$ such that $a+b=-c$ is at least $(1-\varepsilon_0)p$. It is not hard to see that there are $(1-\varepsilon_0)p$ such good indices. Assume that a_0 is such that $|k_{a_0}|$ is the largest among the good a. Without loss of generality we assume that k_{a_0} is positive. Consider $(b,c) \in \mathcal{G}$ such that $a+b=-c$. There are $(1-\varepsilon_0)p$ such pairs, and because most indices are good, there are $(1-2\varepsilon_0)p$ pairs in which b,c are good. Because $k_c \in -(k_{a_0}+k_b)+\{-3,\dots,3\}$, and because k_{a_0} is maximal, the following holds: either k_b is negative, or $0 < k_b \le 2$. So for each case we can decompose $\{0,\dots,p-1\}$ into two sets $\mathcal{P} = \{a, k_a \ge 0\}$ and $\mathcal{N} = \{a, k_a < 0\}$.

Assume that $|\mathcal{N}| \ge 10\varepsilon_0 p$. Let $s \in \mathcal{N}$, then either there exists $t \in \mathcal{N}$ such that $s+t = -k_{a_0}+O(1)$ or $s = -k_{a_0}+O(1)$. In either case, if $k_{a_0} \gg 1$ then we have $|s| \ge |k_{a_0}|/2 + O(1)$. Now the set of $a \in \mathcal{N}$ where $|k_a| > k_{a_0}/2+3$ cannot be of size $\varepsilon_0 p$ because otherwise we could choose two elements a_1, a_2 so that $k_{-a_1-a_2} > k_{a_0}$, a contradiction. Also, the number of of $a \in \mathcal{N}$ such that $|k_a| \le k_{a_0}/2-2$ cannot be more than $\varepsilon_0 p$ because then $|k_{-a_0-a}| \ge k_{a_0}/2+3$, and we have learned that the number of such is at most $\varepsilon_0 p$. Putting this together, we see that the remaining set $\mathcal{N}^*$ of a such that $|k_a| < k_{a_0}/2-2$ has size at least $|\mathcal{N}| - 2\varepsilon_0 p$ which has order around $-k_{a_0}/2$. To this end, consider the set $\{(a,a') \in \mathcal{G}, a+a', a, a' \in \mathcal{N}^*\}$. This set has size at least approximately $|\mathcal{N}^*|$, and if $a'' = -(a+a')$ then $k_{a''}$ is approximately k_{a_0}. So if there are many such a'' and therefore a pair $(a_1'', a_2'') \in \mathcal{G}$, we then see that $k_{-a_1''-a_2''}$ is approximately $2k_{a_0}$, a contradiction. Hence $|\mathcal{N}| < 10\varepsilon_0 p$, and therefore $|\mathcal{P}| \ge (1-11\varepsilon_0)p$, completing the proof. □

Let B be the set of indices satisfying Claim 4.7. Assume that B is a proper subset of $\mathbb{Z}/p\mathbb{Z}$. Let $c \in (\mathbb{Z}/p\mathbb{Z})\backslash B$, then as $|B| \ge (1-O(\varepsilon_0))p$, there are $(1-O(\varepsilon_0^2))p$ pairs $(a,b) \in B^2$ such that $a+b+c=0$. By assumption we have

$$\sum_{a,b;-(a+b)\notin B} \|\frac{s_a+s_b+s_{-a-b}}{2\pi}\|^2 \le \sum_{a,b} \|\frac{s_a+s_b+s_{-a-b}}{2\pi}\|^2 \le \eta^2 p^2/8.$$

Hence

$$\sum_{c,c=-(a+b)\notin B} \|\frac{-s_a-s_b+s_c}{2\pi}\|^2 \le \eta^2(1-O(\varepsilon_0^2))^{-1}p^2/8.$$

Notice that when $a \in B$, as $k_a = O(1)$, we have $\|\frac{s_a}{2\pi}\| = O(\frac{1}{p}) = O(\eta')$. So by the triangle inequality

$$\|\frac{s_c}{2\pi}\| \le (\|\frac{-s_a-s_b+s_c}{2\pi}\| + O(\eta')).$$

Thus we have

$$\sum_{c,c=-(a+b)\notin B} \|\frac{s_c}{2\pi}\|^2 \le \sum_{c,c=-(a+b)\notin B} 2(\|\frac{-s_a-s_b+s_c}{2\pi}\|^2 + O({\eta'}^2)) \le 2\eta^2(1-O(\varepsilon_0^2))^{-1}p^2/8 + 2p^2\eta^2.$$

Recall that there are $(1-O(\varepsilon_0^2))p$ pairs $(a,b) \in B^2$ such that $a+b+c=0$. Then

$$\sum_{c\notin B} \|\frac{s_c}{2\pi}\|^2 \le O({\eta'}^2 p).$$

Altogether,

$$\sum_c \|\frac{s_c}{2\pi}\|^2 = \sum_{c\notin B} \|\frac{s_c}{2\pi}\|^2 + \sum_{c\in B} \|\frac{s_c}{2\pi}\|^2 = O({\eta'}^2 p).$$

This completes the proof of our result for $d=3$.

Treatment for general d. The proof here will be similar to the case $d = 3$, so we will be brief. Let $\mathcal{B}$ be the collection of $(a_1, \dots, a_{d-1})$ for which

$$|\frac{s_{a_1} + \cdots + s_{a_{d-1}} + s_{-\sum a_i}}{2\pi}| \geq \eta\varepsilon_0^{-1}.$$

By assumption,

$$|\mathcal{B}| \leq \varepsilon_0^2 p^{d-1}.$$

Let $\mathcal{G}$ be the complement of $\mathcal{B}$ in $(\mathbb{Z}/p\mathbb{Z})^{d-1}$. Hence for all $(a_1, \dots, a_{d-1}) \in \mathcal{G}$ we have that

$$|\frac{s_{a_1} + \cdots + s_{a_{d-1}} + s_{-\sum a_i}}{2\pi}| \geq \eta\varepsilon_0^{-1} =: \eta'. \tag{19}$$

Let η' be of order p^{-1}. As before, for each a we let $k_a \in \mathbb{Z}$ be such that $-p/2 < k_a < p/2$ and that $|\frac{s_a}{2\pi} - \frac{k_a}{p}| \leq \frac{1}{2p}$. Then by the assumption of Lemma 4.6, $k_a = o(p)$, and also by (19), as long as $(a, b) \in \mathcal{G}$ we have

$$k_{a_1} + \cdots + k_{a_{d-1}} + k_{-a_1 - \cdots - a_{d-1}} \in \{-3d, \dots, 3d\},$$

where A is an absolute constant. As this holds for all $(a, b) \in \mathcal{G}$ (which occupies most of the tuples of $(a_1, \dots, a_{d-1})$), we will show as in the case $d = 3$ the following

Claim 4.8. *Most of $|k_a|$ are at most $O(d)$.*

Proof. We say that a is good if the number of tuples $(a_1, \dots, a_{d-1}) \in \mathcal{G}$ such that $a = -\sum_i a_i$ is at least $(1 - \varepsilon_0)p^{d-1}$. It is not hard to see that there are $(1 - \varepsilon_0)p$ such good indices. Assume that a_0 is such that $|k_{a_0}|$ is largest among the good a. Without loss of generality we assume that k_{a_0} is positive. Consider $(a_1, \dots, a_{d-1}) \in \mathcal{G}$ such that $a_0 = -\sum_i a_i$. There are $(1 - \varepsilon_0)p^{d-2}$ such tuples, and because most of the indices are good, there are $(1 - 2\varepsilon)p^{d-2}$ tuples where for which all a_i are good. Because $k_{a_0} \in (-\sum_i k_{a_i}) + \{-3d, \dots, 3d\}$, and because k_{a_0} is the largest, there must be a good a_i such that k_{a_i} is negative. Arguing as in the case $d = 3$, assume that the set $\mathcal{N}$ of a for which k_a is negative has size at least $10d\varepsilon_0 n$, then most of the k_a must be around $-k_{a_0}/(d-1)$. We can find many a'' for which $k_{a''} \approx k_{a_0}$, and therefore a tuple $(a''_1, \dots, a''_{d-1}) \in \mathcal{G}$. Then $k_{-\sum a''_i} \approx (d-1)k_{a_0}$, which is larger than k_{a_0}, a contradiction. □

The rest of the proof of Lemma 4.6 can be completed as in $d = 3$, hence we omit the details. □

5. The error term: proof of Proposition 2.4

Recall that we are working with

$$\sum_{j=0}^{p-1} (\frac{n_j}{n} - \frac{1}{p})^2 > \frac{b \log n}{n}.$$

Our proof here is similar to [15, Proposition 3.4], which can be divided into four cases

(i) $\mathcal{N}_1$ of $(n_0, \dots, n_{p-1}) \in \mathcal{N}$ with

$$\max_j |n_j/n - 1/p| \leq \delta/p;$$

(ii) $\mathcal{N}_2$ of $(n_0, \dots, n_{p-1}) \in \mathcal{N}$ with

$$(bp \log n)/n < |n_0/n - 1| \leq \delta/p;$$

(iii) $\mathcal{N}_3$ of $(n_0, \dots, n_{p-1}) \in \mathcal{N}$ with

$$|n_0/n - 1| < (bp \log n)/n;$$

(iv) $\mathcal{N}_4$ of the remaining non-equidistributed p-tuples.

We then have

Lemma 5.1. *For $p \ll n^{1/3}$ [3], the sum over $(n_0,\dots,n_{p-1}) \notin \mathcal{N}_3$ is bounded by*

$$\sum_{(n_0,\dots,n_{p-1})\in\mathcal{N}_1\cup\mathcal{N}_2\cup\mathcal{N}_4} \binom{n}{n_0,\dots,n_{p-1}}\binom{dn}{dn_0,\dots,dn_{p-1}}^{-1}\Big|\{(\mathbf{u}_1,\dots,\mathbf{u}_n)\in\mathcal{U}_{d,p}^n : \mathbf{u}_1+\dots+\mathbf{u}_n=(dn_0,\dots,dn_{p-1})\}\Big|$$
$$= O(1/n^{d-2}).$$

The proof of this is identical to that of [15, Proposition 3.4], hence we omit it.

Our new contribution is that the sum from $\mathcal{N}_3$ is also insignificant for $p \ll n^{1/3}$, for which we state below.

Lemma 5.2. *For $p \ll n^{1/3}$ we have*

$$\sum_{(n_0,\dots,n_{p-1})\in\mathcal{N}_3} \binom{n}{n_0,\dots,n_{p-1}}\binom{dn}{dn_0,\dots,dn_{p-1}}^{-1}\Big|\{(\mathbf{u}_1,\dots,\mathbf{u}_n)\in\mathcal{U}_{d,p}^n : \mathbf{u}_1+\dots+\mathbf{u}_n=(dn_0,\dots,dn_{p-1})\}\Big| = o(1).$$

Proof. (of Lemma 5.2) The treatment here is motivated by Case 3 in the proof of [15, Proposition 3.4], although we introduce some minor modifications. We assume that $n_0 = n - m'$ and $n_1 + \dots + n_{p-1} = m'$, where

$$m' \le bp \log n.$$

We list $\mathcal{U}_{d,p}$ as

$$\mathcal{U}_{d,p} = \{\mathbf{w}_1,\dots,\mathbf{w}_{p^d-1}\}, \mathbf{w}_1 = (d,0,\dots,0).$$

Notice that (where $\mathbf{w}(j)$ is the j-th coordinate of $\mathbf{w}$)

$$\mathbf{w}_j(1) + \dots + \mathbf{w}_j(p-1) \ge 2, 2 \le j \le p^{d-1}.$$

For short, we let m be the number of non-zero vectors (and $n-m$ be the number of $\mathbf{w}_1$) in $\mathbf{u}_1,\dots,\mathbf{u}_n$, and $n_0' = m - n_2 - \dots - n_{p-1}$. We have $2m \le dm'$, so

$$m \le dm'/2.$$

This shows that the number of $\mathbf{w}_1$ in $(\mathbf{u}_1,\dots,\mathbf{u}_n)$ must be at least $n - dm'/2$. We thus have $\binom{n}{m}$ ways to arrange the $\mathbf{u}_i$ to be $\mathbf{w}_1$. After that we have a sum of $\mathbf{u}_1 + \dots + \mathbf{u}_m = (dn_0', dn_1, \dots, dn_{p-1})$ and $n_0' + n_1 + \dots + n_{p-1} = m$ where $n' \le (d-2)m/d$.

As we are interested in $\binom{n}{n_0,\dots,n_{p-1}}\binom{dn}{dn_0,\dots,dn_{p-1}}^{-1} \times |\{(\mathbf{u}_1,\dots,\mathbf{u}_m) : \mathbf{u}_1+\dots+\mathbf{u}_m = (dn_0', dn_1,\dots,dn_{p-1})\}|$, we can rewrite the first factor as

$$\frac{n!}{n_0!\dots n_{p-1}!} = \frac{n!n_0'!}{m!n_0!}\frac{m!}{n_0'!\dots n_{p-1}!} = \frac{n!n_0'!}{m!n_0!}\binom{m}{n_0',\dots,n_{p-1}}$$

and we can write the second factor as

$$\frac{dn_0!\dots dn_{p-1}!}{dn!} = \frac{dm!dn_0!}{dn!dn_0'!}\frac{dn_0'!dn_1!\dots dn_{p-1}!}{dm!} = \frac{dm!dn_0!}{dn!dn_0'!}\binom{dm}{dn_0',\dots,dn_{p-1}}^{-1}.$$

Note that $n_0 = n - \sum_{i=1}^{p-1} n_i = n - (m - n_0')$. Hence

$$\frac{n!n_0'!}{m!n_0!} \approx n^{m-n_0'}/m^{m-n_0'} \approx (n/m)^{m-n_0'}$$

and

$$\frac{dm!dn_0!}{dn!dn_0'!} \approx (dn)^{-d(m-n_0')}(dm)^{d(m-n_0')} \approx (n/m)^{-d(m-n_0')}.$$

Thus

$$\frac{n!n_0'!}{m!n_0!}\frac{dm!dn_0!}{dn!dn_0'!} \approx (m/n)^{(d-1)(m-n_0')}.$$

We next apply the following analog of [15, Proposition 3.2] (where n is replaced by m)

[3] In fact the statements here are also true for $p \ll n^{1/2}$.

Lemma 5.3. *We have*

$$\binom{m}{n_0',\dots,n_{p-1}}\binom{dm}{dn_0',\dots,dn_{p-1}}^{-1}|(\mathbf{u}_1,\dots,\mathbf{u}_m),\mathbf{u}_1+\cdots+\mathbf{u}_m=(dn_0',dn_1,\dots,dn_{p-1})|=O(e^{O(p)}).$$

This result is a special case of Lemma 5.4 to be stated below.

By this result, in total we obtain

$$\sum_{m\le bp\log n}\ \sum_{\substack{(n_0',\dots,n_{p-1}),\\ n_0'+\cdots+n_{p-1}=m}} e^{O(p)}\binom{n}{m}(m/n)^{(d-1)(m-n_0')}$$

$$=\sum_{m\le bp\log n}\ \sum_{n_0'\le(d-2)m/d}\ \sum_{\substack{(n_1,\dots,n_{p-1}),\\ n_1+\cdots+n_{p-1}=m-n_0'}} e^{O(p)}\binom{n}{m}(m/n)^{(d-1)(m-n_0')}$$

$$\le\sum_{m\le bp\log n}\ \sum_{n_0'\le(d-2)m/d}\binom{p+m-n_0'}{p-1}e^{O(p)}\binom{n}{m}(m/n)^{(d-1)(m-n_0')}.$$

Case 1. We see that the contribution is small for $p/\log n\ll m\le bp\log n$ because $\binom{p+m-n_0'}{p-1}\le(e(p+m)/p)^p$ and $\binom{n}{m}\le(en/m)^m$, while $(m/n)^{(d-1)(m-n_0')}\le(m/n)^{2(d-1)m/d}$.

Case 2. For $m\ll p/\log n$, Lemma 5.3 is not powerful enough because as $n_0'+n_1+\cdots+n_p=m$, many n_i are zero. To amend this, let ℓ be the number of nonzero n_{i_j}, then $0\le\ell\le m$ and $n_{i_1}+\cdots+n_{i_\ell}=m$. There are $\binom{p}{\ell}$ ways to choose the $i_1,\dots,i_\ell$. So $\binom{m}{n_0',\dots,n_{p-1}}\binom{dm}{dn_0',\dots,dn_{p-1}}^{-1}$ becomes $\binom{m}{n_{i_1},\dots,n_{i_\ell}}\binom{dm}{dn_{i_1},\dots,dn_{i_\ell}}^{-1}$.

Also, as $\mathbf{u}_1+\cdots+\mathbf{u}_m=(dn_0',dn_1,\dots,dn_{p-1})$, the vectors $\mathbf{u}_i$ are from the set $\mathcal{U}_{d;i_1,\dots,i_\ell}$ of vectors $\Phi(x_1,\dots,x_d)$ where $x_i\in\{i_1,\dots,i_\ell\}$ and $\sum_i x_i=0$. Note that this set $\mathcal{U}_{d;i_1,\dots,i_\ell}$ has at most ℓ^{d-1} elements, so

$$|(\mathbf{u}_1,\dots,\mathbf{u}_m):\mathbf{u}_1+\cdots+\mathbf{u}_m=(dn_0',dn_1,\dots,dn_{p-1})|=|\mathcal{U}_{d;i_1,\dots,i_\ell}|^m\times\mathbb{P}(X_1+\cdots+X_m=(dn_{i_1},\dots,dn_{i_\ell})),$$

where X_i are sampled uniformly from the set $\mathcal{U}_{d;i_1,\dots,i_\ell}$.

Lemma 5.4. *We have*

$$\binom{m}{n_{i_1},\dots,n_{i_\ell}}\binom{dm}{dn_{i_1},\dots,dn_{i_\ell}}^{-1}|\{(\mathbf{u}_1,\dots,\mathbf{u}_m),\mathbf{u}_1+\cdots+\mathbf{u}_m=(dn_{i_1},\dots,dn_{i_\ell})\}|\le e^{O(\ell)}.$$

Assuming Lemma 5.4 for a moment, by summing over $(n_0,\dots,n_\ell)$ as a partition of m (of which there are at most $\binom{m+\ell-1}{m}$)) and over the choices of $i_1,\dots,i_\ell$ we have

$$\sum_{m\ll p/\log n}\ \sum_{n_0'\le(d-2)m/d}\ \sum_{1\le\ell\le m}\binom{p}{\ell}\binom{m+\ell-1}{m}e^{O(\ell)}\binom{n}{m}(m/n)^{(d-1)(m-n_0')}.$$

We remark that for $\ell\le m\le p/\log n$ we have $\binom{p}{\ell}\le(ep/\ell)^\ell\le(ep/m)^m$ and $\binom{m+\ell+1}{m}<2^m$, and $\binom{n}{m}\le(en/m)^m$, while $(m/n)^{(d-1)(m-n_0')}\le(m/n)^{2(d-1)m/d}\le(m/n)^{4m/3}$ (where $d=3$ is the worst case). Hence the sum above is trivially bounded by

$$(p/\log n)\times m\times m\times(ep/m)^m2^m(en/m)^m(m/n)^{4m/3}\le(p/\log n)m^2(2e^2)^m\times(p/n^{1/3})^m(1/m)^{2m/3}=o(1)$$

where we used the crucial fact that $p\ll n^{1/3}$. This complete the proof of Lemma 5.2. □

Proof. (of Lemma 5.4) Without loss of generality assume $\{i_1, \dots, i_\ell\} = \{0, \dots, \ell-1\}$. Using (4),

$$\binom{n}{n_0, \dots, n_{\ell-1}} \frac{\prod_{j=0}^{\ell-1}(dn_j)!}{(dm)!} = \frac{m!}{\prod_j n_j!} \frac{\prod_{j=0}^{\ell-1}(dn_j)!}{(dm)!}$$
$$= e^{\frac{1}{12m} - \frac{1}{12dm} + \sum_j \frac{1}{12dn_j} - \frac{1}{12n_j}} \times (\sqrt{d})^{\ell-1} \times [\prod_{j=0}^{\ell-1} (\frac{n_j}{m})^{n_j}]^{d-1}.$$

Write $\mathfrak{n}_j = \frac{n_j}{m}$ and $h_j = \mathfrak{n}_j - 1/\ell$. We then write the expression in Lemma 5.4 as

$$e^{O(\ell)} e^{mI(\mathfrak{n}_0, \dots, \mathfrak{n}_\ell)}$$

where the $e^{O(\ell)}$ term comes from $(\sqrt{d})^{\ell-1}$ and

$$I(\mathfrak{n}_0, \dots, \mathfrak{n}_\ell) = \log |\mathcal{U}_{d;0,\dots,\ell-1}| + (d-1) \sum_j \mathfrak{n}_j \log \mathfrak{n}_j + \inf_{\mathbf{t} \in \mathbb{R}^\ell} (\log \mathbb{E} e^{\langle \mathbf{t}, X \rangle} - d \langle \mathbf{t}, \mathfrak{n} \rangle).$$

It remains to show the following

Claim 5.5. *We have $I(\mathfrak{n}_0, \dots, \mathfrak{n}_\ell) \le 0$ and equality holds only if either $\mathfrak{n}_j = 1/\ell$ for all j or $\mathfrak{n}_0 = 1$ and $\mathfrak{n}_j = 0$ for $j \ne 0$.*

To show this claim we follow [14, Prop 3.3]. Choose $\mathbf{t} = \frac{d-1}{d}(\log \mathfrak{n}_0, \dots, \log \mathfrak{n}_{\ell-1}) + \frac{\log |\mathcal{U}|}{d} \mathbf{1}$. Then I is bounded by

$$\log |\mathcal{U}_{d;0,\dots,\ell-1}| + (d-1) \sum_j \mathfrak{n}_j \log \mathfrak{n}_j + \log \mathbb{E} e^{\langle \mathbf{t}, X \rangle} - d \langle \mathbf{t}, \mathfrak{n} \rangle = \log \mathbb{E} e^{\langle \mathbf{t}, X \rangle},$$

where X is sampled uniformly from $\mathcal{U}_{d;0,\dots,\ell-1}$. We will show that $\mathbb{E} e^{\langle \mathbf{t}, X \rangle} \le 1$. Let $\mathbf{w}_1, \dots, \mathbf{w}_{\ell^{d-1}}$ be an enumeration of $\mathcal{U}_{d;0,\dots,\ell-1}$, we have

$$\mathbb{E} e^{\langle \mathbf{t}, X \rangle} = \frac{1}{|\mathcal{U}|} \sum_{j \in \mathcal{U}} e^{\langle \mathbf{w}_j, \mathbf{t} \rangle} = \frac{1}{|\mathcal{U}|} \sum_{j \in \mathcal{U}} e^{\sum_{k=0}^{\ell-1} \mathbf{w}_j(k)((d-1)/d) \log \mathfrak{n}_k + \mathbf{w}_j(k) \log |\mathcal{U}|/d}$$
$$= \sum_{j \in \mathcal{U}} e^{\sum_{k=0}^{\ell-1} \mathbf{w}_j(k)((d-1)/d) \log \mathfrak{n}_k} = \sum_{j \in \mathcal{U}} \prod_{k=0}^{\ell-1} \mathfrak{n}_k^{((d-1)/d)\mathbf{w}_j(k)}$$
$$= \sum_{\substack{\mathbf{a}=(a_1,\dots,a_d) \in \{0,\dots,\ell-1\}^d, \\ \sum_i a_i = 0}} \prod_{k=0}^{\ell-1} \mathfrak{n}_k^{((d-1)/d)\Phi(\mathbf{a})(k)}$$
$$= \sum_{\substack{\mathbf{a} \in \{0,\dots,\ell-1\}^d, \\ \sum_i a_i = 0}} \prod_{k=0}^{\ell-1} \mathfrak{n}_k^{((d-1)/d) \sum_{r=1}^d 1_{a_r = k}}$$
$$= \sum_{\substack{\mathbf{a} \in \{0,\dots,\ell-1\}^d, \\ \sum_i a_i = 0}} \prod_{r=1}^{d} \mathfrak{n}_{a_r}{}^{(d-1)/d}.$$

Next, note that $\sum_{i \in \{0,\dots,\ell-1\}} \mathfrak{n}_i = 1$ and

$$\prod_{r=1}^d \mathfrak{n}_{a_r}{}^{(d-1)/d} \le \frac{1}{d} \sum_{r=1}^d \prod_{\substack{1 \le s \le d, \\ s \ne r}} \mathfrak{n}_{a_s}.$$

So

$$\begin{aligned}\mathbb{E}e^{\langle \mathbf{t}, X\rangle} &= \sum_{\substack{\mathbf{a}\in\{0,\dots,\ell-1\}^d,\\ \sum_i a_i=0}} \prod_{r=1}^{d} \mathfrak{n}_{a_r}{}^{(d-1)/d} \\ &\le \frac{1}{d} \sum_{\substack{\mathbf{a}\in\{0,\dots,\ell-1\}^d,\\ \sum_i a_i=0}} \sum_{r=1}^{d} \prod_{\substack{1\le s\le d,\\ s\neq r}} \mathfrak{n}_{a_s} \\ &\le (\sum_{i\in\{0,\dots,\ell-1\}} \mathfrak{n}_i)^d = 1.\end{aligned}$$

□

Acknowledgements. The authors are thankful to V. Lev and G. Petridis for fruitful discussion and to Eric Lu for programming assistance. They are grateful to the referees who had provided so many helpful comments and suggestions.

References

[1] R. Adamczak, D. Chafaï, and P. Wolff, Circular law for random matrices with exchangeable entries, *Random Struct. Algoritm.*, 48(3):454–479, 2016.

[2] A. Basak, N. Cook, and O. Zeitouni, Circular law for the sum of random permutation matrices, *Electron. J. Probab.*, 23:1–51, 2018.

[3] A. Basak and M. Rudelson, Invertibility of sparse non-Hermitian matrices, *Adv. Math.*, 310:426–483, 2017.

[4] B. Bollobás, A Probabilistic Proof of an Asymptotic Formula for the Number of Labelled Regular Graphs, *European J. Combin.*, 1(4):311–316, December 1980.

[5] B. Bollobás, *Random Graphs*, volume 73 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, second edition, 2001.

[6] C. Bordenave and D. Chafaï, Around the circular law, *Probab. Surv.* 9 (2012) 1–89.

[7] J. Bourgain, V. Vu, and P.M. Wood, On the singularity probability of discrete random matrices, *J. Funct. Anal.*, 258(2):559–603, 2010.

[8] A. Coja-Oghlan, P. Gao, M. Hahn-Klimroth, J. Lee, N. Muller, M. Rolvien, The full rank condition for sparse random matrices, `https://arxiv.org/abs/2112.14090`.

[9] N. A. Cook. On the singularity of adjacency matrices for random regular digraphs, *Probab. Theory Related Fields*, 167(1-2):143–200, February 2017.

[10] K. P. Costello and V. H. Vu, The rank of random graphs, *Random Struct. Algoritm.*, 33(3):269–285, 2008.

[11] A. Frieze, Random structures and algorithms, In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. 1*, pages 311–340. Kyung Moon Sa, Seoul, 2014.

[12] A. Ferber, M. Kwan, A. Sah and M. Sawhney, Singularity of the k-core of a random graph, *Duke Math. J.* 172 (7) 1293 - 1332, 15 May 2023.

[13] N. Gantert, K. Ramanan and F. Rembart, Large deviations for weighted sums of stretched exponential random variables, *Electron. Commun. Probab.* 19: 1–14 (2014).

[14] J. Huang, Invertibility of adjacency matrices for random d-regular directed graphs, `arXiv:1806.01382`, June 2018.

[15] J. Huang, Invertibility of adjacency matrices for random d-regular graphs. graphs, *Duke Math. J. 170 (2021), no. 18, 3977-4032.*

[16] H. Huang. Rank of sparse Bernoulli matrices, `arXiv:2009.13726`.

[17] V. Jain, A. Sah, and M. Sawhney, Singularity of discrete random matrices, *Geom. Funct. Anal.*, 31(5), 1160–1218.

[18] J. Kahn, J. Komlós, and E. Szemerédi, On the probability that a random ±1-matrix is singular, *J. Amer. Math. Soc.*, 8(1):223–240, 1995.

[19] J. Komlós, On the determinant of (0, 1) matrices, *Studia Sci. Math. Hungar*, 2:7–21, 1967.

[20] A. E. Litvak, A. Lytova, K. Tikhomirov, N. Tomczak-Jaegermann, and P. Youssef, Adjacency matrices of random digraphs: Singularity and anti-concentration, *J. Math. Anal. Appl.*, 445(2):1447–1491, January 2017.

[21] A. E. Litvak, A. Lytova, K. Tikhomirov, N. Tomczak-Jaegermann, and P. Youssef, Structure of eigenvectors of random regular digraphs, *Trans. Amer. Math. Soc., 371(11):8097–8172, 2019*.

[22] A. E. Litvak and K. Tikhomirov, Singularity of sparse Bernoulli matrices, *Duke Math. J.* 171 (2022), no. 5, 1135–1233.

[23] V. Lev, Small doubling in groups with moderate torsion, *SIAM J. Discrete Math.* 36 (2022), no. 1, 315–335.

[24] A. Mészáros, The distribution of sandpile groups of random regular graphs, *Trans. Amer. Math. Soc.*, 373 (2020), 6529–6594.

[25] M. Molloy, H. Robalewska, R. W. Robinson, and N. C. Wormald, 1-factorizations of random regular graphs, *Random Struct. Algoritm.*, 10(3):305–321, 1997.

[26] H. H. Nguyen, On the singularity of random combinatorial matrices, *SIAM J. Discrete Math.*, 27(1):447–458, 2013.

[27] H. H. Nguyen and M. M. Wood, Cokernels of adjacency matrices of random r-regular graphs, arxiv.org/abs/1806.10068.

[28] M. Rudelson and R. Vershynin, The Littlewood-Offord problem and invertibility of random matrices, *Adv. Math.*, 218(2):600–633, 2008.

[29] T. Tao, An inverse theorem for an inequality of Kneser, *Proc. Steklov Inst. Math.* 303 (2018) 193–219.

[30] T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, *J. Amer. Math. Soc.*, 20(3):603–628, 2007.

[31] T. Tao and V. Vu, Additive combinatorics, Volume 105, Cambridge University Press, Cambridge, 2006.

[32] K. Tikhomirov. Singularity of random Bernoulli matrices, *Ann. of Math. (2).*, 191 (2020), no. 2, 593–634.

[33] V. H. Vu. Combinatorial problems in random matrix theory, *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. IV*, pages 489–508. Kyung Moon Sa, Seoul, 2014.

[34] P. M. Wood, Universality and the circular law for sparse random matrices, *Ann. Appl. Probab.*, 22(3):1266–1300, 2012.

[35] M. M. Wood, The distribution of sandpile groups of random graphs, *J. Amer. Math. Soc.*, 30(4):915–958, 2017.

Department of Mathematics, The Ohio State University, 231 W 18th Ave, Columbus, OH 43210 USA

Email address: nguyen.1261@math.osu.edu

Department of Mathematics, The Ohio State University, 231 W 18th Ave, Columbus, OH 43210 USA

Email address: pan.754@osu.edu