The strong circular law: a combinatorial view

Vishesh Jain*

Abstract

Let N_n be an $n \times n$ complex random matrix, each of whose entries is an independent copy of a centered complex random variable z with finite non-zero variance σ^2. The strong circular law, proved by Tao and Vu, states that almost surely, as $n \to \infty$, the empirical spectral distribution of $N_n/(\sigma\sqrt{n})$ converges to the uniform distribution on the unit disc in $\mathbb{C}$.

A crucial ingredient in the proof of Tao and Vu, which uses deep ideas from additive combinatorics, is controlling the lower tail of the least singular value of the random matrix $xI - N_n/(\sigma\sqrt{n})$ (where $x \in \mathbb{C}$ is fixed) with failure probability that is inverse polynomial. In this paper, using a simple and novel approach (in particular, not using tools from additive combinatorics or any net arguments), we show that for any fixed matrix M with operator norm at most $n^{0.51}$ and for all $\eta \geq 0$,

$$\Pr\left(s_n(M + N_n) \leq \eta\right) \lesssim n^C \eta + \exp(-n^c),$$

where $s_n(M + N_n)$ is the least singular value of $M + N_n$ and C, c are absolute constants. Our result is optimal up to the constants C, c and the inverse exponential-type error rate improves upon the inverse polynomial error rate due to Tao and Vu.

During the course of our proof, we extend the solution of the counting problem in inverse Littlewood-Offord theory, recently isolated by the author along with Ferber, Luh, and Samotij, from Rademacher variables to general complex random variables. This significantly improves on estimates for this problem obtained using the optimal inverse Littlewood-Offord theorem of Nguyen and Vu, and may be of independent interest.

1 Introduction

Let N_n be an $n \times n$ complex random matrix, each of whose entries is an independent copy of a complex random variable z with mean 0 and finite non-zero variance σ^2. The *empirical spectral distribution* (ESD) μ_n of N_n is defined on $\mathbb{R}^2$ by the expression

$$\mu_n(s,t) := \frac{1}{n} \cdot \left|\{k \in [n] \mid \Re(\lambda_k) \leq s; \Im(\lambda_k) \leq t\}\right|,$$

where $\lambda_1, \dots, \lambda_n$ denote the eigenvalues of $N_n/\sigma\sqrt{n}$. The celebrated *strong circular law* of Tao and Vu [27] asserts that almost surely, as n tends to infinity, μ_n converges uniformly to

$$\mu_\infty(s,t) := \frac{1}{\pi}\text{area}\{x \in \mathbb{C} \mid |x| \leq 1, \Re(x) \leq s, \Im(x) \leq t\}.$$

The circular law has a long history dating back to the 1950s when it was conjectured as a natural non-Hermitian counterpart to Wigner's famous semi-circle law, and prior to Tao and Vu's definitive work, many researchers obtained partial results requiring extra distributional assumptions on the random variable z and very often weakening the notion of convergence from almost sure convergence

*Massachusetts Institute of Technology. Department of Mathematics. Email: visheshj@mit.edu.

to convergence in probability (this is not just a technical point and genuinely new ideas are required to obtain almost sure convergence; see the discussion in Section 2 of [24]). We refer the reader to the survey [4] and the references therein for a much more detailed discussion of the history of this problem.

In the case when we further assume that z has $2+\eta$ moments for any $\eta > 0$, the approach of Bai [1], Bai and Silverstein [2], and Girko [11] reduces the problem to controlling the lower tail of the least singular value of the random matrix $xI - N_n/(\sigma\sqrt{n})$ where $x \in \mathbb{C}$ is fixed; even when we assume that z has only non-zero finite variance, controlling the lower tail of the least singular value of this random matrix is a fundamental step in Tao and Vu's proof (recall that the least singular value of a complex matrix M_n, denoted by $s_n(M_n)$, is the smallest eigenvalue of the positive semidefinite matrix $\sqrt{M_n^\dagger M_n}$). To this end, Tao and Vu [24] showed using sophisticated techniques from additive combinatorics that for any constants $A, C > 0$, there exists a constant $B > 0$ such that for any $n \times n$ fixed (complex) matrix M of operator norm at most n^C,

$$\Pr\left(s_n(M + N_n) \leq n^{-B}\right) \lesssim n^{-A}. \tag{1}$$

The dependence of B on A and C can be made explicit and was subsequently sharpened in [26]. Note that for the proof of the circular law, fixing $C = n^{0.51}$ (say) is more than sufficient.

Our goal in the present work is to provide a simple and elementary proof of a quantitative strengthening of Equation (1) in the setting of the circular law. More precisely, we show:

Theorem 1.1. *Let z be a complex random variable with mean 0 and variance 1 and let N_n be an $n \times n$ random matrix, each of whose entries is an independent copy of z. Let M be a fixed complex matrix with operator norm at most $n^{0.51}$. Then, for all $\eta \geq 0$,*

$$\Pr\left(s_n(M + N_n) \leq \eta\right) \leq C\left(n^{5/2}\eta + \exp(-cn^{1/50})\right),$$

where C, c are constants depending only on z.

Remark 1.2. (1) In the above theorem, the choice of the power $n^{0.51}$ is arbitrarily made for convenience and could be replaced by $n^{0.75-\epsilon}$ for any $\epsilon > 0$; in follow-up work of the author [14] which builds on some of the ideas in this paper, we will show (using a more complicated proof) how to obtain a bound on the lower tail of $M + N_n$ even if $\|M\| = O(\exp(n^c))$.

(2) Our bound is optimal up to the constants $C, c, 5/2, 1/50$ (none of which we have tried to optimize). Compared to Equation (1), our bound is closer to (optimal) bounds of the form

$$C\sqrt{n}\eta + C\exp(-cn),$$

which have been obtained under stronger assumptions: for the case when z is a real subgaussian random variable and $\|M\| = O(\sqrt{n})$ in the landmark work of Rudelson and Vershynin [21], and for the case when z is a real random variable and (much more restrictively) $M = 0$ by Rebrova and Tikhomirov [19].

Apart from the quantitative strengthening of Equation (1), we believe that our result is also interesting for the simplicity of the proof techniques, making use only of some standard Fourier analytic techniques along with elementary combinatorial ideas. In particular, in contrast to previous works in this area, we make no use of tools from additive combinatorics or net arguments. A part of our proof which we believe may be of independent interest is Theorem 2.11, which extends the 'counting inverse Littlewood-Offord theorem' of Ferber, Jain, Luh, and Samotij (Theorem 1.7 in [9]) from Rademacher random variables to general complex random variables (see Theorem 2.11), and gives significantly stronger bounds for the so-called counting problem in inverse Littlewood-Offord theory than can be obtained from the inverse Littlewood-Offord theorems of Tao and Vu [25], and Nguyen and Vu [17] (see the discussion in Section 2.3). We hope that some of the ideas introduced in this work can aid in proving strong circular laws in other contexts such as [3, 5] where only weak circular laws are known so far.

Organization: The rest of this paper is organized as follows. In Section 2, we collect some auxiliary results needed for the proof of our main theorem – the key results here are Theorem 2.10 (proved in Appendix A), Theorem 2.11 (proved in Section 4 and Appendix B) and Proposition 2.13 (proved in Section 5). In Section 3, we prove Theorem 1.1 by combining these results. The key ingredient there is Proposition 3.3.

Notation: Throughout the paper, we will omit floors and ceilings when they make no essential difference. For convenience, we will also say 'let $p = x$ be a prime', to mean that p is a prime between x and $2x$; again, this makes no difference to our arguments. We will use $\mathbb{S}^{2n-1}$ to denote the set of unit vectors in $\mathbb{C}^n$, $B(x,r)$ to denote the ball of radius r centered at x, and $\Re(\boldsymbol{v}), \Im(\boldsymbol{v})$ to denote the real and imaginary parts of a complex vector $\boldsymbol{v} \in \mathbb{C}^n$. As is standard, we will use $[n]$ to denote the discrete interval $\{1,\dots,n\}$. We will also use the asymptotic notation $\lesssim, \gtrsim, \ll, \gg$ to denote $O(\cdot), \Omega(\cdot), o(\cdot), \omega(\cdot)$ respectively. For a matrix M, we will use $\|M\|$ to denote its standard $\ell^2 \to \ell^2$ operator norm. All logarithms are natural unless noted otherwise.

Acknowledgements: I am indebted to Nick Cook for the suggestion to consider the complex setting, as well as very helpful discussions around the circular law. I would also like to thank Kyle Luh for pointing out that a statement similar to Proposition 2.13 also appears in [20], Hoi Nguyen for discussing his work [17], and Elizaveta Rebrova for discussing her work [19].

2 Tools and auxiliary results

In this section, we collect some preliminary results which will be used in the proof of Theorem 1.1.

2.1 Anti-concentration

The goal of the theory of anti-concentration is to obtain upper bounds on the Lévy concentration function, defined as follows.

Definition 2.1 (Lévy concentration function)**.** Let z be an arbitrary complex random variable and let $\boldsymbol{v} := (v_1,\dots,v_n) \in \mathbb{C}^n$. We define the *Lévy concentration function of $\boldsymbol{v}$ at radius r with respect to z* by

$$\rho_{r,z}(\boldsymbol{v}) := \sup_{x\in\mathbb{C}} \Pr\left(v_1z_1 + \cdots + v_nz_n \in B(x,r)\right),$$

where $z_1,\dots,z_n$ are independent copies of z.

Remark 2.2. In particular, note that $\rho_{r,z}(1) = \sup_{x\in\mathbb{C}} \Pr(z \in B(x,r))$. We will use this notation repeatedly.

The next lemma shows that weighted sums of random variables with finite non-zero variance are not too close to being a constant.

Lemma 2.3. *(see, e.g., Lemma 6.3 in [26]) Let z be a complex random variable with finite non-zero variance. Then, there exists a constant $c_{2.3} \in (0,1)$ depending only on z such that for any $\boldsymbol{v} \in \mathbb{S}^{2n-1}$,*

$$\sup_{\boldsymbol{v}\in\mathbb{S}^{n-1}} \rho_{c_{2.3},z}(\boldsymbol{v}) \leq 1 - c_{2.3}.$$

Combining this with the so-called tensorization lemma (see Lemma 2.2 in [21]), we get the following standard estimate for 'invertibility with respect to a single vector'.

Lemma 2.4. *Let z be a complex random variable with finite non-zero variance. Let M be an arbitrary $n \times n$ complex matrix and let N_n be an $n \times n$ complex random matrix each of whose entries is an independent copy of z. Then, for any fixed $\boldsymbol{v} \in \mathbb{S}^{2n-1}$,*

$$\Pr\left(\|(M+N_n)\boldsymbol{v}\|_2 \leq c_{2.4}\sqrt{n}\right) \leq (1-c_{2.4})^n,$$

where $c_{2.4} \in (0,1)$ is a constant depending only on z.

The next classical lemma, due to Esseen, is a generalization (up to constants) of the Erdős-Littlewood-Offord anti-concentration inequality.

Lemma 2.5 (Theorem 2 in [7])**.** *Let $z_1, \dots, z_n$ be jointly independent complex random variables and let $t_1, \dots, t_n$ be some positive real numbers. Then, for any $t \geq \max_j t_j$, we have*

$$\rho_{t,\sum_{j=1}^n z_j}(1) \leq C_{2.5} t^2 \left(\sum_{j=1}^n t_j^4 (1 - \rho_{t_j,z_j}(1))\right)^{-1/2},$$

where $C_{2.5} \geq 1$ is an absolute constant.

The next definition isolates a convenient property of the random variables we consider in this paper.

Definition 2.6. We say that a complex random variable z is C*-good* if

$$\Pr(C^{-1} \leq |z_1 - z_2| \leq C) \geq C^{-1}, \tag{2}$$

where z_1 and z_2 denote independent copies of z. The smallest $C \geq 1$ with respect to which z is C-good will be denoted by C_z.

Indeed, as the following lemma shows, complex random variables with finite non-zero variance are C-good for some finite C, so that there is no loss of generality for us in imposing this additional restriction.

Lemma 2.7. *Let z be a complex random variable with variance 1. Then, z is C_z-good for some $C_z \geq 1$.*

Proof. Since $\mathrm{Var}(z) = 1$, there must exist some $u_z, v_z \in (0,1)$ such that $\rho_{v_z,z}(1) \leq u_z$. Therefore, letting z' denote an independent copy of z, we have

$$\Pr\left(|z - z'| \leq \frac{v_z}{2}\right) \leq \rho_{v_z,z-z'}(1) \leq \rho_{v_z,z}(1) \leq u_z.$$

Moreover, since $\mathbb{E}[|z-z'|^2] = \mathrm{Var}(z-z') = \mathrm{Var}(z) + \mathrm{Var}(z') = 2$, it follows from Markov's inequality that

$$\Pr\left(|z - z'| \geq 2(1-u_z)^{-1/2}\right) \leq \frac{1-u_z}{2}.$$

Combining these two bounds, we see that

$$\Pr\left(\frac{v_z}{2} \le |z - z'| \le 2(1-u_z)^{-1/2}\right) \ge \frac{1-u_z}{2},$$

which gives the desired conclusion. $\square$

We conclude this subsection with the following consequence of Lemma 2.5.

Lemma 2.8. *Let z be a complex random variable with variance 1. There exists a constant $C_{2.8} \ge 1$ depending only on z such that for all $\boldsymbol{w} := (w_1, \dots, w_n) \in (\mathbb{Z} + i\mathbb{Z})^n$ with support of size at least $n^{0.99}$,*

$$\rho_{1,z}(\boldsymbol{w}) \le C_{2.8} n^{-0.495}.$$

Proof. As above, we know that $\rho_{v_z,z}(1) \le u_z$ for some $u_z, v_z \in (0,1)$. Therefore, for all $j \in \mathbf{supp}(\boldsymbol{w})$,

$$\rho_{v_z, w_j z_j}(1) \le \rho_{|w_j| v_z, w_j z_j}(1) \le \rho_{v_z, z_j}(1) \le u_z.$$

Hence, by Lemma 2.5,

$$\rho_{v_z, \sum_{j=1}^n w_j z_j}(1) \le \frac{C_{2.5}}{\sqrt{|\mathbf{supp}(\boldsymbol{w})|(1-u_z)}}.$$

Since $|\mathbf{supp}(\boldsymbol{w})| \ge n^{0.99}$, and since $\rho_{1,z}(\boldsymbol{w}) \le \max\{1, v_z^{-1}\}\rho_{v_z, \sum_{j=1}^n w_j z_j}(1)$, the desired conclusion follows. $\square$

2.2 The Least Common Denominator

The proof of Theorem 1.1 will be based on a 'rounding argument' which extracts a 'not-too-large' Gaussian integer vector certifying that the least singular value of a complex matrix is small (see [13] for the most basic version of this argument). For this, we will use (albeit in a quite different manner from Rudelson and Vershynin) the notion of the Least Common Denominator (LCD) of a vector, and its connection to the Lévy concentration function, as developed in [21].

Our definition of the LCD is slightly different from the ones appearing in the literature for the complex case, and has been made keeping in mind our application to rounding vectors.

Definition 2.9 (Least Common Denominator (LCD))**.** Let $\boldsymbol{a} \in \mathbb{C}^n \setminus \{\mathbf{0}\}$. For $\gamma \in (0,1)$ and $\alpha > 0$, define

$$\mathrm{LCD}_{\gamma,\alpha}(\boldsymbol{a}) := \inf_{\theta \in \mathbb{C}} \left\{|\theta| > 0 : \mathrm{dist}(\theta \boldsymbol{a}, (\mathbb{Z} + i\mathbb{Z})^n) < \min\{\gamma|\theta|\|\boldsymbol{a}\|_2, \alpha\}\right\}.$$

Note that the requirement that the distance is smaller than $\gamma|\theta|\|\boldsymbol{a}\|_2$ forces us to consider only non-trivial Gaussian integer points as approximations of $\theta\boldsymbol{a}$.

The following theorem shows that vectors with large LCD have small Lévy concentration function on scales which are larger (up to some small polynomial losses) than $\Omega(1/\mathrm{LCD})$.

Theorem 2.10. *Let z denote a C_z-good complex random variable. Then, for every $\boldsymbol{a} \in \mathbb{S}^{2n-1}$, for every $\alpha \in (0, \sqrt{n}), \gamma \in (0,1)$, and for*

$$\delta \ge \frac{n^{0.1}\alpha}{\mathrm{LCD}_{\alpha,\gamma}(\boldsymbol{a})},$$

we have

$$\rho_{\delta,z}(\boldsymbol{a}) \le C_{2.10}\left(\frac{\sqrt{n}\delta}{\gamma} + \exp\left(-C_{2.10}^{-1}\alpha^2\right)\right),$$

where $C_{2.10} \ge 1$ is a constant depending only on C_z.

A more precise version of this theorem appears for real random variables in [22]. Actually, a version for complex random variables is also stated there although, as noted above, their definition of LCD is different from ours. The proof of Theorem 2.10 follows from standard Fourier analytic arguments for the real case (in particular, we will use a crude version of the argument of Friedland and Sodin in [10]) once we use a 'doubling trick'. We provide complete details in Appendix A.

2.3 The counting problem in inverse Littlewood-Offord theory

The inverse Littlewood-Offord problem, posed by Tao and Vu [29], asks for the underlying reason that the Lévy concentration function of a vector $\boldsymbol{v} \in \mathbb{C}^n$ can be large. Using deep Frieman-type results from additive combinatorics, they showed that, roughly speaking, the only reason for this to happen is that most of the coordinates of the vector $\boldsymbol{v}$ belong to a generalized arithmetic progression (GAP) of 'small rank' and 'small volume'. Their results [29, 25] were subsequently sharpened by Nguyen and Vu [17], who proved an 'optimal inverse Littlewood–Offord theorem'. We refer the reader to the survey [18] and the textbook [28] for complete definitions and statements, and much more on both forward and inverse Littlewood-Offord theory.

Recently, motivated by applications, especially those in random matrix theory, the following *counting variant* of the inverse Littlewood–Offord problem was isolated in work [9] of the author along with Ferber, Luh, and Samotij: for *how many* vectors $\boldsymbol{a}$ in a given collection $\mathcal{A} \subseteq \mathbb{Z}^n$ is $\rho_{1,z}(\boldsymbol{a})$ greater than some prescribed value, where z is a symmetric Bernoulli random variable? Indeed, the inverse Littlewood-Offord theorems are typically used precisely through such counting corollaries [18], and one of the main contributions of [9] (see Theorem 1.7 there) was to show that one may obtain useful bounds for the counting variant of the inverse Littlewood-Offord problem directly, *without* providing a precise structural characterization like Tao-Vu. In fact, since this approach is not hampered by losses coming from the black-box application of various theorems from additive combinatorics, it provides quantitatively better bounds, and this was used in [9, 8, 13] to provide quantitative improvements for several problems in combinatorial random matrix theory.

A natural question left open by this line of work is whether one can adapt the strategy of [9] to study random matrices whose entries have 'continuous' distributions as well. However, since the proofs in [9] proceed by viewing (bounded) integer-valued random variables as random variables valued in $\mathbb{F}_p$ for sufficiently large p, it is not clear whether the combinatorial techniques there can be extended.

Here, we answer this question in the affirmative, and prove the following extension of Theorem 1.7 in [9].

Theorem 2.11. *Let z be a C_z-good random variable. For $\rho \in (0,1)$ (possibly depending on n), let*

$$\boldsymbol{V}_\rho := \{\boldsymbol{v} \in (\mathbb{Z} + i\mathbb{Z})^n : \rho_{1,z}(\boldsymbol{v}) \geq \rho\}.$$

There exists a constant $C_{2.11} \geq 1$, depending only on C_z, for which the following holds. Let $n, s, k \in \mathbb{N}$ with $1000C_z \leq k \leq \sqrt{s} \leq s \leq n/\log n$. If $\rho \geq C_{2.11} \max\left\{e^{-s/k}, s^{-k/4}\right\}$ and p is an odd prime such that $2^{n/s} \geq p \geq C_{2.11}\rho^{-1}$, then

$$|\varphi_p(\boldsymbol{V}_\rho)| \leq \left(\frac{5np^2}{s}\right)^s + \left(\frac{C_{2.11}\rho^{-1}}{\sqrt{s/k}}\right)^n,$$

where φ_p denotes the natural map from $(\mathbb{Z} + i\mathbb{Z})^n \to (\mathbb{F}_p + i\mathbb{F}_p)^n$.

Remark 2.12. The inverse Littlewood-Offord theorems may be used to deduce similar statements, *provided we further assume that $\rho \geq n^{-C}$ for some constant $C > 0$.* It is the freedom of taking ρ to be much smaller which allows us to obtain the exponential-type rate in Theorem 1.1.

We provide a complete proof of Theorem 2.11 in Section 4.

2.4 Norms of large projections of random matrices

The key difficulty with extending the geometric techniques of Rudelson and Vershynin [21, 23]) to the setting when the random variables have heavy tails is the lack of control on the operator norm of the random matrix. For our techniques, the following proposition will turn out to be an appropriate substitute for controlling the operator norm.

For a subset $I \subseteq [n]$, let $P_I : \mathbb{C}^n \to \mathbb{C}^n$ denote the orthogonal projection onto the subspace spanned by the vectors $\{e_i : i \in I\}$. We have:

Proposition 2.13. *Let $N_n := (m_{ij})$ be an $n \times n$ complex random matrix with i.i.d. entries, each with mean 0 and variance 1. For $\epsilon, \delta \in (0, 1/2)$ with $\delta \geq 4\epsilon$, there exists $C_{2.13}(\epsilon) \geq 1$ such that, except with probability at most $C_{2.13}(\epsilon) \exp\left(-n^{1-\epsilon}/8\right)$, the following hold.*

1. *There exists $I \subseteq [n]$ with $|I| \geq n - 2n^{1-\epsilon}$ such that*
$$\|P_I N_n\|_{\infty \to 2} \leq C_{2.13}(1) n^{1+\epsilon}.$$
2. *For every $J \subseteq [n]$ with $|J| = n^{1-\delta}$, there exists some $I(J) \subseteq [n]$ such that $|I(J)| \geq n - 2n^{1-\epsilon}$, and*
$$\|P_{I(J)} N_n P_J\|_{\infty \to 2} \leq C_{2.13}(1) n^{1+\epsilon-0.5\delta}.$$

Remark 2.14. A statement similar to the one above, and with some common proof ideas, already appears in the work of Rebrova and Vershynin [20]. In that work, the primary interest is in obtaining optimal bounds on the restricted operator norms and consequently, the proofs are much more involved. In contrast, we do not require such optimal bounds for our application, and are therefore able to give a much shorter proof of the above proposition.

The complete proof of this proposition is deferred to Section 5.

3 Proof of Theorem 1.1

In this section, we will take $\alpha := n^{1/100}$ and $\gamma := n^{-1/2}$. Moreover, since Theorem 1.1 is trivially true for $\eta \geq n^{-2}$, we will henceforth assume that $2^{-n^{0.0001}} \leq \eta < n^{-2}$. Recall that M is a fixed $n \times n$ matrix with operator norm at most $n^{0.51}$; we set $M_n := M + N_n$.

We decompose $\mathbb{S}^{2n-1}$ into $\Gamma^1(\eta) \cup \Gamma^2(\eta)$, where

$$\Gamma^1(\eta) := \left\{\boldsymbol{a} \in \mathbb{S}^{2n-1} : \mathrm{LCD}_{\alpha,\gamma}(\boldsymbol{a}) \geq n^{0.7} \cdot \eta^{-1}\right\}$$

and $\Gamma^2(\eta) := \mathbb{S}^{2n-1} \setminus \Gamma^1(\eta)$. Accordingly, we have

$$\Pr\left(s_n(M_n) \leq \eta\right) \leq \Pr\left(\exists \boldsymbol{a} \in \Gamma^1(\eta) : \|M_n \boldsymbol{a}\|_2 \leq \eta\right) + \Pr\left(\exists \boldsymbol{a} \in \Gamma^2(\eta) : \|M_n \boldsymbol{a}\|_2 \leq \eta\right).$$

Therefore, Theorem 1.1 follows from the following two propositions and the union bound.

Proposition 3.1. $\Pr\left(\exists \boldsymbol{a} \in \Gamma^1(\eta) : \|M_n \boldsymbol{a}\|_2 \leq \eta\right) \leq 2nC_{2.10}\left(n^{3/2}\eta + \exp(-C_{2.10}^{-1} n^{1/50})\right)$.

Proposition 3.2. $\Pr\left(\exists \boldsymbol{a} \in \Gamma^2(\eta) : \|M_n \boldsymbol{a}\|_2 \leq \eta\right) \leq C_{3.2}\left(e^{-n^{0.98}} + \exp(-c_{3.2} n)\right)$, *where $C_{3.2} \geq 1$ and $c_{3.2} > 0$ are constants depending only on z.*

The proof of Proposition 3.1 is relatively simple, and follows from a conditioning argument developed in [15], once we observe the crucial fact (Theorem 2.10) that for any $\boldsymbol{a} \in \Gamma^1(\eta)$,

$$\rho_{\delta,z}(\boldsymbol{a}) \lesssim \gamma^{-1}\sqrt{n}\delta + \exp(-\Omega(n^{1/50}))$$

for all $\delta \geq \eta$.

Proof of Proposition 3.1 following [15, 29]. Since $M_n^\dagger$ and M_n have the same singular values, it follows that a necessary condition for a matrix M_n to satisfy the event in Proposition 3.1 is that there exists a unit row vector $\boldsymbol{a'} = (a'_1, \ldots, a'_n)$ such that $\|\boldsymbol{a'}^T M_n\|_2 \leq \eta$. To every matrix M_n, associate such a vector $\boldsymbol{a'}$ arbitrarily (if one exists) and denote it by $\boldsymbol{a'}_{M_n}$; this leads to a partition of the space of all matrices with least singular value at most η. Then, by taking a union bound, it suffices to show the following.

$$\Pr\left(\exists \boldsymbol{a} \in \Gamma^1(\eta) : \|M_n\boldsymbol{a}\|_2 \leq \eta \bigwedge \|\boldsymbol{a'}_{M_n}\|_\infty = |a'_n|\right) \leq 2C_{2.10}\left(n^{3/2}\eta + \exp(-C_{2.10}^{-1}\sqrt{n})\right). \tag{3}$$

To this end, we expose the first $n-1$ rows $X_1, \ldots, X_{n-1}$ of M_n. Note that if there is some $\boldsymbol{a} \in \Gamma^1(\eta)$ satisfying $\|M_n\boldsymbol{a}\|_2 \leq \eta$, then there must exist a vector $\boldsymbol{y} \in \Gamma^1(\eta)$, depending only on the first $n-1$ rows $X_1, \ldots, X_{n-1}$, such that

$$\left(\sum_{i=1}^{n-1} |X_i \cdot \boldsymbol{y}|^2\right)^{1/2} \leq \eta.$$

In other words, once we expose the first $n-1$ rows of the matrix, either the matrix cannot be extended to one satisfying the event in Proposition 3.1, or there is some unit vector $\boldsymbol{y} \in \Gamma^1(\eta)$, which can be chosen after looking only at the first $n-1$ rows, and which satisfies the equation above. For the rest of the proof, we condition on the first $n-1$ rows $X_1, \ldots, X_{n-1}$ (and hence, a choice of $\boldsymbol{y}$).

For any vector $\boldsymbol{w'} \in \mathbb{S}^{2n-1}$ with $w'_n \neq 0$, we can write

$$X_n = \frac{1}{w'_n}\left(\boldsymbol{u} - \sum_{i=1}^{n-1} w'_i X_i\right),$$

where $\boldsymbol{u} := \boldsymbol{w'}^T M_n$. Thus, restricted to the event $\{s_n(M_n) \leq \eta\} \bigwedge \{\|\boldsymbol{a'}_{M_n}\|_\infty = |a'_n|\}$, we have

$$\begin{aligned}
|X_n \cdot \boldsymbol{y}| &= \inf_{\boldsymbol{w'} \in \mathbb{S}^{2n-1}, w'_n \neq 0} \frac{1}{|w'_n|}\left|\boldsymbol{u} \cdot \boldsymbol{y} - \sum_{i=1}^{n-1} w'_i X_i \cdot \boldsymbol{y}\right| \\
&\leq \frac{1}{|a'_n|}\left(\|\boldsymbol{a'}_{M_n}^T M_n\|_2\|\boldsymbol{y}\|_2 + \|\boldsymbol{a'}_{M_n}\|_2\left(\sum_{i=1}^{n-1}|X_i \cdot \boldsymbol{y}|^2\right)^{1/2}\right) \\
&\leq \eta\sqrt{n}\left(\|\boldsymbol{y}\|_2 + \|\boldsymbol{a'}_{M_n}\|_2\right) \leq 2\eta\sqrt{n},
\end{aligned}$$

where the second line is due to the Cauchy-Schwarz inequality and the particular choice $\boldsymbol{w'} = \boldsymbol{a'}_{M_n}$. It follows that the probability in Equation (3) is bounded by

$$\rho_{2\eta\sqrt{n},z}(\boldsymbol{y}) \leq 2C_{2.10}\left(n^{3/2}\eta + \exp(-C_{2.10}^{-1}n^{1/50})\right),$$

which completes the proof. □

The remainder of this section is devoted to the proof of Proposition 3.2.

3.1 Reduction to Gaussian integer vectors

Let $\mathcal{K} := \{K \subseteq [n] : |K| \geq n - 6n^{0.99}\}$ and

$$\boldsymbol{V} = \{\boldsymbol{v} \in (\mathbb{Z} + i\mathbb{Z})^n \mid \|\Re(\boldsymbol{v})\|_\infty, \|\Im(\boldsymbol{v})\|_\infty \leq 2\eta^{-1}n^{3/4}\}.$$

As a first and crucial step towards the proof of Proposition 3.2, we will prove the following:

Proposition 3.3. *With notation as above,*

$$\begin{aligned}\Pr\left(\exists \boldsymbol{a} \in \Gamma^2(\eta) : \|M_n\boldsymbol{a}\|_2 \leq \eta\right) &\leq C_{3.3}e^{-n^{0.99}/10} + \\ &\Pr(\exists \boldsymbol{w} \in \boldsymbol{V} \text{ and } K \in \mathcal{K} : \|P_K M_n \boldsymbol{w}\|_2 \leq C_{3.3}\min\{n^{0.21}\|\boldsymbol{w}\|_2, n^{0.711}\}),\end{aligned}$$

where $C_{3.3} \geq 1$ is an absolute constant.

Remark 3.4. As we will see shortly, the crucial point in the above proposition is that $n^{0.21} \ll n^{1/2-\epsilon}$ and $n^{0.711} \ll n^{0.75-\epsilon}$.

Proof. Let $\epsilon = 0.01$, $\delta_1 = 0.2$, and $\delta_2 = 0.6$. Let $\mathcal{G}$ denote the event appearing in the conclusion of Proposition 2.13 for (ϵ, δ_1) and (ϵ, δ_2) simultaneously. Since $\Pr(\mathcal{G}^c) \leq 2C_{2.13}(0.01)\exp(-n^{0.99}/8)$, we may restrict ourselves to the event $\mathcal{G}$.

Let $\boldsymbol{a} \in \Gamma^2(\eta)$. Then, by definition, there exists some $\theta \in \mathbb{C}$ with $0 < |\theta| \leq \mathrm{LCD}_{\alpha,\gamma}(\boldsymbol{a}) \leq n^{3/4}\eta^{-1}$ and some $\boldsymbol{w} \in (\mathbb{Z} + i\mathbb{Z})^n \setminus \{\boldsymbol{0}\}$ such that $\|\theta\boldsymbol{a} - \boldsymbol{w}\|_2 \leq \min\{\gamma|\theta|, \alpha\}$. Note also that $\|\theta\boldsymbol{a} - \boldsymbol{w}\|_\infty \leq \min\{\gamma|\theta|, 1\}$. To leverage the control we have over various norms associated to the matrix M_n, we decompose the 'error' vector $\theta\boldsymbol{a} - \boldsymbol{w}$ into a 'small' part (with respect to the ℓ^∞-norm), a 'sparse and small' part, and a 'very sparse' part.

Accordingly, let $\boldsymbol{v}_{\mathrm{sp}} \in \mathbb{C}^n$ denote the vector obtained by keeping the largest (in absolute value) $n^{0.4}$ coordinates of $\theta\boldsymbol{a} - \boldsymbol{w}$, let $\boldsymbol{v}_{\mathrm{ss}}$ denote the vector obtained by keeping the next $n^{0.8} - n^{0.4}$ largest coordinates of $\theta\boldsymbol{a} - \boldsymbol{w}$, and let $\boldsymbol{v}_{\mathrm{sm}} = \theta\boldsymbol{a} - \boldsymbol{w} - \boldsymbol{v}_{\mathrm{sp}} - \boldsymbol{v}_{\mathrm{ss}}$. Then, we have that

$$\|\boldsymbol{v}_{\mathrm{sp}}\|_\infty \leq \min\{\gamma|\theta|, 1\},$$

and

$$\|\boldsymbol{v}_{\mathrm{ss}}\|_\infty \leq \frac{\min\{\gamma|\theta|, \alpha\}}{n^{0.2}}, \|\boldsymbol{v}_{\mathrm{sm}}\|_\infty \leq \frac{\min\{\gamma|\theta|, \alpha\}}{n^{0.4}}. \tag{4}$$

Indeed, the first inequality is immediate from $\|\theta\boldsymbol{a} - \boldsymbol{w}\|_\infty \leq \min\{\gamma|\theta|, 1\}$, whereas the second inequality follows from

$$\max\{n^{0.4}\|\boldsymbol{v}_{\mathrm{ss}}\|_\infty^2, n^{0.8}\|\boldsymbol{v}_{\mathrm{sm}}\|_\infty^2\} \leq \|\theta\boldsymbol{a} - \boldsymbol{w}\|_2^2.$$

Let $J_1 \subseteq [n]$ denote the support of $\boldsymbol{v}_{\mathrm{sp}}$ and let $J_2 \subseteq [n]$ denote the support of $\boldsymbol{v}_{\mathrm{sp}} + \boldsymbol{v}_{\mathrm{ss}}$. By extending these sets if need be, we may assume that $|J_1| = n^{0.4}$ and $|J_2| = n^{0.8}$. Moreover, since we have restricted to $N_n \in \mathcal{G}$, let $I \subseteq [n]$ denote a subset of size at least $n - 2n^{1-\epsilon}$ with respect to which conclusion 1. of Proposition 2.13 holds.

Note that since $\|M\| \leq n^{0.51}$, we have $\|MP_J\|_{\infty\to 2} \leq n^{0.51}\sqrt{|J|}$ for every $J \subseteq [n]$. Therefore,

$$\|P_I M_n\|_{\infty\to 2} \leq \|P_I N_n\|_{\infty\to 2} + \|P_I M_n\|_{\infty\to 2} \lesssim n^{1.01}$$

and similarly,

$$\|P_{I(J_1)} M_n P_{J_1}\|_{\infty\to 2} \lesssim n^{0.71},$$

$$\|P_{I(J_2)}M_nP_{J_2}\|_{\infty\to 2} \lesssim n^{0.91}.$$

Then, from the triangle inequality, we have

$$\begin{aligned}
\|P_{I(J_1)}P_{I(J_2)}P_IM_n(\theta\boldsymbol{a}-\boldsymbol{w})\|_2 &\le \|P_IM_n\boldsymbol{v}_{\mathrm{sm}}\|_2 + \|P_{I(J_2)}M_n\boldsymbol{v}_{\mathrm{ss}}\|_2 + \|P_{I(J_1)}M_n\boldsymbol{v}_{\mathrm{sp}}\|_2 \\
&= \|P_IM_n\boldsymbol{v}_{\mathrm{sm}}\|_2 + \|P_{I(J_2)}M_nP_{J_2}\boldsymbol{v}_{\mathrm{ss}}\|_2 + \|P_{I(J_1)}M_nP_{J_1}\boldsymbol{v}_{\mathrm{sp}}\|_2 \\
\le \|P_IM_n\|_{\infty\to 2}\|\boldsymbol{v}_{\mathrm{sm}}\|_\infty &+ \|P_{I(J_2)}M_nP_{J_2}\|_{\infty\to 2}\|\boldsymbol{v}_{\mathrm{ss}}\|_\infty + \|P_{I(J_1)}M_nP_{J_1}\|_{\infty\to 2}\|\boldsymbol{v}_{\mathrm{sp}}\|_\infty \\
&\lesssim \left(n^{0.61}\min\{\gamma|\theta|,\alpha\} + n^{0.71}\min\{\gamma|\theta|,\alpha\} + n^{0.71}\min\{\gamma|\theta|,1\}\right) \\
&\lesssim \left(\min\{n^{0.21}|\theta|, n^{0.711}\} + \min\{n^{0.21}|\theta|, n^{0.71}\}\right) \\
&\lesssim \min\{n^{0.21}|\theta|, n^{0.711}\},
\end{aligned}$$

where the second line uses that $P_{J_2}\boldsymbol{v}_{\mathrm{ss}} = \boldsymbol{v}_{\mathrm{ss}}$ and $P_{J_1}\boldsymbol{v}_{\mathrm{sp}} = \boldsymbol{v}_{\mathrm{sp}}$; the fourth line uses the above estimates on the ∞-to-2 norms and Equation (4), and the fifth line uses the parameter value $\gamma = n^{-1/2}$.

Thus, if $\|M_n\boldsymbol{a}\|_2 \le \eta$, it follows from the triangle inequality that

$$\begin{aligned}
\|P_{I(J_1)}P_{I(J_2)}P_IM_n\boldsymbol{w}\|_2 &= \|P_{I(J_1)}P_{I(J_2)}P_IM_n(\boldsymbol{w}-\theta\boldsymbol{a}) + P_{I(J_1)}P_{I(J_2)}P_IM_n(\theta\boldsymbol{a})\|_2 \\
&\le \|P_{I(J_1)}P_{I(J_2)}P_IM_n(\theta\boldsymbol{a}-\boldsymbol{w})\|_2 + |\theta|\cdot\|M_n\boldsymbol{a}\|_2 \\
&\lesssim \min\{n^{0.21}|\theta|, n^{0.711}\} + |\theta|\eta \\
&\lesssim \min\{n^{0.21}|\theta|, n^{0.711}\} \\
&\lesssim \min\{n^{0.21}\|\boldsymbol{w}\|_2, n^{0.711}\},
\end{aligned}$$

where the fourth line follows since $\eta \ll n^{0.21}$ and $|\theta|\eta \le n^{0.7} \ll n^{0.711}$, and the last line follows since $\|\boldsymbol{w}\|_2 \ge |\theta|(1-\gamma) \ge |\theta|/2$. Since $|I(J_1)^c \cup I(J_2)^c \cup I^c| \le |I(J_1)^c| + |I(J_2)^c| + |I^c| \le 6n^{0.99}$, we get the desired conclusion. ☐

In view of Proposition 3.3, it suffices to show the following in order to prove Proposition 3.2, and hence, complete the proof of Theorem 1.1.

Proposition 3.5. $\Pr(\exists \boldsymbol{w}\in\boldsymbol{V}$ *and* $K\in\mathcal{K} : \|P_KM_n\boldsymbol{w}\|_2 \le C_{3.3}\min\{n^{0.21}\|\boldsymbol{w}\|_2, n^{0.711}\}) \le C_{3.5}\exp(-c_{3.5}n)$, *where* $C_{3.5}\ge 1$ *and* $c_{3.5} > 0$ *are constants depending only on* z.

The proof of this proposition is the content of the next two subsections.

3.2 Dealing with sparse Gaussian integer vectors

Throughout this subsection and the next one, $p = 2^{n^{0.001}}$ is a prime. Note, in particular, that $p \gg \eta^{-1}n^{3/4}$. The proof of Proposition 3.5 proceeds in two steps. The first step is to show that the probability of the event appearing in Proposition 3.5 is small, provided we restrict ourselves only to sufficiently sparse Gaussian integer vectors. Let

$$\boldsymbol{S} := \{\boldsymbol{w}\in(\mathbb{Z}+i\mathbb{Z})^n\setminus\{\boldsymbol{0}\} \mid \|\Re(\boldsymbol{w})\|_\infty, \|\Im(\boldsymbol{w})\|_\infty \le p, |\mathbf{supp}(\boldsymbol{w})| \le n^{0.99}\}.$$

Lemma 3.6. $\Pr\left(\exists\boldsymbol{w}\in\boldsymbol{S}\right.$ *and* $\left.K\in\mathcal{K} : \|P_KM_n\boldsymbol{w}\|_2 \le C_{3.3}n^{0.21}\|\boldsymbol{w}\|_2\right) \le C_{3.6}\exp(-c_{2.4}n/4)$, *where* $C_{3.6}\ge 1$ *is an absolute constant.*

Proof. By taking the union bound over all the at most $n\binom{n}{6n^{0.99}} \ll \exp(n^{0.991})$ choices of $K\in\mathcal{K}$, it suffices to show that for a fixed $K_0\in\mathcal{K}$,

$$\Pr\left(\exists\boldsymbol{w}\in\boldsymbol{S} : \|P_{K_0}M_n\boldsymbol{w}\|_2 \le C_{3.3}n^{0.21}\|\boldsymbol{w}\|_2\right) \le C\exp(-c_{2.4}n/2)$$

for some absolute constant $C \geq 1$. The number of vectors $\boldsymbol{w} \in \boldsymbol{S}$ is at most

$$\binom{n}{n^{0.99}}(3p^2)^{n^{0.99}} \ll 2^{n^{0.992}}.$$

By Lemma 2.4 applied to the matrix $P_{K_0}M_n$, for any such vector,

$$\Pr\left(\|P_{K_0}M_n\boldsymbol{w}\|_2 \leq c_{2.4}\sqrt{n}\|\boldsymbol{w}\|_2/2\right) \leq \exp(-c_{2.4}n).$$

Therefore, the union bound gives the desired conclusion. □

3.3 Dealing with non-sparse Gaussian integer vectors

It remains to deal with Gaussian integer vectors with support of size at least $n^{0.99}$. Let

$$\boldsymbol{W} := \left\{\boldsymbol{w} \in (\mathbb{Z}+i\mathbb{Z})^n \setminus \{\boldsymbol{0}\} \mid \|\Re(\boldsymbol{w})\|_\infty, \|\Im(\boldsymbol{w})\|_\infty \leq \eta^{-4}, |\mathbf{supp}(\boldsymbol{w})| \geq n^{0.99}\right\}.$$

Note that for our choice of parameters, the natural map

$$\varphi_p : \boldsymbol{W} \to (\mathbb{F}_p + i\mathbb{F}_p)^n$$

is injective.

In view of Lemma 3.6, since $\eta \leq n^{-2}$, and taking the union bound over all the at most $n\binom{n}{6n^{0.99}} \ll \exp(n^{0.991})$ choices of $K \in \mathcal{K}$, the following proposition suffices to prove Proposition 3.5.

Proposition 3.7. *For all $K_0 \in \mathcal{K}$,*

$$\Pr\left(\exists \boldsymbol{w} \in \boldsymbol{W} : \|P_{K_0}M_n\boldsymbol{w}\|_2 \leq C_{3.3}n^{0.711}\right) \leq C_{3.7}\exp(-c_{3.7}n),$$

where $C_{3.7} \geq 1$ and $c_{3.7} > 0$ are constants depending only on z.

The proof of Proposition 3.7 is accomplished by a simple union bound. To execute this, we need the following preliminary claims.

Claim 3.8. *For all $\boldsymbol{w} \in \boldsymbol{W}$, $\rho_{1,z}(\boldsymbol{w}) \geq n^{-1/2}\eta^4/10$.*

Proof. The random variable $\sum_{j=1}^n w_j\xi_j$ has mean 0 and variance at most $n\eta^{-8}$. Therefore, by Markov's inequality,

$$\Pr\left(\left|\sum_{j=1}^n w_j\xi_j\right| \leq 2\sqrt{n}\eta^{-4}\right) \geq \frac{3}{4}.$$

Hence, by the pigeonhole principle, it follows that

$$\rho_{1,\xi}(\boldsymbol{w}) \geq n^{-1/2}\eta^4/10,$$

as desired. □

For the next claim, let

$$\boldsymbol{W}_t := \{\boldsymbol{w} \in \boldsymbol{W} : \rho_{1,\xi}(\boldsymbol{w}) \in [t, 2t)\}.$$

Note that the previous claim along with Lemma 2.8 shows that $\boldsymbol{W}_t$ is nonempty only if $n^{-1/2}\eta^4/10 \leq t \leq C_{2.8}n^{-0.495}$.

Claim 3.9. *For all* $n^{-1/2}\eta^4/10 \le t \le C_{2.8}n^{-0.495}$,

$$|\boldsymbol{W}_t| \le C_{3.9}\left(\frac{C_{2.11}t^{-1}}{n^{0.45}}\right)^n,$$

where $C_{3.9} \ge 1$ *is a constant depending only on* $C_{2.11}, C_{2.8}$.

Proof. Fix $s = n^{0.997}$ and $k = n^{0.097}$. Then, $1 \ll k \le \sqrt{s} \le s \le n/\log n$, $n^{-1/2}\eta^4 \gg \max\{e^{-s/k}, s^{-k/4}\}$, and $2^{n/s} \ge p \gg n^{1/2}\eta^{-4}$. Hence, for large enough n, the hypotheses of Theorem 2.11 are satisfied, so that

$$\begin{aligned}
|\boldsymbol{W}_t| &= |\varphi_p(\boldsymbol{W}_t)| \\
&\le |\varphi_p(\boldsymbol{V}_t)| \\
&\le \left(\frac{5np^2}{s}\right)^s + \left(\frac{C_{2.11}t^{-1}}{n^{0.45}}\right)^n \\
&\le 2\left(\frac{C_{2.11}t^{-1}}{n^{0.45}}\right)^n,
\end{aligned}$$

where the first line follows from the injectivity of φ_p on $\boldsymbol{W}$, the third line follows from Theorem 2.11, and the last line follows since $t^{-1} \gg n^{0.49}$. □

We now have all the ingredients to prove Proposition 3.7.

Proof of Proposition 3.7. Let D_x denote the unit polydisc in $\mathbb{C}^n$ centered at x. For all n sufficiently large, we have

$$\begin{aligned}
\Pr\left(\exists \boldsymbol{w} \in \boldsymbol{W} : \|P_{K_0}M_n\boldsymbol{w}\|_2 \le C_{3.3}n^{0.711}\right) &\le \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} \Pr\left(\exists \boldsymbol{w} \in \boldsymbol{W}_t : \|P_{K_0}M_n\boldsymbol{w}\|_2 \le C_{3.3}n^{0.711}\right) \\
&\lesssim \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} \sum_{x \in B(0,n^{0.712})\cap(\mathbb{Z}+i\mathbb{Z})^n} \Pr\left(\exists \boldsymbol{w} \in \boldsymbol{W}_t : P_{K_0}M_n\boldsymbol{w} \in D_x\right) \\
&\le \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} (400n^{0.212})^{2n} \sup_{x\in(\mathbb{Z}+i\mathbb{Z})^n} \Pr\left(\exists \boldsymbol{w} \in \boldsymbol{W}_t : P_{K_0}M_n\boldsymbol{w} \in D_{\boldsymbol{x}}\right) \\
&\le \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} (16000n^{0.424})^n|\boldsymbol{W}_t|(2t)^{|K_0|} \\
&\lesssim \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} (16000n^{0.424})^n\left(\frac{C_{2.11}t^{-1}}{n^{0.45}}\right)^n \cdot (2t)^{n-6n^{0.99}} \\
&\lesssim \sum_{t=0.1n^{-1/2}\eta^4}^{n^{-0.494}} (32000C_{2.11}n^{-0.02})^n \cdot t^{-6n^{0.99}} \\
&\lesssim n \cdot (32000C_{2.11}n^{-0.02})^n \cdot \eta^{-30n^{0.99}} \\
&\lesssim n \cdot (32000C_{2.11}n^{-0.02})^n \cdot 2^{30n^{0.991}} \\
&\le C_{3.7}\exp(-c_{3.7}n),
\end{aligned}$$

where the third line follows since the number of points of $(\mathbb{Z}+i\mathbb{Z})^n$ in $B(0,n^{0.712})$ is at most $(400n^{0.212})^{2n}$, the fifth line follows from Claim 3.9, and the seventh and eighth lines follow from the assumed bounds on η. □

4 Proof of Theorem 2.11

We begin with the following definition from [24] which will appear in our upper bound on the Lévy concentration function.

Definition 4.1. Let z be an arbitrary complex random variable. For any $w \in \mathbb{C}$, we define

$$\|w\|_z^2 := \mathbb{E}\|\Re\{w(z_1 - z_2)\}\|_{\mathbb{R}/\mathbb{Z}}^2,$$

where z_1, z_2 denote i.i.d. copies of z and $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ denotes the distance to the nearest integer.

Note that $\|\cdot\|_z$ is not a norm in the strict sense, since it does not satisfy homogeneity. However, it does satisfy the triangle inequality, and it is invariant under negation (see Lemma 5.3 in [24]), which will be sufficient for us.

The next proposition, which provides a 'Fourier-bound' on the Lévy concentration function, appears in [24] and will be the starting point of the proof of Theorem 2.11.

Proposition 4.2 (Lemma 5.2 in [24])**.** *Let $\boldsymbol{v} := (v_1, \dots, v_n) \in \mathbb{C}^n$ and let z be an arbitrary complex random variable. Then,*

$$\rho_{r,z}(\boldsymbol{v}) \le e^{\pi r^2} P_z(\boldsymbol{v}) \le e^{\pi r^2} \int_{\mathbb{C}} \exp\left(-\sum_{i=1}^{n} \|v_i\xi\|_z^2/2 - \pi|\xi|^2\right) d\xi.$$

Here,

$$P_z(\boldsymbol{v}) := \mathbb{E}_{x_1,\dots,x_n} \exp(-\pi|v_1x_1 + \cdots + v_nx_n|^2),$$

where $x_1, \dots, x_n$ are i.i.d. copies of $(z_1 - z_2)\cdot\mathrm{Ber}(1/2)$, with z_1, z_2 distributed as z, and $\mathrm{Ber}(1/2), z_1, z_2$ mutually independent.

We now proceed to the proof of Theorem 2.11, which consists of six steps. The first three steps are modelled after the proof of the optimal inverse Littlewood-Offord theorem of Nguyen and Vu [17], whereas the last three steps are modelled after Halász's proof of his anti-concentration inequality [12].

Step 1: Extracting a large sublevel set. For each integer $1 \le m \le M$, where $M := 2s/k$, we define

$$S_m := \left\{\xi \in \mathbb{C} : \sum_{i=1}^{n} \|v_i\xi\|_z^2 + |\xi|^2 \le m\right\}.$$

Since

$$\int_{\mathbb{C}} \exp\left(-\sum_{i=1}^{n} \|v_i\xi\|_z^2/2 - \pi|\xi|^2\right) d\xi \lesssim \sum_{1 \le m \le M} \mu(S_m)\exp(-m/2) + \exp(-M/2),$$

it follows from Proposition 4.2 that

$$\rho_{1,z}(\boldsymbol{v}) \lesssim \sum_{1 \le m \le M} \mu(S_m)\exp(-m/2) + \exp(-M/2).$$

In particular, since it is assumed that $\rho_{1,z}(\boldsymbol{v}) \ge C_{2.11}\exp(-s/k) = C_{2.11}\exp(-M/2)$, it follows that for sufficiently large $C_{2.11} \ge 1$,

$$\rho_{1,z}(\boldsymbol{v}) \lesssim \sum_{1 \le m \le M} \mu(S_m)\exp(-m/2)$$

$$= \sum_{1 \le m \le M} \mu(S_m) \exp(-m/4) \exp(-m/4)$$
$$\lesssim \sum_{1 \le m \le M} \mu(S_m) \exp(-m/4) c_m,$$

where
$$c_m := \frac{e^{-m/4}}{\sum_{m=1}^{M} e^{-m/4}}.$$

Note that in the last line, we have used the fact that $\sum_{m=1}^{\infty} e^{-m/4} = O(1)$. Therefore, by averaging with respect to the probability measure $\{c_m\}_{m=1}^{M}$, it follows that there must exist some non-zero integer $m_0 \in [1, M]$ for which
$$\mu(S_{m_0}) \gtrsim \rho_{1,z}(\boldsymbol{v}) \exp(m_0/4).$$

Step 2: Eliminating the z-norm. From here on, all implicit constants will be allowed to depend on C_z. Since $S_{m_0} \subset B(0, \sqrt{m_0})$, it follows (by averaging) that there must exist some $B(x, 1/16C_z) \subset B(0, \sqrt{m_0})$ for which
$$\mu(S_{m_0} \cap B(x, 1/16C_z)) \gtrsim \rho \exp(m_0/4) m_0^{-1} \gtrsim \rho \exp(m_0/8).$$

Moreover, for $\xi_1, \xi_2 \in B(x, 1/16C_z) \cap S_{m_0}$, we have that

- $\xi_1 - \xi_2 \in B(0, 1/8C_z)$, and
- $\sum_{i=1}^{n} \|v_i(\xi_1 - \xi_2)\|_z^2 \le \sum_{i=1}^{n} (\|v_i\xi_1\|_z + \|v_i\xi_2\|_z)^2 \le 2\sum_{i=1}^{n} \left(\|v_i\xi_1\|_z^2 + \|v_i\xi_2\|_z^2\right) \le 4m_0$.

Since for any $A \subseteq \mathbb{C}$, $\mu(A - A) \ge \mu(A)$, it follows that setting
$$T_{m_0} := \left\{\xi \in B(0, 1/8C_z) : \sum_{i=1}^{n} \|v_i\xi\|_z^2 \le 4m_0\right\},$$

we have that
$$\mu(T_{m_0}) \gtrsim \rho \exp(m_0/8).$$

Next, let $y := z_1 - z_2$, where z_1, z_2 are i.i.d. copies of z. Since
$$\mathbb{E}_y \int_{\mathbb{C}} \sum_{i=1}^{n} \|\Re\{v_i y \xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \mathbf{1}_{T_{m_0}}(\xi) d\xi \le 4m_0 \mu(T_{m_0}),$$

it follows that there exists some $y_0 \in \mathbb{C}$ satisfying $C_z^{-1} \le |y_0| \le C_z$ such that
$$\int_{\mathbb{C}} \sum_{i=1}^{n} \|\Re\{v_i y_0 \xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \mathbf{1}_{T_{m_0}}(\xi) d\xi \le 4m_0 \mu(T_{m_0}) \Pr\left(C_z^{-1} \le |y| \le C_z\right)^{-1} \le 4C_z m_0 \mu(T_{m_0}),$$

where the final inequality follows from the C_z-goodness of z. Hence, by Markov's inequality,
$$\mu\left(\left\{\xi \in T_{m_0} : \sum_{i=1}^{n} \|\Re\{v_i y_0 \xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \le 8C_z m_0\right\}\right) \ge \frac{\mu(T_{m_0})}{2} \gtrsim \rho \exp(m_0/8).$$

Since $T_{m_0} \subset B(0, 1/8C_z)$, this shows that
$$\mu\left(\left\{\xi \in B(0, 1/8C_z) : \sum_{i=1}^{n} \|\Re\{v_i y_0 \xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \le 8C_z m_0\right\}\right) \gtrsim \rho \exp(m_0/8).$$

Finally, after replacing ξ by $y_0\xi$, and noting that the change of measure factor lies in $[C_z^{-1}, C_z]$, it follows that

$$T'_{m_0} := \left\{ \xi \in B(0, 1/8) : \sum_{i=1}^{n} \|\Re\{v_i\xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq 8C_z m_0 \right\}$$

satisfies

$$\mu(T'_{m_0}) \gtrsim \rho \exp(m_0/8).$$

Step 3: Discretization of ξ. For p a prime as in the statement of the theorem, let

$$B_0 := \left\{ \frac{r_1}{p} + i\frac{r_2}{p} : r_1, r_2 \in \mathbb{Z}, -\frac{p}{8} \leq r_1, r_2 \leq \frac{p}{8} \right\},$$

and consider the random set $x + B_0$, where $x \in [0, 1/p] + i[0, 1/p]$ is a uniformly distributed random point. Then, by linearity of expectation, we have

$$\mathbb{E}_{x \in [0,1/p]+i[0,1/p]} \left[\left| (x + B_0) \cap T'_{m_0} \right| \right] \gtrsim \mu(T'_{m_0}) p^2,$$

so there exists some $x_0 \in [0, 1/p] + i[0, 1/p]$ for which

$$|(x_0 + B_0) \cap T'_{m_0}| \gtrsim \mu(T'_{m_0}) p^2 \gtrsim \rho \exp(m_0/8) p^2.$$

Let us now 'recenter' this shifted lattice. Note that for a fixed $\xi_0 \in (x_0 + B_0) \cap T'_{m_0}$, we have for any $\xi \in (x_0 + B_0) \cap T'_{m_0}$ that

$$\sum_{i=1}^{n} \|\Re\{v_i(\xi - \xi_0)\}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq 2 \sum_{i=1}^{n} \left(\|\Re\{v_i\xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 + \|\Re\{v_i\xi_0\}\|_{\mathbb{R}/\mathbb{Z}}^2 \right) \leq 32C_z m_0.$$

Note also that $\xi_0 - \xi \in B_1 := B_0 - B_0 = \{(r_1/p) + i(r_2/p) : r_1, r_2 \in \mathbb{Z}, -p/4 \leq r_1, r_2 \leq p/4\}$. Hence, for a fixed $\xi_0 \in (x_0 + B_0) \cap T'_{m_0}$, setting

$$P_{m_0} := \left\{ \xi_0 - \xi : \xi \in (x_0 + B_0) \cap T'_{m_0} \right\}$$

gives a subset $P_{m_0} \subset B_1$ such that

$$|P_{m_0}| \gtrsim \rho \exp(m_0/8) p^2,$$

and for all $\xi \in P_{m_0}$,

$$\sum_{i=1}^{n} \|\Re\{v_i\xi\}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq 32C_z m_0.$$

Step 4: Embedding P_{m_0} into $\mathbb{F}_p$ and the Halász trick. Let $V := \mathbf{supp}(\varphi_p(\boldsymbol{v}))$. If $|V| < s$, we proceed directly to Step 6. Otherwise, for $I \subseteq V$ such that $|I| \geq s$, we define the sets

$$P'_m(I) := \left\{ r := r_1 + ir_2 \in \mathbb{F}_p + i\mathbb{F}_p : \sum_{i \in I} \left\| \frac{\Re\{v_i r\}}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \leq 32C_z m \right\},$$

Note that since $v_i \in \mathbb{Z} + i\mathbb{Z}$, the map

$$r \mapsto \left\| \frac{\Re\{v_i r\}}{p} \right\|_{\mathbb{R}/\mathbb{Z}}$$

is indeed well-defined as a map from $\mathbb{F}_p + i\mathbb{F}_p$ to $[0,1]$. Note also that, since $P_{m_0} \subset B_1$, the size of $P'_{m_0}(I)$ (as a subset of $\mathbb{F}_p + i\mathbb{F}_p$) is atleast the size of P_{m_0} (as a subset of $\frac{1}{p} \cdot (\mathbb{Z} + i\mathbb{Z})$) i.e. the way we have defined various objects ensures that there are no wrap-around issues. We claim that for all integers $t \geq 1$,

$$tP'_m(I) \subseteq P'_{t^2m}(I). \tag{5}$$

Indeed, for $r_1, \ldots, r_t \in P'_m(I) \subseteq \mathbb{F}_p + i\mathbb{F}_p$, we have

$$\begin{aligned}
\sum_{i\in I} \left\| \Re\left\{ v_i \frac{(r_1 + \cdots + r_t)}{p} \right\} \right\|_{\mathbb{R}/\mathbb{Z}}^2 &= \sum_{i\in I} \left\| \frac{\Re\{v_i r_1\}}{p} + \cdots + \frac{\Re\{v_i r_t\}}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \\
&\leq \sum_{i\in I} \left(\sum_{j=1}^{t} \left\| \frac{\Re\{v_i r_j\}}{p} \right\|_{\mathbb{R}/\mathbb{Z}} \right)^2 \\
&\leq \sum_{i\in I} t \sum_{j=1}^{t} \left\| \frac{\Re\{v_i r_j\}}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \\
&\leq t \sum_{j=1}^{t} \sum_{i\in I} \|\Re\{v_i r_j/p\}\|_{\mathbb{R}/\mathbb{Z}}^2 \\
&\leq 32C_z t^2 m,
\end{aligned}$$

which gives the desired inclusion.

We now use the Cauchy-Davenport theorem for $\mathbb{F}_p + i\mathbb{F}_p \simeq \mathbb{F}_p^2$ (see, e.g., [6]), which states that every pair of nonempty $A, B \subseteq \mathbb{F}_p + i\mathbb{F}_p$ satisfies

$$|A + B| \geq \min\{p^2, |A| + |B| - p\}.$$

It follows that for all integers $t \geq 1$,

$$|tP'_m(I)| \geq \min\{p^2, t|P'_m(I)| - tp\}.$$

Hence, by Equation (5), we have

$$|P'_{t^2m}(I)| \geq \min\{p^2, t|P'_m(I)| - tp\}. \tag{6}$$

We also claim that $|P'_m(I)| < p^2$ as long as $m \leq |I|/500C_z$. Indeed, since the map $\mathbb{F}_p + i\mathbb{F}_p \ni r(= r_1 + ir_2) \mapsto \Re\{ar\} = a_1r_1 - a_2r_2 \in \mathbb{F}_p$ is a p-to-1 surjection for every non-zero $a := a_1 + ia_2 \in \mathbb{F}_p + i\mathbb{F}_p$, we have

$$\begin{aligned}
\sum_{r\in\mathbb{F}_p+i\mathbb{F}_p} \sum_{i\in I} \|\Re\{v_i r\}/p\|_{\mathbb{R}/\mathbb{Z}}^2 &= |I|p \sum_{r\in\mathbb{F}_p} \|r/p\|_{\mathbb{R}/\mathbb{Z}}^2 \\
&\geq |I|p \cdot \sum_{r'=1}^{(p-1)/2} (r'/p)^2 \\
&> \frac{|I| \cdot p^2}{15}.
\end{aligned}$$

On the other hand, from the definition of $P'_m(I)$,

$$\sum_{r\in\mathbb{F}_p+i\mathbb{F}_p} \sum_{i\in I} \|\Re\{v_i r\}/p\|_{\mathbb{R}/\mathbb{Z}}^2 \leq |P'_m(I)| \cdot 32C_z m + \left(p^2 - |P'_m(I)|\right) \cdot |I|.$$

Comparing these two bounds proves the claim. Combining this claim with Equation (6) along with the assumption that $k \geq 1000C_z$ shows that

$$\begin{aligned}|P'_M(I)| &\gtrsim \sqrt{\frac{M}{m_0}}\left(|P'_{m_0}(I)| - p\right) \\ &\gtrsim \sqrt{\frac{M}{m_0}}|P'_{m_0}(I)| \\ &\gtrsim \sqrt{\frac{M}{m_0}}\rho\exp(m_0/8)p^2 \\ &\gtrsim \sqrt{M}\rho\exp(m_0/16)p^2,\end{aligned}$$

where the second line follows since $|P'_{m_0}(I)| \geq |P'_{m_0}| \gtrsim \rho p^2 \geq C_{2.11}p$ by assumption.

Remark 4.3. Whereas we have related the size of $P'_m(I)$ to the size of $P'_{t^2m}(I)$, [17] uses a similar computation to deduce information about the size of iterated sumsets of $\{v_1, \dots, v_n\}$. This information is then combined with Freiman-type inverse theorems to provide structural information about $\{v_1, \dots, v_n\}$. Thus, we see that by 'dualizing' the argument in [17], one is able to bypass the need for Freiman-type theorems, as far as the counting variant of the inverse Littlewood-Offord problem is concerned.

Step 5: Passing to $R_k(\boldsymbol{v})$. Since $\cos(2\pi x) \geq 1 - 20\|x\|^2_{\mathbb{R}/\mathbb{Z}}$ for all $x \in \mathbb{R}$, it follows that

$$P'_M(I) \subseteq P''_M(I) := \left\{r \in \mathbb{F}_p + i\mathbb{F}_p : \sum_{i\in I}\cos(2\pi\Re\{v_i r\}/p) \geq |I| - 2000C_z M\right\}.$$

By considering the random variable $r \ni \mathbb{F}_p + i\mathbb{F}_p \mapsto \sum_{i\in I}\cos(2\pi\Re\{v_i r\}/p)$, we have for any $k \in \mathbb{N}$ that

$$\begin{aligned}|P''_M(I)|(|I| - 2000C_z M)^{2k} &\leq \sum_{r\in\mathbb{F}_p+i\mathbb{F}_p}\left|\sum_{j\in I}\cos(2\pi\Re\{v_j r\}/p)\right|^{2k} \\ &= \frac{1}{2^{2k}}\sum_{r\in\mathbb{F}_p+i\mathbb{F}_p}\left(\sum_{j\in I}e^{2\pi i\Re\{v_j r\}/p} + e^{-2\pi i\Re\{v_j r\}/p}\right)^{2k} \\ &= \frac{1}{2^{2k}}\sum_{r\in\mathbb{F}_p+i\mathbb{F}_p}\sum_{\epsilon_1,\dots,\epsilon_{2k}\in\{\pm1\}}\sum_{j_1,\dots,j_{2k}\in I}e^{2\pi i\Re\{(\epsilon_1 v_{j_1}+\dots+\epsilon_{2k}v_{j_{2k}})r\}/p} \\ &= \frac{1}{2^{2k}}\sum_{r_1\in\mathbb{F}_p}\sum_{r_2\in\mathbb{F}_p}\sum_{\epsilon_1,\dots,\epsilon_{2k}\in\{\pm1\}}\sum_{j_1,\dots,j_{2k}\in I}e^{2\pi i(\epsilon_1\Re\{v_{j_1}\}+\dots+\epsilon_{2k}\Re\{v_{j_{2k}}\})r_1/p}e^{-2\pi i(\epsilon_1\Im\{v_{j_1}\}+\dots+\epsilon_{2k}\Im\{v_{j_{2k}}\})r_2/p} \\ &= \frac{1}{2^{2k}}\sum_{\epsilon_1,\dots,\epsilon_{2k}\in\{\pm1\}}\sum_{j_1,\dots,j_{2k}\in I}p^2\cdot\delta_0(\epsilon_1\Re\{v_{j_1}\}+\dots+\epsilon_{2k}\Re\{v_{j_{2k}}\})\cdot\delta_0(\epsilon_1\Im\{v_{j_1}\}+\dots+\epsilon_{2k}\Im\{v_{j_{2k}}\}) \\ &= \frac{1}{2^{2k}}\sum_{\epsilon_1,\dots,\epsilon_{2k}\in\{\pm1\}}\sum_{j_1,\dots,j_{2k}\in I}p^2\cdot\delta_0(\epsilon_1 v_{j_1}+\dots+\epsilon_{2k}v_{j_{2k}}),\end{aligned} \tag{7}$$

where the second last line follows again using the integrality of $\Re\{v_1\}, \Im\{v_1\} \dots, \Re\{v_n\}, \Im\{v_n\}$.

From here on, we will use a slight modification of the results of [9] to finish the proof. We begin with the following key definition.

Definition 4.4. Suppose that $\boldsymbol{v} \in (\mathbb{F}_p + i\mathbb{F}_p)^n$ for an integer n and a prime p, and let $k \in \mathbb{N}$. For every $\alpha \in [-1, 1]$, we define $R_k^\alpha(\boldsymbol{v})$ to be the number of solutions to

$$\pm v_{i_1} \pm \cdots \pm v_{i_{2k}} = 0$$

that satisfy $|\{i_1, \ldots, i_{2k}\}| \geq (1+\alpha)k$.

The following elementary lemma from [9] shows that for 'small' positive α, $R_k^\alpha(\boldsymbol{v})$ is not much smaller than $R_k^{-1}(\boldsymbol{v})$.

Lemma 4.5 (Lemma 1.6 in [9])**.** *For all integers k, n with $k \leq n/2$, any prime p, vector $\boldsymbol{v} \in (\mathbb{F}_p + i\mathbb{F}_p)^n$, and $\alpha \in [0, 1]$,*

$$R_k^{-1}(\boldsymbol{v}) \leq R_k^\alpha(\boldsymbol{v}) + (40k^{1-\alpha}n^{1+\alpha})^k.$$

Proof. By definition, $R_k^{-1}(\boldsymbol{v})$ is equal to $R_k^\alpha(\boldsymbol{v})$ plus the number of solutions to $\pm v_{i_1} \pm v_{i_2} \cdots \pm v_{i_{2k}} = 0$ that satisfy $|\{i_1, \ldots, i_{2k}\}| < (1+\alpha)k$. The latter quantity is bounded from above by the number of sequences $(i_1, \ldots, i_{2k}) \in [n]^{2k}$ with at most $(1+\alpha)k$ distinct entries times 2^{2k}, the number of choices for the $\pm$ signs. Thus

$$R_k^{-1}(\boldsymbol{v}) \leq R_k^\alpha(\boldsymbol{v}) + \binom{n}{(1+\alpha)k}\big((1+\alpha)k\big)^{2k} 2^{2k} \leq R_k^\alpha(\boldsymbol{v}) + \left(4e^{1+\alpha}k^{1-\alpha}n^{1+\alpha}\right)^k,$$

where the final inequality follows from the well-known bound $\binom{a}{b} \leq (ea/b)^b$. Finally, noting that $4e^{1+\alpha} \leq 4e^2 \leq 40$ completes the proof. $\square$

Let $\boldsymbol{v}_I$ denote the $|I|$-dimensional vector obtained by restricting $\boldsymbol{v}$ to the coordinates corresponding to I. Recognizing the right hand side of Equation (7) as

$$\frac{p^2 R_k^{-1}(\boldsymbol{v}_I)}{2^{2k}},$$

it follows from Equation (7) and the above lemma that for any $k \leq \sqrt{|I|}$ and $\alpha \in [0, 1/8]$,

$$\begin{aligned}
R_k^\alpha(\boldsymbol{v}_I) &\gtrsim (|I| - 2000C_zM)^{2k} 2^{2k} \rho\sqrt{M} - (40k^{1-\alpha}|I|^{1+\alpha})^k \\
&\gtrsim |I|^{2k} 2^{2k} \rho\sqrt{M} - (40k^{1-\alpha}|I|^{1+\alpha})^k \\
&\gtrsim |I|^{2k} 2^{2k} \rho\sqrt{M} - (40|I|^{(3/2)+\alpha})^k \\
&\gtrsim |I|^{(3/2)k}\left(2^{2k}\sqrt{|I|}^k \rho\sqrt{M} - (40)^k|I|^{\alpha k}\right) \\
&\gtrsim |I|^{(3/2)k}\left(2^{2k}\sqrt{|I|}^k \rho\sqrt{M}\right) \\
&\gtrsim |I|^{2k} 2^{2k} \rho\sqrt{M},
\end{aligned}$$

where the second line follows from the assumption that $Mk \leq 2s \leq 2|I|$, the third line follows from the assumption that $k \leq \sqrt{s} \leq \sqrt{|I|}$, and the fifth line follows from the assumption that $\rho > s^{-k/4} \geq s^{-(k/2)+2\alpha k} \geq |I|^{-(k/2)+2\alpha k}$.

Step 6: Applying the counting lemma. Let us summarize where we stand. We have proved that for any complex random variable z satisfying Equation (2), there exists an absolute constant $C := C(C_z) \geq 1$ for which the following holds. If $\boldsymbol{v} \in (\mathbb{Z} + i\mathbb{Z})^n$ satisfies $\rho_{1,z}(\boldsymbol{v}) := \rho \geq C_{2.11} \max\{e^{-s/k}, s^{-k/4}\}$ for some $1000C_z \leq k \leq \sqrt{s} \leq s \leq n/\log n$ and sufficiently large $C_{2.11}$, and if $\alpha \in [0, 1/8]$, then either

1. $|V| < s$ (where $V := \mathbf{supp}(\varphi_p(\boldsymbol{v}))$), or
2. for all $I \subseteq V$ with $|I| \geq s$,

$$R_k^{\alpha}(\boldsymbol{v}_I) \geq \frac{|I|^{2k} 2^{2k} \rho \sqrt{M}}{C}.$$

Hence, it follows that

$$\varphi_p\left(\boldsymbol{V}_\rho\right) \subseteq \boldsymbol{X}_s + \bigcup_{m=s}^{n} \boldsymbol{Y}_{k,s,\rho}^{\alpha}(m), \tag{8}$$

where

$$\boldsymbol{X}_s := \left\{\boldsymbol{a} \in (\mathbb{F}_p + i\mathbb{F}_p)^n : |\mathbf{supp}(\boldsymbol{a})| < s\right\},$$

and

$$\boldsymbol{Y}_{k,s,\rho}^{\alpha}(m) := \left\{\boldsymbol{a} \in (\mathbb{F}_p + i\mathbb{F}_p)^n : |\mathbf{supp}(\boldsymbol{a})| = m \text{ and } R_k^{\alpha}(\boldsymbol{a}_I) \geq \frac{2^{2k}|I|^{2k}\rho\sqrt{M}}{C} \forall I \subseteq \mathbf{supp}(\boldsymbol{a}) \text{ with } |I| \geq s\right\}.$$

We will bound the size of each of these pieces separately. For $|\boldsymbol{X}_s|$, the following simple bound suffices:

$$|\boldsymbol{X}_s| \leq \sum_{\ell=0}^{s-1}\binom{n}{\ell}(p^2)^{\ell} \leq s\binom{n}{s}p^{2s} \leq s\left(\frac{enp^2}{s}\right)^s \leq \left(\frac{5np^2}{s}\right)^s. \tag{9}$$

On the other hand, the desired bound on $\boldsymbol{Y}_{k,s,\rho}^{\alpha}(m)$ follows easily from a slight modification of the work in [9].

Theorem 4.6. *Let p be a prime, let $k, n \in \mathbb{N}$, $s \in [n]$, $t \in [p]$, and let $\alpha \in (0,1)$. Denoting*

$$\boldsymbol{B}_{k,s,\geq t}^{\alpha}(n) := \left\{\boldsymbol{v} \in (\mathbb{F}_p + i\mathbb{F}_p)^n : R_k^{\alpha}(\boldsymbol{v}_I) \geq t \cdot \frac{2^{2k}\cdot|I|^{2k}}{p} \text{ for every } I \subseteq [n] \text{ with } |I| \geq s\right\},$$

we have

$$|\boldsymbol{B}_{k,s,\geq t}^{\alpha}(n)| \leq (\alpha t)^{s-n} p^{n+s}.$$

The proof of this theorem follows easily from a slight modification of the proof of Theorem 1.7 in [9]. For the reader's convenience, we provide complete details in Appendix B.

Corollary 4.7. *For our choice of parameters, $|\boldsymbol{Y}_{k,s,\rho}^{\alpha}(m)| \leq \left(\frac{16C}{\rho\sqrt{M}}\right)^n$.*

Proof. After paying an overall factor of $\binom{n}{m}$, it suffices to count only those $\boldsymbol{a} \in \boldsymbol{Y}_{k,s,\rho}^{\alpha}(m)$ for which $\mathbf{supp}(\boldsymbol{a}) = [m]$. The key point is that, by definition, for any such $\boldsymbol{a}$, we have

$$\boldsymbol{a}|_{[m]} \in \boldsymbol{B}_{k,s,\geq t}^{\alpha}(m),$$

for $t = \lfloor p\rho\sqrt{M}/C \rfloor$. Therefore, by Theorem 4.6, it easily follows that

$$\begin{aligned}
|\boldsymbol{Y}_{k,s,\rho}^{\alpha}(m)| &\leq \binom{n}{m}(\alpha t p)^s \left(\frac{p}{t}\right)^m \\
&\leq 2^n (tp)^s \left(\frac{p}{t}\right)^n \\
&\leq 2^n \left(p^2\sqrt{M}\right)^s \left(\frac{2Cp}{p\rho\sqrt{M}}\right)^n
\end{aligned}$$

$$\leq (p^2\sqrt{M})^s \left(\frac{4C}{\rho\sqrt{M}}\right)^n$$
$$\leq \left(\frac{16C}{\rho\sqrt{M}}\right)^n,$$

as desired. $\square$

From Equations (8) and (9) and Corollary 4.7, and noting that $M = 2s/k$, it follows that

$$|\varphi_p(\boldsymbol{V}_\rho)| \leq \left(\frac{5np^2}{s}\right)^s + n \cdot \left(\frac{16C\rho^{-1}}{\sqrt{s/k}}\right)^n$$
$$\leq \left(\frac{5np^2}{s}\right)^s + \left(\frac{32C\rho^{-1}}{\sqrt{s/k}}\right)^n$$
$$\leq \left(\frac{5np^2}{s}\right)^s + \left(\frac{C_{2.11}\rho^{-1}}{\sqrt{s/k}}\right)^n,$$

where the final inequality follows since we can take $C_{2.11}$ larger than $32C$. This completes the proof of Theorem 2.11.

5 Proof of Proposition 2.13

The proof will make use of the subgaussian concentration inequality, which we now recall.

Definition 5.1. A random variable X is said to be C-subgaussian if, for all $t > 0$,

$$\Pr(|X| > t) \leq 4\exp\left(-\frac{t^2}{C^2}\right).$$

Lemma 5.2 (see, e.g., Corollary 5.17 in [30])**.** *There exists an absolute constant $C_{5.2} > 0$ with the following property. Let $X_1, \dots, X_n$ be independent centered $\tilde{C}_\xi$-subgaussian random variables. Then,*

$$\Pr\left(\sum_{i=1}^n |X_i|^2 \geq C_{5.2}\tilde{C}_\xi^2 n\right) \leq \exp(-2n).$$

We begin with a simple lemma showing that, with high probability, most rows of a random matrix with i.i.d. centered entries of finite variance have small ℓ_1 and ℓ_2 norms.

Lemma 5.3. *Let $A := (a_{ij})$ be an $n \times m$ complex random matrix with i.i.d. entries, each with mean 0 and variance 1. For $\epsilon \in (0, 1/2)$, let $I \subseteq [n]$ denote the (random) subset of coordinates such that for each $i \in I$,*

$$\left(\sum_{j=1}^m |a_{ij}|^2 \leq n^{2\epsilon} m\right) \bigwedge \left(\left|\sum_{j=1}^m a_{ij}\right| \leq n^\epsilon \sqrt{m}\right).$$

Then,

$$\Pr\left(|I^c| \geq 2n^{1-\epsilon}\right) \leq 2\exp\left(-\frac{n^{1-\epsilon}}{4}\right).$$

Proof. Since for each $i \in [n]$,

$$\mathbb{E}\left[\left|\sum_{j=1}^{m} a_{ij}\right|^2\right] = \mathbb{E}\left[\sum_{j=1}^{m} |a_{ij}|^2\right] = m,$$

it follows from Markov's inequality that

$$\Pr\left(\sum_{j=1}^{m} |a_{ij}|^2 > n^{2\epsilon} m\right) \leq n^{-2\epsilon}$$

and

$$\Pr\left(\left|\sum_{j=1}^{m} a_{ij}\right| > n^{\epsilon}\sqrt{m}\right) \leq n^{-2\epsilon}.$$

Let $I_1 \subseteq [n]$ denote the subset of coordinates such that for each $i \in I_1$,

$$\sum_{j=1}^{m} |a_{ij}|^2 \leq n^{2\epsilon} m$$

and let $I_2 \subseteq [n]$ denote the subset of coordinates such that for each $i \in I_2$,

$$\left|\sum_{j=1}^{m} a_{ij}\right| \leq n^{\epsilon}\sqrt{m}.$$

Since the rows of the matrix are independent, it follows from the standard Chernoff bound that for $k \in \{1, 2\}$

$$\Pr\left(|I_k^c| \geq n^{1-\epsilon}\right) \leq \exp\left(-\frac{n^{1-\epsilon}}{4}\right).$$

Hence, by the union bound,

$$|I^c| \leq |I_1^c| + |I_2^c| \leq 2n^{1-\epsilon},$$

except with probability at most $2\exp\left(-\frac{n^{1-\epsilon}}{4}\right)$. □

The next proposition controls the $\infty \to 2$ operator norm of a random matrix with i.i.d. entries, conditioned on no row having ℓ_1 or ℓ_2 norm which is 'too large', and essentially appears as Proposition 3.10 in [19]. Since our statement uses somewhat different parameters than in [19], we provide a complete proof below for the reader's convenience.

Proposition 5.4. *Fix $\epsilon \in (0, 1/2)$. Let $B := (b_{ij})$ be a fixed $n \times m$ complex matrix, with $0.9n \leq m \leq 1.1n$, such that the ℓ_2 norm of every row is at most $n^{\epsilon}\sqrt{m}$ and such that for all $i \in [n]$,*

$$\left|\sum_{j=1}^{m} b_{ij}\right| \leq n^{\epsilon}\sqrt{m}.$$

Let $\pi_1, \ldots, \pi_n$ be independent random permutations uniformly distributed on the symmetric group S_m, and let $\tilde{B} := (\tilde{b}_{ij})$ denote the random $n \times m$ complex matrix whose entries are given by

$$\tilde{b}_{ij} := b_{i,\pi_i(j)}.$$

Then,

$$\Pr\left(\|\tilde{B}\|_{\infty\to 2} \geq C_{5.4}\sqrt{mn}n^{\epsilon}\right) \leq \exp(-2n),$$

where $C_{5.4} \geq 1$ is an absolute constant.

The following concentration inequality will be used to establish the subgaussianity of certain random variables appearing in the proof of Proposition 5.4. It appears as Lemma 3.9 in [19], and is a direct application of Theorem 7.8 in [16].

Lemma 5.5 (Lemma 3.9 in [19])**.** *Let $\boldsymbol{y} := (y_1, \dots, y_m)$ be a non-zero complex vector and let $\boldsymbol{v} \in \{\pm 1\}^m$. Consider the function $f : S_m \to \mathbb{C}$ defined by*

$$f(\pi) := \sum_{j=1}^{m} v_{\pi(j)} y_j.$$

Then, for all $t > 0$,

$$\Pr\left(|f(\pi) - \mathbb{E}f| \geq t\right) \leq 4\exp\left(-\frac{t^2}{128\|\boldsymbol{y}\|_2^2}\right).$$

Remark 5.6. In [19], the above lemma is stated and proved (with better constants) for real vectors $\boldsymbol{y}$. However, the version above for complex vectors immediately follows from this by separately considering the real and imaginary parts of f and using the union bound.

Proof of Proposition 5.4. If $\|\tilde{B}\|_{\infty\to 2} \geq C_{5.4}\sqrt{mn}n^{\epsilon}$, then there exists a complex vector $\boldsymbol{w} = \boldsymbol{w_1} + i\boldsymbol{w_2}$, where $\boldsymbol{w_1}, \boldsymbol{w_2} \in \mathbb{R}^m$ and $\|\boldsymbol{w_1}\|_\infty, \|\boldsymbol{w_2}\|_\infty \leq 1$, such that

$$\|\tilde{B}\boldsymbol{w}_1\|_2 + \|\tilde{B}\boldsymbol{w}_2\|_2 \geq \|\tilde{B}\boldsymbol{w}\|_2 \geq C_{5.4}\sqrt{mn}n^{\epsilon}.$$

Therefore, it suffices to control the ∞-to-2 norm of $\tilde{B}$ restricted to vectors in $\mathbb{R}^m$. For this, it suffices by convexity and the union bound to show that for any fixed $\boldsymbol{v} \in \{\pm 1\}^m$,

$$\Pr\left(\|\tilde{B}\boldsymbol{v}\|_2^2 \geq (128C_{5.2} + 2)mn^{1+2\epsilon}\right) \leq \exp(-2n - m\ln 2).$$

To see this, we begin by noting that the random variables $X_i := \langle \tilde{B}\boldsymbol{v}, e_i\rangle$ are independent and

$$X_i \sim \sum_{j=1}^{m} v_{\pi_i(j)} b_{ij}.$$

In particular, if ℓ denotes the number of ones in $(v_1, \dots, v_m)$, then

$$|\mathbb{E}[X_i]| = \left|\sum_{j=1}^{m} \mathbb{E}\left[v_{\pi_i(j)}\right] b_{ij}\right| = \left|\sum_{j=1}^{m} \frac{2\ell - m}{m} b_{ij}\right| \leq \left|\sum_{j=1}^{m} b_{ij}\right| \leq n^{\epsilon}\sqrt{m}.$$

By Lemma 5.5, for all $t > 0$, we have

$$\Pr\left(|X_i - \mathbb{E}[X_i]| \geq t\right) \leq 4\exp\left(-\frac{t^2}{128\|\boldsymbol{b_i}\|_2^2}\right) \leq 4\exp\left(-\frac{t^2}{128mn^{2\epsilon}}\right).$$

In particular, the random variables $n^{-\epsilon}m^{-1/2}|X_i - \mathbb{E}[X_i]|$ are 16-subgaussian so that by Lemma 5.2

$$\Pr\left(\sum_{i=1}^{n} |X_i - \mathbb{E}[X_i]|^2 \geq 256C_{5.2}mn^{1+2\epsilon}\right) \leq \exp\left(-4n\right) \leq \exp\left(-2n - m\ln 2\right).$$

Finally, since

$$\begin{aligned}\sum_{i=1}^{n}|X_i|^2 &= \sum_{i=1}^{n}|X_i-\mathbb{E}[X_i]+\mathbb{E}[X_i]|^2\\ &\le 2\sum_{i=1}^{n}|X_i-\mathbb{E}[X_i]|^2+2\sum_{i=1}^{n}|\mathbb{E}[X_i]|^2\\ &\le 2\sum_{i=1}^{n}|X_i-\mathbb{E}[X_i]|^2+2mn^{1+2\epsilon},\end{aligned}$$

it follows that

$$\Pr\left(\sum_{i=1}^{n}|X_i|^2 \ge (256C_{5.2}+2)mn^{1+2\epsilon}\right) \le \Pr\left(\sum_{i=1}^{n}|X_i-\mathbb{E}[X_i]|^2 \ge 256C_{5.2}mn^{1+2\epsilon}\right) \le \exp\left(-2n-m\ln 2\right),$$

which completes the proof. $\square$

Given the above results, Proposition 2.13 is almost immediate.

Proof of Proposition 2.13. **1.** Let N_n be the $n\times n$ complex random matrix appearing in the statement of the proposition, and let $\mathcal{E}$ denote the 'good' event appearing in Lemma 5.3 i.e. $\mathcal{E}$ is the event that there exists some $I\subseteq[n]$ with $|I|\ge n-2n^{1-\epsilon}$ such that for all $i\in I$,

$$\left(\sum_{j=1}^{n}|m_{ij}|^2 \le n^{1+2\epsilon}\right)\bigwedge\left(\left|\sum_{j=1}^{n}m_{ij}\right|\le n^{(1/2)+\epsilon}\right).$$

Since $\Pr(\mathcal{E}^c)\le 2\exp(-n^{1-\epsilon}/4)$ by Lemma 5.3, it suffices to show that

$$\Pr\left(\left\{\inf_{i\in\mathcal{I}}\|P_IN_n\|_{\infty\to 2}\ge C_{5.4}n^{1+\epsilon}\right\}\cap\mathcal{E}\right)\le\exp(-n),$$

where $\mathcal{I}$ denotes the collection of subsets of $[n]$ of size at least $n-2n^{1-\epsilon}$. For this, note that since both the event $\mathcal{E}$ as well as our distribution on $n\times n$ matrices are invariant under permuting each row of N_n separately, it suffices to show the following: for each (fixed) $n\times n$ complex matrix A_n for which there exists a subset $I\subseteq[n]$ as above,

$$\Pr\left(\|P_I\tilde{A}_n\|_{\infty\to 2}\ge C_{5.4}n^{1+\epsilon}\right)\le\exp(-n),$$

where $\tilde{A}_n$ is the random complex matrix obtained by permuting each row of A_n independently and uniformly. But this follows immediately from Proposition 5.4 applied to the $n\times n$ matrix P_IA_n.

2. The proof of this part is very similar to the previous one. Let $\mathcal{J}$ denote the collection of all subsets of $[n]$ of size $n^{1-\delta}$ and let $\mathcal{I}$ denote the collection of all subsets of $[n]$ of size at least $n-2n^{1-\epsilon}$. We show that the desired conclusion in 2. holds with sufficiently high probability for fixed $J\in\mathcal{J}$; the proof is completed by taking the union bound over the at most

$$\binom{n}{n^{1-\delta}}\le\exp(n^{1-\delta}\log n)\le C(\epsilon)\exp(n^{1-3\epsilon})$$

choices for $J\in\mathcal{J}$, where $C(\epsilon)\ge 1$ depends only on ϵ, and the last inequality uses that $\delta\ge 4\epsilon$.

For such a fixed $J \in \mathcal{J}$, let $\mathcal{E}_{\epsilon,\delta}$ denote the event that there exists some $I \in \mathcal{I}$ such that for all $i \in I$,

$$\left(\sum_{j \in J} |m_{ij}|^2 \le n^{2\epsilon}|J|\right) \bigwedge \left(\left|\sum_{j\in J} m_{ij}\right| \le n^{\epsilon}\sqrt{|J|}\right).$$

As before, by Lemma 5.3 applied to the operator $N_n P_J$ viewed as an $n \times |J|$ matrix, we see that $\Pr(\mathcal{E}^c_{\epsilon,\delta}) \le 2\exp(-n^{1-\epsilon}/4)$. Therefore, it suffices to show that

$$\Pr\left(\left\{\inf_{i \in \mathcal{I}} \|P_I N_n P_J\|_{\infty \to 2} \ge C_{5.4} n^{1+\epsilon-0.5\delta}\right\} \cap \mathcal{E}_{\epsilon,\delta}\right) \le \exp(-n).$$

But this follows by exactly the same argument (using Proposition 5.4) as above. □

References

[1] Z. Bai. Circular law. *The Annals of Probability*, 25(1):494–529, 1997.

[2] Z. Bai and J. W. Silverstein. *Spectral analysis of large dimensional random matrices*, volume 20. Springer, 2010.

[3] A. Basak, N. Cook, and O. Zeitouni. Circular law for the sum of random permutation matrices. *Electronic Journal of Probability*, 23, 2018.

[4] C. Bordenave and D. Chafaï. Around the circular law. *Probability surveys*, 9, 2012.

[5] N. A. Cook. The circular law for random regular digraphs. *arXiv preprint arXiv:1703.05839*, 2017.

[6] S. Eliahou and M. Kervaire. Some extensions of the Cauchy-Davenport theorem. *Electronic Notes in Discrete Mathematics*, 28:557–564, 2007.

[7] C. Esseen. On the Kolmogorov-Rogozin inequality for the concentration function. *Probability Theory and Related Fields*, 5(3):210–216, 1966.

[8] A. Ferber and V. Jain. Singularity of random symmetric matrices–a combinatorial approach to improved bounds. *arXiv:1809.04718*, 2018.

[9] A. Ferber, V. Jain, K. Luh, and W. Samotij. On the counting problem in inverse Littlewood–Offord theory. *arXiv:1904.10425*, 2019.

[10] O. Friedland and S. Sodin. Bounds on the concentration function in terms of the diophantine approximation. *Comptes Rendus Mathematique*, 345(9):513–518, 2007.

[11] V. L. Girko. Circular law. *Theory of Probability & Its Applications*, 29(4):694–706, 1985.

[12] G. Halász. Estimates for the concentration function of combinatorial number theory and probability. *Periodica Mathematica Hungarica*, 8(3-4):197–211, 1977.

[13] V. Jain. Approximate Spielman-Teng theorems for the least singular value of random combinatorial matrices. *arXiv:1904.10592*, 2019.

[14] V. Jain. Smoothed analysis of the condition number without inverse Littlewood-Offord theory. *In preparation*, 2019.

[15] A. E. Litvak, A. Pajor, M. Rudelson, and N. Tomczak-Jaegermann. Smallest singular value of random matrices and geometry of random polytopes. *Advances in Mathematics*, 195(2):491–523, 2005.

[16] V. D. Milman and G. Schechtman. *Asymptotic theory of finite dimensional normed spaces: Isoperimetric inequalities in riemannian manifolds*, volume 1200. Springer, 2009.

[17] H. H. Nguyen and V. H. Vu. Optimal inverse Littlewood–Offord theorems. *Advances in Mathematics*, 226(6):5298–5319, 2011.

[18] H. H. Nguyen and V. H. Vu. Small ball probability, inverse theorems, and applications. In *Erdős Centennial*, pages 409–463. Springer, 2013.

[19] E. Rebrova and K. Tikhomirov. Coverings of random ellipsoids, and invertibility of matrices with iid heavy-tailed entries. *Israel Journal of Mathematics*, 227(2):507–544, 2018.

[20] E. Rebrova and R. Vershynin. Norms of random matrices: local and global problems. *Advances in Mathematics*, 324:40–83, 2018.

[21] M. Rudelson and R. Vershynin. The Littlewood–Offord problem and invertibility of random matrices. *Advances in Mathematics*, 218(2):600–633, 2008.

[22] M. Rudelson and R. Vershynin. Smallest singular value of a random rectangular matrix. *Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathematical Sciences*, 62(12):1707–1739, 2009.

[23] M. Rudelson and R. Vershynin. Non-asymptotic theory of random matrices: extreme singular values. In *Proceedings of the International Congress of Mathematicians 2010 (ICM 2010) (In 4 Volumes) Vol. I: Plenary Lectures and Ceremonies Vols. II–IV: Invited Lectures*, pages 1576–1602. World Scientific, 2010.

[24] T. Tao and V. Vu. Random matrices: the circular law. *Communications in Contemporary Mathematics*, 10(02):261–307, 2008.

[25] T. Tao and V. Vu. A sharp inverse Littlewood-Offord theorem. *Random Structures Algorithms*, 37(4):525–539, 2010.

[26] T. Tao and V. Vu. Smooth analysis of the condition number and the least singular value. *Mathematics of computation*, 79(272):2333–2352, 2010.

[27] T. Tao, V. Vu, M. Krishnapur, et al. Random matrices: Universality of esds and the circular law. *The Annals of Probability*, 38(5):2023–2065, 2010.

[28] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

[29] T. Tao and V. H. Vu. Inverse Littlewood-Offord theorems and the condition number of random discrete matrices. *Annals of Mathematics*, pages 595–632, 2009.

[30] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. *arXiv:1011.3027*, 2010.

A Proof of Theorem 2.10

Proof. Since $\rho_{\delta,z}(\boldsymbol{a}) = \rho_{1,z}(\delta^{-1}\boldsymbol{a})$, it suffices to bound $\rho_{1,z}(\boldsymbol{v})$ for $\boldsymbol{v} := \delta^{-1}\boldsymbol{a}$. Let $\boldsymbol{w} \in \mathbb{C}^{2n}$ denote the vector whose first n components are $\boldsymbol{v}$ and last n components are $i\boldsymbol{v}$. Then, we have

$$\begin{aligned}
\rho_{1,z}(\boldsymbol{v})^2 &= \rho_{1,z}(\boldsymbol{v})\rho_{1,z}(i\boldsymbol{v}) \\
&\le \exp(2\pi)P_z(\boldsymbol{v})P_z(i\boldsymbol{v}) \\
&\le 2\exp(2\pi)P_z(\boldsymbol{w}) \\
&\le 2\exp(2\pi)\int_{\mathbb{C}} \exp\left(-\sum_{j=1}^{n}\left(\|v_j\xi\|_z^2 + \|iv_j\xi\|_z^2\right)/2 - \pi|\xi|^2\right) d\xi,
\end{aligned}$$

where the first line uses $\rho_{1,z}(\boldsymbol{v}) = \rho_{1,z}(i\boldsymbol{v})$, the second line is due to Proposition 4.2, the third line follows from Lemma 4.5(iii) in [24], and the last line is again due to Proposition 4.2.

Next, note that

$$\begin{aligned}
\sum_{j=1}^{n}\left(\|v_j\xi\|_z^2 + \|iv_j\xi\|_z^2\right) &= \mathbb{E}\sum_{j=1}^{n}\left(\|\Re\{v_j\xi(z_1-z_2)\}\|_{\mathbb{R}/\mathbb{Z}}^2 + \|\Re\{iv_j\xi(z_1-z_2)\}\|_{\mathbb{R}/\mathbb{Z}}^2\right) \\
&= \mathbb{E}\sum_{j=1}^{n}\left(\|\Re\{v_j\xi(z_1-z_2)\}\|_{\mathbb{R}/\mathbb{Z}}^2 + \|\Im\{v_j\xi(z_1-z_2)\}\|_{\mathbb{R}/\mathbb{Z}}^2\right) \\
&= \mathbb{E}\left[\mathrm{dist}^2\left(\boldsymbol{v}\xi(z_1-z_2), (\mathbb{Z}+i\mathbb{Z})^n\right)\right] \\
&\ge \mathbb{E}\left[\mathrm{dist}^2\left(\boldsymbol{v}\xi(z_1-z_2), (\mathbb{Z}+i\mathbb{Z})^n\right)\Big| |z_1-z_2| \in [C_z^{-1}, C_z]\right] C_z^{-1},
\end{aligned}$$

where the final inequality follows from the C_z-goodness of z.

Therefore, from Jensen's inequality, we get that

$$\begin{aligned}
\rho_{1,z}(\boldsymbol{v})^2 &\le 2\exp(2\pi)\mathbb{E}\left[\int_{\mathbb{C}}\exp(-C_z^{-1}\mathrm{dist}^2\left(\boldsymbol{v}\xi(z_1-z_2), (\mathbb{Z}+i\mathbb{Z})^n\right)/2 - \pi|\xi|^2)d\xi\Big| |z_1-z_2| \in [C_z^{-1}, C_z]\right] \\
&\le 2\exp(2\pi)\sup_{|y|\in[C_z^{-1},C_z]}\int_{\mathbb{C}}\exp(-C_z^{-1}\mathrm{dist}^2\left(\boldsymbol{v}\xi y, (\mathbb{Z}+i\mathbb{Z})^n\right)/2 - \pi|\xi|^2)d\xi. \qquad (10)
\end{aligned}$$

Now, fix $y_0 \in \mathbb{C}$ with $|y_0| \in [C_z^{-1}, C_z]$; we will obtain a uniform (in y_0) upper bound on the integral appearing in Equation (10). Let

$$A := \{\xi \in \mathbb{C} \mid \mathrm{dist}(\boldsymbol{v}\xi y_0, (\mathbb{Z}+i\mathbb{Z})^n) \ge \alpha/2\} \cup \{\xi \in \mathbb{C} \mid |\xi| \ge \alpha\},$$

let $B := \mathbb{C}\setminus A = B(0,\alpha)\setminus A$, and split the integral above as

$$\int_{\mathbb{C}} = \int_A + \int_B.$$

Since

$$\int_A \lesssim \exp\left(-\Omega_{C_z}(\alpha^2)\right),$$

it only remains to bound $\int_B$.

For this, we begin by noting that if $\xi', \xi'' \in B$, then by the triangle inequality and the lattice structure of the Gaussian integers,

$$\mathrm{dist}\left(\boldsymbol{a}\delta^{-1}(\xi'-\xi'')y_0, (\mathbb{Z}+i\mathbb{Z})^n\right) = \mathrm{dist}\left(\boldsymbol{v}(\xi'-\xi'')y_0, (\mathbb{Z}+i\mathbb{Z})^n\right) < \alpha.$$

Hence, by the definition of $\mathrm{LCD}_{\gamma,\alpha}(\boldsymbol{a})$, we have one of two possibilities: either

$$\delta^{-1}C_z|\xi' - \xi''| \geq \delta^{-1}|y_0||\xi' - \xi''| \geq \mathrm{LCD}_{\gamma,\alpha}(\boldsymbol{a})$$

or

$$\gamma|\xi' - \xi''|\delta^{-1}C_z^{-1} \leq \gamma|\xi' - \xi''|\delta^{-1}|y_0| < \mathrm{dist}(\boldsymbol{v}(\xi' - \xi'')y_0, (\mathbb{Z} + i\mathbb{Z})^n) < \sqrt{n}.$$

It follows that B is contained in a union of balls of radius $C_z\sqrt{n}\delta/\gamma$ whose centers are separated by at least $\delta\,\mathrm{LCD}_{\gamma,\alpha}(\boldsymbol{a})/C_z$. Each such ball can contribute at most $\pi C_z^2 n\delta^2/\gamma^2$ to the integral, and since $\delta\,\mathrm{LCD}_{\gamma,\alpha}(\boldsymbol{a}) \gg \alpha$, there is at most one such ball in B. It follows that

$$\int_B \leq \frac{\pi C_z^2 n\delta^2}{\gamma^2}.$$

Finally, combining the estimates on $\int_A$ and $\int_B$ and using Equation (10) completes the proof. $\square$

B Proof of Theorem 4.6

In this section, we prove Theorem 4.6 using an elementary double counting argument appearing in [9].

Proof. Let $\mathcal{Z}$ be the set of all triples

$$\Big(I, (i_{s+1}, \ldots, i_n), (F_j, \boldsymbol{\epsilon}^j)_{j=s+1}^n\Big),$$

where

1. $I \subseteq [n]$ and $|I| = s$,
2. $(i_{s+1}, \ldots, i_n) \in [n]^{n-s}$ is a permutation of $[n] \setminus I$,
3. each $F_j := (\ell_{j,1}, \ldots, \ell_{j,2k})$ is a sequence of $2k$ elements of $[n]$, and
4. $\boldsymbol{\epsilon}^j \in \{\pm 1\}^{2k}$ for each j,

that satisfy the following conditions for each j:

a. $\ell_{j,2k} = i_j$ and

b. $(\ell_{j,1}, \ldots, \ell_{j,2k-1}) \in \big(I \cup \{i_{s+1}, \ldots, i_{j-1}\}\big)^{2k-1}$.

Claim B.1. *The number of triples in $\mathcal{Z}$ is at most $(s/n)^{2k-1} \cdot \big(2^{n-s}n!/s!\big)^{2k}$.*

Proof. One can construct any such triple as follows. First, choose an s-element subset of $[n]$ to serve as I. Second, considering all $j \in \{s+1, \ldots, n\}$ one by one in increasing order, choose: one of the $n - j + 1$ remaining elements of $[n] \setminus I$ to serve as i_j; one of the 2^{2k} possible sign patterns to serve as $\boldsymbol{\epsilon}^j$; and one of the $(j-1)^{2k-1}$ sequences of $2k - 1$ elements of $I \cup \{i_{s+1}, \ldots, i_{j-1}\}$ to serve as $(\ell_{j,1}, \ldots, \ell_{j,2k-1})$. Therefore,

$$\begin{aligned}
|\mathcal{Z}| &\leq \binom{n}{s} \cdot \prod_{j=s+1}^{n} \Big((n-j+1) \cdot 2^{2k} \cdot (j-1)^{2k-1}\Big) \\
&= \frac{n!}{s!(n-s)!} \cdot (n-s)! \cdot 2^{2k(n-s)} \cdot \left(\frac{(n-1)!}{(s-1)!}\right)^{2k-1} = \left(\frac{s}{n}\right)^{2k-1} \cdot \left(2^{n-s} \cdot \frac{n!}{s!}\right)^{2k}.
\end{aligned}$$

$\square$

We call $\boldsymbol{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_p + i\mathbb{F}_p)^n$ *compatible* with a triple from $\mathcal{Z}$ if for every $j \in \{s+1, \ldots, n\}$,

$$\sum_{i=1}^{2k} \boldsymbol{\epsilon}_i^j a_{\ell_{j,i}} = 0. \tag{11}$$

Claim B.2. *Each triple from $\mathcal{Z}$ is compatible with at most p^{2s} sequences $\boldsymbol{a} \in (\mathbb{F}_p + i\mathbb{F}_p)^n$.*

Proof. Using a, we may rewrite Equation (11) as

$$\boldsymbol{\epsilon}_{2k}^j a_{i_j} = -\sum_{i=1}^{2k-1} \boldsymbol{\epsilon}_i^j a_{\ell_{j,i}}.$$

It follows from b that once a triple from $\mathcal{Z}$ is fixed, the right-hand side above depends only on those coordinates of the vector $\boldsymbol{a}$ that are indexed by $i \in I \cup \{i_{s+1}, \ldots, i_{j-1}\}$. In particular, for each of the p^{2s} possible values of $(a_i)_{i\in I}$, there is exactly one way to extend it to a sequence $\boldsymbol{a} \in (\mathbb{F}_p + i\mathbb{F}_p)^n$ that satisfies Equation (11) for every j. □

Claim B.3. *Each sequence $\boldsymbol{a} \in \boldsymbol{B}^{\alpha}_{k,s,\geq t}$ is compatible with at least*

$$\left(\frac{2^{n-s} n!}{s!}\right)^{2k} \cdot \left(\frac{\alpha t}{p}\right)^{n-s}$$

triples from $\mathcal{Z}$.

Proof. Given any such $\boldsymbol{a}$, we may construct a compatible triple from $\mathcal{Z}$ as follows. Considering all $j \in \{n, \ldots, s+1\}$ one by one in decreasing order, we do the following. First, we find an arbitrary solution to

$$\pm a_{\ell_1} \pm a_{\ell_2} \pm \cdots \pm a_{\ell_{2k}} = 0 \tag{12}$$

such that $\ell_1, \ldots, \ell_{2k} \in [n] \setminus \{i_n, \ldots, i_{j+1}\}$ and such that ℓ_{2k} is a non-repeated index (i.e., such that $\ell_{2k} \neq \ell_i$ for all $i \in [2k-1]$). Given any such solution, we let ℓ_{2k} serve as i_j, we let the sequence $(\ell_1, \ldots, \ell_{2k})$ serve as F_j, and we let $\boldsymbol{\epsilon}^j$ be the corresponding sequence of signs (so that Equation (11) holds). The assumption that $\boldsymbol{a} \in \boldsymbol{B}^{\alpha}_{k,s,\geq t}(n)$ guarantees that there are at least $t \cdot \frac{2^{2k}\cdot(n-j+1)^{2k}}{p}$ many solutions to Equation (12), each of which has at least $2\alpha k$ nonrepeated indices. Since the set of all such solutions is closed under every permutation of the ℓ_is (and the respective signs), ℓ_{2k} is a non-repeated index in at least an α-proportion of them. Finally, we let $I = [n] \setminus \{i_n, \ldots, i_{s+1}\}$. Since different sequences of solutions lead to different triples, it follows that the number Z of compatible triples satisfies

$$Z \geq \prod_{j=s+1}^{n} \left(\alpha t \cdot \frac{2^{2k} \cdot (n-j+1)^{2k}}{p}\right) = \left(\frac{2^{n-s} n!}{s!}\right)^{2k} \cdot \left(\frac{\alpha t}{p}\right)^{n-s}. \qquad \square$$

Counting the number P of pairs of $\boldsymbol{a} \in \boldsymbol{B}^{\alpha}_{k,s,\geq t}(n)$ and a compatible triple from $\mathcal{Z}$, we have

$$|\boldsymbol{B}^{\alpha}_{k,s,\geq t}(n)| \cdot \left(\frac{2^{n-s} n!}{s!}\right)^{2k} \cdot \left(\frac{\alpha t}{p}\right)^{n-s} \leq P \leq |\mathcal{Z}| \cdot p^{2s} \leq \left(\frac{s}{n}\right)^{2k-1} \cdot \left(\frac{2^{n-s} n!}{s!}\right)^{2k} \cdot p^{2s},$$

which yields the desired upper bound on $|\boldsymbol{B}^{\alpha}_{k,s,\geq t}(n)|$. □