

# LITTLEWOOD-OFFORD BOUNDS ON THE SYMMETRIC GROUPS AND APPLICATIONS

VIET H. DO, HOI H. NGUYEN, KIET H. PHAN, TUAN TRAN, AND VAN H. VU

**ABSTRACT.** The anti-concentration phenomenon in probability theory has been intensively studied in recent years, with applications across many areas of mathematics. In most existing works, the ambient probability space is a product space generated by independent random variables.

In this paper, we initiate a systematic study of anti-concentration when the ambient space is the symmetric group, equipped with the uniform measure. Concretely, we focus on the random sum  $S_\pi = \sum_{i=1}^n w_i v_{\pi(i)}$ , where  $\mathbf{w} = (w_1, \dots, w_n)$  and  $\mathbf{v} = (v_1, \dots, v_n)$  are fixed vectors and  $\pi$  is a uniformly random permutation.

The paper contains several new results, addressing both discrete and continuous anti-concentration phenomena. On the discrete side, we establish a near-optimal structural characterization of the vectors  $\mathbf{w}$  and  $\mathbf{v}$  under the assumption that the concentration probability  $\sup_x \mathbb{P}(S_\pi = x)$  is polynomially large. As applications, we derive and strengthen a number of previous results. In particular, we show that if both  $\mathbf{w}$  and  $\mathbf{v}$  have distinct entries, then  $\sup_x \mathbb{P}(S_\pi = x) \leq n^{-5/2+o(1)}$ . This bound serves as a permutation-space analogue of the classical Erdős–Moser bound in the product-space setting and answers a question posed by Alon–Pohoata–Zhu [2].

From the continuous perspective, we study the small-ball event  $|S_\pi - L| \leq \delta$ . We establish sharp bounds in various settings, including results exhibiting sub-gaussian decay in  $L$ , thereby settling a question of Söze [50]. With additional effort, we are also able to treat the joint distribution of these events. Moreover, we provide a characterization of the vectors  $\mathbf{w}$  and  $\mathbf{v}$  for which these small-ball probabilities are large. As an application, we prove that the number of extremal points of random permutation polynomials is bounded by  $O(\log n)$ , extending results of Söze [49, 50] on the number of real roots.

## 1. INTRODUCTION

**1.1. Anti-concentration in product spaces.** Let  $\mathbf{w} = (w_1, \dots, w_n)$  be a real vector. Consider the random sum

$$S = \sum_{i=1}^n w_i \xi_i, \tag{1}$$

where the  $\xi_i$  are i.i.d. copies of a real-valued random variable  $\xi$  with mean zero and variance one. This sum can be viewed as the inner product of  $\mathbf{w}$  and the random vector  $(\xi_1, \dots, \xi_n)$ .

A typical anti-concentration bound asserts that, under suitable assumptions, the probability that  $S$  lies in a small interval is small. We consider two settings: *discrete* and *continuous*. In the discrete setting, we study the probability of the event  $S = x$  for a fixed value  $x$ . In the continuous setting, we consider small-ball events of the form  $|S - L| \leq \delta$  for some  $L \in \mathbb{R}$  and  $\delta > 0$ .

---

H. Nguyen is supported by a Simons Travel Grant TSM-00013318. T. Tran is supported by the Excellent Young Talents Program (Overseas) of the National Natural Science Foundation of China. A substantial part of this work was carried out during the ADM program 2024; the authors are grateful to the VinBigData Center for its hospitality.

For ease of exposition, we begin with the discrete setting. In the 1940s, Littlewood–Offord [32] and Erdős [13] proved the following fundamental result.

**Theorem 1.1.** *Assume that  $w_i$ ,  $1 \leq i \leq n$ , are nonzero and that the  $\xi_i$  are i.i.d. Rademacher random variables (that is,  $\xi_i$  takes values  $\pm 1$  with probability  $1/2$ , independently). Then*

$$\sup_x \mathbb{P}(S = x) = O\left(\frac{1}{\sqrt{n}}\right).$$

Here and throughout, asymptotic notation is taken in the limit  $n \rightarrow \infty$ .

When the coefficients  $w_i$  are distinct, this bound can be significantly improved. This was shown independently by Erdős–Moser [14], Sárközy–Szemerédi [48], and Stanley [51].

**Theorem 1.2.** *Assume that the  $w_i$  are distinct real numbers and that the  $\xi_i$  are i.i.d. Rademacher random variables. Then*

$$\sup_x \mathbb{P}(S = x) = O(n^{-3/2}).$$

**Remark 1.3.** *In this paper, we focus on orders of magnitude, and all bounds are stated in big-Oh form  $O(\cdot)$ . Bounds of this type remain unchanged (in both the discrete and continuous settings) if we replace  $w_i$  by  $\alpha w_i$ , where  $\alpha = O(1)$ . This observation allows us to normalize many of our assumptions.*

These results initiated a substantial body of work known as *Littlewood–Offord theory*, which has developed over several decades; see [40] for a comprehensive survey. The guiding principle of this theory is that stronger structural assumptions on the coefficients  $w_i$  lead to stronger anti-concentration bounds. Results of this type are commonly referred to as *forward theorems*.

In the early 2000s, Tao and the last author initiated a new line of research, known as the *inverse Littlewood–Offord theory*. The goal is to characterize the additive structure of the coefficients  $w_i$  under the assumption that the concentration probability

$$\sup_{x \in \mathbb{R}} \mathbb{P}(S = x)$$

is *relatively large*. Results of this kind are called *inverse theorems*. In this paper, we focus on the polynomial regime, where “relatively large” means at least  $n^{-C}$  for some constant  $C > 0$ .

Let  $W$  denotes the multi-set  $\{w_1, \dots, w_n\}$ . Let

$$\rho(W) := \sup_{x \in \mathbb{R}} \mathbb{P}(S = x).$$

Assume that  $\rho(W) \geq n^{-C}$  for some constant  $C > 0$ . This implies that at least  $2^n n^{-C}$  of the  $2^n$  subsums of  $W$  coincide, suggesting that  $W$  must possess substantial additive structure. Tao and the last author managed to formalize this intuition in a quantitative way via the notion of *generalized arithmetic progressions* (GAPs).

**Definition 1.4.** A subset  $P \subset \mathbb{R}$  is a *generalized arithmetic progression (GAP)* of rank  $r$  if it can be expressed as

$$P = \left\{ g_0 + m_1 g_1 + \dots + m_r g_r \mid m_i \in \mathbb{Z}, N_i \leq m_i \leq N'_i \right\},$$

where  $g_1, \dots, g_r \in \mathbb{R}$  are called the *generators* of  $P$ , and the integers  $N_i, N'_i$  are its *dimensions*. The *volume* of  $P$  is defined as  $\text{Vol}(P) := \prod_{i=1}^r (N'_i - N_i + 1)$ . We say that  $P$  is *proper* if every element of  $P$  has a unique representation in the above form; this is equivalent to  $|P| = \text{Vol}(P)$ . If  $N_i = -N'_i$  for all  $i$  and  $g_0 = 0$ , we say that  $P$  is *symmetric*.

For two sets  $A, B \subset \mathbb{R}$ , their (Minkowski) sum is defined by

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

For  $n \in \mathbb{Z}^+$ , we define

$$nA := \{a_1 + \cdots + a_n \mid a_i \in A\}.$$

For example, if  $P$  is as in Definition 1.4, then

$$nP = \left\{ ng_0 + m_1 g_1 + \cdots + m_r g_r \mid nN_i \leq m_i \leq nN'_i \right\}.$$

**Example 1.5.** Assume  $P$  is a proper symmetric GAP of rank  $r = O(1)$  and cardinality  $n^{O(1)}$ , and all elements of  $W = \{w_1, \dots, w_n\}$  lie in  $P$ . Then since  $|nP| \leq n^r |P|$ , by the pigeonhole principle, we obtain  $\rho(W) = \Omega(n^{-O(1)})$ .

This example shows that if  $W$  lies inside a proper symmetric GAP with small rank and cardinality, then  $\rho(W)$  is necessarily large. In a series of works, Tao–Vu [59, 58], Nguyen–Vu [39], and more recently Tao [54], demonstrated that these are essentially the only configurations for which  $\rho(W)$  is polynomially large. One may also consider the sub-exponential ( $\rho \geq \exp(-n^c)$ ) or exponential ( $\rho \geq \exp(-cn)$ ) regimes, but we do not address them in this paper.

**Theorem 1.6** (Inverse Littlewood–Offord result for  $\rho$ ). [39, Theorem 2.1] Let  $C > 0$  and  $\varepsilon \in (0, 1)$  be constants. Suppose  $W = \{w_1, \dots, w_n\}$  is a multiset of real numbers such that

$$\rho(W) \geq n^{-C},$$

where  $\xi_i$  are iid copies of a random variable  $\xi$  of mean zero, variance one, and bounded  $(2 + \varepsilon)$ -moment. Then for any  $n^\varepsilon \leq n' \leq n$ , there exists a proper symmetric GAP  $P \subset \mathbb{R}$  of rank  $r = O_{C,\varepsilon}(1)$  such that  $P$  contains all but  $n'$  elements of  $W$  (counting multiplicity), and

$$|P| = \max \left\{ 1, O_{C,\varepsilon} \left( \rho(W)^{-1} (n)^{-r/2} \right) \right\}.$$

There are many extensions to other frameworks, such as the extension from linear forms  $S$  of the  $\xi_i$  to quadratic and higher-order multilinear forms by Costello, Nguyen [10, 36], and Meka et al. [35], and to non-abelian groups by Tiep–Vu [43] and Juskevicius–Semetulskis [26] (see also [29, 38, 54]). Other notable contributions include the works of Tao–Vu [57], Rudelson–Vershynin [47], and, more recently, Fox et al. [15] and Kwan et al. [30, 31]. The discussion of these papers are beyond the scope of our works.

The continuous case proceeds in parallel with the discrete case, and we refer the reader to the survey [40] for further discussion. In particular, the continuous analogue of Theorem 1.6 asserts that the elements of  $W$  lie close to a small GAP.

**1.2. The space of random permutations: discrete setting.** In this paper, we investigate the anti-concentration behavior of random sums in a fundamentally different setting, where the ambient probability space is the symmetric group equipped with the uniform distribution. Let  $\mathbf{w} = (w_1, \dots, w_n)$  and  $\mathbf{v} = (v_1, \dots, v_n)$  be two fixed vectors. We consider the random sum

$$S_\pi(\mathbf{w}, \mathbf{v}) := \sum_{i=1}^n w_i v_{\pi(i)}, \tag{2}$$

where  $\pi$  is a uniformly random permutation of  $\{1, \dots, n\}$ . In most of the paper, when there is no danger of confusion, we use the shorthand  $S_\pi$  for  $S_\pi(\mathbf{w}, \mathbf{v})$ .

1.2.1. *Some forward theorems.* In this subsection, we bound the probability that  $S_\pi = x$  for any fixed value  $x$ . This problem has been studied recently in the combinatorics community. In [50], Söze considered the special case  $\mathbf{v} = (1, 2, \dots, n)$  and proved the following result.

**Theorem 1.7.** *Let  $\mathbf{v} = (1, 2, \dots, n)$  and let  $\mathbf{w} \in \mathbb{R}^n$  be a nonzero vector such that  $\mathbf{w} \cdot \mathbf{1} = 0$ , where  $\mathbf{1}$  denotes the all-ones vector. Then*

$$\sup_x \mathbb{P}(S_\pi = x) = O\left(\frac{1}{n}\right).$$

We remark that the assumption  $\mathbf{w} \cdot \mathbf{1} = 0$  may be imposed without loss of generality. Indeed, if all coordinates of  $\mathbf{w}$  are equal, then  $S_\pi$  is constant and no nontrivial anti-concentration statement can hold. Thus, from the perspective of anti-concentration, it is natural to decompose

$$\mathbf{w} = \alpha \mathbf{1} + \mathbf{w}', \quad \mathbf{w}' \cdot \mathbf{1} = 0,$$

and to focus on  $S_\pi(\mathbf{w}', \mathbf{v})$ .

The bound  $O(1/n)$  is sharp, as shown by taking  $w_1 = 1$ ,  $w_2 = -1$ , and  $w_i = 0$  for  $i \geq 3$ . In [4], Berger *et al.* extended this result to an arbitrary vector  $\mathbf{v}$  with distinct coordinates.

**Theorem 1.8.** *If the  $v_i$  are all distinct and  $\mathbf{w}$  is a nonzero vector such that  $\mathbf{w} \cdot \mathbf{1} = 0$ , then*

$$\sup_x \mathbb{P}(S_\pi = x) = O\left(\frac{1}{n}\right).$$

Both Theorems 1.7 and 1.8 are special cases of continuous theorems that we will discuss later. Theorem 1.8 may be viewed as a permutation analogue of the Littlewood–Offord–Erdős result from the product-space setting. Note that there is a  $\sqrt{n}$  improvement from the bound  $O(n^{-1/2})$  to  $O(n^{-1})$ .

One may also interpret the above problems in terms of orbits of the symmetric group. Given a vector  $\mathbf{v} = (v_1, \dots, v_n)$  with distinct coordinates, consider the orbit  $\pi(\mathbf{v})$  of  $\mathbf{v}$  under  $S_n$ . How many of these orbit points can lie in a fixed hyperplane  $H \subset \mathbb{R}^n$ ? A more precise result was conjectured in [21] (see also [20]) and later verified in [42] (and independently in [2]).

**Theorem 1.9.** *Under the assumptions of Theorem 1.8,*

$$\sup_x \mathbb{P}(S_\pi = x) \leq \frac{2\lfloor n/2 \rfloor}{n(n-1)}. \tag{3}$$

This bound is optimal. Indeed, take  $\mathbf{v} = (1, 2, \dots, n)$  and  $\mathbf{w} = (-\sum_{i=2}^{n-1} i, -\sum_{i=2}^{n-1} i, n+1, \dots, n+1)$ . In this case,  $S_\pi = 0$  if and only if  $v_{\pi(1)} + v_{\pi(2)} = n+1$ .

The proof of Theorem 1.9 is quite involved and relies on tools from algebraic combinatorics. Roughly speaking, if  $\mathbf{v}$  has distinct coordinates and  $S_\pi = x$ , then the set of such permutations  $\pi$  forms an antichain (in a suitable weakening of the Bruhat order on  $S_n$ ). This antichain can be identified with a disjoint union of Bruhat orders on  $S_n/S_\alpha$  for certain parabolic subgroups  $S_\alpha$ . These posets have the Sperner property, which implies that their size is bounded by the largest rank of  $S_n/S_\alpha$ . These ranks correspond to coefficients of the  $q$ -multinomial coefficient  $\binom{n}{\alpha}_q$ , and Theorem 1.9 follows from appropriate bounds on those coefficients.

While Theorem 1.9 is elegant—being optimal and valid for all  $n$ —the above methods do not appear to extend easily to more general settings where additional structure is imposed on  $\mathbf{v}$  and  $\mathbf{w}$ . As observed by

Alon *et al.* in [2], if both the  $v_i$  and the  $w_i$  are distinct, then  $\mathbb{P}(S_\pi = x)$  must lie between  $n^{-3/2}$  and  $n^{-5/2}$ . A sharp bound in this regime would serve as a permutation-space analogue of the Erdős–Moser result in the product-space setting. However, the techniques of [2] and [42] do not resolve this problem. We will address it in Section 1.4.

**1.2.2. An inverse theorem.** One of the main results of our paper is the following analogue of Theorem 1.6, providing a characterization of those vectors  $\mathbf{w}$  and  $\mathbf{v}$  for which  $S_\pi$  admits polynomially large concentration.

**Theorem 1.10** (Inverse result for permutation sums). *Let  $C > 0$  and  $\varepsilon \in (0, 1)$  be constants. Assume that*

$$\rho := \sup_x \mathbb{P}_\pi \left( \sum_{i=1}^n w_i v_{\pi(i)} = x \right) \geq n^{-C}.$$

*Then there exists a proper symmetric GAP  $Q$  of rank  $r = O_{C,\varepsilon}(1)$  and size  $O_\varepsilon(\rho^{-1}n^{-r/2})$  that contains  $(w_i - w_j)(v_k - v_l)$  for at least  $(1 - \varepsilon)n^4$  quadruples  $(i, j, k, l)$ .*

The bound is sharp; we refer the reader to Lemma 3.2 for a proof. In Section 1.4, we will use this theorem to derive and refine various *forward* results. In particular, we will resolve the question posed by Alon *et al.* discussed in the previous subsection.

**1.2.3. A more general setting with two dimensional arrays.** Given an  $n \times n$  array (matrix) with real entries  $(a_{ij})_{1 \leq i,j \leq n}$ , define the random sum

$$S_\pi = \sum_{i=1}^n a_{i\pi(i)},$$

where  $\pi$  is a uniformly random permutation.

Such sums are referred to as *random combinatorial sums* in probability theory. The behavior of this sum, including CLT, has been studied by many authors [6, 7, 8, 9, 18, 44]. However, as far as we know, no anti-concentration result has been proved. We can generalize Theorem 1.10 as follows

**Theorem 1.11** (Inverse result for 2D arrays). *Let  $C > 0$  and  $0 < \varepsilon < 1$  be constants. Let  $(a_{ij})_{1 \leq i,j \leq n}$  be an  $n \times n$  array of real-valued entries. Assume that*

$$\rho := \sup_x \mathbb{P}_\pi \left( \sum_i a_{i\pi(i)} = x \right) \geq n^{-C}.$$

*Then there exists a proper symmetric GAP  $Q$  of rank  $r = O_{C,\varepsilon}(1)$  and size  $O_\varepsilon(\rho^{-1}n^{-r/2})$  that contains  $a_{ik} - a_{jk} - a_{il} + a_{jl}$  for at least  $(1 - \varepsilon)n^4$  quadruples  $(i, j, k, l)$ .*

We also refer the reader to Remark 3.1 for a more detailed discussion of the implications of these structural conclusions. Theorem 1.10 corresponds to the special case  $a_{ij} = w_i v_j$ .

**1.3. The space of random permutations: continuous setting.** In the continuous setting, we study events of the form  $S_\pi \in I$  for a small interval  $I$ . In this context, it is more natural to assume that  $\|\mathbf{v}\|_\infty = O(1)$ . We will often write such events as

$$|S_\pi - L| \leq \delta,$$

where  $L$  is the center of the interval and  $\delta$  its radius. In probability theory, bounds for events of this type are commonly referred to as *small-ball probabilities*. It is clear that the continuous problem is strictly harder, as it contains the discrete problem as a special case (one can shrink the interval to a single point).

In the product-space setting, this problem has been studied extensively, with early foundational results due to Rogozin [46], Kolmogorov [28], and Halász [17]. There have also been many recent developments, especially in the inverse direction; see, for instance, [39, 47, 58] and the survey [40].

For  $S_\pi$ , CLT results and Berry–Esseen–type estimates have been investigated beginning with the classical works of Wald–Wolfowitz [41, 62] and Hoeffding [18] in the early 1950s. More recent approaches based on the Lindeberg exchange method or Stein’s method can be found in [1, 6, 7, 8, 44]. We refer the reader to [9] and the references therein for further contributions concerning this important statistic. The best anti-concentration bound obtainable from these classical approaches is of order  $O(n^{-1/2})$  (independent of the length of the interval), arising from the rate of convergence in the CLT.

Although our methods have the potential to work under very general conditions on  $\mathbf{w}$  and  $\mathbf{v}$  (see, for instance, Theorem 1.22), in what follows we restrict our attention to one of the most natural choices for  $\mathbf{v}$ , namely sequences arising from polynomials.

**1.3.1. A starting point: the linear case**  $v_i = i/n$ . Our starting point is the following result of Söze [50, Lemma 4], in which he studied  $S_\pi$  from (2) for the special choice of  $\mathbf{v}$  given by  $v_i = i/n$ .

**Theorem 1.12.** *Assume that  $\sum_i w_i = 0$  and  $\sum_i w_i^2 = 1$ . Then for every  $L \in \mathbb{R}$ ,*

$$\mathbb{P}\left(|S_\pi - L| \leq \frac{1}{n}\right) = O\left(\frac{1}{n} e^{-\Theta(|L|)}\right).$$

An interesting feature of this theorem is the appearance of the parameter  $L$  in the bound, which implies that  $S_\pi$  exhibits exponential decay. Söze [50] conjectured a sharper estimate of order  $O(n^{-1}e^{-\Theta(L^2)})$ , corresponding to sub-gaussian decay. Notice that once  $L$  appears on the right-hand side, the magnitude of the  $v_i$  becomes relevant.

The proof in [50] is clever but rather involved. Roughly speaking, the author compares the sum  $\sum_i w_i v_i$  with  $\sum_i w_i u_i$ , where the  $u_i$  are i.i.d. uniformly distributed on  $(0, 1)$ , and then exploits certain ad hoc unimodality properties of the resulting sum. Nonetheless, the resulting bound is not optimal.

**Problem 1.13.** *Can one achieve a sub-gaussian bound in Theorem 1.12?*

Other natural questions include weakening the strong restriction  $\mathbf{v} = (1, \dots, n)/n$  and treating scales smaller than  $1/n$ . We will achieve these goals under a modest assumption on  $\mathbf{w}$ . Namely, throughout what follows, we assume the following.

**Condition 1.14** (Non-degeneracy). *We say that a sequence  $w_1, \dots, w_n$  satisfying*

$$\sum_{i=1}^n w_i = 0 \quad \text{and} \quad \sum_{i=1}^n w_i^2 = 1$$

*is non-degenerate if*

$$|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}} \tag{4}$$

*for all distinct  $i, j$  and for some constant  $A$ .*

Roughly speaking, this condition corresponds to  $\mathbf{w}$  being a unit vector orthogonal to  $\mathbf{1}$  and satisfying  $\|\mathbf{w}\|_\infty \ll 1/\sqrt{\log n}$ .

**Theorem 1.15** (New result at scale  $1/n$ ). *Let  $\delta > 0$  be given. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider a sequence  $(v_1, \dots, v_n)$  that is partially specified by*

$$v_i = i/n \quad \text{for all } i \in I.$$

*Then, for every  $L \in \mathbb{R}$ , we have the uniform bound*

$$\mathbb{P}\left(|S_\pi - L| \leq \frac{1}{n}\right) = O_A\left(\frac{1}{n}\right). \quad (5)$$

*If, in addition, there exists a constant  $\tilde{B} > 0$  such that  $|v_i| \leq \tilde{B}$  for all  $i \in [n]$ , then we obtain the sub-gaussian bound*

$$\mathbb{P}\left(|S_\pi - L| \leq \frac{1}{n}\right) = O\left(\frac{1}{n} e^{-\Theta(L^2)}\right). \quad (6)$$

*Here, the implied constants depend only on  $A$  and  $\tilde{B}$ .*

**Corollary 1.16.** *The answer to Problem 1.13 is affirmative for any vector  $\mathbf{w}$  satisfying Condition 1.14.*

The next theorem allows us to treat the smaller scale  $n^{-3/2}$  under the additional assumption that most of the coefficients  $w_i$  are not squeezed into a very small interval. We refer the reader to Remark 4.3 for a discussion of the sharpness of this assumption.

**Theorem 1.17** (New treatment at scale  $n^{-3/2}$ ). *Let  $0 < \varepsilon < 1/2$  and  $\delta > 0$  be given. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . Furthermore, assume that no interval of length  $\varepsilon/\sqrt{n}$  contains more than  $(1 - \varepsilon)n$  of the values  $w_i$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider a sequence  $(v_1, \dots, v_n)$  that is partially specified by*

$$v_i = i/n \quad \text{for all } i \in I.$$

*Then, for every  $L \in \mathbb{R}$ , we have the uniform bound*

$$\mathbb{P}\left(|S_\pi - L| \leq \frac{1}{n^{3/2}}\right) = O_A\left(\frac{1}{n^{3/2}}\right). \quad (7)$$

*If, in addition, there exists a constant  $\tilde{B} > 0$  such that  $|v_i| \leq \tilde{B}$  for all  $i \in [n]$ , then we obtain the sub-gaussian bound*

$$\mathbb{P}\left(|S_\pi - L| \leq \frac{1}{n^{3/2-\varepsilon}}\right) = O\left(\frac{1}{n^{3/2-\varepsilon}} e^{-\Theta(L^2)}\right). \quad (8)$$

*Here, the implied constants depend only on  $A$  and  $\tilde{B}$ .*

This result may be viewed as a continuous analogue of Theorem 1.23. We emphasize that the condition excluding intervals of length  $1/\sqrt{n}$  that contain most of the  $w_i$  is essential for obtaining small-ball estimates at the  $n^{-3/2}$  scale. In the  $L$ -dependent bound (8), we assume the slightly larger radius  $n^{-3/2+\varepsilon}$  purely for technical convenience; see our treatment of the “very large  $|t|$ ” regime in the proof of (8) in Section 4.

Moreover, Theorem 4.4 shows that even finer approximations—down to the scale  $n^{-5/2+o(1)}$ —are possible under stronger assumptions on the coefficients  $w_i$ .

Finally, we remark that Theorem 1.15 may still hold without Condition 1.14. However, for Theorems 1.17 and 4.4, additional assumptions (of the type imposed above) are necessary, since these results fail dramatically when only a few of the  $w_i$  are nonzero.

**1.3.2. More general conditions on  $v_i$ .** In this subsection, we generalize the above theorems by allowing the coefficients  $v_i$  to depend polynomially on  $i$ .

**Theorem 1.18** (Treatment at scale  $1/n$ ). *Let  $d \geq 2$  be a fixed integer, and let  $\delta > 0$ ,  $b \neq 0$ , and  $B > 0$  be constants. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider a sequence  $(v_1, \dots, v_n)$  that is partially specified by*

$$v_i = \frac{P_d(i)}{n^d} \quad \text{for all } i \in I,$$

where  $P_d(i)$  is a real polynomial of degree  $d$  with fixed leading coefficient  $b$ , and whose remaining coefficients are allowed to depend on  $n$ , subject to the bound

$$|v_i| \leq B \quad \text{for all } i \in I.$$

Then, for any  $L \in \mathbb{R}$ , we have the uniform estimate

$$\mathbb{P}\left(\left|S_\pi - L\right| \leq \frac{1}{n}\right) = O_A\left(\frac{1}{n}\right). \quad (9)$$

If, in addition, there exists a constant  $\tilde{B} > 0$  such that  $|v_i| \leq \tilde{B}$  for all  $i \in [n]$ , then

$$\mathbb{P}\left(\left|S_\pi - L\right| \leq \frac{1}{n}\right) = O\left(\frac{1}{n}e^{-\Theta(L^2)}\right). \quad (10)$$

Here, the implied constants depend on  $A, B$  and  $\tilde{B}$ .

It is also possible to treat the next scale  $n^{-3/2}$  in this polynomial setting. However, the argument becomes significantly more involved, and we do not pursue this direction here.

**1.3.3. Joint distributions.** We now turn to the more difficult problem of studying joint distributions. Specifically, we consider three vectors  $\mathbf{w}$ ,  $\mathbf{v}$ , and  $\mathbf{v}'$ , and the event

$$\left\{\left|S_\pi(\mathbf{w}, \mathbf{v}) - L_1\right| \leq \frac{1}{n}\right\} \wedge \left\{\left|S_\pi(\mathbf{w}, \mathbf{v}') - L_2\right| \leq \frac{1}{n}\right\}.$$

**Theorem 1.19** (Joint distribution). *Let  $d \geq 2$  be a fixed integer, and let  $\delta > 0$ ,  $b \neq 0$ ,  $c \neq 0$ , and  $B > 0$  be given. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider the sequences  $(v_1, \dots, v_n)$  and  $(v'_1, \dots, v'_n)$  partially specified by*

$$v_i = \frac{P_d(i)}{n^d} \quad \text{and} \quad v'_i = \frac{P_{d-1}(i)}{n^{d-1}} \quad \text{for all } i \in I,$$

where  $P_d(i)$  and  $P_{d-1}(i)$  are real polynomials of degrees  $d$  and  $d-1$ , respectively, with fixed leading coefficients  $b$  and  $c$ . The remaining coefficients may depend on  $n$ , subject to the bound

$$|v_i|, |v'_i| \leq B \quad \text{for all } i \in I.$$

Then, for any  $L_1, L_2 \in \mathbb{R}$ , we have

$$\mathbb{P}\left(\left|S_\pi(\mathbf{w}, \mathbf{v}) - L_1\right| \leq \frac{1}{n} \wedge \left|S_\pi(\mathbf{w}, \mathbf{v}') - L_2\right| \leq \frac{1}{n}\right) = O\left(\frac{1}{n^2}\right). \quad (11)$$

If, in addition, there exists a constant  $\tilde{B} > 0$  such that  $|v_i|, |v'_i| \leq \tilde{B}$  for all  $i \in [n]$ , then

$$\mathbb{P}\left(|S_\pi(\mathbf{w}, \mathbf{v}) - L_1| \leq \frac{1}{n} \wedge |S_\pi(\mathbf{w}, \mathbf{v}') - L_2| \leq \frac{1}{n}\right) = O\left(\frac{1}{n^2} e^{-\Theta(L_1^2 + L_2^2)}\right). \quad (12)$$

Here, the implied constants depend on  $A, B$  and  $\tilde{B}$ .

It may be possible to extend our approach to sequences of polynomials of non-consecutive degrees; however, we do not pursue this direction in the present paper. We note that the weaker bound

$$O\left(\frac{1}{n} e^{-\Theta(L_1^2 + L_2^2)}\right),$$

involving  $O(1/n)$  rather than  $O(1/n^2)$ , follows immediately from the one-dimensional estimates. We also refer the reader to Theorem 6.6 for an application of the above result comparing the quantities  $S_\pi(\mathbf{w}, \mathbf{v})$  and  $S_\pi(\mathbf{w}, \mathbf{v}')$ .

**1.3.4. An inverse theorem via discretization.** First, one can obtain an inverse theorem in the continuous setting via a simple discretization argument. For simplicity, assume that  $\|\mathbf{w}\|_\infty = \|\mathbf{v}\|_\infty = 1$ . Fix a parameter  $\alpha > 0$  and round each  $w_i$  and  $v_i$  to the nearest integer multiple of  $\alpha$ ; denote the resulting vectors by  $\mathbf{w}'$  and  $\mathbf{v}'$ , respectively. This rounding procedure changes the value of  $S_\pi$  by at most  $3n\alpha$ . Moreover, the new sum  $S_\pi(\mathbf{w}', \mathbf{v}')$  takes values in integer multiples of  $\alpha^2$ .

If  $S_\pi$  lies in an interval of length  $2\delta$ , then  $S_\pi(\mathbf{w}', \mathbf{v}')$  must belong to a discrete set  $D$  of size at most  $m := \left\lceil \frac{1}{\alpha^2} (2\delta + 3n\alpha) \right\rceil$ . Thus, if the (continuous) anti-concentration probability is  $\rho$ , then for some  $x \in D$  we have  $\mathbb{P}(S_\pi(\mathbf{w}', \mathbf{v}') = x) \geq m^{-1}\rho$ , placing us in a position to apply Theorem 1.10.

**Theorem 1.20** (Inverse result for permutation sums: continuous setting). *Let  $\mathbf{w}, \mathbf{v}$  be unit vectors. Let  $C, C' > 0$  and  $\varepsilon \in (0, 1)$  be constants. Assume that for some  $L \in \mathbb{R}$  and  $\delta \leq 1$ ,*

$$\rho := \mathbb{P}(|S_\pi - L| \leq \delta) \geq n^{-C}.$$

*For any  $\alpha \geq n^{-C'}$ , there exists a proper symmetric GAP  $Q$  of rank  $r_0 = O_{C, C', \varepsilon}(1)$  and size  $O_\varepsilon(m\rho^{-1}n^{-r_0/2})$  such that for at least  $(1 - \varepsilon)n^4$  quadruples  $(i, j, k, l)$ , the quantity  $(w_i - w_j)(v_k - v_l)$  is within distance at most  $\alpha$  of a point in  $Q$ .*

Next, we introduce a notion—closely related to the Least Common Denominator (LCD) concept of Rudelson and Vershynin [47]—that captures small-ball probabilities rather efficiently.

**Definition 1.21.** Let  $\kappa \geq n^{3/2}$  and  $0 < \gamma < 1$ . The *Essential Least Common Divisor* of a pair of vectors  $\mathbf{w}, \mathbf{v} \in \mathbb{R}^n$  is defined by

$$\text{LCD}_{\gamma, \kappa}(\mathbf{w}, \mathbf{v}) = \inf \left\{ D > 0 : \text{dist}(D\mathbf{u}, \mathbb{Z}^{n^4}) < \min\{\gamma D\|\mathbf{u}\|_2, \kappa\} \right\},$$

where  $\mathbf{u} \in \mathbb{R}^{n^4}$  is the vector whose  $(i, j, k, l)$ -th coordinate is

$$(v_i - v_j)(w_k - w_l), \quad 1 \leq i, j, k, l \leq n.$$

**Theorem 1.22.** [60, Theorem 3.2] *Under the notation of Definition 1.21, assume that  $\|\mathbf{u}\|_2 \geq n^{3/2}$ . Then, for any  $\delta \geq 1/\text{LCD}_{\gamma, \kappa}(\mathbf{w}, \mathbf{v})$ , we have*

$$\sup_{x \in \mathbb{R}} \mathbb{P}(|S_\pi - x| \leq \delta) \leq C \left( \frac{\delta}{\gamma} + e^{-\kappa^2/2n^3} \right),$$

for some absolute constant  $C$ .

We will include a proof of this result in the appendix for the reader's convenience.

**1.4. Applications.** In this subsection, we apply the theorems from the previous two sections to derive several new forward bounds in the discrete setting, as well as applications to the critical points of random polynomials.

**1.4.1. Forward theorems.** Our first corollary improves Theorems 1.7 and 1.8 under the additional assumption that the multiplicity of any value among the  $w_i$  is not too close to  $n$ .

**Corollary 1.23.** *Let  $0 < c < 1$  be a constant. Suppose that*

$$\sup_y \#\{i : w_i = y\} \leq cn$$

*and that the  $v_i$  are all distinct. Then*

$$\sup_x \mathbb{P}(S_\pi = x) = O\left(\frac{1}{n^{3/2}}\right),$$

*where the implied constant may depend on  $c$ .*

Next, we address a problem raised in [2] and discussed in Subsection 1.2.1. We show that if both the  $w_i$  and the  $v_j$  are distinct, then the optimal decay rate is  $n^{-5/2}$ , up to a logarithmic factor. This result may be viewed as an analogue of Theorem 1.2 in the product-space setting.

**Corollary 1.24.** *If all the  $w_i$  are distinct and all the  $v_j$  are distinct, then*

$$\sup_x \mathbb{P}(S_\pi = x) = O\left(\frac{\log n}{n^{5/2}}\right).$$

Note that we allow the possibility that  $w_i = v_j$  for some  $i, j$ . In particular, taking  $w_i = v_i = i$  yields a bound of order  $\Theta(n^{-5/2})$ . We will derive these results using Theorem 1.10 in Section 3.

We also observe that the continuous theorems can be used to obtain sharper bounds in the discrete setting. For instance, the following result is a direct corollary of Theorem 1.15.

**Corollary 1.25.** *Under the assumptions of Theorem 1.15, we have*

$$\mathbb{P}(S_\pi = x) = O\left(\frac{1}{n} e^{-\Theta(x^2)}\right). \quad (13)$$

**1.4.2. Critical points of random polynomials.** A random polynomial is a function of the form

$$P(x) = \sum_{i=0}^n \xi_i x^i,$$

where the  $\xi_i$  are random variables. This is a central subject in both probability theory and analysis, with a long and rich history beginning with the foundational works of Littlewood–Offord and Kac in the 1940s. One of the main questions in the theory concerns the number and distribution of the real roots and critical points of  $P$ .

Let us first discuss the most basic class of random polynomials, namely the *Kac polynomials*, where the  $\xi_i$  are i.i.d. copies of a random variable  $\xi$  with mean zero and unit variance. Using his celebrated formula, Kac showed that when  $\xi \sim N(0, 1)$ , the expected number of real roots satisfies

$$\mathbb{E}N_{\mathbb{R}}(P) = \left(\frac{2}{\pi} + o(1)\right) \log n. \quad (14)$$

It took more than a decade until Erdős and Offord extended this result to the case where  $\xi$  is Rademacher (taking values  $\pm 1$  with probability  $1/2$ ), using completely different methods. About ten years later, Ibragimov and Maslova [24] showed that (14) holds for any  $\xi$  with zero mean and unit variance.

The problem of counting critical points is even more delicate. Observe that for a differentiable function  $F$ , between any two consecutive real roots of  $F$  there must be a real root of  $F'$ . Consequently, for any fixed  $d$ ,

$$\mathbb{E}N_{\mathbb{R}}(P^{(d)}) \geq \left(\frac{2}{\pi} + o(1)\right) \log n.$$

However, equality does *not* hold. Maslova [34] famously proved that for any fixed  $d$ , the Kac polynomial satisfies

$$\mathbb{E}N_{\mathbb{R}}(P^{(d)}) = \frac{1 + \sqrt{1 + 2d} + o(1)}{\pi} \log n. \quad (15)$$

Far less is known about random polynomials with dependent coefficients. In fact, the only available results appear to be [49, 50] and [3], which treat models in which the coefficients are exchangeable or weakly stationary. In this section, we focus on the family of random polynomials with exchangeable coefficients introduced in [49, 50].

Given a real vector  $\mathbf{w} = (w_1, \dots, w_n)$ , we consider the random polynomial

$$P_{\pi}(x) = \sum_{i=1}^n w_{\pi(i)} x^i,$$

where  $\pi$  is a uniformly random permutation. We start the index at  $i = 1$  to be consistent with our convention that  $\mathbf{w}$  is a vector of length  $n$ . Obviously, the same results hold for  $P_{\pi}(x) = \sum_{i=0}^n w_{\pi(i)} x^i$ .

Assuming  $\mathbf{w} \neq 0$ , Söze [50, Theorem 1] proved that the expected number of *nonzero* real roots  $N_{\mathbb{R}}^*(P_{\pi})$  satisfies

$$\mathbb{E}N_{\mathbb{R}}^*(P_{\pi}) = O(\log n).$$

It is natural to conjecture that the same bound holds for the number of nonzero critical points of  $P_{\pi}$ . Unfortunately, the approach in [50] does not extend to derivatives, since exchangeability breaks down for the sequence  $(i w_{\pi(i)})$ . In this section, using the new anti-concentration results developed in this paper, we answer this question affirmatively under some additional (but natural) conditions on the weights  $w_i$ .

Let<sup>1</sup>

$$\bar{\mathbf{w}} = \frac{1}{n} \sum_{i=1}^n w_i, \quad \sigma(\mathbf{w}) = \sqrt{\sum_{i=1}^n (w_i - \bar{\mathbf{w}})^2}.$$

The following condition is analogous to Condition 1.14, but is invariant under shifts and rescaling.

---

<sup>1</sup>Conceptually, it would be more natural to define  $\sigma(\mathbf{w}) = \sqrt{\frac{1}{n} \sum_{i=1}^n (w_i - \bar{\mathbf{w}})^2}$ . However, we retain the present normalization to remain consistent with the literature.

**Condition 1.26** (Non-degeneracy:  $K$ -balanced). *Let  $K > 1$ . For each  $k \in \mathbb{Z}^+$ , define*

$$M_k(\mathbf{w}) := \frac{1}{n} \sum_{i=1}^n (w_i - \bar{w})^k.$$

We say that  $\mathbf{w} = (w_1, \dots, w_n)$  is  $K$ -balanced if

$$M_4(\mathbf{w}) \leq K M_2(\mathbf{w})^2.$$

Equivalently, the rescaled squares  $X_i := n(w_i - \bar{w})^2 / \sigma(\mathbf{w})^2$  satisfy

$$\frac{1}{n} \sum_{i=1}^n X_i^2 \leq K.$$

By the Cauchy–Schwarz inequality we always have  $M_2(\mathbf{w})^2 \leq M_4(\mathbf{w})$  (and  $\sum_{i=1}^n X_i^2 / n \geq 1$ ).

**Example 1.27.** One simple example is when  $|w_i| = 1$  for all  $i$  and  $|\sum_{i=1}^n w_i| \leq (1 - \varepsilon)n$  for some constant  $\varepsilon > 0$ ; in this case,  $\mathbf{w}$  is  $K$ -balanced for some  $K = K(\varepsilon)$ . Another family of examples is given by vectors of the form  $w_i = a + t b_i$ , where  $a \in \mathbb{R}$ ,  $t \neq 0$ , and  $b_1, \dots, b_n \in \{0, \dots, n\}$  have maximal multiplicity at most  $0.99n$ . This includes, for instance,  $\mathbf{w} = (a, a+t, \dots, a+nt)$  or  $\mathbf{w} = (\underbrace{a, \dots, a}_{(1-\delta)n}, \underbrace{a+t, \dots, a+t}_{\delta n})$ .

**Theorem 1.28.** Assume that  $\mathbf{w}$  satisfies Condition 1.26. Then for any nonnegative integer  $d$ ,

$$\mathbb{E}N_{\mathbb{R}}(P_{\pi}^{(d)}) = O_{K,d}(\log n).$$

Finally, let  $P_{\text{Rad},k}$  denote a Kac polynomial with Rademacher coefficients, conditioned on  $\sum_{i=0}^n \xi_i = k$ , where  $-(1 - \varepsilon)n \leq k \leq (1 - \varepsilon)n$ . For example,  $P_{\text{Rad},0}$  has the uniform distribution over polynomials with  $\pm 1$  coefficients having exactly half of the coefficients equal to 1. Theorem 1.28 implies the following.

**Corollary 1.29** (Critical points of conditional Kac polynomials). *For any nonnegative integer  $d$ ,*

$$\mathbb{E}N_{\mathbb{R}}(P_{\text{Rad},k}^{(d)}) = O_{d,\varepsilon}(\log n).$$

**1.5. Methods and highlights of our results.** To summarize, the highlights of our note include:

- A nearly optimal inverse result characterizing  $a_{ij}$  when  $\sup_x \mathbb{P}(S_{\pi} = x)$  is polynomially large. This result is new and quickly yields several interesting corollaries, such as Theorems 1.23 and 1.24. It also leads to a new conclusion in the setting of the classical inverse result (Theorem 1.6): the support of  $\xi$  must possess additional structure. In the proof of Theorem 1.24, we also uncover an unexpected use of the product of differences in additive combinatorics.
- The establishment of very fine small-ball estimates  $\mathbb{P}(|S_{\pi} - x| < \delta)$  even when  $\delta = o(1/\sqrt{n})$ —thus breaking the Berry–Esseen barrier—for various special cases where  $(a_{ij}) = (w_i v_j)_{1 \leq i,j \leq n}$ . Our result confirms a heuristic from [50] but also extends far beyond the  $O(1/n)$  scale, with optimal decay in the location parameter  $L$ . This is a new aspect compared to most small-ball estimates in the literature, which usually do not account for  $L$ .
- A further highlight of our work is the study of joint distributions of sums induced by  $\pi$  (Theorem 1.19), as well as a comparison between the random variables in Theorem 6.6.

- Although our inverse-type Weyl estimates (e.g., Lemmas 2.6 and 2.7 to be mentioned later) are not entirely new, it is noteworthy that such estimates are required in our analysis of the decay of characteristic functions.
- Anticipation that our results will lead to numerous interesting applications. As a demonstration, we show that the number of critical points of certain random polynomials is of logarithmic order—a new result we believe to be highly nontrivial.

**1.6. Notation.** Throughout this paper, we regard  $n$  as an asymptotic parameter tending to infinity (in particular, we will implicitly assume that  $n$  is larger than any fixed constant, as our claims are all trivial for fixed  $n$ ), and we allow all mathematical objects in the paper to implicitly depend on  $n$  unless they are explicitly declared to be “fixed” or “constant.”

We write  $X = O(Y)$ ,  $X \ll Y$ , or  $Y \gg X$  to denote the claim that  $|X| \leq CY$  for some fixed constant  $C$ ; this constant  $C$  is allowed to depend on other fixed quantities. In the case that  $X \ll Y$  and  $Y \ll X$ , we write  $X \asymp Y$  or  $X = \Theta(Y)$ . We also use  $o(Y)$  to denote any quantity bounded in magnitude by  $c(n)Y$  for some function  $c(n)$  that tends to zero as  $n \rightarrow \infty$ . Again, the function  $c(\cdot)$  is permitted to depend on fixed quantities. We denote by  $\|x\|_{\mathbb{R}/\mathbb{Z}}$  the distance from a real number  $x$  to the nearest integer. For  $x \in \mathbb{R}$ , we set  $e(x) := e^{2\pi i x}$ . For a positive integer  $n$ , we write  $[n] = \{1, 2, \dots, n\}$ .

## 2. SOME LEMMAS

**2.1. Bound for the characteristic function.** Consider the sum  $S_\pi$  in its general form:

$$S_\pi = \sum_{k=1}^n a_{k\pi(k)}.$$

Its characteristic function  $\varphi(t)$  can be expressed as

$$\varphi(t) = \mathbb{E} e^{itS_\pi} = \frac{1}{n!} \sum_{\pi \in \mathfrak{S}_n} \prod_{k=1}^n e^{ita_{k\pi(k)}} = \frac{1}{n!} \text{perm}(M),$$

where  $\text{perm}(M)$  denotes the permanent of the  $n \times n$  matrix  $M$  with entries  $(e^{ita_{kl}})_{1 \leq k, l \leq n}$ .

By establishing upper bounds on the permanent of such matrices, Roos was able to prove the following result in [45, Theorem 1.4]:

**Theorem 2.1** (Roos). *Assume that  $S_\pi = \sum_{k=1}^n a_{k\pi(k)}$ . Let*

$$y_{i,j,k,l} = a_{ik} - a_{jk} - a_{il} + a_{jl}, \quad \text{for } i \neq j, k \neq l.$$

*Then the characteristic function  $\varphi(t) = \mathbb{E} e^{itS_\pi}$  satisfies:*

- For any permutation  $(l(1), \dots, l(n))$  of  $[n]$ , we have

$$|\varphi(t)| \leq \prod_{k=1}^d \left( \frac{1}{n(n-1)} \sum_{i \neq j} \cos^2 \left( \frac{ty_{i,j,l(2k-1),l(2k)}}{2} \right) \right)^{1/2}$$

- and

$$|\varphi(t)| \leq \left( \frac{1}{n^2(n-1)^2} \sum_{i \neq j, k \neq l} \cos^2 \left( \frac{ty_{i,j,k,l}}{2} \right) \right)^{d/2},$$

where  $d = \lfloor n/2 \rfloor$ .

In this paper we will apply the second conclusion. More precisely, in the proof of Theorem 1.11 we will apply the following corollary.

**Corollary 2.2.** *Assume that  $S_\pi = \sum_{k=1}^n a_{k\pi(k)}$ . Then its characteristic function  $\varphi(t) = \mathbb{E}e^{itS_\pi}$  satisfies*

$$|\varphi(2\pi t)| \leq \exp\left(-\frac{1}{2n^3} \sum_{1 \leq i,j,k,l \leq n} \|t(a_{ik} - a_{jk} - a_{il} + a_{jl})\|_{\mathbb{R}/\mathbb{Z}}^2\right).$$

*Proof.* By convexity, we have  $|\sin(\pi x)| \geq 2\|x\|_{\mathbb{R}/\mathbb{Z}}$  for all  $x \in \mathbb{R}$ . Hence  $\cos^2(\pi x) = 1 - \sin^2(\pi x) \leq 1 - 4\|x\|_{\mathbb{R}/\mathbb{Z}}^2$ . Applying this to Theorem 2.1, we obtain

$$\begin{aligned} |\varphi(2\pi t)| &\leq \left(\frac{1}{n^2(n-1)^2} \sum_{i \neq j, k \neq l} \cos^2(\pi t(a_{ik} - a_{jk} - a_{il} + a_{jl}))\right)^{\lfloor n/2 \rfloor / 2} \\ &\leq \left(1 - \frac{4}{n^2(n-1)^2} \sum_{i \neq j, k \neq l} \|t(a_{ik} - a_{jk} - a_{il} + a_{jl})\|_{\mathbb{R}/\mathbb{Z}}^2\right)^{n/8} \\ &\leq \exp\left(-\frac{1}{2n^3} \sum_{i \neq j, k \neq l} \|t(a_{ik} - a_{jk} - a_{il} + a_{jl})\|_{\mathbb{R}/\mathbb{Z}}^2\right) \\ &= \exp\left(-\frac{1}{2n^3} \sum_{1 \leq i,j,k,l \leq n} \|t(a_{ik} - a_{jk} - a_{il} + a_{jl})\|_{\mathbb{R}/\mathbb{Z}}^2\right), \end{aligned}$$

where in the third inequality we used the fact that  $1 - x \leq \exp(-x)$  for any  $0 \leq x \leq 1$ .  $\square$

**2.2. Large deviation result.** The following result, which follows from [1, Theorem 3.1] (or [4, Corollary 2.3]) via Talagrand's concentration inequality, will be crucial.

**Lemma 2.3.** *Let  $S_\pi = \sum_{i=1}^n w_i v_{\pi(i)}$ . Then, for some positive constant  $C_0$ , we have*

$$\mathbb{P}\left(|S_\pi - \mathbb{E}S_\pi| \geq \lambda \sigma(\mathbf{w}) \|\mathbf{v}\|_\infty\right) \leq C_0 e^{-C_0 \lambda^2}.$$

*In other words, the normalized random variable  $(S_\pi - \mathbb{E}S_\pi)/\sigma(\mathbf{w})\|\mathbf{v}\|_\infty$  is subgaussian.*

*As a consequence, if  $|v_i| \leq \tilde{B}$  for all  $i \in [n]$ , then*

$$\mathbb{P}\left(\left|\sum_{i=1}^n w_i v_{\pi(i)} - \left(\sum_{i=1}^n v_i\right) \bar{\mathbf{w}}\right| \geq \lambda \sigma(\mathbf{w})\right) \leq C_0 e^{-C_0 \lambda^2},$$

*where  $C_0$  is a positive constant depending only on  $\tilde{B}$ .*

An immediate consequence of the above lemma is that the moment generating function of the normalized variable

$$\bar{S} := \frac{S_\pi - \mathbb{E}S_\pi}{\sigma(\mathbf{w})\|\mathbf{v}\|_\infty}$$

is bounded (see, for example, [61, Proposition 2.6.1]):

$$m_{\bar{S}}(t) := \mathbb{E} e^{t\bar{S}} \leq C'_0 e^{C'_0 t^2}, \quad \text{for all } t \in \mathbb{R}, \tag{16}$$

for some constant  $C'_0 > 0$ .

**2.3. Diophantine Properties.** We begin with linear forms.

**Lemma 2.4** (Wrapping around for linear forms). *For any  $0 < \delta < 1$ , there exists a constant  $C > 0$  such that the following holds. Let  $I \subset \{-n, \dots, n\}$  with  $|I| \geq \delta n$ . Then, for  $\frac{C}{n} \leq |b| \leq \frac{1}{C}$  and for any  $b_0 \in \mathbb{R}$  we have*

$$\sum_{r \in I} \|br + b_0\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_{\delta} n.$$

The above immediately yields the following simple result.

**Corollary 2.5.** *Let  $0 < \delta < 1$  and  $I \subset \{-n, \dots, n\}$  with  $|I| \geq \delta n$ . For every constant  $C > 0$  sufficiently large in terms of  $\delta$ , and for all  $\frac{1}{Cn} \leq |b| \leq \frac{1}{C}$  and for any  $b_0 \in \mathbb{R}$  we have*

$$\sum_{r \in I} \|br + b_0\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n.$$

*Proof.* (of Corollary 2.5) For  $\frac{C}{n} \leq |b| \leq \frac{1}{C}$ , the result follows directly from Lemma 2.4. Now suppose  $\frac{1}{Cn} \leq |b| \leq \frac{C}{n}$ . Since  $|b|$  is too small in this range, we amplify it slightly. For  $k \in \mathbb{Z}^+$ , Cauchy-Schwarz gives

$$\|br + b_0\|_{\mathbb{R}/\mathbb{Z}}^2 \geq \frac{1}{k^2} \|k(br + b_0)\|_{\mathbb{R}/\mathbb{Z}}^2 = \frac{1}{k^2} \|(kb)r + (kb_0)\|_{\mathbb{R}/\mathbb{Z}}^2.$$

Taking  $k = \lceil C^2 \rceil$  and applying Lemma 2.4 completes the proof.  $\square$

Lemma 2.4 is a special case of a more general result concerning polynomial sequences, which we present below.

**Lemma 2.6** (Wrapping around for polynomial sequences). *Let  $\delta > 0$  and  $d \in \mathbb{Z}^+$  be given. There exists a constant  $C > 0$  such that the following holds. Let  $I \subset \{-n, \dots, n\}$  with  $|I| \geq \delta n$ . Then, for any  $\frac{C}{n} \leq |b| \leq \frac{n^{d-1}}{C}$ , we have*

$$\sum_{r \in I} \left\| \frac{br^d + b'r^{d-1} + \dots}{n^{d-1}} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_{\delta} n,$$

where  $b', b'', \dots \in \mathbb{R}$  are arbitrary.

To prove this result, we will use a very nice inverse-type Weyl estimate by Tao [54, Corollary 5], which is stated below (and proved in Section B for the reader's convenience) for positive density form (instead of full density form,  $I = \{-n, \dots, n\}$ , as in [54]).

**Lemma 2.7.** *Let  $I$  be a subset of  $\{-n, \dots, n\}$  with  $|I| \geq \delta n$  for some  $\delta > 0$ . Let  $P(k) = \sum_{i \leq d} \alpha_i k^i$  be a polynomial of degree at most  $d \geq 0$ , where  $\alpha_0, \dots, \alpha_d \in \mathbb{R}/\mathbb{Z}$ . If*

$$\frac{1}{n} \left| \sum_{k \in I} e(P(k)) \right| \geq \delta,$$

then there is a natural number  $q \ll_d \delta^{-O_d(1)}$  such that

$$\|q\alpha_i\|_{\mathbb{R}/\mathbb{Z}} \ll_d \delta^{-O_d(1)} n^{-i} \quad \text{for all } i = 0, \dots, d.$$

*Proof.* (of Lemma 2.6) Using the inequality  $|\sin(\pi x)| \leq 4\|x\|_{\mathbb{R}/\mathbb{Z}}^2$ , we obtain

$$\cos(2\pi x) = 1 - 2\sin^2(\pi x) \geq 1 - 32\|x\|_{\mathbb{R}/\mathbb{Z}}^2.$$

Suppose, for contradiction, that

$$\sum_{r \in I} \left\| \frac{br^d + b'r^{d-1} + \dots}{n^{d-1}} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \leq (\delta/64)n.$$

Then it follows that

$$\sum_{r \in I} \cos \left( 2\pi \frac{br^d + b'r^{d-1} + \dots}{n^{d-1}} \right) \geq |I| - (\delta/2)n \geq (\delta/2)n.$$

Thus

$$\frac{1}{n} \left| \sum_{r \in I} e \left( \frac{br^d + b'r^{d-1} + \dots}{n^{d-1}} \right) \right| \geq \frac{1}{n} (\delta/2)n \geq \delta/2.$$

By Lemma 2.7, there exists a positive integer  $q \leq \delta^{-O(1)}$  such that

$$\left\| q \cdot \frac{b}{n^{d-1}} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\delta^{-O(1)}}{n^d}.$$

On the other hand, since  $C/n \leq |b| \leq n^{d-1}/C$ , we have

$$\left\| q \cdot \frac{b}{n^{d-1}} \right\|_{\mathbb{R}/\mathbb{Z}} = \left| q \cdot \frac{b}{n^{d-1}} \right| > \frac{\delta^{-O(1)}}{n^d},$$

provided that  $C$  is sufficiently large in terms of  $\delta$  and  $d$ . This yields a contradiction.  $\square$

**2.4. Paper Organization.** The remainder of the paper is organized as follows. In Section 3, we prove the discrete cases using techniques from [39]. In Section 4, we prove the first continuous result, Theorem 1.15, by first addressing the uniform case with error  $O(1/n)$ , and then generalizing to the cases  $O(1/n^{3/2})$  and  $O(1/n^{5/2-o(1)})$ ; then addressing the  $L$ -dependent case in the same order, relying on our refined understanding of the characteristic function and its extension to the complex plane. In Section 5, we treat polynomial sequences. In Section 6, we address the most difficult case: proving Theorem 1.19 involving the two-dimensional case. We will do so by relying on techniques developed in both Section 4 and Section 5. Finally, in Section 8, we prove Theorem 1.28. This argument follows a standard sign-change bound (see also [50] and [4]), and leverages Theorem 1.19.

### 3. DISCRETE SETTINGS: PROOF OF THEOREM 1.11, THEOREM 1.23, AND THEOREM 1.24

In the forward direction of Theorem 1.11, that  $a_{ik} - a_{jk} - a_{il} + a_{jl} \in Q$  for all quadruples, we can easily see that for any  $\pi$  and  $\pi'$ , there is a series of  $O(n^2)$  transpositions that move from  $S_\pi = \sum_i a_{i\pi(i)}$  to  $S_{\pi'} = \sum_i a_{i\pi'(i)}$ , and hence

$$\sup_x \mathbb{P}_\pi(S_\pi = x) \geq n^{-O(1)}.$$

Thus our result claims the converse of this.

**Remark 3.1.** *In some situations, we can exploit a little further from the conclusions  $a_{ik} - a_{jk} - a_{il} + a_{jl} \in Q$  from Theorem 1.11. For instance if we assume that  $a_{ik} - a_{jk} - a_{il} + a_{jl} \in Q$ , where  $Q$  is a symmetric GAP, for all quadruples, then with  $\mathbf{r}_i$  and  $\mathbf{c}_j$ ,  $1 \leq i, j \leq n$  being the rows and columns of  $(a_{ij})_{1 \leq i, j \leq n}$*

(1) *assuming that  $k < l$ , as  $a_{ik} - a_{il} = a_{jk} - a_{jl}$  modulo  $Q$  for all  $i, j$ , we can write*

$$\mathbf{c}_l = \mathbf{c}_k + \boldsymbol{\alpha}_{k,l} + c_{k,l}(1, \dots, 1)^t,$$

where the entries of  $\alpha_{k,l}$  are in  $2Q$ , and  $c_{k,l} \in \mathbb{R}$ . As this is true for all  $(k,l)$ , we can write

$$\mathbf{c}_l = \mathbf{c}_1 + \left( \sum_{s=1}^{l-1} c_{s,s+1} \right) (1, \dots, 1)^t \pmod{2nQ}.$$

(2) Similarly,

$$\mathbf{r}_j = \mathbf{r}_i + \beta_{i,j} + r_{i,j} (1, \dots, 1)$$

where the entries of  $\beta_{i,j}$  are in  $2Q$  and hence

$$\mathbf{r}_j = \mathbf{r}_1 + \left( \sum_{t=1}^{j-1} r_{t,t+1} \right) (1, \dots, 1) \pmod{2nQ}.$$

(3) Putting together, there are  $2(n-1)$  real numbers  $r_{t,t+1}, c_{s,s+1}, 1 \leq s, t \leq n-1$  such that

$$a_{jl} = a_{11} + \sum_{t=1}^{j-1} r_{t,t+1} + \sum_{s=1}^{l-1} c_{s,s+1} \pmod{4nQ}.$$

In other words, there exist  $a'_{jl} \in 4nQ$  such that

$$a_{jl} = a_{11} + \sum_{t=1}^{j-1} r_{t,t+1} + \sum_{s=1}^{l-1} c_{s,s+1} + a'_{jl}.$$

**Lemma 3.2.** *The conclusion of Theorem 1.11 is optimal, in the sense that if  $Q$  is a proper symmetric GAP of rank  $r = O(1)$  and size  $O(\rho^{-1}n^{-r/2})$ , and  $a_{ik} - a_{jk} - a_{il} + a_{jl} \in Q$  for all quadruples, then*

$$\sup_x \mathbb{P}_\pi(S_\pi = x) \gg \rho.$$

*Proof.* Assume that  $Q$  has the form

$$Q = \left\{ \sum_{s=1}^r q_s g_s : |q_s| \leq N_s \right\}.$$

For  $1 \leq i, j \leq n$ , let  $a'_{ij} := a_{ij} - a_{1j} - a_{i1} + a_{11} \in Q$ . Write  $S_\pi((a'_{ij})) = \sum_i a'_{i\pi(i)}$  for a uniform permutation  $\pi$ . Then  $S_\pi((a'_{ij})) = S_\pi + c$  with  $c = na_{11} - \sum_{i=1}^n (a_{i1} + a_{1i})$ . Since  $c$  is independent of  $\pi$ ,

$$\sup_x \mathbb{P}_\pi(S_\pi((a'_{ij})) = x) = \sup_x \mathbb{P}_\pi(S_\pi = x).$$

Since  $a'_{ij} \in Q$ , we can write

$$a'_{ij} = \sum_{s=1}^r a_{ij;s} g_s, \text{ for some integers } |a_{ij;s}| \leq N_s$$

and such that

$$a_{ik;s} - a_{jk;s} - a_{il;s} + a_{jl;s} \in [-4N_s, 4N_s]. \quad (17)$$

Consider an array  $(b_{ij})$ , which plays the role of  $a_{ij;s}$  for each  $1 \leq s \leq r$ . Let

$$\tilde{b}_{ik} = b_{ik} - \frac{1}{n} \sum_{l=1}^n b_{il} - \frac{1}{n} \sum_{j=1}^n b_{jk} + \frac{1}{n^2} \sum_{j,l=1}^n a_{jl}.$$

Observe that

$$b_{ik} - b_{jk} - b_{il} + b_{jl} = \tilde{b}_{ik} - \tilde{b}_{jk} - \tilde{b}_{il} + \tilde{b}_{jl}.$$

Let  $S_\pi((b_{ij})) = \sum_i b_{i\pi(i)}$ , where  $\pi$  is a uniform permutation. We have  $\mathbb{E}S_\pi((b_{ij})) = (1/n) \sum_{ij} b_{ij}$ . It can also be shown that [16, formula (89)]

$$\text{Var } S_\pi((b_{ij})) = [1/4n^2(n-1)] \sum_{i \neq j; k \neq l} (b_{ik} - b_{jk} - b_{il} + b_{jl})^2. \quad (18)$$

So if we assume that  $b_{ik} - b_{jk} - b_{il} + b_{jl} \in [-N, N]$  then

$$\text{Var}(S_\pi((b_{ij}))) \leq nN^2.$$

It follows by Chebyshev that with probability at least  $1 - 16/C^2$ ,

$$|S_\pi((b_{ij})) - \mathbb{E}S_\pi((b_{ij}))| \in [-(C/4)\sqrt{n}N, (C/4)\sqrt{n}N]. \quad (19)$$

For each fixed  $1 \leq s \leq r$ , apply this bound to the sequence  $b_{ij} = a_{ij;s}$  from (17), and take the intersection, we see that there is an event  $\mathcal{E}$  (over the random permutation  $\pi$ ) with  $\mathbb{P}(\mathcal{E}) \geq 1 - 16r/C^2$  on which, simultaneously for all  $s$ ,

$$|S_\pi((a_{ij;s})) - \mu_s| \in [-C\sqrt{n}N_s, C\sqrt{n}N_s],$$

where  $\mu_s = \mathbb{E}S_\pi((a_{ij;s}))$ . Under this event  $\mathcal{E}$ , the original sum  $\sum_i a'_{i\pi(i)}$  belongs to the shifted GAP

$$\sum_i a'_{i\pi(i)} \in \left( [\mu_1 - C\sqrt{n}N_1, \mu_1 + C\sqrt{n}N_1] \cap \mathbb{Z} \right) g_1 + \cdots + \left( [\mu_r - C\sqrt{n}N_r, \mu_r + C\sqrt{n}N_r] \cap \mathbb{Z} \right) g_r.$$

By pigeonhole principle, there exists  $x$  from this GAP such that

$$\mathbb{P}(S_\pi(a'_{ij}) = x) \geq \frac{\mathbb{P}(\mathcal{E})}{(3C)^r n^{r/2} \prod N_i} \geq \rho,$$

with appropriate choices of the constants.  $\square$

We next turn to the proof of our inverse theorem by relying on the method of [39].

*Proof.* (of Theorem 1.11) The proof consists of several steps.

*Embedding.* The following theorem (see [56, Lemma 5.25], [39, Theorem 4.3]) allows us to assume that  $a_{ij}$  are elements of  $\mathbb{F}_p$  for some large prime  $p$ .

**Theorem 3.3.** *Let  $V$  be a finite subset of a torsion-free additive group  $G$ . Then, for any integer  $k$ , there is a map  $\phi : V \rightarrow \phi(V)$  into some finite subset  $\phi(V)$  of the integers  $\mathbb{Z}$  such that*

$$v_1 + \cdots + v_i = v'_1 + \cdots + v'_j \iff \phi(v_1) + \cdots + \phi(v_i) = \phi(v'_1) + \cdots + \phi(v'_j)$$

for all  $i, j \leq k$ . The same holds if we replace  $\mathbb{Z}$  by  $\mathbb{F}_p$ , provided  $p$  is sufficiently large, depending on  $V$ .

*Fourier analysis.* We view elements of  $\mathbb{F}_p$  as integers between 0 and  $p-1$ . Let  $S = \sum_{i=1}^n a_{i\pi(i)}$ , and suppose

$$\rho = \mathbb{P}(S = x)$$

for some  $x \in \mathbb{F}_p$ . Using the standard notation  $e_p(z) = \exp(2\pi iz/p)$ , we have

$$\rho = \mathbb{P}(S = x) = \mathbb{E} \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(t(S - x)) = \mathbb{E} \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(tS) e_p(-tx).$$

Denote by  $A$  the multiset  $\{a_{ik} - a_{jk} - a_{il} + a_{jl} : 1 \leq i, j, k, l \leq n\}$ . Then

$$\rho \leq \frac{1}{p} \sum_{t \in \mathbb{F}_p} |\mathbb{E} e_p(tS)| \leq \frac{1}{p} \sum_{t \in \mathbb{F}_p} \exp \left( -\frac{1}{2n^3} \sum_{a \in A} \left\| \frac{at}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^2 \right),$$

where the second inequality follows from Corollary 2.2.

*Level sets.* For  $m \in \mathbb{N}$ , define  $L_m := \{t \in \mathbb{F}_p : \sum_{a \in A} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 \in [4(m-1)n^3, 4mn^3]\}$ . Then

$$n^{-C} \leq \rho \leq \frac{1}{p} \sum_{t \in \mathbb{F}_p} \exp\left(-\frac{1}{2n^3} \sum_{a \in A} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2\right) \leq \frac{1}{p} + \frac{1}{p} \sum_{m \geq 1} \exp(-2(m-1))|L_m|.$$

Since  $\sum_{m \geq 1} \exp(-m) < 1$  and  $p \geq n^{2C}$ , there exists a level set  $L_m$  such that

$$|L_m| \exp(-m+2) \geq \rho p.$$

As  $\rho \geq n^{-C}$  and  $|L_m| \leq p$ , it follows that  $m = O(\log n)$ .

*Double counting and the triangle inequality.* We have

$$\sum_{a \in A} \sum_{t \in L_m} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 = \sum_{t \in L_m} \sum_{a \in A} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq (4mn^3)|L_m|.$$

Let  $n' = \varepsilon|A| = \varepsilon n^4$ . By averaging, at least a  $(1 - \varepsilon)$ -fraction of  $a \in A$  satisfy

$$\sum_{t \in L_m} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq \frac{4mn^3}{n'}|L_m|.$$

Denote this set by  $A'$ . We will show that  $A'$  is a dense subset of a proper GAP.

Applying the triangle inequality to the norm  $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ , we obtain, for any  $a \in lA'$ ,

$$\sum_{t \in L_m} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq l^2 \frac{4mn^3}{n'}|L_m|. \quad (20)$$

*Dual sets.* Define  $L_m^* := \{a \mid \sum_{t \in L_m} \|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2 \leq \frac{1}{40}|L_m|\}$ . We claim

$$|L_m^*| \leq \frac{8p}{|L_m|}. \quad (21)$$

Indeed, set  $T_a = \sum_{t \in L_m} \cos \frac{2\pi at}{p}$ . Using  $\cos 2\pi z \geq 1 - 20\|z\|_{\mathbb{R}/\mathbb{Z}}^2$ , we see that for  $a \in L_m^*$

$$T_a \geq \sum_{t \in L_m} (1 - 20\|\frac{at}{p}\|_{\mathbb{R}/\mathbb{Z}}^2) \geq \frac{1}{2}|L_m|.$$

On the other hand, since  $\sum_{a \in \mathbb{F}_p} \cos \frac{2\pi az}{p} = p\mathbf{1}_{z=0}$ ,

$$\sum_{a \in \mathbb{F}_p} T_a^2 \leq 2p|L_m|.$$

The bound (21) follows by averaging.

Set  $k = \sqrt{\frac{n'}{160mn^3}}$ . By (20), we have  $\bigcup_{l=1}^k lA' \subset L_m^*$ . Setting  $A'' = A' \cup \{0\}$ , this implies  $kA'' \subset L_m^* \cup \{0\}$ . Hence

$$|kA''| = O\left(\frac{p}{|L_m|}\right) = O(\rho^{-1}e^{-m+2}). \quad (22)$$

The ambient field  $\mathbb{F}_p$  is no longer important, so we may view the  $a_{ij}$  as integers. We now invoke the following long-range inverse theorem (see [39, Theorem 3.2]).

**Theorem 3.4.** *Let  $\gamma > 0$  be a constant. Assume that  $X$  is a subset of a torsion-free group such that  $0 \in X$  and  $|kX| \leq k^\gamma |X|$  for some integer  $k \geq 2$  that may depend on  $|X|$ . Then there is a proper symmetric GAP  $Q$  of rank  $r = O(\gamma)$  and cardinality  $O_\gamma(k^{-r}|kX|)$  such that  $X \subset Q$ .*

Since

$$k = \Omega\left(\sqrt{\frac{n}{m}}\right) = \Omega\left(\sqrt{\frac{n}{\log n}}\right), \quad \rho^{-1} \leq n^C \leq k^{2C+1},$$

(22) allows us to apply Theorem 3.4 with  $\gamma = 2C + 1$  and  $X$  the set of distinct elements of  $A''$  (note that  $kX = kA''$  for  $k \geq 2$ ). Hence  $X$  is contained in a proper symmetric GAP  $Q$  of rank  $r = O_{C,\varepsilon}(1)$  and size

$$O_{C,\varepsilon}(k^{-r}|kX|) = O_{C,\varepsilon}(k^{-r}|kA''|) = O_{C,\varepsilon}\left(\rho^{-1}e^{-m+2}\left(\sqrt{\frac{n}{m}}\right)^{-r}\right) = O_{C,\varepsilon}(\rho^{-1}n^{-r/2}),$$

which completes the proof.  $\square$

To complete the section we quickly deduce Theorem 1.23 and Theorem 1.24.

*Proof.* (of Theorem 1.23) Assume for contradiction that  $\rho := \sup_x \mathbb{P}\left(\sum_{i=1}^n w_i v_{\pi(i)} = x\right) \geq An^{-3/2}$  for some sufficiently large constant  $A$ . Set  $\varepsilon = .1$  and  $C = 3$ . By Theorem 1.11, there is a GAP  $Q$  of rank  $r$  and size  $O(\rho^{-1}n^{-r/2})$  that contains a  $(1 - \varepsilon)$ -portion of the set of quadruples  $\{(w_i - w_j)(v_k - v_l) : 1 \leq i, j, k, l \leq n\}$ . This set must have at least  $\Theta(n)$  (distinct) elements, because by assumption there are  $\Theta_c(n^2)$  pairs  $i, j$  where  $w_i - w_j \neq 0$ , and on average, each such pair  $(i, j)$  is associated with  $\Theta(n^2)$  pairs  $(k, l)$ . Among these pairs, we just chose  $\Theta(n)$  pairs of the form  $(k_0, l_1), \dots, (k_0, l_m)$ ,  $m = \Theta(n)$ . Since  $Q$  has rank at least 1, we have  $n \ll |Q| = O(\rho^{-1}n^{-1/2}) = O(n/A)$ , a contradiction if  $A$  is sufficiently large.  $\square$

*Proof.* (of Theorem 1.24) Let  $S$  be the set  $\{(w_i - w_j)(v_k - v_l)\}$  over a  $(1 - \varepsilon)$ -portion of the quadruples. We claim that  $S$  must have at least  $\Theta(n^2/\log n)$  elements. Since  $Q$  has rank at least 1, this would imply  $n^2 \log n \ll |Q| = O(\rho^{-1}n^{-1/2})$ , which yields  $\rho \ll n^{-5/2} \log n$ , as desired.

It remains to prove  $|S| \gg n^2/\log n$ . Let  $A = \{v_1, \dots, v_n, w_1, \dots, w_n\}$ . For  $x \in A - A$ , let  $r(x)$  denote the number of representations  $a - b = x$  with  $(a, b) \in A^2$ . By [5, Theorem 3]<sup>2</sup> we have

$$|A|^6 \log |A| \gg \sum_{xy=x'y'} r(x)r(x')r(y)r(y') = \sum_z \left| \sum_{xy=z} r(x)r(y) \right|^2.$$

Applying the Cauchy-Schwarz inequality gives

$$|A|^6 \log |A| \geq \frac{1}{|S|} \left( \sum_{xy \in S} r(x)r(y) \right)^2.$$

Moreover,  $\sum_{xy \in S} r(x)r(y)$  counts at least the number of selected quadruples, namely  $(1 - \varepsilon)n^4$ . Therefore,  $|S| \gg n^8/|A|^6 \log |A| = \Theta(n^2/\log n)$ , as claimed.  $\square$

---

<sup>2</sup>The statement in [5] is given for  $A \subset \mathbb{Z}$ , but the proof works verbatim for  $A \subset \mathbb{R}$ .

#### 4. CONTINUOUS SETTING: PROOF OF THEOREMS 1.15 AND 1.17

We will use the following simple fact.

**Fact 4.1.** *Let  $I \subset [n]$  with  $|I| \geq \delta n$  for some constant  $\delta > 0$ . Then, there exists  $\mathcal{R} \subset \{-n, \dots, n\}$  of size  $|\mathcal{R}| \gg_{\delta} n$  such that for every  $r \in \mathcal{R}$ , there are  $\gg_{\delta} n$  pairs  $x, y \in I$  with  $x - y = r$ .*

Throughout this section, let  $\mathcal{R} \subset \{-n, \dots, n\}$  be a set of size  $|\mathcal{R}| = \Theta_{\delta}(n)$ , as defined in Fact 4.1. Let  $C$  and  $A$  be positive constants, with  $C$  sufficiently large relative to  $\delta$  and  $\varepsilon$ , and  $A$  sufficiently large relative to  $C$ .

We will break down the proof of Theorem 1.15 into two parts, the uniform bound (5) and the  $L$ -dependent bound (6).

*Proof of (5) from Theorem 1.15.* Let

$$S = n \sum_i w_i v_{\pi(i)}, \quad \text{and} \quad X = S - Ln.$$

Using Esseen's estimate, we can write

$$\mathbb{P}(|X| \leq 1) \ll \left| \int_{|t| \leq 1} k(t) \varphi_X(t) dt \right| \ll \int_{|t| \leq 1} |\varphi_X(t)| dt, \quad (23)$$

where  $k(t) = 1_{[-1/2, 1/2]} * 1_{[-1/2, 1/2]}(t)$  (see for instance [40]), and  $\varphi_X(t)$  is the characteristic function of  $X = S - Ln$ :

$$\varphi_X(t) = \mathbb{E} e^{it(S - Ln)} = \mathbb{E} e^{itS} e^{-iLn} = \varphi_S(t) e^{-iLn}.$$

Thus,

$$|\varphi_X(t)| = |\mathbb{E} e^{itS}| = |\varphi_S(t)|.$$

We first note that by Corollary 2.2,

$$|\varphi_S(2\pi t)| \leq \exp \left\{ -\frac{1}{2n^3} \sum_{i,j,k,l} \|tn(w_i - w_j)(v_k - v_l)\|_{\mathbb{R}/\mathbb{Z}}^2 \right\}.$$

The exponent on the right-hand side can be bounded from below by

$$\frac{c_{\delta}}{n^2} \sum_{\substack{1 \leq i,j \leq n \\ r \in \mathcal{R}}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2,$$

and so

$$\mathbb{P}(|X| \leq 1) \ll \int_{|t| \leq 1} |\varphi_S(t)| dt \ll \int_{|t| \leq 1} \exp \left\{ -\frac{c_{\delta}}{n^2} \sum_{\substack{1 \leq i,j \leq n \\ r \in \mathcal{R}}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \right\} dt. \quad (24)$$

We will split the integral depending on whether  $|t| \leq (\sqrt{A \log n})/n$  or  $(\sqrt{A \log n})/n \leq |t| \leq 1$ .

**Large  $|t|$ .** Assume that

$$\frac{\sqrt{A \log n}}{n} \leq |t| \leq 1.$$

We first discard those  $(i, j)$  for which  $|w_i - w_j|$  is smaller than  $1/\sqrt{n}$ . Let

$$\mathcal{G} = \{(i, j) : |w_i - w_j| \geq 1/\sqrt{n}\}.$$

Since  $\sum_{1 \leq i, j \leq n} (w_i - w_j)^2 = 2n$ , we see that

$$n \leq \sum_{(i,j) \in \mathcal{G}} (w_i - w_j)^2 \leq 2n.$$

For  $0 \leq k \leq \log\left(\frac{\sqrt{n}}{A\sqrt{\log n}}\right) + 1$  (so that  $\frac{2^{k-1}}{\sqrt{n}} \leq \frac{1}{A\sqrt{\log n}}$  and  $\frac{2^k}{\sqrt{n}} \geq \frac{1}{\sqrt{n}}$ ), let  $\mathcal{G}_k$  be the set of pairs  $(i, j)$  such that

$$D_{k-1} := \frac{2^{k-1}}{\sqrt{n}} < |w_i - w_j| \leq \frac{2^k}{\sqrt{n}} =: D_k.$$

Then  $\mathcal{G} = \bigcup_k \mathcal{G}_k$  and

$$n \leq \sum_k D_k^2 |\mathcal{G}_k| \leq 8n.$$

Now for each fixed pair  $(i, j) \in \mathcal{G}_k$ , we consider the sum  $\sum_{r \in \mathcal{R}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2$ .

If  $|t|D_k \leq \frac{1}{Cn}$ , then  $|t(w_i - w_j)r| \leq \frac{1}{Cn}n = \frac{1}{C} < 1$ , so

$$\sum_{r \in \mathcal{R}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 = \sum_{r \in \mathcal{R}} |t(w_i - w_j)r|^2 \asymp_{\delta} t^2 n^3 D_k^2.$$

On the other hand, if  $|t|D_k > \frac{1}{Cn}$ , then  $\frac{1}{2Cn} < |t(w_i - w_j)| \leq \frac{1}{A\sqrt{\log n}} \leq \frac{1}{2C}$ , so by Corollary 2.5, we have

$$\sum_r \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n.$$

Thus, we obtain

$$\sum_{(i,j) \in \mathcal{G}, r \in \mathcal{R}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_{\delta,C} \sum_{k: |t|D_k \leq 1/(Cn)} t^2 n^3 D_k^2 |\mathcal{G}_k| + \sum_{k: |t|D_k > 1/(Cn)} n |\mathcal{G}_k|.$$

To further estimate the right-hand side, we divide into two cases.

**Case 1:**  $\sum_{k: |t| \leq 1/(CnD_k)} D_k^2 |\mathcal{G}_k| \geq (1/10)n$ .

Since  $t^2 \geq \frac{A \log n}{n^2}$ ,

$$\sum_{k: |t| \leq 1/(CnD_k)} t^2 n^3 D_k^2 |\mathcal{G}_k| \gg An^2 \log n.$$

**Case 2:**  $\sum_{k: |t| > 1/(CnD_k)} D_k^2 |\mathcal{G}_k| > (3/4 - 1/10)n$ .

Since  $D_k^2 \leq \frac{1}{A^2 \log n}$ , we get

$$\sum_{k: |t| > 1/(CnD_k)} n |\mathcal{G}_k| \gg A^2 n^2 \log n \gg An^2 \log n.$$

In both cases, we always have

$$\sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \gg_{\delta,C} An^2 \log n.$$

Therefore, assuming that  $A$  is sufficiently large relative to  $\delta$  and  $C$ , for  $\frac{\sqrt{A \log n}}{n} \leq |t| \leq 1$ , we have

$$\frac{c_\delta}{n^2} \sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \geq 2\sqrt{A} \log n, \quad |\varphi_S(t)| \leq n^{-2\sqrt{A}}. \quad (25)$$

**Small  $|t|$ .** It remains to consider

$$|t| \leq \frac{\sqrt{A \log n}}{n}.$$

Since  $|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}}$ , we have  $|t(w_i - w_j)r| \leq \frac{1}{\sqrt{A}} < 1$ , which implies  $\|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}} = |t(w_i - w_j)r|$ . Thus, we obtain

$$\frac{c_\delta}{n^2} \sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 = \frac{c_\delta}{n^2} \sum_{i,j,r} (t(w_i - w_j)r)^2 \asymp_{\delta} t^2 n^2.$$

Therefore,

$$\int_{|t| \leq (\sqrt{A \log n})/n} |\varphi_S(t)| dt \leq \int_{|t| \leq (\sqrt{A \log n})/n} \exp(-\Theta(t^2 n^2)) dt \ll \frac{1}{n} \int_{\mathbb{R}} \exp(-\Theta(x^2)) dx \ll \frac{1}{n}.$$

□

Next, we modify the above approach to deal with the extra factor  $e^{-cL^2}$ , paying more attention to how the characteristic functions depend on  $L$ . We will mainly establish the following bound:

$$\mathbb{P}\left(\left|\sum_i w_i v_{\pi(i)} - L\right| \leq \frac{1}{n}\right) \ll \max\left\{n^{-\sqrt{A}}, \frac{1}{n} e^{-\Theta(L^2)}\right\}. \quad (26)$$

In fact, for large  $L$ , we can apply Lemma 2.3: if

$$L \geq \frac{2}{\sqrt{C_0}} \sqrt{\log n},$$

then

$$\mathbb{P}\left(\left|n \sum_{i=1}^n v_i w_{\pi(k)} - n \left(\sum_{i=1}^n v_i\right) \bar{\mathbf{w}}\right| \geq Ln \cdot \sigma(\mathbf{w})\right) \leq C_0 e^{-C_0 L^2} \leq \frac{1}{n} e^{-C_0 L^2/2}.$$

Thus, for Theorem 1.15 it suffices to assume

$$L < \frac{2}{\sqrt{C_0}} \sqrt{\log n}. \quad (27)$$

*Proof.* (of (6) (or more precisely (26)) of Theorem 1.15) As mentioned above, assume  $L < (2/\sqrt{C_0})\sqrt{\log n}$ . We first note that the treatment for large  $t$  in the above proof (i.e.,  $|\varphi_S(t)| \leq n^{-2\sqrt{A}}$  for  $(\sqrt{A \log n})/n \leq |t| \leq 1$ ) can be extended all the way to  $(\sqrt{A \log n})/n \leq |t| \leq \sqrt{A \log n}$ .

**Very Large  $|t|$ .** We assume now that

$$1 \leq |t| \leq \sqrt{A \log n}.$$

We first throw away those  $|w_i - w_j|$  that are smaller than  $1/\sqrt{n}$ , and set

$$\mathcal{G} = \{(i, j) : |w_i - w_j| \geq 1/\sqrt{n}\}.$$

Then we have

$$\sum_{(i,j) \in \mathcal{G}} (w_i - w_j)^2 \geq n.$$

Since  $|w_i - w_j| \leq 1/A\sqrt{\log n}$ , it follows that

$$|\mathcal{G}| \geq A^2 n \log n.$$

Now we consider the sum  $\sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2$ , where  $(i, j) \in \mathcal{G}$ . As  $1/\sqrt{n} \leq |w_i - w_j| \leq 1/A\sqrt{\log n}$  and  $1 \leq |t| \leq \sqrt{A \log n}$ , we have  $\frac{1}{\sqrt{n}} \leq |t(w_i - w_j)| \leq \frac{1}{\sqrt{A}} < \frac{1}{C}$ . Thus, by Lemma 2.4, it follows that

$$\sum_{r \in \mathcal{R}} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_{\delta} n.$$

This implies

$$\sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \gg_{\delta} n|\mathcal{G}| \gg_{\delta} A^2 n^2 \log n.$$

Therefore, for  $1 \leq |t| \leq \sqrt{A \log n}$ , we also have

$$|\varphi_S(t)| \leq n^{-A}. \quad (28)$$

Our plan in the proof of (6) is to replace  $k(t)$  in (23) by some smoother function that can be extended holomorphically to  $\mathbb{C}$ . Our starting point is that<sup>3</sup>

$$\int_{\mathbb{R}} e^{-\pi t^2} e^{itx} dt = e^{-\pi x^2/2}. \quad (29)$$

Hence

$$\mathbb{E} \int_{\mathbb{R}} e^{-\pi t^2} e^{itX} dt = \mathbb{E} e^{-\pi X^2/2}.$$

For any  $K$  (noting here and later that the integrals are real valued due to the symmetry of the range of  $t$ ),

$$-\int_{|t| \geq K} e^{-\pi t^2} dt \leq \int_{|t| > K} e^{-\pi t^2} e^{itx} dt \leq \int_{|t| \geq K} e^{-\pi t^2} dt \leq e^{-\Theta(K^2)}.$$

Thus, for sufficiently large  $A$ , with  $X = S - Ln$

$$|\mathbb{E} \int_{|t| \geq \sqrt{A \log n}} e^{-\pi t^2} e^{itX} dt| \leq \int_{|t| \geq \sqrt{A \log n}} e^{-\pi t^2} dt \leq n^{-2\sqrt{A}}.$$

We thus have

$$\begin{aligned} \mathbb{P}(|X| \leq 1) &\leq e^{\pi/2} \mathbb{E} e^{-\pi X^2/2} \leq e^{\pi/2} \left[ \mathbb{E} \int_{|t| \leq \sqrt{A \log n}} e^{-\pi t^2} e^{itX} dt + n^{-2\sqrt{A}} \right] \\ &\leq e^{\pi/2} \int_{|t| \leq \sqrt{A \log n}} e^{-\pi t^2} \mathbb{E} e^{itX} dt + e^{\pi/2} n^{-2\sqrt{A}}. \end{aligned} \quad (30)$$

At this point, if  $\mathbb{P}(|X| \leq 1) \leq 2e^{\pi/2} n^{-2\sqrt{A}}$ , then there is nothing to prove. In the remaining case, from (30) we have reached that

$$\mathbb{P}(|X| < 1) \leq 2e^{\pi/2} \int_{|t| \leq \sqrt{A \log n}} e^{-\pi t^2} \varphi_X(t) dt.$$

---

<sup>3</sup>This identity is also frequently used to estimate small ball probabilities, see [56, Section 7].

Combining (28) with (25) from the proof of (5), we get: for  $(\sqrt{A \log n})/n \leq |t| \leq \sqrt{A \log n}$ ,

$$|\varphi_X(t)| \leq n^{-2\sqrt{A}}.$$

It follows that

$$\int_{(\sqrt{A \log n})/n \leq |t| \leq \sqrt{A \log n}} e^{-\pi t^2} \varphi_X(t) dt \leq (2\sqrt{A \log n}) n^{-2\sqrt{A}} \ll n^{-\sqrt{A}}.$$

It remains to bound  $\int_{|t| \leq (\sqrt{A \log n})/n} e^{-\pi t^2} \varphi_X(t) dt$ . We will decompose the integral to

$$\int_{|t| \leq (\sqrt{A \log n})/n} e^{-\pi t^2} \varphi_X(t) dt = \int_{L/n < |t| \leq (\sqrt{A \log n})/n} e^{-\pi t^2} \varphi_X(t) dt + \int_{|t| \leq L/n} e^{-\pi t^2} \varphi_X(t) dt.$$

For the first integral, recall from the proof of (5) in the case of “small  $|t|$ ” that for  $|t| \leq (\sqrt{A \log n})/n$ ,  $|\varphi_X(t)| \leq \exp(-\Theta(t^2 n^2))$ , so

$$\int_{L/n < |t| \leq (\sqrt{A \log n})/n} e^{-\pi t^2} \varphi_X(t) dt \leq \frac{1}{n} \int_{L < |x|} e^{-\Theta(x^2)} dx \leq \frac{1}{n} e^{-\Theta(L^2)}.$$

It remains to work with the second integral

$$\int_{|t| \leq L/n} e^{-\pi t^2} \varphi_X(t) dt,$$

which, by the change of variable  $x = nt$ , can be rewritten as

$$\frac{1}{n} \int_{|x| \leq L} e^{-\pi x^2/n^2} \varphi_{X/n}(x) dx,$$

where

$$\varphi_{X/n}(x) = \mathbb{E} e^{ixX/n} = \mathbb{E} e^{ix(S/n - L)} = e^{-ixL} \varphi_{S/n}(x).$$

Note that if we extend  $\varphi_{S/n}(t)$  (or  $\varphi_{X/n}(t)$ ) to the complex plane, since  $S$  is bounded (for each fixed  $n$ ), we obtain a holomorphic function

$$\varphi_{S/n}(z) = \mathbb{E} e^{iz(S/n)}.$$

Let

$$h(t) = e^{-\pi t^2/n^2} \varphi_{S/n}(t).$$

This function can be extended holomorphically to

$$h(z) = e^{-\pi z^2/n^2} \varphi_{S/n}(z).$$

Since  $|\mathbb{E}Y| \leq \mathbb{E}|Y|$  for any complex-valued random variable  $Y$ , inequality (16) gives

$$|\varphi_{S/n}(z)| = \left| \mathbb{E} e^{izS/n} \right| = \left| \mathbb{E} e^{i(t+is)S/n} \right| = \left| \mathbb{E} e^{i(t/n)S} e^{-s(S/n)} \right| \leq \mathbb{E} e^{-s(S/n)} \leq C'_0 e^{C'_0 s^2}. \quad (31)$$

Now we establish the bound  $O(\frac{\exp(-cL^2)}{n})$  for some sufficiently small constant  $c$  (such as  $c = 1/(4C'_0)$ ). Write

$$\frac{1}{n} \int_{|x| \leq L} e^{-\pi x^2/n^2} \varphi_{X/n}(x) dx = \frac{1}{n} \int_{|x| \leq L} e^{-ixL} e^{-\pi x^2/n^2} \varphi_{S/n}(x) dx = \frac{1}{n} \int_{|x| \leq L} e^{-ixL} h(x) dx.$$

First, using contour integration, we pass to the line  $\mathbb{R} - icL$ :

$$\begin{aligned} \frac{1}{n} \int_{|x| \leq L} e^{-ixL} h(x) dx &= \Re \left[ \frac{1}{n} \int_{\substack{z \in \mathbb{R} - icL \\ |\Re(z)| \leq L}} e^{-izL} h(z) dz \right] \\ &= \frac{1}{n} \Re \left[ \int_{|t| \leq L} e^{-i(t-icL)L} h(t - icL) dt \right] \\ &= \frac{e^{-cL^2}}{n} \Re \left[ \int_{|t| \leq L} e^{-itL} h(t - icL) dt \right], \end{aligned} \quad (32)$$

where it is crucial to notice that the first integral is real-valued because  $h(-t) = \overline{h(t)}$ , and the real parts of the integrals (with opposite orientation) on the lines  $\Re(z) = -L$  and  $\Re(z) = L$  cancel each other. More specifically,

$$\Re \int_{z=-L-it, 0 \leq t \leq cL} e^{-izL} h(z) dt = \Re \int_{z=L-it, 0 \leq t \leq cL} e^{-izL} h(z) dt$$

since they are conjugates of each other. This follows from  $S \in \mathbb{R}$  and

$$h(-x + iy) = e^{-\pi(-x+iy)^2/n^2} \mathbb{E} e^{i(-x+iy)S/n} = e^{-\pi(x^2-y^2-2ixy)/n^2} \mathbb{E} e^{-ixS/n} e^{-yS/n},$$

while

$$h(x + iy) = e^{-\pi(x+iy)^2/n^2} \mathbb{E} e^{i(x+iy)S/n} = e^{-\pi(x^2-y^2+2ixy)/n^2} \mathbb{E} e^{ixS/n} e^{-yS/n}.$$

Thus, by (32),

$$\mathbb{P}(|X| \leq 1) \leq \frac{e^{-cL^2}}{n} \left| \int_{|t| \leq L} e^{-itL} h(t - icL) dt \right|.$$

Note that

$$\left| e^{-\pi(t-icL)^2/n^2} \right| = e^{-\pi(t^2-c^2L^2)/n^2} \asymp 1, \quad \text{as } n \rightarrow \infty \text{ and } |t| \leq L = O(\sqrt{\log n}),$$

and by (31),

$$|\varphi_{S/n}(t - icL)| \leq C'_0 e^{C'_0 c^2 L^2}.$$

Putting these together, by choosing  $c = 1/(4C'_0)$ , we obtain (in the case  $\mathbb{P}(|X| \leq 1) \geq e^{\pi/2} n^{-A/2}$ )

$$\mathbb{P}(|X| \leq 1) \leq \frac{e^{-cL^2}}{n} \cdot e^{C'_0 c^2 L^2} \cdot 2L \ll \frac{e^{-L^2/(16C'_0)} L}{n} \ll \frac{e^{-\Theta(L^2)}}{n}.$$

□

**Remark 4.2.** We observe that the assumption  $|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}}$  in Theorem 1.15 cannot be relaxed to  $|w_i - w_j| \gg \frac{1}{\sqrt{\log n}}$  when using only the characteristic function method (i.e., relying solely on Theorem 2.1). Indeed<sup>4</sup>, suppose we partition  $[n]$  into two disjoint sets  $I \cup J = [n]$  with  $|I| = 2c \log n$  for some constant  $c > 0$ . Let  $w_i = \frac{1}{\sqrt{2c \log n}}$  and  $-\frac{1}{\sqrt{2c \log n}}$  for half of the  $i \in I$  respectively, and  $w_j = 0$  for all  $j \in J$ . Then,

$$\begin{aligned} \frac{1}{n^2} \sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 &= \frac{1}{n^2} \left[ \sum_{(i,j) \in I \times J} \sum_r \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 + \sum_{(i,j) \in I \times I} \sum_r \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \right] \\ &\leq \frac{1}{n^2} \left( 2c \log n \cdot n + (c \log n)^2 \right) \cdot n \leq 3c \log n. \end{aligned}$$

---

<sup>4</sup>In this example, the matrix is very sparse, making the permanent-based bound weak. This suggests that a more refined approach may be needed, possibly restricting attention to the support of the  $w_i$ .

Therefore,

$$\int_{|t| \leq 1} \exp\left(-\frac{1}{n^2} \sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2\right) dt \geq \int_{|t| \leq 1} e^{-3c \log n} dt = \Theta(n^{-3c}),$$

which is too large to obtain meaningful decay.

We next move to a finer scale, proving Theorem 1.17.

*Proof of (7) of Theorem 1.17.* Let  $\Delta > 0$  be a constant chosen sufficiently large in terms of  $\varepsilon$  and  $\delta$ .<sup>5</sup> Define

$$S' = \sum_i \frac{n^{3/2}}{\Delta} w_i v_{\pi(i)} = \frac{n^{1/2}}{\Delta} S \quad \text{and} \quad X' = S' - \frac{n^{3/2}}{\Delta} L.$$

To prove (7), it suffices to show  $\mathbb{P}(|X'| \leq 1) = O_{\varepsilon, \delta, \Delta, A}(\frac{1}{n^{3/2}})$ . Using Esseen's estimate together with Corollary 2.2, we can write

$$\sup_x \mathbb{P}(|S' - x| \leq 1) \ll \int_{|t| \leq 1} |\varphi_{S'}(t)| dt \ll \int_{|t| \leq 1} \exp\left\{-\frac{1}{2n^3} \sum_{i,j,k,l} \left\|\frac{tn^{3/2}}{\Delta} (w_i - w_j)(v_k - v_l)\right\|_{\mathbb{R}/\mathbb{Z}}^2\right\} dt.$$

Recalling that  $v_i = i/n$  for  $i \in I$ , and following the argument from the proof of (5), the exponent on the right-hand side can be bounded from below by

$$\frac{c_\delta}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\|\frac{tn^{1/2}}{\Delta} (w_i - w_j)r\right\|_{\mathbb{R}/\mathbb{Z}}^2,$$

and so

$$\mathbb{P}(|X'| \leq 1) \ll \int_{|t| \leq 1} \exp\left\{-\frac{c_\delta}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\|\frac{tn^{1/2}}{\Delta} (w_i - w_j)r\right\|_{\mathbb{R}/\mathbb{Z}}^2\right\} dt. \quad (33)$$

We note that this differs from (24) in that we have an extra factor of  $n^{1/2}$  in the exponent. As such, our case analysis for  $t$  will be different, and we will need more information in addition to (4) about the  $w_i$  (as assumed in Theorem 1.17).

We discard pairs  $(i, j)$  for which  $|w_i - w_j|$  is much smaller than  $1/\sqrt{n}$ , and set

$$\mathcal{G} = \{(i, j) : |w_i - w_j| \geq \varepsilon/2\sqrt{n}\}.$$

Since there is no interval of length  $\varepsilon/\sqrt{n}$  containing at least  $(1 - \varepsilon)n$  elements from  $w_1, \dots, w_n$ , the number of pairs  $(i, j)$  such that  $|w_i - w_j| < \varepsilon/2\sqrt{n}$  is at most  $(1 - \varepsilon)n^2$ . Thus, we have

$$|\mathcal{G}| \geq \varepsilon n^2, \quad \sum_{(i,j) \in \mathcal{G}} (w_i - w_j)^2 \asymp_\varepsilon n. \quad (34)$$

**Intermediate  $|t|$ .** We first focus on the range

$$\frac{(\sqrt{A \log n})\Delta}{n^{3/2}} \leq |t| \leq \frac{\Delta}{n^{1/2}}.$$

---

<sup>5</sup>Only the small- $|t|$  regime considered below requires  $\Delta$  to be a constant. The other regimes hold for *any*  $\Delta = \Delta(n)$  sufficiently large with respect to  $\varepsilon$  and  $\delta$ .

Now, for  $\log\left(\frac{2}{\varepsilon}\right) \leq k \leq \log\left(\frac{\sqrt{n}}{A\sqrt{\log n}}\right) + 1$  (so that  $\frac{2^{k-1}}{\sqrt{n}} \leq \frac{1}{A\sqrt{\log n}}$  and  $\frac{2^k}{\sqrt{n}} \geq \frac{\varepsilon}{2\sqrt{n}}$ ), let  $\mathcal{G}_k$  be the collection of pairs  $(i, j)$  for which

$$D_{k-1} = \frac{2^{k-1}}{\sqrt{n}} < |w_i - w_j| \leq \frac{2^k}{\sqrt{n}} = D_k.$$

Then we see that  $\mathcal{G} = \bigcup_k \mathcal{G}_k$  and

$$\sum_k D_k^2 |\mathcal{G}_k| \asymp_\varepsilon n.$$

Given a fixed pair  $(i, j) \in \mathcal{G}_k$ , we consider the sum  $\sum_{r \in \mathcal{R}} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2$ . For  $\frac{tn^{1/2}}{\Delta} D_k \leq \frac{1}{Cn}$ , we have  $|\frac{tn^{1/2}}{\Delta} (w_i - w_j)r| \leq \frac{1}{C} < 1$ , so

$$\sum_{r \in \mathcal{R}} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 = \sum_{r \in \mathcal{R}} \left| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right|^2 \asymp_\delta \frac{t^2 n^4 D_k^2}{\Delta^2}.$$

On the other hand, if  $\frac{tn^{1/2}}{\Delta} D_k > \frac{1}{Cn}$ , then  $\frac{1}{2Cn} \leq |\frac{tn^{1/2}}{\Delta} (w_i - w_j)| \leq \frac{1}{A\sqrt{\log n}}$ , and by Corollary 2.5, we get

$$\sum_{r \in \mathcal{R}} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n.$$

From the above discussion, we conclude that

$$\sum_{i,j,r} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \gg_{\delta,C} \sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k \leq \frac{1}{Cn}} \frac{t^2 n^4 D_k^2}{\Delta^2} |\mathcal{G}_k| + \sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k > \frac{1}{Cn}} n |\mathcal{G}_k|.$$

To lower bound the right-hand side, we distinguish two cases.

**Case 1:**  $\sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k \leq \frac{1}{Cn}} D_k^2 |\mathcal{G}_k| \asymp_\varepsilon n$ .

Since  $t^2 \geq \frac{(A \log n) \Delta^2}{n^3}$ , we have

$$\sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k \leq \frac{1}{Cn}} \frac{t^2 n^4 D_k^2}{\Delta^2} |\mathcal{G}_k| \gg_\varepsilon A n^2 \log n.$$

**Case 2:**  $\sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k > \frac{1}{Cn}} D_k^2 |\mathcal{G}_k| \asymp_\varepsilon n$ .

As  $D_k^2 \leq 1/(A^2 \log n)$ , we obtain  $\sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k > \frac{1}{Cn}} |\mathcal{G}_k| \gg_\varepsilon A^2 n \log n$ , which implies

$$\sum_{k: \frac{|t|n^{1/2}}{\Delta} D_k > \frac{1}{Cn}} n |\mathcal{G}_k| \gg_\varepsilon A^2 n^2 \log n.$$

Therefore, in both cases,

$$\sum_{i,j,r} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \gg_{\varepsilon,\delta,C} A n^2 \log n.$$

Assuming  $A$  is sufficient large relative to  $\varepsilon, \delta$ , and  $C$ , this implies that for  $\frac{\sqrt{A \log n}}{n^{3/2}} \leq |t| \leq \frac{1}{n^{1/2}}$ , we have

$$\frac{c_\delta}{n^2} \sum_{i,j,r} \|t(w_i - w_j)r\|_{\mathbb{R}/\mathbb{Z}}^2 \geq 2\sqrt{A \log n}, \quad |\varphi_{S'}(t)| \leq n^{-2\sqrt{A}}.$$

**Large  $|t|$ .** We now focus on the range

$$\frac{\Delta}{n^{1/2}} \leq |t| \leq 1.$$

Let  $\mathcal{G}_0$  be the set obtained from  $\mathcal{G}$  by removing pairs  $(i, j)$  with  $|w_i - w_j| > 2/\sqrt{\varepsilon n}$ . Since  $\sum_{i,j} (w_i - w_j)^2 = 2n$ , at most  $(\varepsilon/2)n^2$  pairs were removed. From (34), we see that  $|\mathcal{G}_0| \geq |\mathcal{G}| - (\varepsilon/2)n^2 \geq (\varepsilon/2)n^2$ . For every  $(i, j) \in \mathcal{G}_0$ , as  $\frac{\varepsilon}{2\sqrt{n}} \leq |w_i - w_j| \leq \frac{2}{\sqrt{\varepsilon n}}$ , we have

$$\frac{\varepsilon}{2\sqrt{n}} \leq \left| \frac{tn^{1/2}}{\Delta} (w_i - w_j) \right| \leq \frac{2}{\Delta\sqrt{\varepsilon}}.$$

Assuming  $\Delta$  is sufficiently large in terms of  $\varepsilon$  and  $\delta$ , Corollary 2.5 then gives

$$\frac{c_\delta}{n^2} \sum_{\substack{(i,j) \in \mathcal{G}_0 \\ r \in \mathcal{R}}} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_\delta \frac{1}{n^2} \cdot |\mathcal{G}_0| \cdot n \asymp_{\delta, \varepsilon} n.$$

**Small  $|t|$ .** It remains to consider

$$|t| \leq \frac{(\sqrt{A \log n})\Delta}{n^{3/2}}.$$

In this case, as  $|w_i - w_j| \leq 1/(A\sqrt{\log n})$ , we have

$$\left| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right| \leq \frac{1}{\sqrt{A}} < 1.$$

Therefore,

$$\frac{c_\delta}{n^2} \sum_{i,j,r} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 = \frac{c_\delta}{n^2} \sum_{i,j,r} \left| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right|^2 \asymp_{\delta, \Delta} t^2 n^3.$$

Hence,

$$\int_{|t| \leq \frac{(\sqrt{A \log n})\Delta}{n^{3/2}}} \exp \left\{ - \frac{c_\delta}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\| \frac{tn^{1/2}}{\Delta} (w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \right\} dt \leq \int_{\mathbb{R}} e^{-\Theta(t^2 n^3)} dt = O(n^{-3/2}).$$

□

**Remark 4.3.** Consider the case where  $w_1 = \dots = w_{(1-t)n} = 0$  and  $w_{(1-t)n+1} = \dots = w_n = \pm 1/\sqrt{\delta n}$ , which satisfies the condition of Theorem 1.15. In this setting, it can be shown that the weighted sum  $\sqrt{\delta} \sum_i w_i \pi(i)$  spreads rather evenly over the interval  $[-Ct^{1/2}n^{3/2}, Ct^{1/2}n^{3/2}]$  for some constant  $C > 0$ .<sup>6</sup> By pigeonhole principle, the point anti-concentration of this integer-valued sum is  $\Theta(t^{-1/2}n^{-3/2})$ ,  $\sup_x \mathbb{P}(|\sqrt{tn} \sum_i w_i \pi(i) - x| \gg t^{-1/2}n^{-3/2})$ . Hence for any  $\delta > 0$

$$\sup_x \mathbb{P} \left( \left| \sum_i w_i \pi(i)/n - x \right| \leq \delta \right) \gg t^{-1/2}n^{-3/2}.$$

---

<sup>6</sup>This follows because the variance of the sum is of order  $tn^3$ .

In what follows, we turn to the proof of the  $L$ -dependent estimate in this finer scale. Our general method is similar to the proof of (8), although the details are slightly different.

*Proof of (8) of Theorem 1.17.* Define

$$S' = \sum_i n^{3/2-\varepsilon} w_i v_{\pi(i)} = n^{1/2-\varepsilon} S \quad \text{and} \quad X' = S' - n^{3/2-\varepsilon} L.$$

These random variables correspond to those defined in the proof of (7), obtained by setting  $\Delta = n^\varepsilon$ . It suffices to assume  $L = O(\sqrt{\log n})$ .

We first observe that our treatment of the intermediate- and large- $|t|$  regimes above, namely

$$|\varphi_{S'}(t)| \leq n^{-2\sqrt{A}} \quad \text{for} \quad \frac{\sqrt{A \log n}}{n^{3/2-\varepsilon}} \leq t \leq 1,$$

in fact extends all the way to  $|t| \leq \sqrt{A \log n}$ .

**Very large  $|t|$ .** We now assume that

$$1 \leq |t| \leq \sqrt{A \log n}.$$

Similarly to the treatment of the large- $|t|$  regime in the proof of (7), there exists a set  $\mathcal{G}_0$  containing at least  $(\varepsilon/2)n^2$  pairs  $(i, j)$  for which  $\frac{\varepsilon}{2\sqrt{n}} \leq |w_i - w_j| \leq \frac{2}{\sqrt{\varepsilon n}}$ . For each such pair, we have

$$\frac{\varepsilon}{2n^\varepsilon} \leq |tn^{1/2-\varepsilon}(w_i - w_j)| \leq \frac{2\sqrt{A \log n}}{\sqrt{\varepsilon n^\varepsilon}}.$$

It then follows from Corollary 2.5 that

$$\frac{c_\delta}{n^2} \sum_{\substack{(i,j) \in \mathcal{G}_0 \\ r \in \mathcal{R}}} \left\| tn^{1/2-\varepsilon}(w_i - w_j)r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_\delta \frac{1}{n^2} \cdot |\mathcal{G}_0| \cdot n \asymp_{\delta, \varepsilon} n.$$

As such, in the case  $1 \leq |t| \leq \sqrt{A \log n}$ , we also have

$$|\varphi_{S'}(t)| \leq e^{-\Omega(n)}.$$

Our next step is similar to the proof of (6) of Theorem 1.15, so we will be brief. Starting from

$$\int_{t \in \mathbb{R}} e^{-\pi t^2} e^{itx} d\xi = e^{-\pi x^2/2},$$

and assuming that  $\mathbb{P}(|X| \leq 1) \leq 2e^{\pi/2} n^{-2\sqrt{A}}$ , we arrive at

$$\mathbb{P}(|X'| \leq 1) \leq 2e^{\pi/2} \int_{|t| \leq \sqrt{A \log n}} e^{-\pi t^2} \varphi_{X'}(t) dt.$$

Since we have shown  $|\varphi_{X'}(t)| \leq n^{-2\sqrt{A}}$  for  $\frac{\sqrt{A \log n}}{n^{3/2-\varepsilon}} \leq |t| \leq \sqrt{A \log n}$ , it follows that

$$\mathbb{P}(|X'| \leq 1) \leq 2e^\pi \int_{|t| \leq \frac{\sqrt{A \log n}}{n^{3/2-\varepsilon}}} e^{-\pi t^2} \varphi_{X'}(t) dt + (2\sqrt{A \log n}) n^{-2\sqrt{A}}.$$

Similarly to the proof of Theorem 1.15, we decompose the integral on the right-hand side into

$$\int_{|t| \leq L/n^{3/2-\varepsilon}} e^{-\pi t^2} \varphi_{X'}(t) dt + \int_{L/n^{3/2-\varepsilon} < |t| \leq (\sqrt{A \log n})/n^{3/2-\varepsilon}} e^{-\pi t^2} \varphi_{X'}(t) dt.$$

The treatment of the second integral is similar to the method used for small- $|t|$  regime (i.e.,  $|t| \leq \frac{\sqrt{A \log n}}{n^{3/2}}$ ) in the proof of (7), where we obtained a bound of the type

$$\frac{1}{n^{3/2}} \int_{L \leq |x|} \exp(-cx^2) dx = \frac{\exp(-cL^2)}{n^{3/2}}.$$

For the first integral, by the change of variables  $x = n^{3/2-\varepsilon}t$ , we can rewrite it as

$$\frac{1}{n^{3/2-\varepsilon}} \int_{|x| \leq L} e^{-\pi x^2} \varphi_{X'/n^{3/2-\varepsilon}}(x) dx,$$

where

$$\varphi_{X'/n^{3/2-\varepsilon}}(x) = \mathbb{E} e^{ix(S'/n^{3/2-\varepsilon} - L)}.$$

If we extend this to the complex plane, then, as  $S'$  is bounded, we obtain a holomorphic function

$$\varphi_{S'/n^{3/2-\varepsilon}}(z) = \mathbb{E} e^{izS'/n^{3/2-\varepsilon}}.$$

Let

$$h(t) = e^{-\pi t^2/n^{3/2-\varepsilon}} \varphi_{S'/n^{3/2-\varepsilon}}(t),$$

which extends holomorphically to

$$h(z) = e^{-\pi z^2/n^{3/2-\varepsilon}} \varphi_{S'/n^{3/2-\varepsilon}}(z).$$

By (16),

$$|\varphi_{S'}(z/n^{3/2-\varepsilon})| = |\varphi_S(z/n)| \leq C'_0 e^{C'_0 s^2}. \quad (35)$$

Next, by using contour integration, we pass to the line  $\mathbb{R} + icL$ :

$$\begin{aligned} \mathbb{P}(|X'| \leq 1) &\leq \frac{1}{n^{3/2-\varepsilon}} \int_{|t| \leq L} e^{-itL} h(t) dt \\ &= \Re \left( \int_{\substack{z \in \mathbb{R} - icL \\ |\Re(z)| \leq L}} e^{-izL} h(z) dz \right) \\ &= \frac{1}{n^{3/2-\varepsilon}} \Re \left( \int_{|t| \leq L} e^{-i(t-icL)L} h(t - icL) dt \right) \\ &= \frac{e^{-cL^2}}{n^{3/2-\varepsilon}} \Re \left( \int_{|t| \leq L} e^{itL} h(t - icL) dt \right). \end{aligned} \quad (36)$$

By (35),

$$|\varphi_{S'/n^{3/2-\varepsilon}}(t - icL)| = O\left(e^{C'_0 c^2 L^2}\right).$$

Putting this together, by choosing  $c = 1/(4C'_0)$ , we obtain the bound

$$\mathbb{P}(|X'| \leq 1) \leq \frac{e^{-cL^2}}{n^{3/2-\varepsilon}} \cdot e^{C'_0 c^2 L^2} \cdot 2AL = O\left(\frac{e^{-\Theta(L^2)}}{n^{3/2-\varepsilon}}\right). \quad \square$$

To conclude this section, we can further refine the scaling under an additional—but still quite generic—condition on the  $w_i$ , as follows.

**Theorem 4.4.** Let  $0 < \varepsilon < 1/2$  and  $\delta > 0$  be given. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . In addition, assume that no interval of length  $\varepsilon/\sqrt{n}$  contains more than  $(1 - \varepsilon)n$  of the values  $w_i$ , and that there are at least  $An \log n$  pairs  $(i, j)$  for which

$$\frac{1}{n^{3/2}} \leq |w_i - w_j| \leq \frac{1}{n^{3/2-\varepsilon}}.$$

Then, for every  $L \in \mathbb{R}$ , we have

$$\mathbb{P}\left(\left|\sum_i w_i \frac{\pi(i)}{n} - L\right| \leq \frac{1}{n^{5/2-\varepsilon}}\right) = O\left(\frac{1}{n^{5/2-\varepsilon}}\right).$$

We can also obtain an  $L$ -dependent bound, as in Theorems 1.15 and 1.17. This result can be seen as a continuous analog of Theorem 1.24. Here, roughly speaking, if the  $w_i$  are spread out evenly over the interval  $[-C/\sqrt{n}, C/\sqrt{n}]$ , then the average consecutive spacing is  $1/n^{3/2}$ . The above condition requires that most of the consecutive spacings asymptotically attain this bound.

## 5. CONTINUOUS SETTING: PROOF OF THEOREM 1.18 FOR THE POLYNOMIAL SEQUENCES

We will use the method in a similar way to that in Theorem 1.15.

*Proof.* (of (9) Theorem 1.18) From Esseen's estimate and Corollary 2.2, we can write

$$\sup_L \mathbb{P}(|n \sum_i w_i v_{\pi(i)} - Ln| \leq 1) \ll \int_{|t| \leq 1} |\varphi(t)| dt \ll \int_{|t| \leq 1} e^{-\frac{1}{n^3} \sum_{i,j,k,l} \|tn(w_i - w_j)(v_k - v_l)\|_{\mathbb{R}/\mathbb{Z}}^2}.$$

Here we recall that  $v_i = P_d(i)/n^d$  for  $i \in I$ , where  $P_d(i) = bi^d + b'_n i^{d-1} + b''_n i^{d-2} + \dots$  is a real polynomial of degree  $d$  with fixed leading coefficient  $b$  such that

$$|v_i| \leq B \quad \text{for all } i \in I. \tag{37}$$

The exponent of the right-hand side can be bounded from below by

$$\frac{1}{n^3} \sum_{1 \leq i,j \leq n; k,l \in I} \|t(w_i - w_j)(P_d(k) - P_d(l))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2. \tag{38}$$

As in the proof of Theorem 1.15, we will break down the integral depending on whether  $|t| \leq (\sqrt{A \log n})/n$  or  $(\sqrt{A \log n})/n \leq |t| \leq 1$ .

**Large  $|t|$ .** We assume now that

$$\frac{\sqrt{A \log n}}{n} \leq |t| \leq 1.$$

We first throw away those  $|w_i - w_j|$  that are smaller than  $1/\sqrt{n}$ , and set

$$\mathcal{G} = \{(i, j) : |w_i - w_j| \geq 1/\sqrt{n}\}.$$

Then we have

$$\sum_{(i,j) \in \mathcal{G}} (w_i - w_j)^2 \asymp n.$$

Now for  $0 \leq k \leq \log\left(\frac{\sqrt{n}}{A\sqrt{\log n}}\right) + 1$ , we let  $\mathcal{G}_k$  be the collection of pairs  $(i, j)$  for which

$$D_{k-1} = \frac{2^{k-1}}{\sqrt{n}} < |w_i - w_j| \leq \frac{2^k}{\sqrt{n}} = D_k.$$

Then we see that

$$\sum_k D_k^2 |\mathcal{G}_k| \asymp n.$$

We use the following corollary of Lemma 2.6 to estimate the expression in (38).<sup>7</sup>

**Corollary 5.1.** *Let  $r_0 \in [n]$  be fixed.*

(i) *We have*

$$\sum_{r \in I} (P_d(r) - P_d(r_0))^2 \asymp_C n^{2d+1}.$$

(ii) *For  $D_{k-1} \leq |w| \leq D_k$  and  $\frac{1}{CnD_k} \leq |t| \leq \frac{n^{d-1}}{CD_k}$ , we have*

$$\sum_{r \in I} \|t(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n.$$

As a consequence, for

$$\frac{1}{CnD_k} \leq |t| \leq 1$$

we obtain

$$\frac{1}{n^3} \sum_{(i,j) \in \mathcal{G}_k} \sum_{r,r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C \frac{1}{n} |\mathcal{G}_k|.$$

Consider

$$|t| \leq \frac{1}{CnD_k}.$$

In this case, for  $(i, j) \in \mathcal{G}_k$ , using (37)

$$\|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}} = |t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}|.$$

Thus

$$\begin{aligned} \frac{1}{n^3} \sum_{(i,j) \in \mathcal{G}_k} \sum_{r,r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 &= \frac{1}{n^3} \sum_{(i,j) \in \mathcal{G}_k} \sum_{r,r_0 \in I} |t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}|^2 \\ &\asymp \frac{1}{n^3} t^2 D_k^2 |\mathcal{G}_k| n^4 \asymp t^2 n D_k^2 |\mathcal{G}_k|. \end{aligned}$$

Putting together,

$$\frac{1}{n^3} \sum_{(i,j) \in \mathcal{G}} \sum_{r,r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp \sum_{k: |t|D_k \leq 1/(Cn)} t^2 n D_k^2 |\mathcal{G}_k| + \frac{1}{n} \sum_{k: |t|D_k > 1/(Cn)} |\mathcal{G}_k|.$$

**Case 1:**  $\sum_{k: |t|D_k \leq 1/(Cn)} D_k^2 |\mathcal{G}_k| \geq (1/10)n$ .

---

<sup>7</sup>Part (ii) of Corollary 5.1 follows from Lemma 2.6 in the same way that Corollary 2.5 follows from Lemma 2.4.

Then as  $t^2 \geq \frac{A \log n}{n^2}$

$$\sum_{k: |t|D_k \leq 1/(Cn)} t^2 n D_k^2 |\mathcal{G}_k| \gg A \log n.$$

**Case 2:**  $\sum_{k: |t|D_k > 1/(Cn)} D_k^2 |\mathcal{G}_k| > (9/10)n$ .

Then as  $D_k^2 \leq 1/A^2 \log n$ , we have that

$$\sum_{k: |t|D_k \geq 1/(Cn)} |\mathcal{G}_k| \gg A^2 n \log n.$$

We thus conclude that in the case of large  $|t|$ , similarly to (25)

$$|\varphi_S(t)| \leq n^{-2\sqrt{A}}, \quad (39)$$

provided that  $A$  is sufficiently large with respect to  $C$ .

**Small  $|t|$ .** It remains to focus on

$$|t| \leq \frac{\sqrt{A \log n}}{n}.$$

As  $|w_i - w_j| \leq 1/(A\sqrt{\log n})$  and  $|P_d(r)/n^{d-1}| \leq Bn$ , if we choose  $A$  sufficiently large,

$$\|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}} = |t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}|.$$

Then

$$\begin{aligned} \frac{1}{n^3} \sum_{1 \leq i, j \leq n; r, r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 &= \frac{1}{n^3} \sum_{1 \leq i, j \leq n; r, r_0 \in I} |t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}|^2 \\ &\asymp t^2 n^2, \end{aligned}$$

where we used the fact that  $\sum_{1 \leq i, j \leq n} (w_i - w_j)^2 = 2n$ , and that  $\sum_{r, r_0 \in I} (P_d(r) - P_d(r_0))^2 \asymp n^{2d+2}$ . We then have

$$\int_{|t| \leq (\sqrt{A \log n})/n} \exp(-\Theta(t^2 n^2)) dt \leq \frac{1}{n} \int_{\mathbb{R}} \exp(-\Theta(x^2)) dx = O(1/n).$$

□

*Proof.* (of (10) of Theorem 1.18) We begin by considering the case where  $|t|$  is very large, and show that the characteristic function is very small in this regime.

**Very Large  $|t|$ .** We assume now that

$$1 \leq |t| \leq \sqrt{A \log n}.$$

We again throw away those  $|w_i - w_j|$  that are smaller than  $1/\sqrt{n}$ . Let

$$\mathcal{G} = \{(i, j) : |w_i - w_j| \geq 1/\sqrt{n}\}.$$

Then we have

$$\sum_{(i, j) \in \mathcal{G}} (w_i - w_j)^2 \geq n.$$

It thus follows that, as  $(w_i - w_j)^2 \leq 1/A^2 \log n$

$$|\mathcal{G}| \geq A^2 n \log n.$$

Now consider the sum  $\sum_{(i,j) \in \mathcal{G}; r, r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2$ . As  $\frac{1}{\sqrt{n}} \leq |w_i - w_j| \leq \frac{1}{A\sqrt{\log n}}$  and  $1 \leq |t| \leq \sqrt{A \log n}$ , we have  $\frac{1}{\sqrt{n}} \leq |t(w_i - w_j)| \leq \frac{1}{\sqrt{A}} \leq \frac{1}{C}$ . As such, Corollary 5.1 implies that

$$\sum_{r \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp n.$$

Hence we have

$$\sum_{1 \leq i, j \leq n; r, r_0 \in I} \|t(w_i - w_j)(P_d(r) - P_d(r_0))/n^{d-1}\|_{\mathbb{R}/\mathbb{Z}}^2 \gg n^2 |\mathcal{G}| \gg A^2 n^3 \log n.$$

As such, in the case that  $1 \leq |t| \leq \sqrt{A \log n}$  we also have

$$|\varphi_S(t)| \leq n^{-A}, \quad (40)$$

provided that  $A$  is sufficiently large.

The rest of the proof is almost identical to that of (6) and of (8), and hence we omit the details.  $\square$

## 6. PROOF OF THEOREM 1.19 FOR THE JOINT DISTRIBUTIONS

We will justify for the case  $d = 2$  only, the case  $d \geq 3$  can be treated similarly. We restate the result below (after scaling up by a factor of  $n$ ).

**Theorem 6.1** (Smoothness of the joint vector,  $d = 2$ ). *Let  $b, B > 0$  be constants. Suppose that the sequence  $(w_1, \dots, w_n)$  satisfies Condition 1.14 for some sufficiently large constant  $A > 0$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider the sequences  $(v_1, \dots, v_n)$  and  $(v'_1, \dots, v'_n)$  partially defined by*

$$v_i = \frac{bi^2 + b'_n i + b''_n}{n^2} \quad \text{and} \quad v'_i = \frac{i}{n} \quad \text{for all } i \in I,$$

such that

$$|v_i|, |v'_i| \leq B \quad \text{for all } i \in I.$$

Then, for any given  $L_1, L_2 \in \mathbb{R}$ , we have:

- (Uniform bound)

$$\mathbb{P}\left(\left|n \sum_{i=1}^n v_i w_{\pi(i)} - L_1 n\right| \leq 1 \wedge \left|n \sum_{i=1}^n v'_i w_{\pi(i)} - L_2 n\right| \leq 1\right) = O_A\left(\frac{1}{n^2}\right), \quad (41)$$

If, additionally  $|v_i|, |v'_i| \leq \tilde{B}$  for all  $i \in [n]$ , for some constant  $\tilde{B} > 0$ , then we have:

- ( $L$ -dependent bound)

$$\mathbb{P}\left(\left|n \sum_{i=1}^n v_i w_{\pi(i)} - L_1 n\right| \leq 1 \wedge \left|n \sum_{i=1}^n v'_i w_{\pi(i)} - L_2 n\right| \leq 1\right) = O\left(\frac{1}{n^2} e^{-\Theta(L_1^2 + L_2^2)}\right). \quad (42)$$

Here the implied constants are allowed to depend on  $A$  and  $\tilde{B}$ .

Let

$$S_1 = n \sum_{i=1}^n v_i w_{\pi(i)}, \quad S_2 = n \sum_{i=1}^n v'_i w_{\pi(i)},$$

and define the vector  $\mathbf{S} = (S_1, S_2)$ . We are interested in the event

$$\left| \frac{S_1}{n} - L_1 \right| \leq \frac{1}{n} \quad \text{and} \quad \left| \frac{S_2}{n} - L_2 \right| \leq \frac{1}{n},$$

or equivalently,

$$|S_1 - nL_1| \leq 1 \quad \text{and} \quad |S_2 - nL_2| \leq 1.$$

For convenience, we will also let  $\mathbf{X} = (X_1, X_2) := (S_1 - nL_1, S_2 - nL_2)$ .

*Proof.* (of Equation (41)) We consider the characteristic function of  $\mathbf{X}$ : for any  $\mathbf{t} = (t_1, t_2) \in \mathbb{R}^2$ ,

$$\varphi_{\mathbf{X}}(\mathbf{t}) = \mathbb{E} e^{i(t_1 X_1 + t_2 X_2)} = \mathbb{E} e^{it_1(S_1 - L_1 n) + it_2(S_2 - L_2 n)} = \mathbb{E} e^{i(t_1 S_1 + t_2 S_2)} e^{-it_1 L_1 n - it_2 L_2 n}.$$

We first establish the following estimate.

**Lemma 6.2** (large  $\|\mathbf{t}\|_2$ ). *For  $\mathbf{t} = (t_1, t_2)$  such that  $(\sqrt{A \log n})/n \leq \|\mathbf{t}\|_2 \leq 1$  we have*

$$|\varphi_{\mathbf{X}}(\mathbf{t})| \leq n^{-2\sqrt{A}}.$$

We remark that this generalizes (25) of Theorem 1.15 (where  $t_2 = 0$ ) and (39) of Theorem 1.18 (where  $t_1 = 0$ ).

*Proof.* (of Lemma 6.2) Given  $v_k = t_1 \frac{bk^2 + b'_n k + b''_n}{n^2} + t_2 \frac{k}{n}$  for  $k \in I$ , we start with

$$|\varphi_{\mathbf{X}}(\mathbf{t})| \leq \exp \left( -\frac{1}{2n^3} \sum_{i,j,k,l} \|n(w_i - w_j)(v_k - v_l)\|_{\mathbb{R}/\mathbb{Z}}^2 \right).$$

It boils down to bound from below the following

$$\frac{1}{n^3} \sum_{1 \leq i,j \leq n; r,s \in I} \left\| t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b''_n s}{n} + t_2(w_i - w_j)(r - s) \right\|_{\mathbb{R}/\mathbb{Z}}^2.$$

**Case 1.** Assume that

$$\frac{\sqrt{A \log n}}{2n} \leq |t_1| \leq 1.$$

Our goal is to use Lemma 2.6, but for this, we will first need to simplify the term involving  $t_2$ . We use the following claim.

**Claim 6.3.** *Let  $w_i, w_j$  be fixed. Then there exists a subset  $I_0 \subset [n]$ , and for each  $s \in I_0$ , a corresponding subset  $J_s \subset \{-n, \dots, n\}$ , such that all of these sets have size  $\Theta_\delta(n)$ , and that*

$$\begin{aligned} & \sum_{r,s \in I} \left\| t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b''_n s}{n} + t_2(w_i - w_j)(r - s) \right\|_{\mathbb{R}/\mathbb{Z}}^2 \\ & \geq \sum_{s \in I_0} \sum_{h \in J_s} \left\| t_1(w_i - w_j) \frac{b(h+2s)h + b'_n h}{n} + t_2(w_i - w_j)h \right\|_{\mathbb{R}/\mathbb{Z}}^2. \end{aligned}$$

*Proof.* By Fact 4.1, there exists a subset  $\mathcal{R} \subset \{-n, \dots, n\}$  with  $|\mathcal{R}| = \Theta_\delta(n)$ , such that for every  $h \in \mathcal{R}$ , there are  $\Theta_\delta(n)$  pairs  $r, s \in I$  with  $r - s = h$ . For each  $s \in I$ , let  $J_s$  denote the set of  $h \in \mathcal{R}$  such that  $s + h \in I$ . By double counting the pairs  $r, s \in I$  with  $r - s \in \mathcal{R}$ , we deduce that  $|J_s| = \Theta_\delta(n)$  for  $\Theta_\delta(n)$  many  $s \in I$ . Denote the set of such  $s$  by  $I_0$ .

The sum is bounded from below by

$$\sum_{h \in \mathcal{R}} \sum_{r, s \in I: r-s=h} \|t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b'_n s}{n} + t_2(w_i - w_j)(r - s)\|_{\mathbb{R}/\mathbb{Z}}^2,$$

which simplifies to

$$\sum_{s \in I} \sum_{h \in J_s} \|t_1(w_i - w_j) \frac{b(h+2s)h + b'_n h}{n} + t_2(w_i - w_j)h\|_{\mathbb{R}/\mathbb{Z}}^2,$$

by the substitution  $r = s + h$ . Restricting the outer sum to  $s \in I_0$ , we obtain the desired inequality.  $\square$

To complete the treatment in this case, we just proceed as how we proved (39) for each of the sum  $\sum_{h \in J_s} \|t_1(w_i - w_j) \frac{b(h+2s)h + b'_n h}{n} + t_2(w_i - w_j)h\|_{\mathbb{R}/\mathbb{Z}}^2$ , using Lemma 2.6.

**Case 2.** Assume that  $|t_1| < \frac{\sqrt{A \log n}}{2n}$ . Then since  $\frac{\sqrt{A \log n}}{n} \leq \|\mathbf{t}\|_2 \leq 1$ , we must have

$$\frac{\sqrt{A \log n}}{2n} \leq |t_2| \leq 1.$$

As in the proof of (25), we consider  $\mathcal{G}$  to be the collection of pairs  $i, j$  where  $|w_i - w_j| \geq 1/2\sqrt{n}$ . First notice that because  $|t_1| < \frac{C\sqrt{\log n}}{2n}$  and  $|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}}$ , we have

$$|t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b'_n s}{n}| \leq \frac{2}{\sqrt{A}}. \quad (43)$$

For any fixed  $s$ , applying Corollary 2.5 with  $b = t_2(w_i - w_j)$  and  $b_0 = -t_2(w_i - w_j)s$  and assuming that  $|t_2|D_k \geq 1/Cn$ , gives

$$\sum_r \|t_2(w_i - w_j)(r - s)\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n,$$

and, together with (43), we obtain

$$\sum_r \|t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b'_n s}{n} + t_2(w_i - w_j)(r - s)\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_C n.$$

Now if  $|t_2|D_k < 1/Cn$ , then

$$\|t_1(w_i - w_j) \frac{br^2 + b'_n r - bs^2 - b'_n s}{n} + t_2(w_i - w_j)(r - s)\|_{\mathbb{R}/\mathbb{Z}}^2 = (w_i - w_j)^2 |t_1 \frac{br^2 + b'_n r - bs^2 - b'_n s}{n} + t_2(r - s)|^2.$$

To finish, we use the following fact.

**Claim 6.4.** For any fixed  $s \in I$ , the 2-dimensional vectors  $(\frac{br^2 + b'_n r - bs^2 - b'_n s}{n^2}, \frac{r-s}{n})$ ,  $r \in I$  completely span  $\mathbb{R}^2$  in the sense that for any unit vector  $(t_1, t_2)$  we have

$$\sum_{r \in I} |(t_1, t_2) \cdot (\frac{br^2 + b'_n r - bs^2 - b'_n s}{n^2}, \frac{r-s}{n})|^2 \asymp n.$$

*Proof.* We only restrict to  $r$  for which  $r-s$  has order  $n$ . We rewrite  $(\frac{br^2+b'_n r-bs^2-b'_n s}{n^2}, \frac{r-s}{n})$  as  $(\frac{b(h+2s)h+b'_n h}{n^2}, \frac{h}{n})$ , where  $h := r - s$ . Choose any pairs  $h, h'$  of order  $n$  (i.e.  $|r - s|, |r' - s|$  is of order  $n$ ) so that

$$|h - h'| \asymp n.$$

We see that the vectors  $(\frac{b(h+2s)h+b'_n h}{n^2}, \frac{h}{n})$  and  $(\frac{b(h'+2s)h'+b'_n h'}{n^2}, \frac{h'}{n})$  both have norm of order 1, and area of the parallelogram formed by them is

$$|\frac{b(h+2s)h+b'_n h}{n^2} \frac{h}{n} - \frac{b(h'+2s)h'+b'_n h'}{n^2} \frac{h'}{n}| = |\frac{b(h-h')hh'}{n^3}| \asymp 1.$$

As such, for any unit vector  $(t_1, t_2)$

$$|(t_1, t_2) \cdot (\frac{b(h+2s)h+b'_n h}{n^2}, \frac{h}{n})|^2 + |(t_1, t_2) \cdot (\frac{b(h'+2s)h'+b'_n h'}{n^2}, \frac{h'}{n})|^2 \asymp 1.$$

To finish the proof, we just choose  $\Theta(n^2)$  distinct pairs  $(r, r')$  from  $I^2$  satisfying the above properties, and sum up the estimates.  $\square$

As a corollary, for each fixed  $s$ , by the claim

$$\sum_r (w_i - w_j)^2 |t_1(\frac{br^2+b'_n r-bs^2-b'_n s}{n^2}) + t_2(r-s)|^2 \asymp (w_i - w_j)^2 (t_1^2 + t_2^2) n^3.$$

The rest of the proof from this point on is similar to our proof of (25), we omit the details. This completes our proof of Lemma 6.2.  $\square$

**Lemma 6.5** (Very large  $\|\mathbf{t}\|_2$ ). *For  $\mathbf{t} = (t_1, t_2)$  such that  $1 \leq \|\mathbf{t}\|_2 \leq \sqrt{A \log n}$  we have*

$$|\varphi_{\mathbf{X}}(\mathbf{t})| \leq n^{-2\sqrt{A}}.$$

*Proof.* (of Lemma 6.5) If  $1 \leq |t_1| \leq \sqrt{A \log n}$ , then we can argue as in the proof of (10) for very large  $|\mathbf{t}|$ . If  $(\sqrt{A \log n})/n \leq |t_1| \leq 1$ , we can also argue as in the proof of (9) for large  $|\mathbf{t}|$ . It remains to assume  $|t_1| \leq (\sqrt{A \log n})/n$ , in which case  $1/2 \leq |t_2| \leq \sqrt{A \log n}$ . To this end, we recall (43) that  $|t_1(w_i - w_j)\frac{br^2+b'_n r-bs^2-b'_n s}{n}| \leq \frac{2}{\sqrt{A}}$ . We can then argue as in the proof of (10), again applying Corollary 2.5.  $\square$

By Lemmas 6.2 and 6.5, it suffices to focus on  $\|\mathbf{t}\|_2 \leq \frac{\sqrt{A \log n}}{n}$ . In this case,

$$|\varphi_{\mathbf{X}}(\mathbf{t})| \leq \exp \left( -\frac{1}{2n^3} \sum_{1 \leq i, j \leq n; r, s \in I} \left| t_1(w_i - w_j) \frac{br^2+b'_n r-bs^2-b'_n s}{n} + t_2(w_i - w_j)(r-s) \right|^2 \right).$$

Since  $\sum_{1 \leq i, j \leq n} (w_i - w_j)^2 = 2n$ , the exponent simplifies to

$$\frac{1}{n^2} \sum_{r, s \in I} \left| t_1 \frac{br^2+b'_n r-bs^2-b'_n s}{n} + t_2(r-s) \right|^2.$$

Again by Claim 6.4,

$$\frac{1}{n^2} \sum_{r, s \in I} \left| t_1 \frac{br^2+b'_n r-bs^2-b'_n s}{n} + t_2(r-s) \right|^2 \asymp (t_1^2 + t_2^2) n^2.$$

Using this, we are done with the proof of (41).  $\square$

*Proof.* (of Equation (42)) For simplicity, we replace  $bk^2 + b'_n k + b''_n$  with  $k^2$ ; the argument extends without change to the general case. Our starting point is a two-dimensional variant of (29):

$$\int_{\mathbb{R}^2} e^{-\pi\|\mathbf{t}\|_2^2} e^{i\mathbf{t}\cdot\mathbf{x}} d\mathbf{t} = e^{-\pi\|\mathbf{x}\|_2^2/2}. \quad (44)$$

Hence

$$\mathbb{E} \int_{\mathbb{R}^2} e^{-\pi\|\mathbf{t}\|_2^2} e^{i\mathbf{t}\cdot\mathbf{X}} d\mathbf{t} = \mathbb{E} e^{-\pi\|\mathbf{X}\|_2^2/2}.$$

For any  $K$  (noting here and later that the integrals are real-valued because of the symmetry of the range of  $t$ ),

$$-\int_{\|\mathbf{t}\|_2 \geq K} e^{-\pi\|\mathbf{t}\|_2^2} d\mathbf{t} \leq \int_{\|\mathbf{t}\|_2 > K} e^{-\pi\|\mathbf{t}\|_2^2} e^{i\mathbf{t}\cdot\mathbf{x}} d\mathbf{t} \leq \int_{\|\mathbf{t}\|_2 \geq K} e^{-\pi\|\mathbf{t}\|_2^2} d\mathbf{t} \leq e^{-C'K^2}.$$

Thus, for sufficiently large  $A$ , with

$$\mathbf{X} = \mathbf{S} - n\mathbf{L} = (S_1 - nL_1, S_2 - nL_2),$$

$$\left| \mathbb{E} \int_{\|\mathbf{t}\|_2 \geq \sqrt{A \log n}} e^{-\pi\|\mathbf{t}\|_2^2} e^{i\mathbf{t}\cdot\mathbf{X}} d\mathbf{t} \right| \leq \int_{\|\mathbf{t}\|_2 \geq \sqrt{A \log n}} e^{-\pi\|\mathbf{t}\|_2^2} d\mathbf{t} \leq n^{-2\sqrt{A}}.$$

We thus have (note that the integral is real because of the symmetry of the range of  $t$ )

$$\begin{aligned} \mathbb{P}(\|\mathbf{X}\|_2 \leq 1) &\leq e^\pi \mathbb{E} e^{-\pi\|\mathbf{X}\|_2^2/2} \\ &\leq e^\pi \left[ \mathbb{E} \int_{\|\mathbf{t}\|_2 \leq \sqrt{A \log n}} e^{-\pi\|\mathbf{t}\|_2^2} e^{i\mathbf{t}\cdot\mathbf{X}} d\mathbf{t} + n^{-2\sqrt{A}} \right] \\ &\leq e^\pi \int_{\|\mathbf{t}\|_2 \leq \sqrt{A \log n}} e^{-\pi\|\mathbf{t}\|_2^2} \mathbb{E} e^{i\mathbf{t}\cdot\mathbf{X}} d\mathbf{t} + e^\pi n^{-2\sqrt{A}}. \end{aligned}$$

Next, if  $\mathbb{P}(\|\mathbf{X}\|_2 \leq 1) \leq 2e^{\pi/2}n^{-2\sqrt{A}}$ , then there is nothing to prove. Assume otherwise, then from the above we have

$$\mathbb{P}(\|\mathbf{X}\|_2 \leq 1) \leq 2e^\pi \int_{\|\mathbf{t}\|_2 \leq \sqrt{A \log n}} e^{-\pi\|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t}.$$

It remains to bound the RHS. As we assume that  $L_1, L_2 = O(\sqrt{\log n})$ , by Lemma 6.2 and Lemma 6.5, it suffices to focus on  $\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n$ . Without loss of generality<sup>8</sup>, let us assume

$$L_2 \geq L_1.$$

We will establish the bound

$$\int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n} e^{-\pi\|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} = O\left(\frac{e^{-cL_2^2}}{n^2}\right).$$

---

<sup>8</sup>The case  $L_1 > L_2$  can be treated similarly by applying (16) to the sequence of squares corresponding to the sum  $S_1$  in (31) instead.

We first write

$$\begin{aligned} \int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} &\leq \int_{|t_1| \leq L_2/n, |t_2| \leq L_2/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} \\ &+ \int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n, L_2/n \leq |t_1| \leq (\sqrt{A \log n})/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} \\ &+ \int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n, L_2/n \leq |t_2| \leq (\sqrt{A \log n})/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t}. \end{aligned}$$

For the second integral, recall that for  $\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n$ , we have  $|\varphi_{\mathbf{X}}(\mathbf{t})| \leq \exp(-\Theta(\|\mathbf{t}\|_2^2 n^2))$ , so

$$\int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n, L_2/n \leq |t_1| \leq (\sqrt{A \log n})/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} \leq \frac{1}{n^2} \int_{L_2 \leq |x_1|} e^{-\Theta(x_1^2 + x_2^2)} dx_1 dx_2 \leq \frac{1}{n^2} e^{-\Theta(L_2^2)}.$$

The third integral is bounded similarly:

$$\int_{\|\mathbf{t}\|_2 \leq (\sqrt{A \log n})/n, L_2/n \leq |t_2| \leq (\sqrt{A \log n})/n} e^{-\pi \|\mathbf{t}\|_2^2} \varphi_{\mathbf{X}}(\mathbf{t}) d\mathbf{t} \leq \frac{1}{n^2} \int_{L_2 \leq |x_2|} e^{-\Theta(x_1^2 + x_2^2)} dx_1 dx_2 \leq \frac{1}{n^2} e^{-\Theta(L_2^2)}.$$

It remains to work with the first integral. By the change of variables  $x_1 = nt_1$ ,  $x_2 = nt_2$ , it becomes

$$\frac{1}{n^2} \int_{|x_1| \leq L_2, |x_2| \leq L_2} e^{-\pi \|\mathbf{x}\|_2^2 / n^2} \varphi_{\mathbf{X}/n}(\mathbf{x}) dx_2 dx_1,$$

where (recalling that  $S_1 = \sum_{k \in I} k^2 w_{\pi(k)}/n$ ,  $S_2 = \sum_{k \in I} k w_{\pi(k)}$ )

$$\varphi_{\mathbf{X}/n}(\mathbf{x}) = \mathbb{E} e^{i\mathbf{x} \cdot \mathbf{X}/n} = \mathbb{E} e^{ix_1 X_1 + ix_2 (S_2/n - L_2)} = e^{-ix_2 L_2} \mathbb{E} e^{ix_1 X_1 + ix_2 S_2/n}.$$

In what follows we will fix  $x_1 \in [-L_2, L_2]$  and consider only the inner integral with respect to  $x_2$ ,

$$\begin{aligned} f(x_1) &= \int_{|x_2| \leq L_2} e^{-\pi \|\mathbf{x}\|_2^2 / n^2} (\varphi_{\mathbf{X}/n}(x_1, x_2) + \varphi_{\mathbf{X}/n}(-x_1, x_2)) dx_2 \\ &=: \int_{|x_2| \leq L_2} e^{-\pi \|\mathbf{x}\|_2^2 / n^2} (\varphi_{\mathbf{X}/n, x_1}(x_2) + \varphi_{\mathbf{X}/n, -x_1}(x_2)) dx_2 \end{aligned}$$

To treat with this integral, we first extend  $x_2$  to complex numbers via

$$\begin{aligned} \varphi_{\mathbf{X}/n, x_1}(z) &= e^{-iz L_2} \mathbb{E} e^{ix_1 X_1 + iz(S_2/n)} \\ \varphi_{\mathbf{X}/n, -x_1}(z) &= e^{-iz L_2} \mathbb{E} e^{-ix_1 X_1 + iz(S_2/n)}. \end{aligned}$$

For short, let

$$\begin{aligned} h_{x_1}(x_2) &= e^{-\pi(x_1^2 + x_2^2)/n^2} (\mathbb{E} e^{ix_1 X_1 + ix_2 (S_2/n)} + \mathbb{E} e^{-ix_1 X_1 + ix_2 (S_2/n)}) \\ &= e^{-\pi(x_1^2 + x_2^2)/n^2} \mathbb{E} (e^{ix_1 X_1} + e^{-ix_1 X_1}) e^{ix_2 (S_2/n)}. \end{aligned} \tag{45}$$

This function can be extended holomorphically to

$$h_{x_1}(z) = e^{-\pi(x_1^2 + z^2)/n^2} (\mathbb{E} e^{ix_1 X_1 + iz(S_2/n)} + \mathbb{E} e^{-ix_1 X_1 + iz(S_2/n)}).$$

Since  $|\mathbb{E}Y| \leq \mathbb{E}|Y|$  for any complex-valued random variable  $Y$ , for  $z = t + is$ , inequality (16) gives

$$|\mathbb{E} e^{ix_1 X_1 + i(t+is)(S_2/n)} + \mathbb{E} e^{-ix_1 X_1 + i(t+is)(S_2/n)}| \leq 2 \mathbb{E} e^{-s S_2/n} \leq 2C'_0 e^{C'_0 s^2}. \tag{46}$$

We write

$$f(x_1) = \int_{|x_2| \leq L_2} e^{-\pi \|\mathbf{x}\|_2^2 / n^2} (\varphi_{\mathbf{X}/n, x_1}(x_2) + \varphi_{\mathbf{X}/n, -x_1}(x_2)) dx_2 = \int_{|x_2| \leq L_2} e^{-ix_2 L_2} h_{x_1}(x_2) dx_2.$$

By using contour integral, we pass to the line  $\mathbb{R} - icL$

$$\begin{aligned} \int_{|x_2| \leq L_2} e^{-ix_2 L_2} h_{x_1}(x_2) dx_2 &= \Re\left(\int_{z \in \mathbb{R} - icL_2, |\Re(z)| \leq L_2} e^{-iz L_2} h_{x_1}(z) dz\right) \\ &= \Re\left(\int_{|t| \leq L_2} e^{-i(t - icL_2)L_2} h_{x_1}(t - icL_2) dt\right) \\ &= (e^{-cL_2^2}) \Re\left(\int_{|t| \leq L_2} e^{-itL_2} h_{x_1}(t - icL_2) dt\right), \end{aligned} \quad (47)$$

where it is crucial to notice that the first integral is real-valued because  $h_{x_1}(-x_2) = \overline{h_{x_1}(x_2)}$  from (45) and the real part of the integrals (with opposite orientation) on the lines  $\Re(z) = -L_2$  and  $\Re(z) = L_2$  cancel each other. More specifically

$$\Re \int_{z = -L_2 - it, 0 \leq t \leq cL} e^{-izL_2} h_{x_1}(z) dt = \Re \int_{z = L_2 - it, 0 \leq t \leq cL} e^{-izL_2} h_{x_1}(z) dt$$

as they are conjugate to each other: this follows from that fact that  $S_1, S_2 \in \mathbb{R}$  and  $h_{x_1}(-x + it) = \overline{h_{x_1}(x + it)}$ , which can be seen from

$$\begin{aligned} h_{x_1}(-x + iy) &= e^{-\pi x_1^2/n^2 - \pi(-x+iy)^2/n^2} \mathbb{E}(e^{ix_1 X_1/n} + e^{-ix_1 X_1/n}) e^{i(-x+iy) S_2/n} \\ &= e^{-\pi(x_1^2 + x^2 - y^2)/n^2} e^{2\pi ixy/n^2} \mathbb{E}(e^{ix_1 X_1/n} + e^{-ix_1 X_1/n}) e^{-ix S_2/n} e^{-y X_2/n}, \end{aligned}$$

while

$$h_{x_1}(x + iy) = e^{-\pi(x_1^2 + x^2 - y^2)/n^2} e^{-2\pi ixy/n^2} \mathbb{E}(e^{ix_1 X_1/n} + e^{-ix_1 X_1/n}) e^{ix X_2/n} e^{-y S_2/n}.$$

To continue (47), note that

$$|e^{-\pi(t - icL_2)^2/n^2}| = e^{-\pi(t^2 - c^2 L_2^2)/n^2} \approx 1, \text{ as } n \rightarrow \infty \text{ and } L_2 = O(\sqrt{\log n})$$

and so by (46),

$$\begin{aligned} |h_{x_1}(t - icL_2)| &= |e^{-\pi(t - icL_2)^2/n^2}| |\mathbb{E} e^{ix_1 X_1 + i(t + icL_2)(S_2/n)} + \mathbb{E} e^{-ix_1 X_1 + i(t - icL_2)(S_2/n)}| \\ &= O(e^{C'_0 c^2 L_2^2}). \end{aligned}$$

Putting together, by choosing  $c = 1/8C'_0$ , we have obtained a bound

$$|f(x_1)| \leq (e^{-cL_2^2}) \times e^{C'_0 c^2 L_2^2} \times 2L_2 = O(e^{-\Theta(L_2^2)}).$$

All together, in the case  $\mathbb{P}(\|\mathbf{X}\|_2 \leq 1) \leq 2e^{\pi/2} n^{-2\sqrt{A}}$  we have

$$\mathbb{P}(\|\mathbf{X}\|_2 \leq 1) \leq \frac{1}{n^2} \int_{|x_1| \leq L_2} |f(x_1)| dx_1 = O\left(\frac{1}{n^2} L_2 e^{-\Theta(L_2^2)}\right) = O\left(\frac{1}{n^2} e^{-\Theta(L_2^2)}\right),$$

completing the proof.  $\square$

To conclude this section, we present below a comparison estimate, which will be useful for the next section.

**Theorem 6.6.** *Let  $d \geq 2$  be a fixed integer, and let  $\delta > 0$ ,  $b \neq 0$ ,  $c \neq 0$ , and  $\tilde{B} > 0$  be constants. Suppose<sup>9</sup> that the sequence  $(w_1, \dots, w_n)$  satisfies  $\sigma(\mathbf{w}) = 1$ , and that*

$$|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}} \quad \text{for all } i, j,$$

---

<sup>9</sup>Note that  $\sum_i w_i$  is not necessarily zero.

for some sufficiently large constant  $A > 0$ . Let  $I \subset [n]$  be any subset with  $|I| \geq \delta n$ , and consider the sequences  $(v_1, \dots, v_n)$  and  $(v'_1, \dots, v'_n)$  partially specified by

$$v_i = \frac{P_d(i)}{n^d} \quad \text{and} \quad v'_i = \frac{P_{d-1}(i)}{n^{d-1}} \quad \text{for all } i \in I,$$

where  $P_d$  and  $P_{d-1}$  are real polynomials of degrees  $d$  and  $d-1$ , respectively, with fixed leading coefficients  $b$  and  $c$ , and whose remaining coefficients may depend on  $n$ . Assume that

$$|v_i|, |v'_i| \leq \tilde{B} \quad \text{for all } i \in [n], \quad \text{and} \quad \left| \sum_{i=1}^n v'_i \right| \leq \tilde{B} \left| \sum_{i=1}^n v_i \right|.$$

Then,

$$\mathbb{P}\left(\left| \sum_{i=1}^n w_i v_{\pi(i)} \right| \leq \frac{1}{n} \left| \sum_{i=1}^n w_i v'_{\pi(i)} \right|\right) = O_A\left(\frac{1}{n}\right). \quad (48)$$

Our proof shows that we can actually relax the condition  $|\sum_i v'_i| \ll |\sum_i v_i|$  to  $|\bar{v}' \cdot \bar{w}| \ll |\bar{v} \cdot \bar{w}|$ . In the centered case, where  $\bar{w} = 0$ , the latter condition holds for all  $v_i$  and  $v'_i$ . Note also that a weaker version of this result, in which the right-hand side is  $O\left(\frac{\sqrt{\log n}}{n}\right)$ , can be handled by a much simpler method (by not relying on Theorem 1.19 for the joint event, but instead using Theorem 1.18 together with Lemma 2.3). We leave the details to the reader.

*Proof of Theorem 6.6.* Let

$$X_1 = \sum_{i=1}^n w_i v_{\pi(i)}, \quad X_2 = \sum_{i=1}^n w_i v'_{\pi(i)}.$$

Then, define  $a := \mathbb{E}X_1 = \bar{v}' \cdot \bar{w}$  and  $b := \mathbb{E}X_2 = \bar{v} \cdot \bar{w}$ . By the assumption,

$$|a| \leq \tilde{B}|b|.$$

Let  $I_k = [k-1, k]$  if  $k$  is a positive integer, and  $I_k = [-k, -k+1]$  if  $k$  is a negative integer. We will consider the joint events that  $|X_2| \in I_k$  and  $|X_1| \in I_l/n$  for some integer  $l$  with  $1 \leq |l| \leq |k|$ .

By Theorem 1.19, and by decomposing  $I_k$  into  $n$  intervals of length  $1/n$  each, we have

$$\mathbb{P}(|X_2| \in I_k, |X_1| \in I_l/n) \ll n \cdot \frac{1}{n^2} e^{-\Theta((k-a)^2)} e^{-\Theta((l/n-b)^2)} \ll \frac{1}{n} e^{-\Theta((k-a)^2)} e^{-\Theta((l/n-b)^2)}.$$

Summing over  $l$  with  $1 \leq |l| \leq |k|$  and over  $k$  gives the bound

$$\mathbb{P}(|X_1| \leq |X_2|/n) \ll \frac{1}{n} \sum_{1 \leq |l| \leq |k|} e^{-\Theta((k-a)^2)} e^{-\Theta((l/n-b)^2)}.$$

To estimate the above double sum, we consider two regimes:  $|k| \geq 2|a|$  and  $|k| < 2|a|$ . Since  $(k-a)^2 \geq k^2/4$  for  $|k| \geq 2|a|$ , we see that

$$\begin{aligned} \frac{1}{n} \sum_{1 \leq |l| \leq |k|; |k| \geq 2|a|} e^{-\Theta((k-a)^2)} e^{-\Theta((l/n-b)^2)} &\leq \frac{1}{n} \sum_{1 \leq |l| \leq |k|; |k| \geq 2|a|} e^{-\Theta(k^2)} \\ &\leq \frac{1}{n} \sum_k 2|k| e^{-\Theta(k^2)} = O\left(\frac{1}{n}\right). \end{aligned}$$

For  $1 \leq |l| \leq |k| < 2|a|$ , we have  $|l|/n < (2|a|)/n < (2B'|b|)/n \leq |b|/2$ , so  $(l/n - b)^2 \geq b^2/4$ . It follows that

$$\frac{1}{n} \sum_{1 \leq |l| \leq |k| < 2|a|} e^{-\Theta((k-a)^2)} e^{-\Theta((l/n-b)^2)} \ll \frac{1}{n} \sum_{1 \leq |l| \leq |k| < 2|a|} e^{-\Theta(b^2)} \ll \frac{a^2 e^{-\Theta(b^2)}}{n} \ll \frac{1}{n}$$

for  $|a| \leq \tilde{B}|b|$ .  $\square$

## 7. SOME GENERALIZATIONS OF OUR RESULTS

In this section we discuss a few more generalizations of our results. First of all, Condition (4) can be replaced by the following weaker assumption.

**Condition 7.1** (Non-degeneracy II). *Let  $\varepsilon > 0$ , and suppose  $A$  is sufficiently large depending on  $\varepsilon$ . A sequence  $w_1, \dots, w_n$  is said to be not too degenerate if*

$$\sum_{\substack{i < j \\ |w_i - w_j|/\sigma(\mathbf{w}) \leq 1/A\sqrt{\log n}}} (w_i - w_j)^2 > \varepsilon n \sigma^2(\mathbf{w}). \quad (49)$$

In other words, we allow distances of order larger than  $\sigma(\mathbf{w})/A\sqrt{\log n}$ , but require that the contribution from pairs at smaller distances is not too small relative to the main term  $n\sigma^2(\mathbf{w})$ .

**Theorem 7.2.** *All of our results, including Theorem 1.15, Theorem 1.17, Theorem 4.4, Theorem 1.18, Theorem 1.19 and Theorem 6.6 extend to  $(w_i)$  satisfying (49) (with the normalization  $\sigma(\mathbf{w}) = 1$ ).*

*Proof.* Since in the proofs of all these theorems we focused only on pairs  $w_i, w_j$  with  $|w_i - w_j| \leq \frac{1}{A\sqrt{\log n}}$ , Condition (49) ensures that the contribution from such pairs is significant. For example, in the proof of Theorem 1.15, this condition was invoked in Case 1 of the analysis for “large  $|t|$ ”, in the treatment of “small  $|t|$ ”, and again in the treatment of “very large  $|t|$ ”.  $\square$

In the remainder of this section, we present several preparatory observations that will serve as useful ingredients for the proof of Theorem 1.28 in Section 8.

**Lemma 7.3.** *Let  $w_1, \dots, w_n \in \mathbb{R}$  satisfy  $\bar{w} = 0$  and  $\sigma(\mathbf{w}) = 1$ . Fix  $\varepsilon \in (0, 1]$  and  $K \geq \sqrt{2/\varepsilon}$ . Assume that*

$$\sum_{i: |w_i| \leq K/\sqrt{n}} w_i^2 \geq \varepsilon.$$

*Then there exist disjoint subsets  $I, J \subset [n]$  with  $|I| = |J| \geq \lfloor (\varepsilon/32K^2)n \rfloor$ , such that*

$$\sqrt{\frac{\varepsilon}{2n}} \leq |w_i - w_j| \leq \frac{2K}{\sqrt{n}} \quad \text{for all } i \in I, j \in J.$$

*Proof.* (of Lemma 7.3) Let  $S$  denote the set of indices  $i \in [n]$  satisfying  $|w_i| \leq K/\sqrt{n}$ . We begin by proving

$$\sum_{\substack{i < j \\ i, j \in S}} (w_i - w_j)^2 \geq \varepsilon n/2.$$

Indeed,

$$\sum_{\substack{i < j \\ i, j \in S}} (w_i - w_j)^2 = |S| \sum_{i \in S} w_i^2 - \left( \sum_{i \in S} w_i \right)^2 = |S| \sum_{i \in S} w_i^2 - \left( \sum_{i \in S^c} w_i \right)^2.$$

We bound the two terms separately. Since  $|w_i| > K/\sqrt{n}$  for  $i \in S^c$ ,

$$|S^c| \leq n/K^2.$$

As  $K \geq \sqrt{2/\varepsilon} \geq \sqrt{2}$ , we obtain

$$|S| \geq n - n/K^2 \geq n/2.$$

Moreover, by Cauchy–Schwarz,

$$\left( \sum_{i \in S} w_i \right)^2 = \left( \sum_{i \in S^c} w_i \right)^2 \leq |S^c| \sum_{i \in S^c} w_i^2 \leq |S^c|(1 - \varepsilon) \leq (1 - \varepsilon)n/K^2.$$

Combining these estimates and using  $\sum_{i \in S} w_i^2 \geq \varepsilon$ , we obtain

$$\sum_{\substack{i < j \\ i, j \in S}} (w_i - w_j)^2 \geq |S|\varepsilon - (1 - \varepsilon)n/K^2 \geq (n - n/K^2)\varepsilon - (1 - \varepsilon)n/K^2 \geq \varepsilon n/2.$$

We now proceed to construct  $I$  and  $J$ . Without loss of generality, assume  $S = [m]$  and  $w_1 \geq w_2 \geq \dots \geq w_m$ . Let  $p := \lfloor (\varepsilon/32K^2)n \rfloor$ , and define  $I := \{1, 2, \dots, p\}$ ,  $J := \{m - p + 1, \dots, m\}$ . It suffices to show that

$$w_p - w_{m-p+1} \geq \sqrt{\varepsilon/2n}.$$

Suppose instead that  $w_p - w_{m-p+1} < \sqrt{\varepsilon/2n}$ . Then  $|w_i - w_j| < \sqrt{\varepsilon/n}$  whenever  $p + 1 \leq i < j \leq m - p$ , and  $|w_i - w_j| \leq 2K/\sqrt{n}$  whenever  $i \in I \cup J$ ,  $j \in S$ . Consequently,

$$\sum_{\substack{i < j \\ i, j \in S}} (w_i - w_j)^2 < |I \cup J||S| \left( \frac{2K}{\sqrt{n}} \right)^2 + \binom{|S|}{2} \left( \sqrt{\frac{\varepsilon}{2n}} \right)^2.$$

Since  $|I \cup J| \leq (\delta/16K^2)n$  and  $|S| \leq n$ , this gives

$$\sum_{\substack{i < j \\ i, j \in S}} (w_i - w_j)^2 < (\varepsilon/16K^2)n^2 \left( \frac{2K}{\sqrt{n}} \right)^2 + \binom{n}{2} \left( \sqrt{\frac{\varepsilon}{n}} \right)^2 < \varepsilon n/2,$$

contradicting the earlier bound. The lemma follows.  $\square$

**Lemma 7.4.** *Let  $w_1, \dots, w_n \in \mathbb{R}$  satisfy  $\bar{w} = 0$  and  $\sigma(\mathbf{w}) = 1$ . Suppose there exists  $K \geq 1$  such that*

$$\frac{1}{n} \sum_{i=1}^n (nw_i^2)^2 \leq K.$$

For  $m \in [n]$ , sample an ordered tuple  $(w'_1, \dots, w'_m)$  uniformly without replacement from  $\{w_1, \dots, w_n\}$ , and set

$$S_m := \sum_{k=1}^m (w'_k)^2.$$

Then for any  $C > 0$ ,

$$\mathbb{P}\left( \left| S_m - \frac{m}{n} \right| \geq C \frac{m}{n} \right) \leq \frac{K}{C^2 m}.$$

*Proof.* (of Lemma 7.4) Let  $Y_i := w_i^2$  and note that  $\mu := \frac{1}{n} \sum_{i=1}^n Y_i = \frac{1}{n}$ , so  $\mathbb{E} S_m = m\mu = m/n$ . The variance of a without-replacement sum is

$$\text{Var}(S_m) = \frac{m(n-m)}{n-1} \sigma_Y^2, \quad \sigma_Y^2 := \frac{1}{n} \sum_{i=1}^n (Y_i - \mu)^2.$$

We bound  $\sigma_Y^2$  using the moment condition.

$$\frac{1}{n} \sum_i Y_i^2 = \frac{1}{n^2} \frac{1}{n} \sum_{i=1}^n (nw_i^2)^2 \leq \frac{K}{n^2}.$$

Hence  $\sigma_Y^2 = \frac{1}{n} \sum Y_i^2 - \mu^2 \leq Kn^{-2}$ . Therefore

$$\text{Var}(S_m) \leq \frac{Kn}{n^2}.$$

Applying Chebyshev inequality gives

$$\mathbb{P}\left(\left|S_m - \frac{m}{n}\right| \geq C \frac{m}{n}\right) \leq \frac{\text{Var}(S_m)}{(Cm/n)^2} \leq \frac{K}{C^2 m}. \quad \square$$

**Corollary 7.5.** *Let  $w_1, \dots, w_n \in \mathbb{R}$  satisfy Condition 1.26 for some  $K > 1$ . That is the rescaled squares  $X_i := n(w_i - \bar{w})^2 / \sigma^2(\mathbf{w})$  satisfy the  $\ell_2$  moment bound*

$$\frac{1}{n} \sum_{i=1}^n X_i^2 \leq K.$$

For  $m \in [n]$ , sample an ordered tuple  $(w'_1, \dots, w'_m)$  uniformly without replacement from  $\{w_1, \dots, w_n\}$ . Then, with probability at least  $1 - O_K(1/m)$ ,

- (i)  $(w'_i)$  is not too degenerate;
- (ii)  $\sup_x |\{i : w'_i = x\}| \leq cm$ , for some constant  $c \in (0, 1)$  depending only on  $K$ .

*Proof.* (of Corollary 7.5) We first deduce from Condition 1.26 that

$$\sum_{|w_i - \bar{w}|/\sigma(\mathbf{w}) \leq K/\sqrt{n}} (w_i - \bar{w})^2 \geq (1 - 1/K) \sigma^2(\mathbf{w}).$$

Indeed, by assumption

$$\sum_{|w_i - \bar{w}|/\sigma(\mathbf{w}) > K/\sqrt{n}} (K\sigma(\mathbf{w})/\sqrt{n})^2 n(w_i - \bar{w})^2 / \sigma^4(\mathbf{w}) \leq \sum_{|w_i - \bar{w}|/\sigma(\mathbf{w}) > K/\sqrt{n}} n(w_i - \bar{w})^4 / \sigma^4(\mathbf{w}) \leq K.$$

So

$$\sum_{|w_i - \bar{w}|/\sigma(\mathbf{w}) > K/\sqrt{n}} (w_i - \bar{w})^2 \leq \sigma^2(\mathbf{w})/K,$$

and hence

$$\sum_{|w_i - \bar{w}|/\sigma(\mathbf{w}) \leq K/\sqrt{n}} (w_i - \bar{w})^2 \geq (1 - 1/K) \sigma^2(\mathbf{w}).$$

Next, without loss of generality, assume  $\bar{w} = 0$  and  $\sigma(\mathbf{w}) = 1$ . By the above estimate, Lemma 7.3 applies to the sequence  $(w_i)$  (with  $\varepsilon = 1 - 1/K$ ) and yields two disjoint subsets  $I, J \subset [n]$  with  $|I| = |J| = \Omega(n)$  such that  $\frac{2K}{\sqrt{n}} \geq |w_i - w_j| \geq \sqrt{\frac{\varepsilon}{2n}}$  for all  $i \in I, j \in J$ . Then, by Hoeffding's inequality for sampling without

replacement (see [19]), with probability at least  $1 - \exp(-\Theta(m))$ , the sample contains two disjoint subsets  $I', J' \subset [m]$ , each of size  $\Omega(m)$ , satisfying

$$\sqrt{\frac{\varepsilon}{2n}} \leq |w'_i - w'_j| \leq \frac{2K}{\sqrt{n}} \quad \text{for all } i \in I', j \in J'.$$

On the intersection of this event with the concentration event from Lemma 7.4, we see that

$$\frac{m}{2n} \leq \sigma^2(\mathbf{w}') \leq \frac{3m}{2n}.$$

For any  $i \in I'$  and  $j \in J'$ , we have  $\sqrt{\frac{\varepsilon}{2n}} \leq |w'_i - w'_j| \leq \frac{2K}{\sqrt{n}} \leq \frac{3K\sigma(\mathbf{w}')}{\sqrt{m}}$ , and hence

$$\sum_{\substack{i < j \\ |w'_i - w'_j|/\sigma(\mathbf{w}') \leq 3K/\sqrt{m}}} (w'_i - w'_j)^2 \geq |I'| |J'| \left( \sqrt{\frac{\varepsilon}{2n}} \right)^2 = \Omega\left(\frac{m^2}{n}\right) = \Omega(m \sigma^2(\mathbf{w}')).$$

Thus  $(w'_i)$  is not too degenerate. Finally,

$$\sup_x \left| \{i : w'_i = x\} \right| \leq \min(m - |I'|, m - |J'|) = (1 - \Omega(1))m. \quad \square$$

## 8. APPLICATION TO RANDOM POLYNOMIALS: PROOF OF THEOREM 1.28

We will use Descartes' rule of signs to relate the number of nonzero critical points to various events involving the coefficients. For notational convenience, we prove Theorem 1.28 under the assumption  $d \geq 1$ , which we maintain throughout this section. A slight adjustment allows our proof to also handle the case  $d = 0$ .

For a real polynomial  $Q$  and an interval  $I \subset \mathbb{R}$ , let  $N_I(Q)$  be the number of roots of  $Q$  in  $I$ , counted with multiplicity. For  $x \in \mathbb{R}$  and  $d \in \mathbb{N}$ , the notation  $(x)_d$  denotes the falling factorial  $x(x-1) \cdots (x-d+1)$ .

**Lemma 8.1.** *Let  $t \geq 2$  be an integer, and let  $\pi$  be a uniform permutation of  $\{1, \dots, n\}$ . The expected number of real roots of  $P_\pi^{(d)}$  in  $\mathbb{R} \setminus \{-1, 0, 1\}$ , counted with multiplicity, is bounded by*

$$4(t-1) + \sum_{m=2}^{n-d+1} \mathbb{P}\left(\left|\sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i\right| < \left|\sum_{i=1}^m \binom{m-i+t-2}{t-2} a_i\right|\right),$$

where the sum runs over  $4(n-d)$  events with  $2 \leq m \leq n-d+1$ , and  $\mathbf{a} = (a_1, \dots, a_{n-d+1})$  is one of the following four random vectors

$$\begin{aligned} ((d)_d w_{\pi(d)}, \dots, (n)_d w_{\pi(n)}), \quad & ((d)_d w_{\pi(d)}, -(d+1)_d w_{\pi(d+1)}, \dots, (-1)^{n-d}(n)_d w_{\pi(n)}), \\ ((n)_d w_{\pi(n)}, \dots, (d)_d w_{\pi(d)}), \quad & ((-1)^{n-d}(n)_d w_{\pi(n)}, \dots, -(d+1)_d w_{\pi(d+1)}, (d)_d w_{\pi(d)}). \end{aligned}$$

*Proof.* (of Lemma 8.1) For notational convenience, define

$$Q_1(x) = P_\pi^{(d)}(x), \quad Q_2(x) = P_\pi^{(d)}(-x), \quad Q_3(x) = x^{n-d} P_\pi^{(d)}(1/x), \quad Q_4(x) = x^{n-d} P_\pi^{(d)}(-1/x).$$

Each  $Q_i$  is a real polynomial of degree at most  $n-d$ , and

$$N_{(-1,0)}(Q_1) = N_{(0,1)}(Q_2), \quad N_{(1,\infty)}(Q_1) = N_{(0,1)}(Q_3), \quad N_{(-\infty,-1)}(Q_1) = N_{(0,1)}(Q_4).$$

Hence, the expected number of roots of  $P_\pi^{(d)}(x)$  in  $\mathbb{R} \setminus \{-1, 0, 1\}$  equals  $\sum_{i=1}^4 \mathbb{E}N_{(0,1)}(Q_i)$ .

Given  $Q \in \{Q_1, Q_2, Q_3, Q_4\}$ , write  $Q(x) = a_1 + a_2 x + \cdots + a_{n-d+1} x^{n-d}$  and set  $F(x) = Q(x)/(1-x)^t$ . Then  $(a_1, \dots, a_{n-d+1})$  is one of the four vectors described in Lemma 8.1. Clearly,  $F$  and  $Q$  have the same number of roots in  $(0, 1)$ . In this interval,  $F$  admits an absolutely convergent power series expansion:

$$F(x) = Q(x) \cdot \sum_{k=0}^{\infty} \binom{k+t-1}{t-1} x^k = \sum_{m=1}^{\infty} \left( \sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i \right) x^{m-1},$$

where  $a_i = 0$  for  $i > n - d + 1$  by convention. By Descartes' rule of signs, the number of roots of  $Q$  in  $(0, 1)$  is at most the number of sign changes in the sequence  $c_m := \sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i$ ,  $m \geq 1$ .

If  $m \geq n - d + 1$ , then  $c_m = \sum_{i=1}^{n-d+1} \binom{m-i+t-1}{t-1} a_i$ , which is a polynomial in  $m$  of degree at most  $t-1$ . Thus, there are at most  $t-1$  sign changes beyond this point.

Now consider  $2 \leq m \leq n - d + 1$ . If  $c_{m-1}$  and  $c_m$  have different signs, then  $|c_m| < |c_m - c_{m-1}|$ . Hence, the sign change here requires

$$\left| \sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i \right| < \left| \sum_{i=1}^{m-1} \binom{m-i+t-2}{t-2} a_i \right|.$$

Therefore,  $\mathbb{E}N_{(0,1)}(Q)$  is bounded by  $(t-1) + \sum_{m=2}^{n-d+1} \mathbb{P}\left(\left| \sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i \right| < \left| \sum_{i=1}^{m-1} \binom{m-i+t-2}{t-2} a_i \right|\right)$ .  $\square$

*Proof.* (of Theorem 1.28) It is clear that under the hypotheses of the theorem, the expected number of zero roots (critical points) is of order  $O(1)$ ,  $\mathbb{E}(\#\{\text{zeros (critical points) at } 0\}) = O(1)$ . We will treat roots (critical points) at  $\pm 1$  and non-zero roots different from  $\pm 1$  separately.

**Counting  $\pm 1$  roots.** We aim to show  $\mathbb{E}N_{\{\pm 1\}}(P_{\pi}^{(d)}) = O(1)$ . Suppose that 1 is a root of  $P_{\pi}^{(d)}$ . Then

$$P_{\pi}^{(d)}(1) = \sum_{k=d}^n (k)_d w_{\pi(k)} = 0.$$

To analyze this event, sample an ordered  $(n-d+1)$ -tuple  $(w'_1, \dots, w'_{n-d+1})$  uniformly without replacement from the multiset  $\{w_1, \dots, w_n\}$ , and let  $\sigma$  be a uniform random permutation of  $\{1, \dots, n-d+1\}$ . Then  $(w'_{\sigma(1)}, \dots, w'_{\sigma(n-d+1)})$  is distributed as  $(w_{\pi(d)}, \dots, w_{\pi(n)})$ . Consequently,

$$\mathbb{P}\left(P_{\pi}^{(d)}(1) = 0\right) = \mathbb{P}\left(\sum_{i=1}^{n-d+1} (i+d-1)_d w'_{\sigma(i)} = 0\right).$$

By Corollary 7.5, there exists a constant  $c \in (0, 1)$  such that the event  $\sup_x |\{i : w'_i = x\}| \leq c(n-d+1)$  holds with probability at least  $1 - O(1/n)$ . Conditioning on this event, and noting that the coefficients  $(d)_d, \dots, (n)_d$  are distinct for  $n \geq d \geq 1$ , Theorem 1.23 implies

$$\mathbb{P}\left(\sum_{i=1}^{n-d+1} (i+d-1)_d w'_{\sigma(i)} = 0\right) = O\left(\frac{1}{n^{3/2}}\right).$$

Therefore, we can bound the probability that 1 is a root of  $P_{\pi}^{(d)}$  from above by  $O(\frac{1}{n} + \frac{1}{n^{3/2}}) = O(\frac{1}{n})$ . Since the root at 1 has multiplicity at most  $n$ , it follows that  $\mathbb{E}N_{\{1\}}(P_{\pi}^{(d)}) = O(1)$ . By an identical argument, we also have  $\mathbb{E}N_{\{-1\}}(P_{\pi}^{(d)}) = O(1)$ .

**Counting roots in  $\mathbb{R} \setminus \{-1, 0, 1\}$ .** Let  $t \geq d + 2$  be a fixed integer.<sup>10</sup> For each  $2 \leq m \leq n - d + 1$ , and for  $\mathbf{a} = (a_1, \dots, a_{n-d+1})$  being one of the four sequences described in Lemma 8.1, let  $\mathcal{E}_m$  be the event that

$$\left| \sum_{i=1}^m \binom{m-i+t-1}{t-1} a_i \right| < \left| \sum_{i=1}^m \binom{m-i+t-2}{t-2} a_i \right|.$$

We will show that  $\mathbb{P}(\mathcal{E}_m) = O(1/m)$  for  $m \geq \log n$ , which would then lead to

$$\sum_{m=2}^{n-d+1} \mathbb{P}(\mathcal{E}_m) = O\left(\sum_{m=1}^{\log n} 1 + \sum_{m=\log n}^{n-d+1} \frac{1}{m}\right) = O(\log n). \quad (50)$$

Now we focus on the regime  $\log n \leq m \leq n - d + 1$ .

We first consider the (easier) case.

*Case 1:*  $\mathbf{a} = ((d)_d w_{\pi(d)}, \dots, (n)_d w_{\pi(n)})$ .

We can rephrase the event  $\mathcal{E}_m$  as follows. For  $1 \leq i \leq m$ , define

$$v_i = \frac{\binom{m-i+t-1}{t-1}(i+d-1)_d}{m^{t+d-1}}, \quad v'_i = \frac{\binom{m-i+t-2}{t-2}(i+d-1)_d}{m^{t+d-2}}.$$

We sample an ordered  $(m+1)$ -tuple  $(w'_1, \dots, w'_m)$  uniformly at random from  $\{w_1, \dots, w_n\}$ , and let  $\sigma$  be a random permutation of  $\{0, \dots, m\}$ . Then

$$\mathbb{P}(\mathcal{E}_m) = \mathbb{P}\left(\left| \sum_{i=1}^m v_i w'_{\sigma(i)} \right| < \left| \sum_{i=1}^m v'_i w'_{\sigma(i)} \right|\right).$$

We observe that  $\binom{m-i+t-1}{t-1}(i+d-1)_d$  and  $\binom{m-i+t-2}{t-2}(i+d-1)_d$  are polynomials in  $i$  of degree  $t+d-1$  and  $t+d-2$ , respectively, with leading coefficients  $\frac{(-1)^{t-1}}{(t-1)!}$  and  $\frac{(-1)^{t-2}}{(t-2)!}$ . It is straightforward to see that  $|v_i|, |v'_i| = O_{t,d}(1)$ , and that both  $|\sum_{i=1}^m v_i|$  and  $|\sum_{i=1}^m v'_i|$  are of order  $\Theta_{t,d}(m)$ .

Thus, the sequences  $(v_i)$  and  $(v'_i)$  satisfy the conditions of Theorem 6.6. Moreover, by Corollary 7.5, with probability at least  $1 - \Theta(1/m)$ , the sequence  $(w'_i)$  is not too degenerate in the sense of Condition 7.1. Therefore, by applying Theorem 7.2, we can invoke Theorem 6.6 to  $I = \{1, \dots, m\}$  and the sequence  $(w'_i)$ , yielding the desired probability bound  $O(1/m)$  for  $\mathcal{E}_m$ .

We next deal with the (harder) case.

*Case 2:*  $\mathbf{a} = ((d)_d w_{\pi(d)}, -(d+1)_d w_{\pi(d+1)}, \dots, (-1)^{n-d}(n)_d w_{\pi(n)})$ .

Define

$$v_i = \frac{(-1)^{i-1} \binom{m-i+t-1}{t-1}(i+d-1)_d}{m^{t+d-1}}, \quad v'_i = \frac{(-1)^{i-1} \binom{m-i+t-2}{t-2}(i+d-1)_d}{m^{t+d-2}} \quad \text{for all } 1 \leq i \leq m.$$

The treatment of this case closely follows that of the previous one, with the key difference being the verification of the condition

$$\left| \sum_{i=1}^m v'_i \right| \asymp \left| \sum_{i=1}^m v_i \right|.$$

---

<sup>10</sup>In the cases where  $\mathbf{a} = ((d)_d w_{\pi(d)}, \dots, (n)_d w_{\pi(n)})$  or  $\mathbf{a} = ((n)_d w_{\pi(n)}, \dots, (d)_d w_{\pi(d)})$ , one can take  $t = 2$ . For the other two cases, our proof does require  $t \geq d + 2$ .

While this step was straightforward in the previous case, the proof of the present estimate is more delicate, and we postpone its justification to Lemma 8.2 below.

Finally, the cases  $\mathbf{a} = ((n)_d w_{\pi(n)}, \dots, (d)_d w_{\pi(d)})$  and  $\mathbf{a} = ((-1)^{n-d} (n)_d w_{\pi(n)}, \dots, (d)_d w_{\pi(d)})$  can be handled as in Case 1 and Case 2, respectively. The details are left to the reader. This completes the proof of (50) (up to Lemma 8.2), and thereby establishes the theorem.  $\square$

We now conclude this section with the statement and proof of a technical lemma, which was used in the above proof.

**Lemma 8.2.** *Let  $S_{t,d}(m) = \sum_{i=0}^m (-1)^i \binom{m-i+t}{t} (i+d)_d$ . For fixed non-negative integers  $t$  and  $d$ ,*

$$|S_{t,d}(m)| = \Theta_{t,d}(m^{\max\{t,d\}}).$$

*Proof.* We begin by noting that there are two real polynomials,  $P_{t,d}^0(m)$  and  $P_{t,d}^1(m)$ , each of degree at most  $t+d$ , with coefficients depending solely on  $t$  and  $d$ , such that  $S_{t,d}(m) = P_{t,d}^i(m)$  when  $m \equiv i \pmod{2}$ . To prove the lemma, it suffices to show that the polynomials  $P_{t,d}^i(m)$  have degree exactly  $\max\{t,d\}$ . We will prove this by induction on  $\min\{t,d\}$ , analyzing the discrete derivative  $S_{t,d}(m) - S_{t,d}(m-2)$ .

For  $t = 0$ , we have

$$S_{0,d}(m) - S_{0,d}(m-2) = \sum_{i=m-1}^m (-1)^i (i+d)_d = (-1)^m d(m+1) \cdots (m+d-1).$$

Thus, for each  $i \in \{0, 1\}$ , we have  $P_{0,d}^i(m) - P_{0,d}^i(m-2) = (-1)^i d(m+1) \cdots (m+d-1)$ , which is a polynomial of degree  $d-1$ . It follows that  $P_{0,d}^i(m)$  has degree  $d$ .

For  $d = 0$ , we have

$$S_{t,0}(m) - S_{t,0}(m-2) = \sum_{i=0}^1 (-1)^i \binom{m-i+t}{t} = \binom{m+t-1}{t-1},$$

a polynomial of degree  $t-1$ . Therefore, each  $P_{t,0}^i(m)$  has degree  $t$ .

Now we prove the claim for a pair  $t, d \geq 1$ , assuming that the hypothesis holds for all pairs  $t', d'$  with  $\min\{t', d'\} < \min\{t, d\}$ . We start by expressing

$$S_{t,d}(m) - S_{t,d}(m-1) = \sum_{i=0}^m (-1)^i \left[ \binom{m-i+t}{t} - \binom{m-1-i+t}{t} \right] (i+d)_d.$$

Applying Pascal's identity  $\binom{m-i+t}{t} - \binom{m-1-i+t}{t} = \binom{m-i+t-1}{t-1}$ , we simplify this to

$$S_{t,d}(m) - S_{t,d}(m-1) = \sum_{i=0}^m (-1)^i \binom{m-i+t-1}{t-1} (i+d)_d = S_{t-1,d}(m).$$

It follows that

$$\begin{aligned} S_{t,d}(m) - S_{t,d}(m-2) &= S_{t-1,d}(m) + S_{t-1,d}(m-1) \\ &= \sum_{i=0}^m (-1)^i \binom{m-i+t}{t} [(i+d)_d - (i-1+d)_d]. \end{aligned}$$

Using the identity  $(i+d)_d - (i-1+d)_d = d(i+d-1)_{d-1}$ , we obtain

$$S_{t,d}(m) - S_{t,d}(m-2) = d \sum_{i=0}^m (-1)^i \binom{m-i+t}{t} (i+d-1)_{d-1} = d \cdot S_{t-1,d-1}(m).$$

Thus, for each  $i \in \{0, 1\}$ , we have  $P_{t,d}^i(m) - P_{t,d}^i(m-2) = d \cdot P_{t-1,d-1}^i(m)$ . By the induction hypothesis,  $P_{t-1,d-1}^i(m)$  has degree  $\max\{t-1, d-1\}$ , so  $P_{t,d}^i(m)$  has degree  $\max\{t-1, d-1\} + 1 = \max\{t, d\}$ .  $\square$

## 9. FURTHER COMMENTS

Beyond the applications presented in this note, Theorem 1.20 and Theorem 1.22 also appear to be useful in a variety of counting problems. For instance, Theorem 1.22 is a key tool for establishing strong quantitative invertibility estimates for matrices with fixed row sums and for adjacency matrices of  $d$ -regular digraphs [60, 25].<sup>11</sup>

To illustrate its application to singularity problems, consider the random 0/1 matrix  $\mathcal{Q}_{n,d}$  (introduced in [37]), whose rows are independent vectors containing exactly  $d$  ones, where  $\min(d, n-d) = \Omega(n)$ . We construct  $\mathcal{Q}_{n,d}$  row by row. Suppose the first  $n-1$  rows are independent and span a hyperplane with normal vector  $\mathbf{v} = (v_1, \dots, v_n)$ . Conditioned on these rows, the probability that  $\mathcal{Q}_{n,d}$  is singular is

$$\mathbb{P}(\mathbf{w} \cdot \mathbf{v} = 0) = \mathbb{P}(S_\pi = 0),$$

where  $\mathbf{w} = (w_1, \dots, w_n)$  is the last row. If the LCD of the pair  $(\mathbf{w}, \mathbf{v})$  is large, Theorem 1.22 shows that this probability is small. Tran [60] used this approach to obtain the optimal bound  $\exp(-cn)$  for some constant  $c > 0$ . We also note the related work of Jain, Sah, and Sawhney [25] where the authors employed Theorem 1.22 to give a nearly optimal bound for the same problem.

In general, it is expected that if either  $\mathbf{w}$  or  $\mathbf{v}$  arises from a random source, then the LCD is large. We hope to return to this phenomenon in a different venue.

**9.1. Further problems.** Directly related to our paper, we record below a few further interesting directions.

- Theorems 1.23 and 1.24 address the problem of determining when  $\sup_x \mathbb{P}(S_\pi = x) \geq n^{-3/2}$  or  $n^{-5/2}$ . Our approach does not, however, yield a seemingly near-optimal inverse result—namely, that if  $\sup_x \mathbb{P}(S_\pi = x)$  has order  $n^{-1}$ , then most of the  $w_i$  must be zero.
- It would be interesting to remove the  $\log n$  factor from Theorem 1.24.
- While Theorem 1.10 is almost optimal in terms of the size of  $Q$ , it is interesting to deduce more structure on the sequences  $(w_i)$  and  $(v_i)$  separately. Similarly for Theorems 1.20 and 1.22.
- While Remark 4.2 shows that Condition 4 is nearly optimal if we rely on Theorem 2.1, our Theorem 1.15 may remain valid without this condition (whereas Theorems 1.17 and 4.4 would require additional assumptions on the  $w_i$ , as stated). It is therefore of interest to remove this condition from Theorem 1.15.
- Similarly, we suspect that Theorem 1.28 remains valid without the condition (4), though this appears to be a difficult problem.

---

<sup>11</sup>More precisely, [60, 25] give sharp lower bounds on the smallest singular value of these random matrices.

- It would be interesting to extend Theorems 1.15, 1.17, 4.4, and 1.18 beyond polynomial sequences.
- While Theorem 1.28 provides an optimal upper bound, it remains unclear under what conditions on  $w_1, \dots, w_n$  the expected number of real roots  $\mathbb{E}N_{\mathbb{R}}$  is truly of order  $\log n$ . Relatedly, we still need effective techniques to compute the asymptotics of the number of real roots and critical points of  $P_{\pi}$  for natural choices of  $w_1, \dots, w_n$ . For instance, even in the simple case  $w_i = i$ , the asymptotic behavior of  $\mathbb{E}N_{\mathbb{R}}(P_{\pi})$  is still unknown.

#### APPENDIX A. PROOF OF THEOREM 4.4

Let  $\mathcal{R} \subset \{-n, \dots, n\}$  be a set such that  $|\mathcal{R}| = \Theta_{\delta}(n)$ , as defined in Fact 4.1. Let  $\Delta$  and  $A$  be positive constants, chosen sufficiently large with respect to  $\delta$  and  $\varepsilon$  (for instance, one may take  $\Delta = A$ ).

To prove Theorem 4.4, it suffices to show  $\sup_x \mathbb{P}\left(\left|\sum_i n^{3/2-\varepsilon} w_i \pi(i) - x\right| \leq \Delta\right) = O_{\Delta, A}\left(\frac{1}{n^{5/2-\varepsilon}}\right)$ . Using Esseen's estimate together with Corollary 2.2, we can write

$$\sup_x \mathbb{P}\left(\left|\sum_i n^{3/2-\varepsilon} w_i \pi(i) - x\right| \leq \Delta\right) \ll \int_{|t| \leq 1} \exp\left\{-\frac{1}{2n^3} \sum_{i,j,k,l} \left\|\frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j)(k - l)\right\|_{\mathbb{R}/\mathbb{Z}}^2\right\} dt.$$

The right-hand side can be reduced to

$$\int_{|t| \leq 1} \exp\left\{-\frac{c_{\delta}}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\|\frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j)r\right\|_{\mathbb{R}/\mathbb{Z}}^2\right\}. \quad (51)$$

Let  $\mathcal{G}$  denote the set of pairs  $(i, j) \in [n]^2$  satisfying  $|w_i - w_j| \geq \varepsilon/2\sqrt{n}$ . Then we have

$$|\mathcal{G}| \geq \varepsilon n^2, \quad \sum_{(i,j) \in \mathcal{G}} (w_i - w_j)^2 \asymp_{\varepsilon} n. \quad (52)$$

We divide our analysis into four cases.

**Intermediate  $|t|$ , range 1.** Consider

$$\frac{(\sqrt{A \log n})\Delta}{n^{5/2-\varepsilon}} \leq |t| \leq \frac{\Delta}{n^{3/2-\varepsilon}}.$$

We can argue as in the proof of (5) for large  $|t|$  (using (52)), and conclude that

$$\frac{c_{\delta}}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\|\frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j)r\right\|_{\mathbb{R}/\mathbb{Z}}^2 \geq 2\sqrt{A \log n}.$$

**Intermediate  $|t|$ , range 2.** Now take

$$\frac{\Delta}{n^{3/2-\varepsilon}} \leq |t| \leq \frac{1}{n^{1-\varepsilon}}.$$

Let  $\mathcal{G}_0 \subset \mathcal{G}$  denote the set of pairs  $(i, j)$  such that  $|w_i - w_j| \leq \frac{2}{\sqrt{\varepsilon n}}$ . Then  $\mathcal{G}_0$  contains at least  $(\varepsilon/2)n^2$  pairs  $(i, j)$  satisfying  $\frac{\varepsilon}{2\sqrt{n}} \leq |w_i - w_j| \leq \frac{2}{\sqrt{\varepsilon n}}$ . For  $(i, j) \in \mathcal{G}_0$ , we find

$$\frac{\varepsilon}{2\sqrt{n}} \leq \left| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) \right| \leq \frac{2}{\Delta\sqrt{\varepsilon}}.$$

Corollary 2.5 then gives

$$\frac{c_\delta}{n^2} \sum_{\substack{(i,j) \in \mathcal{G}_0 \\ r \in \mathcal{R}}} \left\| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \asymp_\delta \frac{1}{n^2} \cdot |\mathcal{G}_0| \cdot n \asymp_{\delta, \varepsilon} n.$$

**Large  $|t|$ .** Consider

$$\frac{1}{n^{1-\varepsilon}} \leq |t| \leq 1.$$

By our assumption, there are  $An \log n$  pairs  $(i, j)$  with  $\frac{1}{n^{3/2}} \leq |w_i - w_j| \leq \frac{1}{n^{3/2-\varepsilon}}$ . For each such pair,

$$\frac{1}{\Delta n^{1-\varepsilon}} \leq \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) \leq \frac{1}{\Delta}.$$

Applying Corollary 2.5 once again, we conclude

$$\frac{c_\delta}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \gg_\delta \frac{1}{n^2} \cdot An \log n \cdot n \gg_\delta A \log n.$$

**Small  $|t|$ .** It remains to deal with

$$|t| \leq \frac{(\sqrt{A \log n}) \Delta}{n^{5/2-\varepsilon}}.$$

Since  $|w_i - w_j| \leq 1/(A\sqrt{\log n})$ ,

$$\left| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right| \leq \frac{1}{\sqrt{A}} < 1.$$

It follows that

$$\sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right\|_{\mathbb{R}/\mathbb{Z}}^2 = \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right|^2 \asymp_{\delta, \Delta} t^2 n^{5-2\varepsilon}.$$

Therefore

$$\int_{|t| \leq \frac{(\sqrt{A \log n}) \Delta}{n^{5/2-\varepsilon}}} \exp \left\{ -\frac{c_\delta}{n^2} \sum_{\substack{1 \leq i, j \leq n \\ r \in \mathcal{R}}} \left\| \frac{tn^{3/2-\varepsilon}}{\Delta} (w_i - w_j) r \right\|_{\mathbb{R}/\mathbb{Z}}^2 \right\} dt \leq \int_{\mathbb{R}} e^{-\Theta(t^2 n^{5-2\varepsilon})} dt = O\left(\frac{1}{n^{5/2-\varepsilon}}\right).$$

## APPENDIX B. EQUIDISTRIBUTION OF POLYNOMIAL PHASES: PROOF OF LEMMA 2.7

Here we will follow [54] closely with some modifications, that we are now dealing with a subset of positive density of the interval  $\{-N, \dots, N\}$  and not with the entire interval.

**Lemma B.1.** [54, Lemma 3] Let  $0 < \delta < 1$ ,  $\varepsilon \leq 10^{-2}\delta$ , and let  $N$  be an integer with  $N \geq 2/\delta$ . Suppose that a real number  $\theta$  satisfies  $\|n\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$  for all  $n \in I$ , where  $I$  is a subset of size at least  $\delta N$  of  $Q = \{-N, \dots, N\}$ . Then there is a natural number  $q \leq 2/\delta$  such that

$$\|q\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{3\varepsilon}{\delta N}.$$

*Proof.* As  $|I| \geq \delta N$  and  $\|n\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$  for all  $n \in I$ , we can find  $n_1 < n_2$  in  $I$  with  $\|n_1\theta\|_{\mathbb{R}/\mathbb{Z}}, \|n_2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$  and  $n_2 - n_1 \leq \frac{2}{\delta}$ . By the triangle inequality, we conclude that there exists at least one natural number  $q \leq \frac{2}{\delta}$  for which

$$\|q\theta\|_{\mathbb{R}/\mathbb{Z}} \leq 2\varepsilon.$$

We take  $q$  to be minimal amongst all such natural numbers, then we see that there exists a coprime to  $q$  and  $|\kappa| \leq 2\varepsilon$  such that

$$\theta = \frac{a}{q} + \frac{\kappa}{q}. \quad (53)$$

If  $\kappa = 0$  then we are done, so suppose that  $\kappa \neq 0$ . Suppose that  $n < m$  are elements of  $I$  such that  $\|n\theta\|_{\mathbb{R}/\mathbb{Z}}, \|m\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$  and  $m - n \leq \frac{1}{10\kappa}$ . Writing  $m - n = qk + r$  for some  $0 \leq r < q$ , we have

$$\|(m - n)\theta\|_{\mathbb{R}/\mathbb{Z}} = \left\| \frac{ra}{q} + (m - n)\frac{\kappa}{q} \right\|_{\mathbb{R}/\mathbb{Z}} \leq 2\varepsilon.$$

By hypothesis,  $(m - n)\frac{\kappa}{q} \leq \frac{1}{10q}$ ; note that as  $q \leq 2/\delta$  and  $\varepsilon \leq 10^{-2}\delta$  we also have  $\varepsilon \leq \frac{1}{10q}$ . This implies that  $\|\frac{ra}{q}\|_{\mathbb{R}/\mathbb{Z}} < \frac{1}{q}$  and thus  $r = 0$ . We then have

$$|k\kappa| \leq 2\varepsilon.$$

We conclude that for fixed  $n \in I$  with  $\|n\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$ , there are at most  $\frac{2\varepsilon}{|\kappa|}$  elements  $m$  of  $[n, n + \frac{1}{10|\kappa|}]$  such that  $\|m\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$ . Iterating this with a greedy algorithm, we see that the number of  $n \in I$  with  $\|n\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$  is at most

$$\left( \frac{N}{1/10|\kappa|} + 1 \right) \frac{2\varepsilon}{|\kappa|};$$

since  $\varepsilon \leq 10^{-2}\delta$ , this implies that

$$\delta N \leq \frac{3\varepsilon}{\kappa}$$

and the claim follows.  $\square$

Note that we can give an alternative proof with somewhat implicit constants. Indeed, it is known that if  $I \subset Q$ , and  $|I| \geq \delta|Q|$ , then for some sufficiently large  $k$  depending on  $\delta$ , the sumset  $J = kI - kI$  contains a symmetric arithmetic progression  $Q' = \{-Nd, -(N-1)d, \dots, (N-1)d, Nd\}$  of step  $d = O_\delta(1)$  and of length  $2N + 1$ . This is an elementary version of the so called Sárközy-type theorem in progression, where many more is known (see for instance [52, Lemma 4.4, 5.5] and [53, Lemma B3]). Next, by triangle inequality, for each  $n \in J$  we have

$$\|n\delta\| \leq 2k\varepsilon.$$

It thus follows that  $\|l(d\theta)\|_{\mathbb{R}/\mathbb{Z}} \leq 2k\varepsilon$ , from which we can deduce easily that

$$\|d\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{2k\varepsilon}{N}.$$

We next deal with polynomials. The following is a version of [54, Proposition 4], where we don't assume  $I$  to be interval.

**Proposition B.2.** *Let  $\delta > 0$  be a given positive number and  $d \geq 1$  be a given natural number. The following holds for sufficiently large  $N$ . Let  $I$  be a subset of size at least  $\delta N$  of the interval  $Q = \{-N, \dots, N\}$ . Let  $P(n) = \sum_{i \leq d} \alpha_i n^i$  be a polynomial from  $\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$  of degree at most  $d$ . If*

$$\frac{1}{N} \left| \sum_{n \in I} e(P(n)) \right| \geq \delta$$

*then there exists a subprogression  $Q'$  of  $Q$  with  $|Q'| \gg_d \delta^{O_d(1)} N$  such that  $P$  varies by at most  $\delta$  on  $Q'$ .*

Before proving the result, let us deduce Lemma 2.7 (which, in turn, will be used in the induction scheme of the proof of Proposition B.2).

*Proof.* (of Lemma 2.7) To simplify notation we allow implied constants to depend on  $d$ . We may assume that  $\delta \leq c$  for some small constant  $c > 0$  depending only on  $d$ . We will also assume that  $N$  is sufficiently large.

Applying Proposition B.2, we can find a natural number  $q \ll \delta^{-O(1)}$  and an arithmetic subprogression  $Q'$  of  $Q$  such that  $|Q'| \gg \delta^{O(1)} N$  and such that  $P$  varies by at most  $\delta$  on  $Q'$ . Writing

$$Q' = \{qn + r : n \in I'\}$$

for some interval  $I' \subset Q$  of length  $\gg \delta^{O(1)} N$  and some  $0 \leq r < q$ , we conclude that the polynomial  $n \mapsto P(qn + r)$  varies by at most  $\delta$  on  $I'$ .

Taking  $d^{\text{th}}$  order differences, we conclude that the  $d^{\text{th}}$  coefficient of this polynomial is  $O(\delta^{-O(1)} / N^d)$ ; by the binomial theorem, this implies that  $n \mapsto P(qn + r)$  differs by at most  $O(\delta)$  on  $I'$  from a polynomial of degree at most  $d - 1$ . Iterating this, we conclude that the  $i^{\text{th}}$  coefficient of  $n \mapsto P(qn + r)$  is  $O(\delta N^{-i})$  for  $i = 0, \dots, d$ , and the claim then follows by inverting the change of variables  $n \mapsto qn + r$  (and replacing  $q$  with a larger quantity such as  $q^d$  as necessary).  $\square$

*Proof.* (of Proposition B.2) We will induct on  $d$ . The cases  $d = 1$  is immediate from Lemma B.1. Now suppose that  $d \geq 2$ , and that the claim had already been proven for  $d - 1$ . It follows from our assumption that

$$\frac{1}{N^2} \sum_{n_1, n_2 \in I} e(P(n_1) - P(n_2)) \geq \delta^2.$$

For each  $h \in 2Q = \{-2N, \dots, 2N\}$ , let  $I_h \subset Q$  denote the collection of  $n \in I$  such that  $n + h \in I$ . We can rewrite the above as

$$\frac{1}{N^2} \sum_h \sum_{n \in I_h} e(P(n + h) - P(n)) \geq \delta^2.$$

Note that for each  $h$ ,  $|\sum_{n \in I_h} e(P(n + h) - P(n))| \leq 2N$ , we see that for  $\gg \delta^2 N$  choices of  $h \in 2Q$  such that

$$\frac{1}{N} \left| \sum_{n \in I_h} e(P(n + h) - P(n)) \right| \gg \delta^2.$$

Note that  $P(n + h) - P(n)$  is a polynomial of degree at most  $d - 1$  with leading coefficient  $h\alpha_d n^{d-1}$ . We conclude from induction hypothesis (namely Lemma 2.7 for  $\alpha_d$ ) that for each such  $h$ , there exists a natural number  $q_h \ll \delta^{-O(1)}$  such that

$$\|q_h h \alpha_d\|_{\mathbb{R}/\mathbb{Z}} \ll \delta^{-O(1)} / N^{d-1}.$$

As there are  $\gg \delta^2 N$  choices of  $h \in 2Q$  such that the above holds, there are  $\gg \delta^{O(1)} N$  integers  $n$  in the set  $\{-\delta^{-O(1)} N, \delta^{-O(1)} N\}$  such that

$$\|n\alpha_d\|_{\mathbb{R}/\mathbb{Z}} \ll \delta^{-O(1)}/N^{d-1}.$$

Applying Lemma B.1, we conclude that

$$\|q\alpha_d\|_{\mathbb{R}/\mathbb{Z}} \ll \delta^{-O(1)}/N^d. \quad (54)$$

Next, we partition  $Q$  into arithmetic progressions  $Q'$  of spacing  $q$  and length comparable to  $\delta^C N$ , for a sufficiently large constant  $C$  to be chosen. By hypothesis, and by the pigeonhole principle, we have

$$\frac{1}{|Q'|} \left| \sum_{n \in I \cap Q'} e(P(n)) \right| \geq \delta$$

for at least one such progression  $Q'$ . Assume that  $Q' = \{i_0, i_0 + q, \dots, i_0 + n'q\}$  where  $n' \asymp \delta^C N$ . On this progression, for each  $0 \leq k \leq n'$  we write

$$\alpha_d(i_0 + kq)^d = \alpha_d(kq)^d + R(k),$$

where  $R(k)$  is a polynomial of degree  $d-1$  in  $k$ . Note that by (54), and as  $k \leq n' \leq \delta^C N$  and  $kq \leq N$ ,

$$|\alpha_d(kq)^d| = |(\alpha_d q)k(kq)^{d-1}| \ll \delta^{C-O(1)}, \forall 0 \leq k \leq n'.$$

to write  $\alpha_d n^d$  as a polynomial in  $n$  of degree at most  $d-1$ , plus an error of size  $O(\delta^{C-O(1)})$ . We thus can write

$$P(n) = R(n) + O(\delta^{C-O(1)})$$

for  $n \in Q'$  for some polynomial  $R$  of degree at most  $d-1$ . Thus, for  $C$  large enough, by the triangle inequality we have that

$$\frac{1}{|Q'|} \left| \sum_{n \in I \cap Q'} e(R(n)) \right| \gg \delta$$

and hence by induction hypothesis we may find a subprogression  $Q''$  of  $Q'$  of size  $|Q''| \gg \delta^{O(1)} N$  such that  $R$  varies by most  $\delta/2$  on  $Q''$ , and thus (for  $C$  large enough again) that  $P$  varies by at most  $\delta$  on  $Q''$ .  $\square$

## APPENDIX C. PROOF OF THEOREM 1.22

Let  $\varphi(t) := \mathbb{E}e^{itS_\pi}$  denote the characteristic function of  $S_\pi$ . By Esseen's inequality and Corollary 2.2, we have

$$\sup_{x \in \mathbb{R}} \mathbb{P}(|S_\pi - x| \leq \delta) \ll \int_{|t| \leq 1} |\varphi(t/\delta)| dt \ll \int_{|t| \leq 1} \exp\left(-\frac{1}{2n^3} \sum_{i,j,k,l} \left\| \frac{t}{\delta} (w_i - w_j)(v_k - v_l) \right\|_{\mathbb{R}/\mathbb{Z}}^2\right) dt.$$

Recall that  $\mathbf{u} \in \mathbb{R}^{n^4}$  is the vector whose  $(i, j, k, l)$ -th coordinate is

$$(w_i - w_j)(v_k - v_l), \quad 1 \leq i, j, k, l \leq n.$$

With this notation, the exponent may be rewritten as

$$-\frac{1}{2n^3} \text{dist}^2\left(\frac{t}{\delta} \mathbf{u}, \mathbb{Z}^{n^4}\right).$$

Since  $1/\delta \leq \mathbf{LCD}_{\gamma, \kappa}(\mathbf{w}, \mathbf{v})$ , the definition of  $\mathbf{LCD}_{\gamma, \kappa}(\mathbf{w}, \mathbf{v})$  implies that for any  $t \in [-1, 1]$ ,

$$\text{dist}\left(\frac{t}{\delta} \mathbf{u}, \mathbb{Z}^{n^4}\right) \geq \min\left\{\gamma \left\| \frac{t}{\delta} \mathbf{u} \right\|_2, \kappa\right\} \geq \min\left\{\gamma n^{3/2} \frac{|t|}{\delta}, \kappa\right\},$$

provided that  $\|\mathbf{u}\|_2 \geq n^{3/2}$ . Therefore,

$$\sup_{x \in \mathbb{R}} \mathbb{P}(|S_\pi - x| \leq \delta) \ll \int_{|t| \leq 1} \left( \exp\left(-\frac{1}{2} \left(\frac{\gamma t}{\delta}\right)^2\right) + \exp\left(-\frac{\kappa^2}{2n^3}\right) \right) dt \ll \frac{\delta}{\gamma} + e^{-\kappa^2/2n^3}.$$

## REFERENCES

- [1] R. Adamczak, D. Chafai and P. Wolff, *Circular law for random matrices with exchangeable entries*, Random Struct. Algor. 48 (2016), 454-479.
- [2] N. Alon, C. Pohoata and D. G. Zhu, *Permutations on hyperplanes*, private communication.
- [3] J. Angst, O. Nguyen and G. Poly, *Roots of random trigonometric polynomials with general dependent coefficients*, arXiv: 2409.15057
- [4] A. Berger, R. Berkowitz, P. Devlin and V. Vu, *Anti-concentration with respect to random permutations*, preprint.
- [5] T. F. Bloom and A. Walker, *GCD sums and sum-product estimates*, Isr. J. Math. 235 (2020), 1-11.
- [6] E. Bolthausen, *An estimate of the remainder in a combinatorial central limit theorem*, Z. Wahrscheinlichkeitstheor. Verw. Geb. 66 (1984), 379-386.
- [7] L. H. Y. Chen and X. Fang, *On the error bound in a combinatorial central limit theorem*, Bernoulli 21 (2015), 335-359.
- [8] L. H. Y. Chen and S.-T. Ho, *An  $p$  bound for the remainder in a combinatorial central limit theorem*, Ann. Probab. 6 (1978), 231-249.
- [9] L. H. Y. Chen, Larry Goldstein and Q.-M. Shao, *Normal approximation by Stein's method*, Probability and its applications (New York), Springer, Heidelberg, 2011. MR-2732624.
- [10] K. P. Costello, *Bilinear and quadratic variants on the Littlewood-Offord problem*, Isr. J. Math. 194 (2013), 359-394.
- [11] Y. Do, *Real roots of random polynomials with coefficients of polynomial growth: a comparison principle and applications*, Electron. J. Probab. 26 (2021), article no. 144, 1-45.
- [12] Y. Do, O. Nguyen and V. Vu, *Roots of random polynomials with coefficients of polynomial growth*, Ann. Probab. 46 (2018), 2407-2494.
- [13] P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. 51 (1945), 898-902.
- [14] P. Erdős and L. Moser, *Elementary Problems and Solutions*, Amer. Math. Monthly, 54 (1947), 229-230.
- [15] J. Fox, M. Kwan and H. Spink, *Geometric and o-minimal Littlewood-Offord problems*, Ann. Probab. 51 (2023), 101-126.
- [16] L. Goldstein,  *$L^1$  bounds in normal approximation*, Ann. Probab. 35 (2007), 1888-1930.
- [17] G. Halász, *Estimates for the concentration function of combinatorial number theory and probability*, Period. Math. Hung. 8 (1977), 197-211.
- [18] W. Hoeffding, *A combinatorial central limit theorem*, Ann. Math. Statist. 22 (1951), 558-566.
- [19] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, J. Amer. Statist. Assoc. 58 (1963), 13-30.
- [20] G. Hegedus and Gy. Karolyi, *Covering the permutohedron by affine hyperplanes*, Acta Math. Hungar. 174 (2024), 453-461.
- [21] J. Huang, D. McKinnon and M. Satriano, *What fraction of an  $S_n$ -orbit can lie on a hyperplane?*, Linear Algebra Appl. 613 (2021), 1-23.
- [22] I. Ibragimov and N. Maslova, *The average number of zeros of random polynomials*, Vestnik Leningrad. Univ, 23:171-172, 1968.
- [23] I. Ibragimov and N. Maslova, *The average number of real roots of random polynomials*, Soviet Math. Dokl., 12:1004–1008, 1971.
- [24] I. A. Ibragimov and N. B. Maslova, *On the expected number of real zeros of random polynomials. ii. coefficients with non-zero means*, Theory Probab. Appl. 16 (1971), 485-493.
- [25] V. Jain, A. Sah and M. Sawhney, *The smallest singular value of dense random regular digraphs*, Int. Math. Res. Not. 24 (2022), 19300-19334.
- [26] T. Juskevicius and G. Semetulskis, *Optimal Littlewood-Offord inequalities in groups*, Combinatorica 39 (4) (2019) 911-921.
- [27] G. Katona, *On a conjecture of Erdős and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar 1 (1966), 59-63.

- [28] A. Kolmogorov, *Sur les propriétés des fonctions de concentrations de M. P. Lévy*, Ann. Inst. H. Poincaré 16 (1958), 27-34.
- [29] J. Koenig, H. Nguyen and A. Pan, A note on inverse results of random walks in Abelian groups, Combinatorics and Number Theory, Vol. 13 (2024), No. 1, 67–92.
- [30] M. Kwan, A. Sah, L. Sauermann and M. Sawhney, *Anticoncentration in Ramsey graphs and a proof of the Erdős-McKay conjecture*, Forum of Mathematics, Pi (2023) Vol. 11:e21 1-74.
- [31] M. Kwan and L. Sauermann, *Resolution of the quadratic Littlewood-Offord problem*, arXiv preprint arXiv:2312.13826.
- [32] J. E. Littlewood and A. C. Offord, *On the number of real roots of a random algebraic equation. III*, Rec. Math. [Mat. Sbornik] N.S. 12(54) (1943), 277–286.
- [33] 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 (2017), 1447-1491.
- [34] N. Maslova, *On the distribution of the number of real roots of random polynomials*, Theory of Probability & Its Applications, 19(3):461–473, 1975.
- [35] R. Meka, O. Nguyen and V. Vu, *Anti-concentration for polynomials of independent random variables*, Theory Comput. 12 (2016), Paper No. 11, 16.
- [36] H. H. Nguyen, *Inverse Littlewood-Offord problems and the singularity of random symmetric matrices*, Duke Math. J. 161 (2012), no. 4, 545-586.
- [37] H. Nguyen, *On the singularity of random combinatorial matrices*, SIAM J. Discrete Math. 27 (1) (2013), 447-458.
- [38] H. Nguyen, Anti-concentration of inhomogeneous random walks, <https://arxiv.org/abs/1508.01393>.
- [39] H. Nguyen and V. Vu, *Optimal Littlewood-Offord theorems*, Adv. Math. 226 (2011), 5298-5319.
- [40] H. Nguyen and V. Vu, *Small ball probability, inverse theorems, and applications*, Erdős Centennial Proceeding, Eds. L. Lovász et. al., Springer 2013.
- [41] G. E. Noether, *On a Theorem by Wald and Wolfowitz*, Ann. Math. Statist. 20 (1949), 455-458.
- [42] B. Pawłowski, *The fraction of an  $S_n$ -orbit on a hyperplane*, Linear Algebra Appl. 702 (2024), 98-111.
- [43] T. Pham and V. Vu, *Non-abelian Littlewood-Offord inequalities*, Adv. Math. 302 (2016), 1233-1250.
- [44] B. Roos, *On the accuracy in a combinatorial central limit theorem: the characteristic function method*, Theory Probab. Appl. 67 (2022), 118-139.
- [45] B. Roos, *New inequalities for permanents and hafnians and some generalizations*, Linear and Multilinear Algebra 73 (2025), 1634-1667.
- [46] B. A. Rogozin, *An estimate for concentration functions*, Theory Probab. Appl. 6 (1961), 94-97.
- [47] M. Rudelson and R. Vershynin, *The Littlewood-Offord Problem and invertibility of random matrices*, Adv. Math. 218 (2008), 600-633.
- [48] A. Sárközy and E. Szemerédi, *Über ein Problem von Erdős und Moser*, Acta Arithmetica 11 (1965), 205-208.
- [49] K. Söze, *Real zeroes of random polynomials, I. Flip-invariance, Turán's lemma, and the Newton-Hadamard polygon*, Isr. J. Math. 220 (2017), 817-836.
- [50] K. Söze, *Real zeroes of random polynomials, II: Descartes' rule of signs and anti-concentration on the symmetric group*, Isr. J. Math. 220 (2017), 837-872.
- [51] R. Stanley, *Weyl groups, the hard Lefschetz theorem, and the Sperner property*, SIAM J. Algebraic Discrete Methods 1 (1980), no. 2, 168-184.
- [52] E. Szemerédi and V. Vu, *Long arithmetic progressions in sumsets: Thresholds and bounds*, J. Amer. Math. Soc. 19 (1) (2006), 119-169.
- [53] T. Tao, *Freiman's theorem in solvable groups*, Contrib. Discrete Math. 5 (2) (2010), 137-184.
- [54] T. Tao, *Inverse theorems for sets and measures of polynomial growth*, Q. J. Math. 68 (2017), 13-57.
- [55] T. Tao, *Equidistribution for multidimensional polynomial phases*. Available at <https://terrytao.wordpress.com/tag/weyl-equidistribution-theorem/>.
- [56] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.
- [57] T. Tao and V. Vu, *Random matrices: The Circular Law*, Communication in Contemporary Mathematics 10 (2008), 261-307.

- [58] T. Tao and V. Vu, *Inverse Littlewood–Offord theorems and the condition number of random matrices*, Ann. Math. 169 (2009), 595–632.
- [59] T. Tao and V. Vu, *A sharp inverse Littlewood–Offord theorem*, Random Struct. Algor. 37 (2010), 525–539.
- [60] T. Tran, *The smallest singular value of random combinatorial matrices*, <https://arxiv.org/abs/2007.06318>.
- [61] R. Vershynin, *High-Dimensional Probability: An Introduction with Applications in Data Science*.
- [62] A. Wald and J. Wolfowitz, *Statistical tests based on permutations of the observations*, Ann. Math. Statist. 15 (1944), 358–372.

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CT 06511

*Email address:* viet.do@yale.edu

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, COLUMBUS OH 43210

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

SCHOOL OF MATHEMATICS AND STATISTICS, UNSW SYDNEY, SYDNEY NSW 2052, AUSTRALIA

*Email address:* kevin.phan4@student.unsw.edu.au

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA, HEFEI, ANHUI 230026, CHINA

*Email address:* trantuan@ustc.edu.cn

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CT 06511

*Email address:* van.vu@yale.edu