

SOME NEW RESULTS IN RANDOM MATRICES OVER FINITE FIELDS

KYLE LUH, SEAN MEEHAN, AND HOI H. NGUYEN

ABSTRACT. In this note we give various characterizations of random walks with possibly different steps that have relatively large discrepancy from the uniform distribution modulo a prime p , and use these results to study the distribution of the rank of random matrices over \mathbb{F}_p and the equi-distribution behavior of normal vectors of random hyperplanes. We also study the probability that a random square matrix is eigenvalue-free, or when its characteristic polynomial is divisible by a given irreducible polynomial in the limit $n \rightarrow \infty$ in \mathbb{F}_p . We show that these statistics are universal, extending results of Stong and Neumann-Praeger beyond the uniform model.

1. INTRODUCTION

Let q be a prime power, and let $\text{Mat}(n, q)$ ($GL(n, q)$) be the group of all $n \times n$ (resp. non-singular) matrices with entries in the field of q elements. Given a (class) function f that depends on M (such as the rank of M , or the factors of its characteristic polynomial, etc), it is natural to study the behavior of f for a “typical” matrix, such as for one sampled uniformly at random, we call this the uniform model.

1.1. Some statistics for the uniform model. Our first example is on the rank of M . By exposing the columns of M one by one, it is not hard to show that the probability that M belongs to $GL(n, q)$ is exactly

$$\mathbf{P}(M \in GL(n, \mathbb{F}_q)) = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{q^{n^2}} = \prod_{i=1}^n (1 - q^{-i}).$$

More generally, for $0 \leq k \leq n$ we can show that

$$\mathbf{P}(M \text{ has rank } n - k) = \frac{1}{q^{k^2}} \frac{\prod_{i=1}^n (1 - q^{-i}) \prod_{i=k+1}^n (1 - q^{-i})}{\prod_{i=1}^k (1 - q^{-i}) \prod_{i=1}^{n-k} (1 - q^{-i})}. \quad (1)$$

Our next example is the probability that M does not have eigenvalue in \mathbb{F}_q (equivalently, M does not have one dimensional invariant subspace). Beautiful results by Stong [36] and Neumann-Praeger [25] (see also [15]) showed that this probability tends to the derangement probability of a random permutation. We have

$$\lim_{q \rightarrow \infty} \lim_{n \rightarrow \infty} \mathbf{P}(M \text{ is eigenvalue-free}) = 1/e. \quad (2)$$

More generally, Stong showed that in the $q \rightarrow \infty$ limit, the probability that the characteristic polynomial of M factors into n_i degree i irreducible factors is the same as the probability of an element of S_n factors into n_i cycles of degree i , and Hansen and Schmutz [19] also obtained similar results for joint cycle structures.

In a different direction, random matrices over finite field is also a source to generate random partitions. For instance it follows from [16] (and the references therein) for the uniform model:

$$\lim_{n \rightarrow \infty} \mathbf{P}(\lambda_{z-1}(M) = \lambda) = \prod_{r=1}^{\infty} (1 - \frac{1}{q^r}) \frac{1}{q^{\sum_i (\lambda'_i)^2} \prod_i (1/q)_{m_i(\lambda)}}, \quad (3)$$

where $\lambda_{z-1}(M)$ is the partition corresponding to $z - 1$ in the rational canonical form of a uniform matrix M . We refer the reader to Section 2 for a precise definition of $\lambda_\phi(M)$.

The measure above had been studied extensively in Number Theory in the context of the Cohen-Lenstra heuristics. Indeed, assume that B is a p -group, $B = \mathbb{Z}/p^{\lambda_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\lambda_m}\mathbb{Z}$, Friedman and Washington [14] showed that for a Haar random matrix M in \mathbb{Z}_p

$$\lim_{n \rightarrow \infty} \mathbf{P}(M(\mathbb{Z}_p^n)/\mathbb{Z}_p^n \simeq B) = M_p(\lambda) = \frac{\prod_{k=1}^{\infty} (1 - p^{-k})}{|\mathbf{Aut}(B)|}.$$

We also refer the reader to [42, 43] and the references therein for related results.

In the spirit of (3), Fulman [15, 16] also showed for the uniform model that as $n \rightarrow \infty$, for any fixed irreducible polynomial ϕ ,

$$\lim_{n \rightarrow \infty} \mathbf{P}(\lambda_{\phi}(M) = \lambda) = M_{q^{\deg(\phi)}}(\lambda)$$

and in particular,

$$\mathbf{P}(\phi(x) | \det(M - x)) = \mathbf{P}(\lambda_{\phi}(M) \neq \emptyset) \rightarrow 1 - \prod_{i=1}^{\infty} (1 - q^{i \deg(\phi)}). \quad (4)$$

Moreover, it was also shown that these statistics are asymptotically independent for different ϕ in the sense that for any different irreducible polynomials ϕ_1, \dots, ϕ_k

$$\lim_{n \rightarrow \infty} \mathbf{P}(\wedge_{i=1}^k \lambda_{\phi_i} = \lambda_i) = \prod_{i=1}^k \lim_{n \rightarrow \infty} \mathbf{P}(\lambda_{\phi_i} = \lambda_i). \quad (5)$$

We invite the reader to Section 2 for a useful tool to deduce Equations (2), (3) and (4).

1.2. Our main results. Motivated by the universality phenomenon in Random Matrix Theory, we wonder if the above statistics also hold for other models of M . While there have been many results addressing universality of random matrices in characteristic zero (to study the spectral behavior of various models of random matrices), we have not seen much in the literature addressing universality behavior in the finite fields setting. In fact, to the best of our knowledge, although there had been partial results such as [1, 2, 3, 6, 10, 12, 20, 21, 35], universality results of matrices in finite fields only appeared very recently in [23, 24, 27, 30, 42, 43]. For instance, regarding the rank distribution, a simple consequence of results of Maples [23, 24] (see also [27]) and of Wood [42] showed

Theorem 1.3. *Let $\alpha > 0$ be fixed. Assume that $M = (m_{ij})$ is a random matrix where m_{ij} are iid copies of a random α -balanced distribution in \mathbb{F}_p . Then we have*

$$\lim_{n \rightarrow \infty} \mathbf{P}(M \text{ has rank } n - k) = \frac{1}{p^{k^2}} \frac{\prod_{i=k+1}^{\infty} (1 - p^{-i})}{\prod_{i=1}^k (1 - p^{-i})}.$$

Here we say that a random variable ξ in \mathbb{F}_p is α -balanced ¹ if

$$\max_a \mathbf{P}(\xi = a) \leq 1 - \alpha.$$

The method of [23, 24] (see also [27]) relies on a swapping technique from [9, 38, 4], and can yield exponentially small error bound of type $\exp(-c\alpha n)$ in Theorem 1.3. However this technique is quite delicate, and does not seem to extend to other interesting models of matrices such as symmetric matrices. The method of [42, 43] mainly rely on the moment method, which extends rather easily to matrices of entries over $\mathbb{Z}/r\mathbb{Z}$ for composite r (and to control other algebraic statistics beside the ranks), but one has to assume r to be sufficiently small.

One of the main goals of this note is to provide three alternative methods, which we will call the ‘‘arithmetic approach’’ (after [28, 40]), ‘‘geometric approach’’ (after [32]) and ‘‘combinatorial approach’’ (after [8]). Although the error bounds obtained by these methods are usually of subexponential type (rather than exponential type), we believe that the methods will be extremely useful for the study of random matrices in finite

¹For simplicity, our notion here is weaker than those from [23, 24, 27, 30] in that α is fixed.

fields. For instance the methods can be adapted to matrices with constraints such as symmetric matrices and antisymmetric matrices [31] to answer a question from [5]. To highlight a result of this method, we show in Section 6 the following result

Theorem 1.4 (Rank distribution). *Assume that $0 \leq d \leq n^c$ for a sufficiently small constant c . Assume that $p \leq \exp(n^c)$. Then for a random $n \times n$ matrix M with entries being iid copies of an α -balanced random variable ξ in \mathbb{F}_p we have*

$$\mathbf{P}(\text{rank}(M) = n - d) = \frac{1}{p^{d^2}} \frac{\prod_{i=d+1}^{\infty} (1 - p^{-i})}{\prod_{i=1}^d (1 - p^{-i})} + O(e^{-n^{c'}}),$$

where c' is another (sufficiently small) positive constant depending on c and α .

Note that we can also establish similar rank distribution for rectangular matrices of size $(n + u) \times n$ for a fixed u by a similar method. These results are not new and weaker than existing results in the literature (see for instance [23, 24] and [27, Theorem A.4], [30, Theorem 5.3].) However, as mentioned, our approach is new and seems to be robust. (For instance it can be used to prove Theorems 1.5, 1.6, 1.7 and 1.8 below.) More precisely, to establish Theorem 1.4 we will analyze the normal vectors $\mathbf{w} = (w_1, \dots, w_n)$ of random subspaces for which we will show that the random sum $\sum_i \xi_i w_i$ spreads out in \mathbb{F}_p uniformly very quickly.

Theorem 1.5 (Non-structure of the normal vectors). *With the same assumption as in Theorem 1.4, let $X_1, \dots, X_{n-d}, X_{n-d+1}$ be the first $n - d + 1$ column vectors of M . Let $\mathbf{w} = (w_1, \dots, w_n)$ be any non-zero vector that is orthogonal to $W_{n-d} = \langle X_1, \dots, X_{n-d} \rangle$. Then with probability at least $1 - \exp(-\Theta(n))$ with respect to X_1, \dots, X_{n-d} we have*

$$\sup_{a \in \mathbb{F}_p} |\mathbf{P}(\sum \xi_i w_i = a) - 1/p| \leq \exp(-n^c),$$

where ξ_i are iid copies of ξ .

We will prove the above result by showing that with very high probability the normal vectors do not have any structure (in any arithmetic, geometric, or combinatorial sense). On the other hand, we will also show that the normal vectors actually behave like a uniform vector in \mathbb{F}_p^n . This can be seen as a discrete analog of [29] where it was shown that normalized normal vectors of a random hyperplane in \mathbb{R}^n behave like a uniform vector on the unit sphere.

Theorem 1.6 (Uniformity of the normal vectors). *With the same assumption as in Theorem 1.4, and conditioning on the event that the subspace W_{n-1} generated by X_1, \dots, X_{n-1} has full rank, we have*

- For each $i \in \{1, \dots, n\}$,

$$|\mathbf{P}(w_i = 0) - 1/p| \leq O(\exp(-n^{c'})).$$

- For each $i \neq j$, and for any $a \in \mathbb{F}_p$ we have

$$|\mathbf{P}(\exists \mathbf{w} = (w_1, \dots, w_n) \in W_{n-1}^\perp : w_i = a \wedge w_j = 1) - 1/p| \leq O(\exp(-n^{c'})).$$

- Furthermore, with n_a being the number of i such that $w_i = a$, if we assume $\delta < 1$ and $\delta^{-2}p = o(n/\log n)$ then

$$\mathbf{P}(\wedge_{a=0}^{p-1} (|n_a/n - 1/p| \leq \delta/p) \geq 1 - e^{-c\delta^2 n/p}. \quad (6)$$

where $c > 0$ is absolute.

We need p to be smaller than n in Eq. (6) so that n_a is not vanishing on average. We remark that the above result holds trivially for the uniform model (when X_1, \dots, X_{n-1} is chosen uniformly at random from \mathbb{F}_p^n) as in this case \mathbf{w} is distributed as a uniform vector. However, it is not clear at all as to why \mathbf{w} also behaves like a random uniform vector even when the X_i are sampled differently.

In the above results there is a natural connection between the ranks and the normal vectors. Somewhat more surprisingly, we show that these quantities can also be used to study the characteristics polynomials. Namely we can obtain the following analog of Equation (4).

Theorem 1.7 (Divisibility of the characteristic polynomials). *With the same assumption as in Theorem 1.4, let $\varepsilon < 1$ be any fixed constant. For a prime p and fixed polynomial ϕ such that $C_\phi \leq p \leq n^{(1-\varepsilon)/2}$ and ϕ is irreducible over \mathbb{F}_p we have*

$$\left| \mathbf{P}(\phi(x) | \det(M - x)) - [1 - \prod_{i=1}^{\infty} (1 - p^{-i \deg(\phi)})] \right| = O(\exp(-cn^{1-\varepsilon}/p^2)),$$

where c and the implied constant depend on ε and C_ϕ is a constant that depends only on the degree of ϕ .

Also, we will show the following analog of Equation (2).

Theorem 1.8 (Universality for eigenvalue-free matrices). *Assume that M is as in Theorem 1.4. We have*

$$\lim_{p \rightarrow \infty} \lim_{n \rightarrow \infty} \mathbf{P}(M \text{ is eigenvalue-free}) = 1/e.$$

Thus, for instance, our result works for the following simple-looking model of random matrices of (mean zero) integral entries. Let $A \subset \mathbb{Z}$ be a finite deterministic set of integers (such as $A = \{-1, 0, 3\}$ or $A = \{-7, -1, 0, 1, 2\}$, etc.), and let p be a prime so that the projection $\pi(A)$ of A onto $\mathbb{Z}/p\mathbb{Z}$ is not a single point. Let ξ be the image of the uniform measure on A under π , then with the same notations as above we have the following result.

Corollary 1.9. *Among all $|A|^{n^2}$ matrices whose entries are all in A , there are*

- $(\frac{1}{p^{d^2}} \frac{\prod_{i=d+1}^{\infty} (1-p^{-i})}{\prod_{i=1}^d (1-p^{-i})} + O(e^{-n^{c'}}))$ -portion of them have rank $n - d$ in \mathbb{F}_p^n ;
- $(1 - \prod_{i=1}^{\infty} (1 - p^{-i \deg(\phi)}) + O(\exp(-cn^{1-o(1)}/p^2)))$ -portion of them have characteristic polynomial divisible by a given irreducible polynomial $\phi(x)$ for primes $p \lesssim n^{1-o(1)}$;
- $(e^{-1} + o(1))$ -portion of them are eigenvalue-free as $n \rightarrow \infty$ and $p \rightarrow \infty$;
- the normal vectors satisfy Theorem 1.5 and 1.6.

1.10. Notation. We write \mathbf{P} for probability and \mathbf{E} for expected value. For an event \mathcal{E} , we write $\bar{\mathcal{E}}$ for its complement. We write $\exp(x)$ for the exponential function e^x . We use $[n]$ to denote $\{1, \dots, n\}$.

For a given index set $J \subset [n]$ and a vector $\mathbf{x} = (x_1, \dots, x_n)$, we write $\mathbf{x}|_J$ to be the subvector of \mathbf{x} of components indexed from J . Similarly, if H is a subspace then $H|_J$ is the subspace spanned by $\mathbf{x}|_J$ for $\mathbf{x} \in H$.

For a vector $\mathbf{w} = (w_1, \dots, w_n)$ we let $\text{supp}(\mathbf{w}) = \{i \in [n] | w_i \neq 0\}$. We will also write $\mathbf{x} \cdot \mathbf{w}$ for the dot product $\sum_{i=1}^n x_i w_i$. We say \mathbf{w} is a *normal* vector for a subspace H if $\mathbf{x} \cdot \mathbf{w} = 0$ for every $\mathbf{x} \in H$.

For $I, J \subset [n]$, the matrix $M_{I \times J}$ is the submatrix of the rows and columns indexed from I and J respectively. Sometimes we will also write M_n for $M_{n \times n}$ if there is no confusion.

We write $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ to be the distance to the nearest integer. Sometimes, for a matrix M we write $\mathbf{r}_i(M)$ and $\mathbf{c}_i(M)$ for this i -th row and column respectively. We write $X = O(Y)$, $Y = \Omega(X)$, $X \lesssim Y$, or $Y \gtrsim X$ if $|X| \leq CY$ for some fixed C . We also write that $X \asymp Y$ if $X \lesssim Y$ and $Y \gtrsim X$.

Our paper is organized as follows. We will first discuss tools to prove Equations (2), (3) and (4) in Section 2. We will present our characterization methods in Sections 3, 4, 5, and then use these results to prove Theorem 1.5 in Section 6. We will present a short proof of Theorem 1.4 in Section 7 and of Theorem 1.6 in Section 8. The remaining two sections are reserved to prove Theorem 1.7 and Theorem 1.8 respectively.

2. THE UNIFORM MODEL

In this part we discuss the method to prove Equations (2), (3) and (4). Although this is not the main goal of the note, we would like to present it here for pedagogical purposes, as for most of the cases the universal statistics are computed from the uniform model. We refer the reader to [16] for a comprehensive survey on the method and its other applications.

We first introduce a simple representative for $\text{Mat}(n, q)$ (or $GL(n, q)$) modulo the conjugacy action of $GL(n, q)$. To motivate the formulas, let us first introduce a simpler variant for the permutation groups S_n . For a permutation π let $n_i(\pi)$ be the number of cycles of length i of π . The cycle index of a subgroup G of S_n is defined as $\frac{1}{|G|} \sum_{\pi \in G} \prod_{i \geq 1} x_i^{n_i(\pi)}$. The function $f(u, \mathbf{x}) = 1 + \sum_{n \geq 1} \frac{u^n}{n!} \sum_{\pi \in S_n} \prod_{i \geq 1} x_i^{n_i(\pi)}$ is called the *cycle index generating function* of the symmetric groups and Pólya's result shows that $f(u, \mathbf{x}) = \prod_{m \geq 1} e^{\frac{x_m u^m}{m}}$. This formula is useful in the study of (conjugacy) class functions of permutations.

For matrices over \mathbb{F}_q , the cycle index generating functions can be described by first giving some information on the conjugacy classes. Let λ be a partition of some non-negative integer $|\lambda|$ into integer parts $\lambda_1 \geq \lambda_2 \geq \dots \geq 0$. In what follows $m_i(\lambda)$ denotes the number of parts of λ of size i , λ' is the partition dual to λ , and $(u/q)_i$ denotes $(1 - u/q) \cdots (1 - u/q^i)$.

Recall that we define the characteristic polynomial of an $n \times n$ matrix M as $\det(M - x)$. Assume that the irreducible decomposition of the characteristic polynomial of a matrix M has the form $\det(M - x) = \prod_{i=1}^k \phi_i(x)^{\lambda_{\phi_i}}$. The *rational canonical form* of the conjugacy class containing M is a matrix of form

$$\begin{pmatrix} R_1 & 0 & 0 & \dots & 0 \\ 0 & R_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & R_k \end{pmatrix}.$$

where each matrix R_i has the form

$$R = \begin{pmatrix} C(\phi_i^{\lambda_1}) & 0 & 0 & \dots & 0 \\ 0 & C(\phi_i^{\lambda_2}) & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & C(\phi_i^{\lambda_m}) \end{pmatrix},$$

and $\sum_i \lambda_i = \lambda_{\phi_i}$. Also we have the constraint that $\sum_{i=1}^k \lambda_{\phi_i} \deg(\phi_i) = n$. Here for $\phi(x) = \sum_{i=0}^{d-1} a_i x^i + x^d$, the companion matrix $C(\phi)$ is defined as

$$C(\phi) := \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{d-2} & -a_{d-1} \end{pmatrix}.$$

In other words, we have the decomposition of $\mathbb{F}_q^n = \bigoplus_{\phi} V_{\phi}$ where the characteristic polynomial of α on V_{ϕ} is ϕ^k , and furthermore $V_{\phi} = \bigoplus_i V_i$ where V_i are *cyclic subspaces* with dimension $\lambda_i \deg(\phi)$.

Note that in the data given above, each irreducible polynomial ϕ is assigned a partition $\lambda_{\phi}(\alpha)$. For example for $M = I_n$, then $\lambda_{z-1} = (1, 1, \dots, 1)$, and $\lambda_{\phi} = \emptyset$ for all other ϕ ; while for

$$M = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & 1 \end{pmatrix}$$

then $\lambda_{z-1} = (2, 1, \dots, 1)$, and $\lambda_\phi = \emptyset$ for all other ϕ .

To introduce the *cycle index formula* for $Mat(n, q)$, let $x_{\phi, \lambda}$ be variables corresponding to pairs of polynomials and partitions. Define

$$Z_{Mat(n, q)} := \frac{1}{|GL(n, q)|} \sum_{\alpha \in Mat(n, q)} \prod_{\phi, |\lambda_\phi(\alpha)| > 0} x_{\phi, \lambda_\phi(\alpha)}.$$

Beautiful results of Kung [22] and Stong [36] showed that

$$1 + \sum_{n=1}^{\infty} Z_{Mat(n, q)} u^n = \prod_{\phi} \left[1 + \sum_{n \geq 1} \sum_{\lambda \vdash n} x_{\phi, \lambda} \frac{u^{n \deg(\phi)}}{q^{\deg(\phi) \sum_i (\lambda'_i)^2 \prod_{i \geq 1} \left(\frac{1}{q^{\deg(\phi)}}\right)^{m_i(\lambda_\phi)}}} \right].$$

Note that one can also define $Z_{GL(n, q)}$ similarly. The above formula allows one to study class functions for matrices over \mathbb{F}_q , for which we now give a proof for Equation (2), a proof for Equations (3) and (4) can be done similarly by specifying the variables $x_{\phi, \lambda}$ appropriately.

Proof. (of Equation (2)) In the cycle index formula above, by specializing the variables $x_{\phi, \lambda}$ we may count different subsets of $Z_{Mat(n, q)}$. For instance if we set $x_{\phi, \lambda} = 1$ we get everything so,

$$\prod_{\phi} \left[1 + \sum_{n \geq 1} \sum_{\lambda \vdash n} \frac{u^{n \deg(\phi)}}{q^{\deg(\phi) \sum_i (\lambda'_i)^2 \prod_{i \geq 1} \left(\frac{1}{q^{\deg(\phi)}}\right)^{m_i(\lambda_\phi)}}} \right] = (1 - u)^{-1}. \quad (7)$$

We want to count matrices with no fixed subspace. In terms of $x_{\phi, \lambda}$ this is the same as $x_{\phi, \lambda} = 0$ for linear ϕ and $x_{\phi, \lambda} = 1$ otherwise. Making this assignment and using (7) we have,

$$1 + \sum_{n=1}^{\infty} \frac{H_{n, q}}{|GL(n, q)|} u^n = \left(1 + \sum_{i=1}^{\infty} \sum_{\lambda \vdash i} \frac{u^i}{q^{\sum_i (\lambda'_i)^2 \prod_{i \geq 1} \left(\frac{1}{q}\right)^{m_i(\lambda_\phi)}}} \right)^{1-q} (1 - u)^{-1},$$

where $H_{n, q}$ is the number of derangements in $GL(n, q)$. Now the n^{th} coefficient of this generating function is going to the first term in the product evaluated at $u = 1$ and by a result of Fine-Herstein [13] we have (with $[q]_i = \prod_{k=0}^{i-1} (q^i - q^k)$),

$$\frac{H_{n, q}}{|GL(n, q)|} \rightarrow \left(1 + \sum_{i=1}^{\infty} \frac{q^{i(i-1)}}{[q]_i} \right)^{1-q} \text{ as } n \rightarrow \infty.$$

Some cursory analysis (using the fact that the asymptotic behavior of the sum is determined by its first term) shows

$$\left(1 + \sum_{i=1}^{\infty} \frac{q^{i(i-1)}}{[q]_i} \right)^{1-q} \rightarrow 1/e \text{ as } q \rightarrow \infty,$$

as desired. □

3. STRUCTURES OF VECTORS IN \mathbb{F}_p^n : AN ALMOST OPTIMAL CHARACTERIZATION

Let G be an (additive) abelian group. A set Q is a *generalized arithmetic progression* (GAP) of rank r if it can be expressed in the form

$$Q = \{a_0 + x_1 a_1 + \dots + x_r a_r \mid M_i \leq x_i \leq M'_i \text{ and } x_i \in \mathbb{Z} \text{ for all } 1 \leq i \leq r\}$$

for some elements a_0, \dots, a_r of G , and for some integers M_1, \dots, M_r and M'_1, \dots, M'_r . One can think of Q as the image of an integer box $B = \{(x_1, \dots, x_r) \in \mathbb{Z}^r \mid M_i \leq x_i \leq M'_i\}$ under the linear map

$$\Phi : (x_1, \dots, x_r) \rightarrow a_0 + x_1 a_1 + \dots + x_r a_r.$$

Given Q with a representation as above, the numbers a_i are *generators* of Q , the numbers M_i and M'_i are *dimensions* of Q , and $\text{Vol}(Q) := |B|$ is the *volume* of Q associated to this presentation (i.e. this choice

of a_i, M_i, M'_i). We say that Q is *proper* for this presentation if the above linear map is one to one, or equivalently if $|Q| = |B|$. For an integer $t \geq 1$, we let Q_t denote the dilation of Q by t , i.e.

$$Q_t = \{a_0 + x_1 a_1 + \cdots + x_r a_r \mid tM_i \leq x_i \leq tM'_i \text{ and } x_i \in \mathbb{Z} \text{ for all } 1 \leq i \leq r\}$$

and we say Q is *t-proper* if Q_t is also proper. If $-M_i = M'_i$ for all $i \geq 1$ and $a_0 = 0$, we say that Q is *symmetric* for this presentation. A *coset progression* in G is a set of type $H + Q$, where H is a subgroup of G .

Our main result here is that, if a random walk in $\mathbb{Z}/p\mathbb{Z}$ does not spread out evenly fast, then the steps must be arithmetically correlated (and vice versa).

Theorem 3.1 (Arithmetic structure, characterization I). *Let $\varepsilon < 1$ and C be positive constants. Suppose μ is a random variable that is α -balanced taking values in $\mathbb{Z}/p\mathbb{Z}$ and that $\mathbf{w} = (w_1, \dots, w_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ is such that*

$$\rho(\mathbf{w}) = \sup_{a \in \mathbb{Z}/p\mathbb{Z}} \left| \mathbf{P}(\mu_1 w_1 + \cdots + \mu_n w_n = a) - \frac{1}{p} \right| = \Theta(n^{-C}),$$

where μ_1, \dots, μ_n are independent and identically distributed copies of μ and p is an odd prime possibly depending on n . Then for any $n^{\varepsilon/2} \leq n' \leq n$, there is a set W' of $n - n'$ components w_i such that one of the following holds.

- For $p \lesssim n^C$, there exists a GAP of rank one Q that contains W' , where

$$|Q| \leq O_{C,\varepsilon}(1 + p\sqrt{(\log n)/n'}).$$

- For $p \gtrsim n^C$, there exists a proper symmetric GAP Q of rank $r = O_{C,\varepsilon}(1)$ that contains W' , where

$$|Q| = O_{C,\varepsilon}(1 + \rho^{-1}/n'^{r/2}).$$

Note that our characterization is almost optimal in the sense that it nearly implies the backward direction: if \mathbf{w} satisfies the conclusion of the theorem, then $\rho = \Omega(n^{-C})$. It also implies that for $\rho \lesssim n^{-1/2+o(1)}$ (for any p), recovering a result by Maples (see Theorem 4.1. This is because that if a positive portion of the w_i are non-zero, then the set Q must have size at least 1 and $r \geq 1$.) Our presentation here follows from [30] with some modifications (as in [30] we focused only on large p , and on the quantity $\sup_{a \in \mathbb{Z}/p\mathbb{Z}} \mathbf{P}(\mu_1 w_1 + \cdots + \mu_n w_n = a)$ rather than on ρ as above.) We will make use of two results from [39] by Tao and Vu. The first result allows one to pass from coset progressions to proper coset progressions without any substantial loss.

Theorem 3.2. [39, Corollary 1.18] *There exists a positive integer C_1 such that the following statement holds. Let Q be a symmetric coset progression of rank $d \geq 0$ and let $t \geq 1$ be an integer. Then there exists a t -proper symmetric coset progression P of rank at most d such that we have*

$$Q \subset P \subset Q_{(C_1 d)^{3d/2} t}.$$

We also have the size bound

$$|Q| \leq |P| \leq t^d (C_1 d)^{3d^2/2} |Q|.$$

The second result, which is directly relevant to us, says that as long as $|kX|$ grows slowly compared to $|X|$, then it can be contained in a structure. This is a long-range version of the Freiman-Ruzsa theorem.

Theorem 3.3. [39, Theorem 1.21] *There exists a positive integer C_2 such that the following statement holds: whenever $d, k \geq 1$ and $X \subset G$ is a non-empty finite set such that*

$$k^d |X| \geq 2^{2^{C_2 d^2 2^{6d}}} |kX|,$$

then there exists a proper symmetric coset progression $H + Q$ of rank $0 \leq d' \leq d - 1$ and size $|H + Q| \geq 2^{-2^{C_2 d^2 2^{6d}}} k^{d'} |X|$ and $x, x' \in G$ such that

$$x + (H + Q) \subset kX \subset x' + 2^{2^{C_2 d^2 2^{6d}}} (H + Q).$$

Note that any GAP $Q = \{a_0 + x_1 a_1 + \cdots + x_r a_r : -N_i \leq x_i \leq N_i \text{ for all } 1 \leq i \leq r\}$ is contained in a symmetric GAP $Q' = \{x_0 a_0 + x_1 a_1 + \cdots + x_r a_r : -1 \leq x_0 \leq 1, -N_i \leq x_i \leq N_i \text{ for all } 1 \leq i \leq r\}$. Thus, by combining Theorem 3.3 with Theorem 3.2 we obtain the following

Corollary 3.4. *Whenever $d, k \geq 1$ and $X \subset G$ is a non-empty finite set such that*

$$k^d |X| \geq 2^{2^{C_2 d^2 2^{6d}}} |kX|,$$

then there exists a 2-proper symmetric coset progression $H + P$ of rank $0 \leq d' \leq d$ and size $|H + P| \leq 2^d (C_1 d)^{3d^2/2} 2^{d^2 2^{6d}} |kX|$ such that

$$kX \subset H + P.$$

Proof. (of Theorem 3.1) First, for convenience we will pass to symmetric distributions. Let $\psi = \mu - \mu'$ be the symmetrization and let ψ' be a lazy version of ψ so that

$$\mathbf{P}(\psi' = x) = \begin{cases} \frac{1}{2} \mathbf{P}(\psi = x) & \text{if } x \neq 0 \\ \frac{1}{2} \mathbf{P}(\psi = x) + \frac{1}{2}, & \text{if } x = 0. \end{cases}$$

Notice that ψ' is symmetric as ψ is symmetric. We can check that $\max_x \mathbf{P}(\psi = x) \leq 1 - \alpha$, and so

$$\sup_x \mathbf{P}(\psi' = x) \leq 1 - \alpha/2.$$

We assume that $\mathbf{P}(\psi' = t_j) = \mathbf{P}(\psi' = -t_j) = \beta_j/2 > 0$ for $1 \leq j \leq l$, $t_j \neq 0$, and that $\mathbf{P}(\psi' = 0) = \beta_0$, where $t_{j_1} \pm t_{j_2} \neq 0 \pmod p$ for all $1 \leq j_1, j_2 \leq l$ and $j_1 \neq j_2$. Denote $S = \mu_1 w_1 + \cdots + \mu_n w_n$. Consider $a \in \mathbb{Z}/p\mathbb{Z}$ where $\mathbf{P}(S = a)$ is maximum (or minimum). Using the standard notation $e_p(x)$ for $\exp(2\pi\sqrt{-1}x/p)$, we have

$$\mathbf{P}(S = a) = \mathbf{E} \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} e_p(x(S - a)) = \mathbf{E} \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} e_p(\xi S) e_p(-xa) = \frac{1}{p} + \mathbf{E} \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} e_p(xS) e_p(-xa). \quad (8)$$

So

$$\rho = |\mathbf{P}(S = a) - \frac{1}{p}| \leq \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} |\mathbf{E} e_p(xS)|. \quad (9)$$

By independence

$$\begin{aligned} |\mathbf{E} e_p(xS)| &= \prod_{i=1}^n |\mathbf{E} e_p(x\mu_i w_i)| \leq \prod_{i=1}^n \left(\frac{1}{2} (|\mathbf{E} e_p(x\mu_i w_i)|^2 + 1) \right) = \prod_{i=1}^n |\mathbf{E} e_p(x\psi' w_i)| \\ &= \prod_{i=1}^n \left(\beta_0 + \sum_{j=1}^l \beta_j \cos \frac{2\pi x t_j w_i}{p} \right). \end{aligned}$$

It follows that

$$\begin{aligned} \rho &\leq \frac{1}{p} \left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} \prod_{i=1}^n \left(\beta_0 + \sum_{j=1}^l \beta_j \cos \frac{2\pi x t_j w_i}{p} \right) \right| \\ &\leq \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} \prod_{i=1}^n \left(\beta_0 + \sum_{j=1}^l \beta_j \left| \cos \frac{\pi x t_j w_i}{p} \right| \right), \end{aligned} \quad (10)$$

where we made the change of variable $x \rightarrow x/2$ (in $\mathbb{Z}/p\mathbb{Z}$) and used the triangle inequality.

By convexity, we have that $|\sin \pi z| \geq 2\|z\|$ for any $z \in \mathbb{R}$, where $\|z\| := \|z\|_{\mathbb{R}/\mathbb{Z}}$ is the distance of z to the nearest integer. Thus,

$$\left| \cos \frac{\pi x}{p} \right| \leq 1 - \frac{1}{2} \sin^2 \frac{\pi x}{p} \leq 1 - 2\left\| \frac{x}{p} \right\|^2. \quad (11)$$

Hence for each w_i

$$\beta_0 + \sum_{j=1}^l \beta_j \left| \cos \frac{\pi x t_j w_i}{p} \right| \leq 1 - 2 \sum_{j=1}^l \beta_j \left\| \frac{x t_j w_i}{p} \right\|^2 \leq \exp(-2 \sum_{j=1}^l \beta_j \left\| \frac{x t_j w_i}{p} \right\|^2).$$

Consequently, we obtain a key inequality

$$\rho \leq \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}, x \neq 0} \prod_{i=1}^n (\beta_0 + \sum_{j=1}^l \beta_j \left| \cos \frac{\pi x t_j w_i}{p} \right|) \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2 \sum_{i=1}^n \sum_{j=1}^l \beta_j \left\| \frac{x t_j w_i}{p} \right\|^2). \quad (12)$$

Large level sets. Now we consider the level sets $S_m := \{x | x \neq 0 \wedge \sum_{i=1}^n \sum_{j=1}^l \beta_j \left\| \frac{x t_j w_i}{p} \right\|^2 \leq m\}$. We have

$$n^{-C} \leq \rho \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2 \sum_{i=1}^n \sum_{j=1}^l \beta_j \left\| \frac{x t_j w_i}{p} \right\|^2) \leq \frac{1}{p} \sum_{m \geq 1} \exp(-2(m-1)) |S_m|.$$

As $\sum_{m \geq 1} \exp(-m) < 1$, there must be a large level set S_m such that

$$|S_m| \exp(-m+2) \geq \rho p. \quad (13)$$

In fact, since $\rho \geq n^{-C}$, we can assume that $m = O(\log n)$. The bound $|S_m| \geq \exp(m-2)\rho p$ guarantees that S_m is non-empty.

Now we consider two cases.

Case 1. We assume $p \lesssim n^C$. We know that S_m is non-empty, and hence there exists $x_0 \neq 0$ so that

$$\sum_{i=1}^n \sum_{j=1}^l \beta_j \left\| \frac{x_0 t_j w_i}{p} \right\|^2 \leq m.$$

Set

$$\alpha' := \sum_{j=1}^l \beta_j = 1 - \beta_0. \quad (14)$$

Then by definition of ξ , we have

$$\alpha' \geq \alpha/2.$$

Thus we can rewrite the above as

$$\sum_{j=1}^l \beta_j \sum_{i=1}^n \left\| \frac{x_0 t_j w_i}{p} \right\|^2 \leq 2\alpha^{-1} m \sum_j \beta_j.$$

Thus there exists an index j_0 so that $\beta_{j_0} \sum_{i=1}^n \left\| \frac{x_0 t_{j_0} w_i}{p} \right\|^2 \leq 2\alpha^{-1} m \beta_{j_0}$, that is

$$\sum_{i=1}^n \left\| \frac{x_0 t_{j_0} w_i}{p} \right\|^2 \leq 2\alpha^{-1} m.$$

So, for most w_i

$$\left\| \frac{x_0 t_{j_0} w_i}{p} \right\|^2 \leq \frac{2\alpha^{-1} m}{n'}. \quad (15)$$

More precisely, by averaging, the set of w_i satisfying (15) has size at least $n - n'$. We call this set W' . The set $\{w_1, \dots, w_n\} \setminus W'$ has size at most n' and this is the exceptional set that appears in Theorem 3.1. By definition, for w_i from this set we have

$$\left\| \frac{x_0 t_{j_0} w_i}{p} \right\|^2 = O\left(\frac{m}{n'}\right). \quad (16)$$

Hence we have seen that, after a dilation by $x_0 t_{j_0}$, W' belongs to the arithmetic progression P of rank one and of size $O(p\sqrt{(\log n)/n'})$,

$$P = \{x \in \mathbb{F}_p, \|\frac{x}{p}\| = O(\sqrt{\frac{m}{n'}})\}.$$

Notice that in this case we don't have to assume $n' \geq n^{\varepsilon/2}$.

Case 2. We assume $p \gtrsim n^C$. By double-counting we have

$$\sum_{i=1}^n \sum_{x \in S_m} \sum_{j=1}^l \beta_j \|\frac{xt_j w_i}{p}\|^2 = \sum_{x \in S_m} \sum_{i=1}^n \sum_{j=1}^l \beta_j \|\frac{xt_j w_i}{p}\|^2 \leq m|S_m|.$$

So, for most w_i ,

$$\sum_{x \in S_m} \sum_{j=1}^l \beta_j \|\frac{xt_j w_i}{p}\|^2 \leq \frac{m}{n'} |S_m| \quad (17)$$

for some large constant C_0 .

By averaging, the set of w_i satisfying (17) has size at least $n - n'$. We call this set W' . The set $\{w_1, \dots, w_n\} \setminus W'$ has size at most n' and this is the exceptional set that appears in Theorem 3.1. In the rest of the proof, we are going to show that W' is a dense subset of a proper GAP.

Since $\|\cdot\|$ is a norm, by the triangle inequality, we have for any $a \in kW'$

$$\sum_{x \in S_m} \sum_{j=1}^l \beta_j \|\frac{xt_j a}{p}\|^2 \leq k^2 \frac{m}{n'} |S_m|. \quad (18)$$

More generally, for any $k' \leq k$ and $a \in k'W'$,

$$\sum_{x \in S_m} \sum_{j=1}^l \beta_j \|\frac{xt_j a}{p}\|^2 \leq k'^2 \frac{m}{n'} |S_m|. \quad (19)$$

Dual sets. Define

$$S_m^* := \{a \mid \sum_{x \in S_m} \sum_{j=1}^l \beta_j \|\frac{xt_j a}{p}\|^2 \leq \frac{\alpha'}{200} |S_m|\}$$

where the constant 200 is ad hoc and any sufficiently large constant would do. We have

$$|S_m^*| \leq \frac{8p}{|S_m|}. \quad (20)$$

To see this, define $T_a := \sum_{x \in S_m} \sum_{j=1}^l \beta_j \cos \frac{2\pi a t_j x}{p}$. Using the fact that $\cos 2\pi z \geq 1 - 100\|z\|^2$ for any $z \in \mathbb{R}$, we have, for any $a \in S_m^*$,

$$T_a \geq \sum_{x \in S_m} (1 - 100 \sum_{j=1}^l \beta_j \|\frac{xt_j a}{p}\|^2) \geq \frac{\alpha'}{2} |S_m|.$$

One the other hand, using the basic identity $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \cos \frac{2\pi a z}{p} = p \mathbf{1}_{z=0}$, we have (taking into account that $t_{j_1} \not\equiv t_{j_2} \pmod{p}$)

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} T_a^2 \leq 2p|S_m| \sum_j \beta_j^2 \leq 2p|S_m| \max_{1 \leq j \leq l} \beta_j (\sum_{j=1}^l \beta_j) \leq 2p|S_m| \alpha'^2.$$

Equation (20) then follows from the last two estimates and averaging.

Next, for a properly chosen constant c_1 we set

$$k := c_1 \sqrt{\frac{\alpha' n'}{m}}.$$

By (19) we have $\cup_{k'=1}^k k'W' \subset S_m^*$. Next, set

$$W'' := W' \cup \{0\}.$$

We have $kW'' \subset S_m^* \cup \{0\}$. This results in the critical bound

$$|kW''| = O\left(\frac{p}{|S_m|}\right) = O(\rho^{-1} \exp(-m+2)). \quad (21)$$

We are now in a position to apply Corollary 3.4 with X as the set of distinct elements of W'' . As $k = \Omega(\sqrt{\frac{\alpha'_n n'}{m}}) = \Omega(\sqrt{\frac{\alpha'_n n'}{\log n}})$,

$$\rho^{-1} \leq n^C \leq k^{4C/\varepsilon+1}. \quad (22)$$

It follows from Corollary 3.4 that kX is a subset of a 2-proper symmetric coset progression $H + P$ of rank $r = O_{C,\varepsilon_0}(1)$ and cardinality

$$|H + P| \leq O_{C,\varepsilon}|kX|.$$

Now we use the special property of $\mathbb{Z}/p\mathbb{Z}$ that it has only trivial proper subgroup. As $|kX| = O(n^C)$, and as $p \gtrsim n^C$, the only way that $|kX| \gtrsim |H + P|$ is that $H = \{0\}$. Consequently, kX is now a subset of P , a 2-proper symmetric GAP of rank $r = O_{C,\varepsilon_0}(1)$ and cardinality

$$|P| \leq O_{C,\varepsilon}|kX|. \quad (23)$$

To this end, we apply the following dividing trick from [28, Lemma A.2].

Lemma 3.5. *Assume that $0 \in X$ and that $P = \{\sum_{i=1}^r x_i a_i : |x_i| \leq N_i\}$ is a 2-proper symmetric GAP that contains kX . Then $X \subset \{\sum_{i=1}^r x_i a_i : |x_i| \leq 2N_i/k\}$.*

Combining (23) and Lemma 3.5 we thus obtain a GAP Q that contains X and

$$\begin{aligned} |Q| &= O_{C,\varepsilon_0}(k^{-r}|kX|) = O_{C,\varepsilon_0}(k^{-r}|kW''|) = O_{C,\varepsilon_0}\left(\rho^{-1} \exp(-m)\left(\sqrt{\frac{\alpha'_n n'}{m}}\right)^{-r}\right) \\ &= O_{C,\varepsilon_0}(\rho^{-1}(\alpha'_n n')^{-r}), \end{aligned}$$

concluding the proof. \square

Before concluding the section, we record here an elementary but useful result beyond the polynomial regime.

Theorem 3.6 (degenerate case). *Let $\varepsilon < 1$ and δ be positive constants such that $\delta < \varepsilon$. Let p be an odd prime number. Suppose μ is a random variable that is α -balanced taking values in $\mathbb{Z}/p\mathbb{Z}$. Also, assume that $\mathbf{w} = (w_1, \dots, w_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ is such that*

$$\rho(\mathbf{w}) = \sup_{a \in \mathbb{Z}/p\mathbb{Z}} |\mathbf{P}(\mu_1 w_1 + \dots + \mu_n w_n = a) - \frac{1}{p}| \geq \exp(-n^\delta),$$

where μ_1, \dots, μ_n are independent and identically distributed copies of μ . Then for any $n^{\varepsilon/2} \leq n' \leq n$, there is a set W' of $n - n'$ components w_i and then a GAP of rank one Q that contains W' , where

$$|Q| \leq O_{C,\varepsilon}(p\sqrt{n^\delta/n'}).$$

We note that the bound on Q above is very close to the trivial bound p . The result is effective for not too large p .

Proof. We proceed as in the proof of Theorem 3.1 until (12) that

$$\rho \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp\left(-2 \sum_{i=1}^n \sum_{j=1}^l \beta_j \left\| \frac{xt_j w_i}{p} \right\|^2\right).$$

We recall the level sets $S_m = \{x | x \neq 0 \wedge \sum_{i=1}^n \sum_{j=1}^l \beta_j \|\frac{x t_j w_i}{p}\|^2 \leq m\}$. We have

$$\exp(-n^\delta) \leq \rho \leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2 \sum_{i=1}^n \sum_{j=1}^l \beta_j \|\frac{x t_j w_i}{p}\|^2) \leq \frac{1}{p} \sum_{m \geq 1} \exp(-2(m-1)) |S_m|.$$

As $\sum_{m \geq 1} \exp(-m) < 1$, there must be a large level set S_m such that

$$|S_m| \exp(-m+2) \geq \rho p. \quad (24)$$

In fact, since $\rho \geq \exp(-n^\delta)$, we can assume that $m = O(n^\delta)$. The bound $|S_m| \geq \exp(m-2)\rho p$ guarantees that S_m is non-empty.

Our next step is almost identical to the proof of the first part of Theorem 3.1. As S_m is non-empty, there exists $x_0 \neq 0$ so that

$$\sum_{i=1}^n \sum_{j=1}^l \beta_j \|\frac{x_0 t_j w_i}{p}\|^2 \leq m.$$

With α' as in (14) we have $\alpha' \geq \alpha/2$, and we can rewrite the above as

$$\sum_{j=1}^l \beta_j \sum_{i=1}^n \|\frac{x_0 t_j w_i}{p}\|^2 \leq 2\alpha^{-1} m \sum_j \beta_j.$$

Thus there exists an index j_0 so that $\beta_{j_0} \sum_{i=1}^n \|\frac{x_0 t_{j_0} w_i}{p}\|^2 \leq 2\alpha^{-1} m \beta_{j_0}$, that is

$$\sum_{i=1}^n \|\frac{x_0 t_{j_0} w_i}{p}\|^2 \leq 2\alpha^{-1} m.$$

So, with W' be the set of w_i such that $\|\frac{x_0 t_{j_0} w_i}{p}\|^2 \leq \frac{2\alpha^{-1} m}{n'}$ then W' has at least $n - n'$ elements. By definition, for $w_i \in W'$ we have $\|\frac{x_0 t_{j_0} w_i}{p}\|^2 = O(\frac{m}{n'})$. and this implies that after a dilation by $x_0 t_{j_0}$ the set W' belongs to the arithmetic progression P of rank one

$$P = \{x \in \mathbb{F}_p, \|\frac{x}{p}\| = O(\sqrt{\frac{m}{n'}})\}.$$

Notice that the size of P is bounded by $O(p\sqrt{(m)/n'}) = O(p\sqrt{n^\delta/n'})$ as desired. □

4. STRUCTURES OF VECTORS IN \mathbb{F}_p^n : A GEOMETRIC APPROACH

From now on, for simplicity we will assume our random variables are iid Bernoulli (taking values ± 1 with probability $1/2$) and $p \geq 3$, the general α -balanced case can be treated almost identically (see Remark 4.9.)

Let $\mathbf{w} = (w_1, \dots, w_n)$ be a non-zero vector in \mathbb{F}_p^n , where p is a prime. We first cite a result of Erdős-Littlewood-Offord type from [23]

Theorem 4.1. *Let $c_{nsp} > 0$ be a constant, and assume that*

$$|\text{supp}(\mathbf{w})| \geq c_{nsp} n. \quad (25)$$

Then

$$\rho(\mathbf{w}) = \sup_r |\mathbf{P}(X \cdot \mathbf{w} = r \pmod{p}) - \frac{1}{p}| = O(\frac{1}{\sqrt{n}})$$

where the implied constant depends on c_{nsp} , and where $X = (x_1, \dots, x_n)$ and x_i are iid Bernoulli.

In what follows, if not specified, we always assume our deterministic vector \mathbf{w} to satisfy the non-sparsity property (25). We remark that this non-sparsity property passes to all other dilations $t\mathbf{w}$ of \mathbf{w} in \mathbb{F}_p^n for non-zero t .

As mentioned in the introduction, our treatment in this section is motivated by the work of Rudelson and Vershynin (in characteristic zero) [32] and we hope to develop a “geometric” characterization of the steps of our random walk in \mathbb{F}_p if the walk spreads out slowly. This task is not straightforward; as we will see, there are many simple concepts in characteristic zero that are hard to find natural (and equally useful) analogs in the finite field setting (for instance, the notion of compressible and incompressible vectors).

In some situations, if $\mathbf{w} = (w_1, \dots, w_n)$ is a vector in \mathbb{F}_p^n , then by viewing \mathbb{F}_p as the interval $\mathbf{I}_p = [-(p-1)/2, (p-1)/2]$ in \mathbb{Z} , we will consider the components w_i as integers from this interval. We then write \mathbf{w}' as the vector in \mathbb{R}^n

$$\mathbf{w}' = (w'_1, \dots, w'_n) = \frac{1}{p}\mathbf{w} = (w_1/p, \dots, w_n/p).$$

Definition 4.2. Let $0 < \gamma < 1$ and κ be given. Let $\mathbf{w}' = (w'_1, \dots, w'_n) \in \mathbb{R}^n$ be a non-zero vector in $\frac{1}{p}\mathbb{Z}^n$ where $\|\mathbf{w}'\|_\infty \leq 1/2$. We denote by $\mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}')$ to be the smallest (infimum) positive integer L such that

$$\text{dist}(L\mathbf{w}', \mathbb{Z}^n) \leq \min\{\gamma\|L\mathbf{w}'\|_2, \kappa\}$$

where $\text{dist}(L\mathbf{w}', \mathbb{Z}^n)$ denotes the smallest Euclidean distance from $L\mathbf{w}'$ to an element of \mathbb{Z}^n .

Throughout this paper, $\gamma < 1$ is an absolute constant (such as $\gamma = 1/8$), and $\kappa \leq n^c$, for some positive constant $c \leq 1/2$ to be chosen.

This definition is in characteristic zero. Here we used the notion of \mathbf{ULCD} (compared to the notion of \mathbf{LCD} from [32]) to emphasize that (w'_1, \dots, w'_n) is not normalized (i.e. its ℓ_2 -norm might not be unit). Notice that

$$2 \leq \mathbf{ULCD}_{\gamma, \kappa} \leq p.$$

Furthermore, if $\mathbf{ULCD}_{\gamma, \kappa} = p$ then by definition we would have for all $1 \leq L \leq p-1$ that

$$\text{dist}(L\mathbf{w}', \mathbb{Z}^n) \geq \min\{\gamma\|L\mathbf{w}'\|_2, \kappa\}. \quad (26)$$

Remark 4.3. Note that if for some $T > 1$ we have $|w'_i| \leq 1/2T$ for all i , then

$$\mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}') \geq T.$$

This is because otherwise, $\|Lw'_i\|_{\mathbb{R}/\mathbb{Z}} = |Lw'_i|$ and hence $\sum_i \|Lw'_i\|_{\mathbb{R}/\mathbb{Z}}^2 = \sum_i \|Lw'_i\|_2^2$, which cannot be smaller than $\gamma^2\|L\mathbf{w}'\|_2^2$ by definition as $\gamma < 1$.

Our result below says that if $\mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}')$ is large then the concentration probability is small. In our notation $t\mathbf{w}$ is another vector in \mathbb{F}_p^n , which again can be viewed as a vector in $\mathbf{I}_p^n = [-(p-1)/2, (p-1)/2]^n$. We then define $(t\mathbf{w})'$ as $\frac{1}{p}t\mathbf{w}$ accordingly in this projection to characteristic zero.

Theorem 4.4 (Geometric structure, characterization II). *Let $p \geq 3$ be a prime, and let $C > 0$ be an arbitrary constant. Let $\mathbf{w} = (w_1, \dots, w_n)$ be a non-zero vector in \mathbb{Z}^n , where $|w_i| \leq p/2$, and let $\mathbf{w}' = \frac{1}{p}\mathbf{w} = (\frac{w_1}{p}, \dots, \frac{w_n}{p})$. Then*

(1) *If there is no non-zero $t \in \mathbb{F}_p$ such that $\|(t\mathbf{w})'\|_2 < \kappa$ then we have*

$$\rho(\mathbf{w}) \leq \exp(-\kappa^2/2).$$

(2) *Otherwise, assume that $1 \leq \|\mathbf{w}'\|_2 \leq \kappa$ and \mathbf{w} satisfies (25), with $\kappa \leq C\sqrt{n}$ and*

$$\mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}') \geq L.$$

Then

$$\rho(\mathbf{w}) \leq O\left(\frac{1}{L\|\mathbf{w}'\|_2} + \exp(-\Theta(\kappa^2))\right),$$

where the implied constants depend on $C, \gamma, c_{n,sp}$, and where $X = (x_1, \dots, x_n)$ and x_i are iid Bernoulli in the concentration definition $\rho(w)$.

Corollary 4.5. Assume that there exists a quantity $\rho \gtrsim \exp(-\Theta(\kappa^2))$ such that $\rho(\mathbf{w}) \geq \rho$, then there exists a dilation $t\mathbf{w}$ of \mathbf{w} , where $t \in \mathbb{F}_p$ non-zero, so that with $\mathbf{w}' = t\mathbf{w}$ we have $\|\mathbf{w}'\|_2 < \kappa$ and there exists $L = L(\mathbf{w}) \geq 1$ such that

$$L = O\left(\frac{\rho^{-1}}{\|\mathbf{w}'\|_2}\right)$$

and

$$\text{dist}(L\mathbf{w}', \mathbb{Z}^n) \leq \kappa.$$

We next deduce another elementary but useful result, which will be used later on in the applications.

Corollary 4.6. Assume that \mathbf{w} has at least m non-zero coordinates, and $p < \sqrt{m}$. We then have

$$\rho(\mathbf{w}) \leq \exp(-m/2p^2).$$

Proof. As $t\mathbf{w}'$ has at least m non-zero coordinates for any non-zero t , we have that

$$\|t\mathbf{w}'\|_2 \geq \sqrt{m(1/p)^2} = \sqrt{m}/p,$$

and we are in scenario (1) of Theorem 4.4. □

We now present a proof of Theorem 4.4.

Proof. (of Theorem 4.4) Write $e_p(x) = e^{2\pi ix/p}$, then for any $r \in \mathbb{F}_p$ we have

$$\mathbf{P}(X \cdot \mathbf{w} = r) - \frac{1}{p} = \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} \prod_{l=1}^n \mathbf{E} e_p(x_l w_l t) e_p(-tr).$$

So

$$\begin{aligned} |\mathbf{P}(X \cdot \mathbf{w} = r) - \frac{1}{p}| &\leq \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} \left| \prod_{l=1}^n \mathbf{E} e_p(x_l w_l t) \right| \\ &= \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} \prod_{l=1}^n |\cos(2\pi w_l t/p)| \\ &= \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} \prod_{l=1}^n |\cos(\pi w_l t/p)| \\ &\leq \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e^{-2 \sum_{l=1}^n \|\frac{w_l t}{p}\|^2} \\ &\leq \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e^{-2 \sum_{l=1}^n \|tw'_l\|_{\mathbb{R}/\mathbb{Z}}^2}, \end{aligned}$$

where we used the fact that $|\sin \pi z| \geq 2\|z\|_{\mathbb{R}/\mathbb{Z}}$ for any $z \in \mathbb{R}$, where $\|z\|_{\mathbb{R}/\mathbb{Z}}$ is the distance of z to the nearest integer, and that

$$\left| \cos \frac{2\pi x}{p} \right| \leq 1 - \frac{1}{2} \sin^2 \frac{2\pi x}{p} \leq 1 - 2\left\| \frac{2x}{p} \right\|^2.$$

From here, (1) follows as $\|tw'_l\|_{\mathbb{R}/\mathbb{Z}} = \|(tw)_l\|_{\mathbb{R}/\mathbb{Z}}$.

We are now in the assumption of (2). For each integer m , let $T(m, p/2)$ be the (level) set of $t \in \mathbb{F}_p$ corresponding to m ,

$$T(m, p/2) = \left\{ t \in \mathbb{F}_p : \|\mathbf{tw}'\|_{\mathbb{R}/\mathbb{Z}}^2 := \sum_{l=1}^n \|tw'_l\|_{\mathbb{R}/\mathbb{Z}}^2 \leq m \right\} = \left\{ t \in \mathbf{I}_p : \|\mathbf{tw}'\|_{\mathbb{R}/\mathbb{Z}}^2 \leq m \right\}.$$

By the non-sparsity of \mathbf{w} , we can show that $T(c_{nsp}n/64, p/2)$ is not all of \mathbb{F}_p (we can show this by using the fact that if $w_i \neq 0$ then $\sum_{t \in \mathbb{F}_p} \|\frac{tw_i}{p}\|_{\mathbb{R}/\mathbb{Z}} = \sum_{t \in \mathbb{F}_p} \|\frac{t}{p}\|_{\mathbb{R}/\mathbb{Z}}$). Thus

$$|T(c_{nsp}n/64, p/2)| \leq p - 1.$$

Our next claim shows that the level sets consist of well separated intervals.

Claim 4.7 (spacing of the level sets). *Assume that $m < \kappa^2/4 < c_{nsp}n/64$ and $s_1 < s_2 \in T(m, p/2)$ and*

$$|s_2 - s_1| \geq \gamma^{-1}\kappa/\|\mathbf{w}'\|_2.$$

Then

$$s_2 - s_1 \geq L.$$

Consequently we have

$$|T(m, p/2)| \leq \frac{p \lceil \gamma^{-1}\kappa/\|\mathbf{w}'\|_2 \rceil}{L}.$$

Proof. (of Claim 4.7) Assume that $t_1, t_2 \in T(m, p/2)$, then by the triangle inequality,

$$\|(t_1 - t_2)\mathbf{w}'\|_{\mathbb{R}/\mathbb{Z}} \leq \|t_1\mathbf{w}'\|_{\mathbb{R}/\mathbb{Z}} + \|t_2\mathbf{w}'\|_{\mathbb{R}/\mathbb{Z}} \leq 2\sqrt{m} < \kappa.$$

Thus

$$\text{dist}((t_2 - t_1)\mathbf{w}', \mathbb{Z}^n) = \|(t_2 - t_1)\mathbf{w}'\|_{\mathbb{R}/\mathbb{Z}} < \kappa \leq \gamma(t_2 - t_1)\|\mathbf{w}'\|_2,$$

where in the last estimate we used $|t_2 - t_1| > \gamma^{-1}\kappa/\|\mathbf{w}'\|_2$. Thus by the definition of $\text{ULCD}_{\gamma, \kappa}$ we must have

$$t_2 - t_1 \geq L.$$

□

Next, we will need a Cauchy-Davenport-type bound on size of sumsets in \mathbb{F}_p . Observe from the Cauchy-Schwarz inequality, $k(\|x_1\|_{\mathbb{R}/\mathbb{Z}}^2 + \dots + \|x_k\|_{\mathbb{R}/\mathbb{Z}}^2) \geq \|x_1 + \dots + x_k\|_{\mathbb{R}/\mathbb{Z}}^2$, and so

$$k|T(m, p/2)| \leq |T(k^2m, p/2)|,$$

where we view these sets as subsets of \mathbb{F}_p . Hence, by Cauchy-Davenport's inequality in \mathbb{F}_p ([37]) we have that

$$|T(k^2m)| \geq |kT(m)| \geq k|T(m)| - (k-1).$$

Thus for all $m \leq \min\{c_{nsp}\kappa^2/64, c_{nsp}n/64\}$, by choosing $k = \lfloor \sqrt{\min\{c_{nsp}\kappa^2/64, c_{nsp}n/64\}/m} \rfloor$ we have

$$|T(m, p/2)| - 1 \leq k^{-1}(|T(c_{nsp}n/64, p/2)| - 1) \leq \sqrt{\frac{m}{O_{c_{nsp}, C}(\kappa^2)}} p, \quad (27)$$

where we used $|T(c_{nsp}n/64, p/2)| - 1 < p$.

We deduce

$$\begin{aligned} |\mathbf{P}(X \cdot \mathbf{w} = r) - \frac{1}{p}| &\leq \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e^{-2 \sum_{i=1}^n \|t\mathbf{w}'\|^2} \\ &\leq \frac{1}{p} \left(\frac{p \lceil \gamma^{-1}\kappa/\|\mathbf{w}'\|_2 \rceil}{L \sqrt{O_{c_{nsp}, C}(\kappa^2)}} \sum_{m \leq \min\{c_{nsp}\kappa^2/64, c_{nsp}n/64\}} \sqrt{m} e^{-m/2} + p \sum_{m > \min\{c_{nsp}\kappa^2/64, c_{nsp}n/64\}} e^{-m/2} \right) \\ &= O_{c_{nsp}, C, \gamma} \left(\frac{1}{L \|\mathbf{w}'\|_2} + \exp(-\Theta_{C, c_{nsp}}(\kappa^2)) \right), \end{aligned}$$

completing the theorem proof. □

Remark 4.8. *Under the assumption of (2) of Theorem 4.4, we have actually shown a stronger estimate that*

$$\frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e^{-2 \sum_{i=1}^n \|t\mathbf{w}'\|^2} \leq O \left(\frac{\lceil c_{nsp}^{-1/2} \gamma^{-1} \kappa / \|\mathbf{w}'\|_2 \rceil}{\kappa L} + \exp(-c_{nsp}\kappa^2/64) \right).$$

We note that Theorem 4.1 can be deduced from Theorem 4.4 by setting $\kappa = C\sqrt{n}$ with sufficiently large C ; for this there is a dilation $\mathbf{w} = t\mathbf{w}'$ with $\|\mathbf{w}'\|_2$ of order \sqrt{n} but $\|\mathbf{w}'\|_2 < \kappa$. We then just apply (2) of Theorem 4.4, noting that $L \geq 1$.

Remark 4.9. *When x_i are iid copies of an α -balanced random variable, then by Equation (12), by convexity, and by the fact that $1 - \alpha/2 \leq \sum_{j=1}^l \beta_j \leq 1$ we have*

$$\begin{aligned} \rho &\leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2 \sum_{i=1}^n \sum_{j=1}^l \beta_j \|\frac{xt_j w_i}{p}\|^2) \\ &\leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2 \sum_{j=1}^l \frac{\beta_j}{\sum_{j=1}^l \beta_j} (\sum_{j=1}^l \beta_j) \sum_{i=1}^n \|\frac{xt_j w_i}{p}\|^2) \\ &\leq \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \sum_{j=1}^l \frac{\beta_j}{\sum_{j=1}^l \beta_j} \exp(-2 (\sum_{j=1}^l \beta_j) \sum_{i=1}^n \|\frac{xt_j w_i}{p}\|^2). \\ &\leq \sum_{j=1}^l \frac{\beta_j}{\sum_{j=1}^l \beta_j} \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2(1 - \alpha/2) \sum_{i=1}^n \|\frac{xw_i}{p}\|^2) \\ &= \frac{1}{p} \sum_{x \in \mathbb{F}_p, x \neq 0} \exp(-2(1 - \alpha/2) \sum_{i=1}^n \|\frac{xw_i}{p}\|^2). \end{aligned}$$

It thus boils down to study the bounds for concentration probability of \mathbf{w} , for which we have done in the proof of Theorem 4.4.

4.10. Some properties of ULCD. Roughly speaking, our next result is similar to Theorem 4.4, but instead of working with the concentration event $X \cdot \mathbf{w} = r$ we are working with a coarser event that $X \cdot \mathbf{w}$ belongs to an arc in \mathbb{F}_p . We find it more convenient to write in mod 1 as follows.

Theorem 4.11 (anti-concentration modulo one). *Assume that $0 < a_1, \dots, a_n < 1$. Assume that*

$$\text{ULCD}_{\gamma, \kappa}((a_1, \dots, a_n)) = L \geq 1.$$

Then for any

$$\varepsilon > 2/L$$

we have

$$\mathbf{P}(\|\sum_i \xi_i a_i\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon) \leq O\left(\varepsilon + \log(1/\varepsilon)[\exp(-\kappa^2) + \exp(-4\gamma^2 \sum_i a_i^2)]\right)$$

where ξ_i are iid Bernoulli.

Note that we need this result because at some point we need to pass to characteristic zero, and take distance to \mathbb{Z} . A key difference of this bound compared to the classical small ball estimate (say studied in [32]) is that we are looking at the balls modulo one, rather than with respect to the whole real line.

Proof. (of Theorem 4.11) Let μ be the distribution of $\sum_i a_i \xi_i$ modulo one, where we can write $\mu = \mu_1 * \dots * \mu_n$, and where $\mu_i(a_i) = \mu(-a_i) = 1/2$. Let $L_0 = \lceil 1/\varepsilon \rceil$. We use the Erdős-Turán inequality,

$$\mu([-\varepsilon, \varepsilon]) = \mathbf{P}(\|\sum_i a_i \xi_i\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon) \leq \varepsilon + \frac{1}{L_0} + \sum_{k=1}^{L_0} \frac{|\widehat{\mu}(k)|}{k},$$

As ξ_i are iid Bernoulli, bounding the cosine as in the proof of Theorem 4.4 we have

$$|\widehat{\mu}(k)| = \left| \int_0^1 e^{2\pi\sqrt{-1}k\theta} d\mu(\theta) \right| = \left| \prod_i \int_0^1 e^{2\pi\sqrt{-1}k\theta} d\mu_i(\theta) \right| \leq \exp(-\sum_i \|2a_i k\|_{\mathbb{R}/\mathbb{Z}}^2).$$

Now by definition of $\mathbf{ULCD}_{\gamma,\kappa}$, as $L_0 \leq 1/\varepsilon < \mathbf{ULCD}_{\gamma,\kappa}((a_1, \dots, a_n))/2$, for any $k \leq L_0$ we have

$$\sum_i \|2a_i k\|_{\mathbb{R}/\mathbb{Z}}^2 \geq \min\{\kappa^2, 4\gamma^2 k^2 \sum_i a_i^2\},$$

and so

$$\exp(-\sum_i \|2a_i k\|_{\mathbb{R}/\mathbb{Z}}^2) \leq \exp(-\kappa^2) + \exp(-4\gamma^2 k^2 \sum_i a_i^2) \leq \exp(-\kappa^2) + \exp(-4\gamma^2 \sum_i a_i^2).$$

Summing over all $k \leq L_0$ we have

$$\mathbf{P}(\|\sum_i \xi_i a_i\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon) \leq O(\varepsilon) + \log(1/\varepsilon)[\exp(-\kappa^2) + \exp(-4\gamma^2 \sum_i a_i^2)],$$

as desired. \square

It is remarked that the bound above depends on $\|\mathbf{a}\|_2$, which becomes almost meaningless if $\|\mathbf{a}\|_2$ is small, say of order $O(1)$. To avoid this situation, we will need to consider vectors \mathbf{w}' that have large size and large $\mathbf{ULCD}_{\gamma,\kappa}(\mathbf{w}')$ at the same time.

Our next result roughly says that a non-sparse vector cannot have very small \mathbf{ULCD} , at least with respect to \mathbb{F}_p with not too large and not too small p . To be more precise, we have the following.

Remark 4.12. *As we will be working with vectors \mathbf{w} satisfying (25), we easily see that for any $t \neq 0$ in \mathbb{F}_p*

$$\|(t\mathbf{w})'\|^2 \geq cn\left(\frac{1}{p}\right)^2.$$

Notice that this quantity is larger than κ^2 if $p \leq n^{1/2}/\kappa$, and in this case the first part of 4.4 holds, and hence automatically

$$\rho(\mathbf{w}) \leq \exp(-c\kappa^2).$$

As such, in what follows we will be working with

$$p \gtrsim n^{1/2}/\kappa.$$

Lemma 4.13 (LCD and size in fields of small order). *Assume that $\kappa = n^c$ for a positive constant $c < 1/16$. Assume that p is a prime smaller than $\exp(c\kappa^2)$, and $w \in \mathbb{F}_p^n$ is a vector satisfying (25) and such that $\rho(\mathbf{w}) \geq 2\exp(-\kappa^2/2)$. Then there exists $t \in \mathbb{F}_0$ so that with $\mathbf{w} = t\mathbf{w}$ we have $\|\mathbf{w}'\|_2$ has order κ and either $\mathbf{ULCD}_{\gamma,\kappa}(\mathbf{w}') = p$ (in which case we can apply (26)) or else*

$$\mathbf{ULCD}_{\gamma,\kappa}(\mathbf{w}') \geq \kappa^{5/4-c}.$$

We remark that this result is perhaps the most important one in our treatment, as it allows us to assume that the \mathbf{ULCD} to be sufficiently large to make sense of the bounds. In characteristic zero, this bound is straightforward if the vector is incompressible (being far from sparse vectors).

Before proving this lemma, we first need the following simple statement.

Claim 4.14. *Assume that $\mathbf{w} \in \mathbb{F}_p^n$ is a non-zero vector satisfying (25) and such that $\rho(\mathbf{w}) \geq 2\exp(-\kappa^2/2)$, with $\kappa = o(\sqrt{n})$. Then there exists $t \in \mathbb{F}_0 = \mathbb{F}_p \setminus 0$ so that with $\mathbf{w} = t\mathbf{w}$ we have*

$$\kappa/2 \leq \|\mathbf{w}'\|_2 < \kappa.$$

Proof. (of Claim 4.14) As \mathbf{w} satisfies (25) and $\rho(\mathbf{w}) \geq 2\exp(-\kappa^2/2)$, (1) of Theorem 4.4 does not apply, and so there is a fiber $\mathbf{w} = t\mathbf{w}$ such that $\|\mathbf{w}'\|_2 < \kappa$. If $\|\mathbf{w}'\|_2 \geq \kappa/2$ then we would be done. Otherwise we just consider the sequence $\mathbf{w}, 2\mathbf{w}, 3\mathbf{w}$, etc. By the triangle inequality (where we recall that $(t\mathbf{w})' = \frac{1}{p}(tw_1 \pmod{p}, \dots, tw_n \pmod{p})$) we have

$$\|((k+1)\mathbf{w})'\|_2 \leq \|(k\mathbf{w})'\|_2 + \|\mathbf{w}'\|_2.$$

On the other hand, by (25) $\sum_{k \in \mathbb{F}_p} \|(k\mathbf{w})'\|_2$ has order \sqrt{np} , so there must exist a smallest $k_0 \geq 2$ such that $\|((k_0 + 1)\mathbf{w})'\|_2 \geq \kappa$. It then follows that $\kappa/2 \leq \|(k_0\mathbf{w})'\|_2 < \kappa$. \square

Proof. (of Lemma 4.13) Assume that we are not in the first case, and also assume to the contrary that we are not in the second case either. We will iterate the following process, which will then result in a contradiction. Set

$$\beta = 1/4 - c.$$

We start from any $\mathbf{u}_1 = \mathbf{w}' = (w_1/p, \dots, w_n/p)$ in the fiber $t\mathbf{w}$ of \mathbf{w} with $\kappa/2 \leq \|\mathbf{u}_1\|_2 < \kappa$.

Step 1: Let $D_1 = \text{ULCD}(\mathbf{u}_1)$, then $2 \leq D_1 \leq \min\{\kappa^{1+\beta}, p-1\}$. Let $\mathbf{u}'_1 = D_1\mathbf{u}_1 (= (D_1\mathbf{w})')$, then we have

$$\|\mathbf{u}'_1\|_2 \leq \kappa.$$

Step 2: If this vector has norm smaller than $\kappa/2$, then we use Claim 4.14 to dilate appropriately by $C_1 \geq 2$ so that $\kappa/2 \leq \|C_1\mathbf{u}'_1\|_2 \leq \kappa$, and set

$$\mathbf{u}_2 = C_1\mathbf{u}'_1 (= (C_1D_1\mathbf{w})').$$

We then return to Step 1 and iterate the process, note that while the D_i are bounded by $\kappa^{1+\varepsilon}$, we don't have such a bound for the C_i .

Now for each $1 \leq t \leq p-1$ we can always write

$$t = D_1(C_1(D_2(\dots) + r_2) + s_1) + r_1,$$

where $r_1 < D_1, s_1 < C_1, r_2 < D_2, s_2 < C_2, \dots$. Indeed, to verify this we first divide t by D_1 and get a remainder r_1 ; we then divide the quotient by C_1 to get a remainder s_1 , and then divide the new quotient by D_2 , etc until the last step. Now as $t \leq p-1 \leq 2\kappa^2$ (this is where we require p to be small), and as $C_i, D_i \geq 2$, we must stop the division process after κ^2 steps.

Next we analyze the norm of $\|t\mathbf{u}_1\|_2 = \|(t\mathbf{w})'\|_2$. We write, with $t_1 = t$

$$t_1\mathbf{u}_1 = D_1(C_1(D_2(\dots) + r_2) + s_1)\mathbf{u}_1 + r_1\mathbf{u}_1 = (C_1(D_2(\dots) + r_2) + s_1)D_1\mathbf{u}_1 + r_1\mathbf{u}_1 := t'_1\mathbf{u}'_1 + r_1\mathbf{u}_1.$$

Thus by the triangle inequality, and as $r_1 \leq D_1 - 1 < \kappa^{1+\beta}$ we have

$$\|t_1\mathbf{u}_1\|_2 = \|t\mathbf{u}_1\|_2 \leq \|t'_1\mathbf{u}'_1\|_2 + \kappa^{2+\beta}.$$

We next consider

$$t'_1\mathbf{u}'_1 = (C_1(D_2(\dots) + r_2) + s_1)\mathbf{u}'_1 = C_1(D_2(\dots) + r_2)\mathbf{u}'_1 + s_1\mathbf{u}'_1 = (D_2(\dots) + r_2)\mathbf{u}_2 + s_1\mathbf{u}'_1 := t_2\mathbf{u}_2 + s_1\mathbf{u}'_1.$$

By the triangle inequality

$$\|t'_1\mathbf{u}'_1\|_2 \leq \|t_2\mathbf{u}_2\|_2 + \|s_1\mathbf{u}'_1\|_2 \leq \|t_2\mathbf{u}_2\|_2 + \kappa,$$

where in the last estimate we used the fact that $0 \leq s_1 \leq C_1 - 1$ and C_1 is the largest integer so that $\kappa/2 \leq \|C_1\mathbf{u}'_1\|_2 \leq \kappa$ (where we recall that $\|\mathbf{u}'_1\|_2 \leq \kappa$, and the role of C_1 was only to dilate this vector if its norm was much smaller than this, as in the proof of Claim 4.14). The analysis for $\|t_2\mathbf{u}_2\|_2$ and other terms can be done similarly.

Adding all the bounds, we hence obtain

$$\|t\mathbf{u}_1\|_2 \leq \kappa^2 \times \kappa^{2+\beta} = \kappa^{4+\beta}.$$

Now as this is true for all $t \in \mathbb{F}_p$, we thus have

$$\sum_{t \in \mathbb{F}_p} \|t\mathbf{w}'\|_2^2 = O(p\kappa^{4+\beta}).$$

On the other hand, by (25), as w' has at least $c_{nsp}n$ non-zero entries, the left hand side can be shown to be at least $c_{nsp}np/64$, which is a contradiction if $\kappa \leq n^c = n^{1/4-\beta}$. \square

With the same proof, we record the following corollary which will be used later.

Corollary 4.15 (ULCD cannot be small). *Assume that $p \leq \exp(ck^2)$ and that $\kappa = n^c$ for $c < 1/16$. Assume that $\mathbf{w} \in \mathbb{F}_p^m$, for $m \geq \kappa^{4+2\varepsilon}$, and \mathbf{w} has at least $\kappa^{4+2(1/4-c)}$ non-zero components. Then we either have either $\|(t\mathbf{w})'\|_2 > \kappa$ for all t , or there exists such $\mathbf{w}' = (t\mathbf{w})'$ such that $\kappa/2 \leq \|\mathbf{w}'\|_2 < \kappa$ and that*

$$\text{ULCD}_{\gamma, \kappa}(\mathbf{w}') \geq \kappa^{5/4-c}.$$

5. STRUCTURES OF VECTORS IN \mathbb{F}_p^n : A COMBINATORIAL APPROACH

Now we present our third characterization. Let μ be an α -balanced distribution in \mathbb{F}_p . For simplicity, we again assume μ to be Bernoulli ± 1 , the general α -balanced case can be treated almost identically as in the previous two sections. Our goal here is the following.

Theorem 5.1 (Combinatorial structure, characterization III). *Let $k \geq 1$ be an integer. Let $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ be any function such that $f(x) \leq x/100$. For any non-zero vector $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{F}_p^n$ we have*

$$\rho(\mathbf{w}) = \sup_{a \in \mathbb{Z}/p\mathbb{Z}} |\mathbf{P}(\mu_1 w_1 + \dots + \mu_n w_n = a) - \frac{1}{p}| \leq \frac{R_k(\mathbf{w})}{2^{2k} n^{2k} \sqrt{f(|\text{supp}(\mathbf{w})|)}} + e^{-f(|\text{supp}(\mathbf{w})|)/2}.$$

where μ_1, \dots, μ_n are independent and identically distributed copies of μ , and where $R_k(\mathbf{w})$ is the number of solutions to $\pm w_{i_1} \pm \dots \pm w_{i_k} = 0 \pmod{p}$, and $k \leq n/f(|\text{supp}(\mathbf{w})|)$.

Our approach here is somewhat similar to [8], which in turn follows the original approach of Halász in [18]). However, the key difference here is that we are estimating the deviation of $\sup_{a \in \mathbb{Z}/p\mathbb{Z}} |\mathbf{P}(\mu_1 w_1 + \dots + \mu_n w_n = a)|$ from $1/p$ rather than giving an upper bound for $\sup_{a \in \mathbb{Z}/p\mathbb{Z}} |\mathbf{P}(\mu_1 w_1 + \dots + \mu_n w_n = a)|$ as in [8].

Proof. (of Theorem 5.1) We follow the proof of Theorem 4.4 until Equation (27) that

$$|T(m, p/2)| - 1 \leq k^{-1} (|T(|\text{supp}(\mathbf{w})|/64, p/2)| - 1),$$

where $k = \Theta(\sqrt{f(|\text{supp}(\mathbf{w})|)/m})$.

Denote $T' := \{l \in \mathbb{F}_p, |\sum_{j=1}^n \cos(2\pi l w_j/p)| \geq n - 100f(|\text{supp}(\mathbf{w})|)\}$. Then we see that

$$T(|\text{supp}(\mathbf{w})|/64, p/2) \leq |T'|.$$

By Markov's inequality,

$$|T'| \leq \frac{1}{(n - 100f(|\text{supp}(\mathbf{w})|))^{2k}} \sum_{l \in T'} \left| \sum_{j=1}^n \cos(2\pi l w_j/p) \right|^{2k}.$$

By expanding out the RHS and summing over $l \in \mathbb{F}_p$ instead, we can bound the RHS from above by

$$T(|\text{supp}(\mathbf{w})|/64, p/2) \leq |T'| \leq \frac{\sqrt{2} p R_k(\mathbf{w})}{2^{2k} n^{2k}}.$$

The rest can be completed as in Theorem 4.4:

$$\begin{aligned} |\mathbf{P}(X \cdot \mathbf{w} = r) - \frac{1}{p}| &\leq \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e^{-2 \sum_{i=1}^n \|t \mathbf{w}'\|^2} \\ &\leq \frac{1}{p} \left(\sum_{m \leq f(|\text{supp}(\mathbf{w})|)} \sqrt{\frac{m}{f(|\text{supp}(\mathbf{w})|)}} \frac{\sqrt{2} p R_k(\mathbf{w})}{2^{2k} n^{2k}} e^{-m} + p \sum_{m > f(|\text{supp}(\mathbf{w})|)} e^{-m} \right) \\ &\leq \frac{R_k(\mathbf{w})}{2^{2k} n^{2k} \sqrt{f(|\text{supp}(\mathbf{w})|)}} + e^{-f(|\text{supp}(\mathbf{w})|)/2}, \end{aligned}$$

as claimed. □

6. NON-STRUCTURES OF NORMAL VECTORS

In this section we use the three characterizations above to establish Theorem 1.5. First, it is easy to show that normal vectors are non-sparse with high probability.

Lemma 6.1. *There exists an absolute constant $c_{nsp} > 0$ such that with probability $1 - \exp(-\Theta(n))$ any normal vector w of $\text{span}(X_1, \dots, X_{n-1})$ satisfies (25).*

Proof. This follows from Odylzko's lemma, see for instance [30, 27]. □

Now we use the results from Sections 3, 4, and 5 to show that the normal vectors cannot have any structure. In our first proposition, we use the structure from Section 3.

Proposition 6.2 (Normal vectors cannot have additive structures). *Let $C > 0$. Let X_1, \dots, X_{n-d} be the first $n-d$ columns of a matrix M whose entries are iid copies of a α -balanced random variable, where $d \leq cn$ for some sufficiently small constant c . Let \mathbf{w} be any non-zero vector that is orthogonal to X_1, \dots, X_{n-d} . Then with probability at least $1 - \exp(-\Theta(n))$, the vector \mathbf{w} cannot have structure as in the conclusion of Theorem 3.1. In particular, we have*

$$\rho(\mathbf{w}) = O(n^{-C})$$

where the implied constant depends on C .

Proof. (of Proposition 6.2) First of all, from Lemma 6.1, with a loss of $\exp(-\Theta(n))$ in probability we can assume that \mathbf{w} is not sparse. Assume that

$$\rho = \rho(\mathbf{w}) \asymp n^{-C},$$

where $C \geq 1/2$. Also, by Corollary 4.6, it suffices to assume $p \gtrsim n^{1/2}$.

For convenience, let $p' = \min\{p, \rho^{-1}\}$, and so $p' \gtrsim n^{1/2}$. Then by Theorem 3.1, we have a generalized arithmetic progression P of rank $O(1)$ in \mathbb{F}_p and of size $O(1 + \min\{\rho^{-1}/n^\varepsilon, p/n^\varepsilon\}) = O(p'/n^\varepsilon)$ that contains all but $n^{2\varepsilon}$ entries of \mathbf{w} . Note that the number of ways to choose such a P is bounded by

$$p^{O(1)} \rho^{-O(1)}.$$

Given P , the number of vectors \mathbf{w} whose $n - n^{2\varepsilon}$ components are from P is at most

$$\binom{n}{n^{2\varepsilon}} |P|^{n-n^{2\varepsilon}} p^{n^{2\varepsilon}} \leq 2^n (p'/n^\varepsilon)^{n-n^{2\varepsilon}} p^{n^{2\varepsilon}} \leq 8^n (p'/n^\varepsilon)^n,$$

provided that $p \leq \exp(n^{1-2\varepsilon})$.

Given \mathbf{w} for which $\rho(\mathbf{w}) \geq \rho$, the probability that \mathbf{w} is orthogonal to X_1, \dots, X_{n-d} is bounded by

$$8^n (p'/n^\varepsilon)^n \left(\frac{1}{p} + \rho\right)^{n-d} \leq 8^n (p'/n^\varepsilon)^n \left(\frac{2}{p'}\right)^{n-d} \leq n^{-\varepsilon n/2},$$

provided that $d \leq cn$ for some small positive constant c .

Taking union bound over only $p^{O(1)} \rho^{-O(1)}$ choices of P , we obtain the claim. □

We next use the result from Section 4 to show that the random normal vector does not have small $\mathbf{ULCD}_{\gamma, \kappa}$.

Proposition 6.3 (Normal vectors cannot have small ULCD). *Assume that $p \leq \exp(c\kappa^2)$ and that $\kappa = n^c$ for $c < 1/16$. Let X_1, \dots, X_{n-d} be the first $n-d$ columns of a random $(-1, 1)$ Bernoulli matrix, where $d \leq n^c$. Let \mathbf{w} be any non-zero vector that is orthogonal to X_1, \dots, X_{n-d} . Then with probability at least $1 - \exp(-\Theta(n))$, we have*

$$\mathbf{ULCD}_\kappa(\mathbf{w}) \geq \exp(c'\kappa^2)$$

with some c' depending on c and γ . In particular, Theorem 1.5 holds.

We remark that in the above theorem we assume M to be a $(-1, 1)$ Bernoulli matrix. Our treatment also works for other integral matrices ² with $\|M\|_2 = O(\sqrt{n})$ but it does not seem to extend to α -balanced ensemble as in Proposition 6.2 (although Theorem 4.4 holds for this setting). The main reason is that at some point in the proof we pass to a net of vectors in \mathbb{R}^n , and then under the action of M the size of this net will blow up if M has large norm, see (28).

Proof. (of Proposition 6.3) We will show that with high probability, there does not exist \mathbf{w} in the fiber of $t\mathbf{w}$ such that $\kappa/2 \leq \|\mathbf{w}'\|_2 < \kappa$ and that

$$\kappa^{1+(1/4-c)} < \mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}') \leq \exp(c'\kappa^2/2)/\kappa.$$

To do this, we divide this range into $O(\kappa^2)$ dyadic intervals $(D_i, D_{i+1} = 2D_i)$. For $D = D_i$, let

$$S_D = \left\{ \mathbf{w}' = (w_1/p, \dots, w_n/p) : \kappa/2 \leq \|\mathbf{w}'\|_2 < \kappa \wedge D \leq \mathbf{ULCD}_{\gamma, \kappa}(\mathbf{w}') \leq 2D \right\}.$$

Lemma 6.4 (Size of the approximating net). *Let $c_0 > 0$ be given sufficiently small compared to c (where $\kappa = n^c$). S_D accepts a $O(\kappa/D)$ -net \mathcal{N} of size $D(C\kappa D/\sqrt{n})^n$ if $\kappa D \geq c_0\sqrt{n}$ and of size Dn^{c_0n} if $\kappa D < c_0\sqrt{n}$ and such that $\mathcal{N} \subset S_D$.*

Before proving this result by following [32], let us introduce a fact that will be useful to our nets.

Fact 6.5. *Assume that \mathcal{S} accepts a δ -net \mathcal{U} of size $|\mathcal{N}|$, then \mathcal{S} also accepts a 2δ -net \mathcal{U}' such that $\mathcal{U}' \subset \mathcal{S}$ and which has size at most $|\mathcal{N}|$.*

Proof. By throwing away vectors from \mathcal{U} if needed, we assume that each $u \in \mathcal{U}$ δ -approximates at least one vector s' from \mathcal{S} . Let \mathcal{N}' be a collection of such s' (we choose an arbitrary s' from \mathcal{S} that is δ -approximated by any u .) Thus $\mathcal{N}' \subset \mathcal{S}$ and $|\mathcal{N}'| \leq |\mathcal{N}|$. Now for any $s \in \mathcal{S}$, there exists $u \in \mathcal{U}$ such that $\|u - s\|_2 \leq \delta$, and also by definition there also exists $s' \in \mathcal{U}'$ such that $\|u - s'\|_2 \leq \delta$. Thus we have $\|s - s'\|_2 \leq 2\delta$, so \mathcal{U}' is a 2δ -net of \mathcal{S} . \square

Proof of Lemma 6.4. By taking union bound over a small number of choices (at most $O(\kappa \times (D/\kappa)) = O(D)$ choices) we assume that for some $T \in \kappa/D \cdot \mathbb{Z}$ we have

$$T - \kappa/D \leq \|\mathbf{w}'\|_2 \leq T + \kappa/D.$$

By definition, as $\|L\mathbf{w}'\|_{\mathbb{R}/\mathbb{Z}} \leq \kappa$ and $D \leq L \leq 2D$, there exists $\mathbf{p} \in \mathbb{Z}^n$ such that

$$\|L\mathbf{w}' - \mathbf{p}\|_2 \leq \kappa.$$

This implies that

$$\left\| \mathbf{w}' - \frac{\mathbf{p}}{L} \right\|_2 \leq \frac{\kappa}{L} \leq \frac{\kappa}{D},$$

and hence

$$T - 2\frac{\kappa}{D} \leq \frac{\|\mathbf{p}\|_2}{L} \leq T + 2\frac{\kappa}{D}.$$

Thus

$$\begin{aligned} \left\| \mathbf{w}' - T \frac{\mathbf{p}}{\|\mathbf{p}\|_2} \right\|_2 &\leq \left\| \mathbf{w}' - \frac{\mathbf{p}}{L} \right\|_2 + \left\| T \frac{\mathbf{p}}{\|\mathbf{p}\|_2} - \frac{\mathbf{p}}{L} \right\|_2 \\ &\leq \frac{\kappa}{D} + \|\mathbf{p}\|_2 \left| \frac{T}{\|\mathbf{p}\|_2} - \frac{1}{L} \right| \\ &\leq 3\frac{\kappa}{D}. \end{aligned}$$

²Here the random entries of M take value in \mathbb{Z} , although in our results we view M as a matrix of entries from $\mathbb{Z}/p\mathbb{Z}$ (or \mathbb{F}_p) via the natural map $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$.

Now as $\|\mathbf{w}'\|_2 < T + 2\kappa/L$, we also have $\|\mathbf{p}/L\|_2 \leq T + 3\kappa/L$ and so

$$\|\mathbf{p}\|_2 \leq 2DT + 3\kappa \leq 2D(\kappa + \kappa/D) + 2\kappa < 4D\kappa.$$

Let \mathcal{N} be the collection of vectors $T \frac{\mathbf{p}}{\|\mathbf{p}\|_2}$, where T ranges over $O(D)$ choices in the set $\kappa/D \cdot \mathbb{Z}$, and \mathbf{p} ranges over all integer vectors in \mathbb{Z}^n satisfying $\|\mathbf{p}\|_2 \leq 4D\kappa$.

Now we bound the size of \mathcal{N} basing on the magnitude of κD .

Case 1. If $\kappa D \geq c_0\sqrt{n}$, then the number of integral vectors \mathbf{p} of norm at most $3\kappa D$ is known to be bounded by $(C\kappa D/\sqrt{n})^n$, and so

$$|\mathcal{N}| \leq D(C\kappa D/\sqrt{n})^n.$$

Case 2. If $\kappa D \leq c_0\sqrt{n}$, where c_0 is sufficiently small, then all but $O((\kappa D)^2)$ entries of \mathbf{p} are zero. So the number of such vectors \mathbf{p} is bounded by $\binom{n}{(\kappa D)^2} (O(1))^{(\kappa D)^2}$, and so

$$|\mathcal{N}| \leq D \binom{n}{(\kappa D)^2} C^{(\kappa D)^2} \leq Dn^{c_0 n}.$$

Finally, we can always assume \mathcal{N} to consist of vectors from S_D by using Fact 6.5. □

Now we use the obtained net to show that normal vectors in iid matrices cannot have small **ULCD**.

For short, the method below works as follows: for \mathbf{w}' (viewed as vectors in \mathbf{Q}^n) we have $M\mathbf{w}' \in \mathbb{Z}^n$, where $\mathbf{w}' = (w_1/p, \dots, w_n/p)$. Then we approximate this vector by an element from the obtained net, and then pass to consider the probability from each net element. After approximation, we have that $M\mathbf{u}'$ is close to \mathbb{Z}^n in ℓ_2 -norm, and so we can apply the classical Erdős-Turán bound.

Now we complete the proof of the proposition. Assume otherwise, then by the argument above, by passing to an appropriate $t\mathbf{w}$, we can assume that $\kappa/2 \leq \|\mathbf{w}'\|_2 < \kappa$, and that $\mathbf{w}' \in S_D$ for some D_i from $O(\kappa^2)$ dyadic intervals. As \mathbf{w} is orthogonal to X_1, \dots, X_{n-1} in \mathbb{F}_p , we then have the following key property for $\mathbf{w}' = \frac{1}{p}\mathbf{w}$

$$M\mathbf{w}' \in \mathbb{Z}^{n-d},$$

where M is the $n \times (n-d)$ matrix formed by X_1, \dots, X_{n-1} .

By Lemma 6.4, there exists $\mathbf{u}' \in \mathcal{N}$ such that

$$\|\mathbf{w}' - \mathbf{u}'\|_2 = O(\kappa/D).$$

It is well known that $\|M\| = O(\sqrt{n})$ with probability at least $1 - \exp(-\Theta(n))$ (We note that this is the only place where we used $M = O(\sqrt{n})$ to prevent the net from expanding), and so we will condition on this event. We then have

$$\|M^T \mathbf{w}' - M^T \mathbf{u}'\|_2 \leq O(\sqrt{n}\kappa/D). \tag{28}$$

Therefore,

$$\text{dist}(M^T \mathbf{u}', \mathbb{Z}^{n-d}) \leq O(\sqrt{n}\kappa/D).$$

Let \mathcal{E} be this event, whose probability will be bounded shortly. By Theorem 4.11, as obviously $\kappa/D > 1/D$, we have

$$\begin{aligned} \mathbf{P}(\|X_i \cdot \mathbf{u}'\|_{\mathbb{R}/\mathbb{Z}} = O(\kappa/D)) &= O(\kappa/D + (\log(D/\kappa))(\exp(-\kappa^2) + \exp(-4\gamma^2\|\mathbf{u}'\|_2^2))) \\ &= O(\kappa/D), \end{aligned} \tag{29}$$

where in the last estimate we used the fact that $D \leq \exp(c'\kappa^2)$ with sufficiently small c' .

By Lemma A.1 we thus have for some absolute positive constant C'

$$\mathbf{P}(\mathcal{E}) \leq (C'\kappa/D)^{n-d}.$$

Putting together using union bound over all \mathbf{u}' from the net, as $\kappa = n^c$, we obtain in the case $\kappa D \geq c_0\sqrt{n}$ a bound

$$\begin{aligned} \mathbf{P}(\exists \mathbf{u}' \in \mathcal{N}, \|M\mathbf{u}'\|_{\mathbb{R}/\mathbb{Z}} = O(\sqrt{n}\kappa/D)) &\leq D(C\kappa D/\sqrt{n})^n \times (C'\kappa/D)^{n-d} \\ &\leq D^2(CC'\kappa^2/\sqrt{n})^n < \exp(-\Theta(n)). \end{aligned}$$

Note that here we have to assume $\kappa = o(n^{1/4})$ at least.

Also, in the second case that $\kappa D < c_0\sqrt{n}$, noting that $D \geq k^{5/4-c}$

$$\begin{aligned} \mathbf{P}(\exists \mathbf{u}' \in \mathcal{N}, \|M\mathbf{u}'\|_{\mathbb{R}/\mathbb{Z}} = O(\sqrt{n}\kappa/D)) &\leq n^{c_0n} \times (C'\kappa/D)^{n-d} \\ &\leq n^{c_0n} \times (C'/\kappa)^{(1/4-c)n} \\ &\leq C'^n n^{c_0n} \times n^{-c(1/4-c)n} \\ &\leq n^{-cn/8}, \end{aligned}$$

assuming that c_0 is sufficiently large compared to c , and that $c \leq 1/16$. □

In our last result of this subsection, by using the terminology of Section 5, we show the following.

Proposition 6.6 (Normal vectors cannot have combinatorial structure). *Assume that $p \leq \exp(c\kappa^2)$ and that $\kappa = n^c$ for $c < 1/16$. Let X_1, \dots, X_{n-d} be the first $n-d$ columns of a matrix M whose entries are iid copies of an α -balanced random variable, where $d \leq c'n$ for some sufficiently small constant c' . Let \mathbf{w} be any non-zero vector that is orthogonal to X_1, \dots, X_{n-d} . Then with probability at least $1 - \exp(-\bar{c}n)$, we have that*

$$\rho(\mathbf{w}) \leq e^{-\hat{c}\kappa^2}$$

where c', \bar{c} and \hat{c} are constants that only depend on c and α .

Note that this result holds for α -balanced ensembles where we don't have to assume $\|M\|_2 = O(\sqrt{n})$.

Let $Z = (z_1, \dots, z_n)$ be any vector in \mathbb{F}_p^n . We first record the following elementary relation (where we recall $\rho(\cdot)$ from Theorems 3.1 and 4.1).

Fact 6.7. *For any $I \subset [n]$ we have*

$$\rho(Z_I) \geq \rho(Z).$$

Proof. It suffices to show this for $I = [k]$. We first write

$$\begin{aligned} \mathbf{P}(z_1w_1 + \dots + z_nw_n = r) - 1/p &= \mathbf{E}_{w_{k+1}, \dots, w_n} [\mathbf{P}(\sum_{1 \leq i \leq k} z_iw_i = r - \sum_{k+1 \leq i \leq n} z_iw_i | w_{k+1}, \dots, w_n) - 1/p] \\ &\leq \max_{r'} \mathbf{P}(\sum_{1 \leq i \leq k} z_iw_i = r') - 1/p, \end{aligned}$$

and hence

$$\max_r \mathbf{P}(z_1w_1 + \dots + z_nw_n = r) - 1/p \leq \max_{r'} \mathbf{P}(\sum_{1 \leq i \leq k} z_iw_i = r') - 1/p,$$

where we note that both sides are non-negative.

We can bound the minimum in a similar fashion

$$\begin{aligned} \mathbf{P}(z_1w_1 + \dots + z_nw_n = r) - 1/p &= \mathbf{E}_{w_{k+1}, \dots, w_n} [\mathbf{P}(\sum_{1 \leq i \leq k} z_iw_i = r - \sum_{k+1 \leq i \leq n} z_iw_i | w_{k+1}, \dots, w_n) - 1/p] \\ &\leq \min_{r'} \mathbf{P}(\sum_{1 \leq i \leq k} z_iw_i = r') - 1/p, \end{aligned}$$

and so

$$\min_r \mathbf{P}(z_1 w_1 + \cdots + z_n w_n = r) - 1/p \leq \min_{r'} \mathbf{P}\left(\sum_{1 \leq i \leq k} z_i w_i = r'\right) - 1/p,$$

where we note that both sides are non-positive.

Putting this together, we thus obtain

$$\max_r |\mathbf{P}(z_1 w_1 + \cdots + z_n w_n = r) - 1/p| \leq \max_{r'} |\mathbf{P}\left(\sum_{1 \leq i \leq k} z_i w_i = r'\right) - 1/p|,$$

completing the proof. \square

We next need the following key definitions and results from [8].

Definition 6.8. For an $\mathbf{a} \in \mathbb{F}_p^n$, $k \in \mathbb{N}$ and $\delta \in [0, 1]$, we define $R_k^\delta(\mathbf{a})$ to be the number of solutions to

$$\pm a_{i_1} \pm a_{i_2} \cdots \pm a_{i_{2k}} = 0 \pmod{p}$$

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

We will make use of the observation from [8] that $R_k(\mathbf{a})$ is never much larger than $R_k^\delta(\mathbf{a})$.

Lemma 6.9 (Lemma 1.6, [8]). *For all integers k, n with $k \leq n/2$ and any prime p , $\mathbf{a} \in \mathbb{F}_p^n$ and $\delta \in (0, 1)$,*

$$R_k(\mathbf{a}) \leq R_k^\delta(\mathbf{a}) + (40k^{1-\delta}n^{1+\delta})^k.$$

As we will have the occasion to deal with subsets of vectors which we consider as vectors in their own right, we introduce the notation $|\mathbf{a}|$ to mean the dimension of a vector \mathbf{a} . By $\mathbf{b} \subset \mathbf{a}$ we mean that \mathbf{b} is a truncation of \mathbf{a} . The key technical result in [8] is the following combinatorial lemma, which helps control the number of vectors with many ‘‘local’’ arithmetic relations.

Lemma 6.10. [8, Theorem 1.7] *Denote*

$$\mathbf{B}_{k,s,\geq t}^\delta := \left\{ \mathbf{a} \in \mathbb{F}_p^n, R_k^\delta(\mathbf{b}) \geq t \frac{2^{2k} |\mathbf{b}|^{2k}}{p} \text{ for every } \mathbf{b} \subset \mathbf{a} \text{ with } |\mathbf{b}| \geq s \right\}.$$

Then

$$|\mathbf{B}_{k,s,\geq t}^\delta| \leq \left(\frac{s}{n}\right)^{2k-1} (\delta t)^{s-n} p^n.$$

At this point, we fix $\delta = 1/2$, $k = \lceil n^{1/8} \rceil$ and define

$$H_t = \left\{ \mathbf{a} \in \mathbb{F}_p^n, \exists \mathbf{b} \subset \mathbf{a}, \text{supp}(\mathbf{b}) \geq n^{1/4}, R_k^{1/2}(\mathbf{b}) \leq t \frac{2^{2k} |\mathbf{b}|^{2k}}{p} \right\}.$$

So roughly speaking, this is the set of \mathbf{a} which are not arithmetically rich. As Lemma 6.10 suggests, this set captures most of the vectors. More precisely we have the following (see also [8]).

Corollary 6.11. *If $p \leq \exp(c\kappa^2)$ and $\kappa = n^c$ for $c < 1/16$, then for $t \geq n^{1/16}$*

$$|\{\mathbf{a}, |\text{supp}(\mathbf{a})| \geq n^{1/4}, \mathbf{a} \notin H_t\}| \leq \left(\frac{4p}{t}\right)^n t^{n^{1/4}}.$$

Proof. (of Corollary 6.11) We can assume that $t \leq p$, otherwise the statement is trivially true as the left-hand side is zero. Fix a subset $S \subset [n]$ with $|S| \geq n^{1/4}$ and enumerate the vectors \mathbf{a} with $\text{supp}(\mathbf{a}) = S$. By assumption, $\mathbf{a} \notin H_t$ so the restriction $\mathbf{a}|_S$ of \mathbf{a} to the set S is an element of $\mathbf{B}_{k,n^{1/4},\geq t}(|S|)$. Therefore, Lemma 6.10 guarantees that the number of possible choices for $\mathbf{a}|_S$ is at most

$$\left(\frac{n^{1/4}}{|S|}\right)^{2k-1} \left(\frac{2p}{t}\right)^{|S|} (t/2)^{n^{1/4}} \leq \left(\frac{2p}{t}\right)^n t^{n^{1/4}}$$

where the second inequality follows from our assumption that $t \leq p$. We obtain the final result by summing over all subsets S . \square

The next lemma is a simple consequence of Theorem 5.1.

Lemma 6.12. *Suppose that $\mathbf{a} \in H_t$. If $p \leq \exp(c\kappa^2)$ and $\kappa = n^c$ for $c < 1/16$, then if $t \geq n^{1/16}$, there exists a constant $C > 0$ such that*

$$\rho(\mathbf{a}) \leq \frac{Ct}{pn^{1/8}}.$$

Proof. (of Lemma 6.12) Let \mathbf{b} be a subvector of \mathbf{a} with $|\text{supp}(\mathbf{b})| \geq n^{1/4}$ and $R_k^\delta(\mathbf{b}) \leq t2^{2k}|b|^{2k}/p$. In the notation of Theorem 5.1, if we let $f(x) = \sqrt{x}$ then

$$\begin{aligned} \rho(\mathbf{b}) &\leq \frac{R_k(\mathbf{b})}{2^{2k}|\mathbf{b}|^{2k}n^{1/8}} + e^{-n^{1/8}/2} \\ &\leq \frac{R_k^{1/2}(\mathbf{b}) + (40k^{1/2}|\mathbf{b}|^{3/2})^k}{2^{2k}|\mathbf{b}|^{2k}n^{1/8}} + e^{-n^{1/8}/2} \\ &\leq \frac{t2^{2k}|\mathbf{b}|^{2k}/p + (40k^{1/2}|\mathbf{b}|^{3/2})^k}{2^{2k}|\mathbf{b}|^{2k}n^{1/8}} + e^{-n^{1/8}/2} \\ &\leq \frac{t}{pn^{1/8}} + \left(\frac{20k}{|\mathbf{b}|}\right)^{k/2} + e^{-n^{1/8}/2}. \end{aligned}$$

This expression is dominated by the first term by our bound on the range of p and our choice of k . We recall that

$$\rho(\mathbf{a}) \leq \rho(\mathbf{b})$$

to finish the proof. \square

Now we complete one of our main results of the section.

Proof. (of Proposition 6.6) We let \mathcal{V} denote the vectors in \mathbb{F}_p^n with support larger than $c_{nsp}n$ and \mathcal{W} the set of non-zero vectors $\mathbf{w} \in F_p^n$ that such that

$$\rho(\mathbf{w}) \geq e^{-\tilde{c}\kappa^2}.$$

By Corollary 4.6, we can assume $p \gtrsim \sqrt{n}$. Observe that

$$\mathbf{P}(\exists \mathbf{v} \in \mathcal{W}, \mathbf{v} \perp X_1, \dots, X_{n-d}) = \mathbf{P}(\exists \mathbf{v} \in \mathcal{W} \cap \mathcal{V}, \mathbf{v} \perp X_1, \dots, X_{n-d}) + \mathbf{P}(\exists \mathbf{v} \in \mathcal{W} \cap \mathcal{V}^c, \mathbf{v} \perp X_1, \dots, X_{n-d}).$$

By Lemma 6.1,

$$\mathbf{P}(\exists \mathbf{v} \in \mathcal{W}, \mathbf{v} \in \mathcal{V}^c) \leq \exp(-\Theta(n)).$$

Therefore, it suffices to focus on the vectors in \mathcal{V} . Note that any $\mathbf{w} \in \mathcal{V}$ must reside in H_p since $R_k^{1/2} \leq 2^{2k}|\mathbf{b}|^{2k}$.

There are two cases to consider.

Case 1. We begin with vectors in $\mathcal{V} \cap \mathcal{W} \cap H_{n^{1/16}}$. Let \mathbf{a} be such a vector, then by definition of \mathcal{W} and By Lemma 6.12,

$$e^{-\tilde{c}\kappa^2} \leq \rho(\mathbf{a}) \leq \frac{1}{p}.$$

Because of the lower bound, by Theorem 3.6 there exists a generalized arithmetic progression P of rank one in \mathbb{F}_p and of size $O(p/n^\varepsilon)$ that contains all but $n^{2\varepsilon}$ entries of \mathbf{a} . Note that the number of ways to choose

such a P is bounded by $p^{O(1)}$. For a fixed P , the number of vectors \mathbf{a} with at least $n - n^{2\varepsilon}$ components in P is at most

$$\binom{n}{n^{2\varepsilon}} |P|^{n-n^{2\varepsilon}} p^{n^{2\varepsilon}} \leq 2^n (p/n^\varepsilon)^{n-n^{2\varepsilon}} p^{n^{2\varepsilon}} \leq 8^n (p/n^\varepsilon)^n.$$

The probability that any $\mathbf{a} \in \mathcal{V} \cap \mathcal{W} \cap H_{n^{1/16}}$ with at least $n - n^{2\varepsilon}$ components in P is orthogonal to X_1, \dots, X_{n-d} is bounded by

$$8^n (p/n^\varepsilon)^n \left(\frac{1}{p} + \frac{Cn^{1/16}}{pn^{1/8}} \right)^{n-d} \leq 8^n (p/n^\varepsilon)^n (2/p)^{n-d} \leq n^{-\varepsilon n/2},$$

provided that $d \leq cn$ for some small constant c . Finally, we take a union bound over $p^{O(1)}$ choices of P to conclude the proof.

Case 2. We address the remaining vectors. Let $\tau = n^{1/16}$. We show that no vector in $(\mathcal{W} \cap \mathcal{V}) \setminus H_{n^{1/16}}$ is orthogonal to X_1, \dots, X_{n-d} . We can now partition $(\mathcal{W} \cap \mathcal{V}) \setminus H_{n^{1/16}}$ as

$$\bigsqcup_{j=1}^J H_{2^j \tau} \setminus H_{2^{j-1} \tau}$$

where J is the smallest integer such that $2^J \tau \geq p$. Clearly, $J \leq \kappa^2$. We then have

$$\mathbf{P}(\exists v \in (\mathcal{W} \cap \mathcal{V}) \setminus H_{n^{1/16}}, \mathbf{v} \perp X_1, \dots, X_{n-d}) = \sum_{j=1}^J \mathbf{P}(\exists v \in (\mathcal{W} \cap \mathcal{V}) \cap (H_{2^j \tau} \setminus H_{2^{j-1} \tau}), \mathbf{v} \perp X_1, \dots, X_{n-d}).$$

Combining Corollary 6.11 and Lemma 6.12, we have (noting trivially that $2^j \tau \geq n^{1/16}$)

$$\begin{aligned} \sum_{j=1}^J \mathbf{P}(\exists v \in \mathcal{W} \cap (H_{2^j \tau} \setminus H_{2^{j-1} \tau}), \mathbf{v} \perp X_1, \dots, X_{n-d}) &\leq \sum_{j=1}^J \left(\frac{4p}{2^{j-1} \tau} \right)^n (2^{j-1} \tau)^{n^{1/4}} \left(\frac{1}{p} + \frac{C2^j \tau}{pn^{1/16}} \right)^{n-d} \\ &\leq \sum_{j=1}^J \left(\frac{4p}{2^{j-1} \tau} \right)^n (2^{j-1} \tau)^{n^{1/4}} \left(\frac{2C2^j \tau}{pn^{1/16}} \right)^{n-d} \\ &\leq n^{-(n-d)/16} C^n p^d \sum_{k=n+1}^p (2^{j-1} \tau)^{n^{1/4}} \\ &\leq \kappa^2 n^{-n/32} p^{d+2n^{1/4}} \\ &\leq \exp(-n \log n / 64) \end{aligned}$$

where the last line follows from small enough c'' .

Combining the above estimates, we can conclude that

$$\mathbf{P}(\exists v \in \mathcal{W}, \mathbf{v} \perp X_1, \dots, X_{n-d}) \leq \exp(-\Theta(n)) + \exp(-c'n \log n),$$

as desired. \square

7. DISTRIBUTION OF RANKS REVISITED

In this section we give a short proof for Theorem 1.4. We start with a high-dimensional lemma, which, in some sense, is a discrete analog of [33] where they considered distance of a random vector to a subspace of codimension d in \mathbb{R}^n .

Lemma 7.1. *Assume that H is a subspace in \mathbb{F}_p^n of codimension d , and such that for any $\mathbf{w} \in H$ we have $\rho(\mathbf{w}) \leq \delta$. Then*

$$|\mathbf{P}(X \in H) - 1/p^d| \leq \delta.$$

Proof. (of Lemma 7.1) Let $\mathbf{v}_1, \dots, \mathbf{v}_d$ be a basis of H . Our assumption says that for any t_1, \dots, t_d , not all zero, we have

$$\rho\left(\sum_i t_i \mathbf{v}_i\right) \leq \delta.$$

Note that in \mathbb{F}_p^n

$$1_{a_1=0, \dots, a_d=0} = p^{-d} \sum_{t_1, \dots, t_d \in \mathbb{F}_p} e_p(t_1 a_1 + \dots + t_d a_d).$$

We have

$$\begin{aligned} \mathbf{P}(\wedge_{i=1}^d X \cdot \mathbf{v}_i = 0) &= p^{-d} \sum_{t_1, \dots, t_d \in \mathbb{F}_p} \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(t[t_1 X \cdot \mathbf{v}_1 + \dots + t_d X \cdot \mathbf{v}_d]) \\ &= p^{-d} + p^{-d} \sum_{t_i \in \mathbb{F}_p, \text{ not all zero}} \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(t(X \cdot \sum_i t_i \mathbf{v}_i)). \end{aligned}$$

Now by our assumption

$$\left| \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(t(X \cdot \sum_i t_i \mathbf{v}_i)) \right| \leq \delta.$$

Thus we have

$$|\mathbf{P}(\wedge_i X \cdot \mathbf{v}_i = 0) - p^{-d}| \leq \delta,$$

completing the proof. \square

Now we apply Propositions 6.2, 6.3 and 6.6 to prove the following.

Lemma 7.2. *Assume that $p \leq \exp(c\kappa^2)$ and that $\kappa = n^c$ for $c < 1/16$ and $0 \leq d, u \leq n^c$. There exists an event \mathcal{E}_d with probability $\mathbf{P}(\mathcal{E}) \geq 1 - e^{-n^{c'}}$ such that the following holds*

$$\left| \mathbf{P}(X \in W_{n-u} | \mathcal{E} \wedge \text{rank}(W_{n-u}) = n - u - d) - 1/p^{u+d} \right| \leq \exp(-n^{c'}),$$

where W_{n-u} is the subspace generated by X_1, \dots, X_{n-u} .

Assume this Lemma, we can then complete Theorem 1.4 by direct calculations, or by applying [30, Theorem 5.3], we leave it for the reader as an exercise.

Proof. (of Lemma 7.2) We have seen from Propositions 6.3 and 6.6 that there is an event \mathcal{E} with $\mathbf{P}(\mathcal{E}) \geq 1 - e^{-n^{c'}}$ such that for any $\mathbf{w} \in W_{n-u}$ we have

$$\rho(\mathbf{w}) \leq e^{-n^{c'}}.$$

Now conditioning on this event, if $\text{rank}(W_{n-u}) = n - u - d$ then the codimension of W_{n-u} is $u + d$, and hence by Lemma 7.1 we have

$$\left| \mathbf{P}(X \in W_{n-u}) - \frac{1}{p^{d+u}} \right| \leq e^{-n^{c'}},$$

as claimed. \square

8. EQUI-DISTRIBUTION OF THE NORMAL VECTORS

In this section we prove Theorem 1.6. For convenience we decompose the task into two parts.

Proposition 8.1. *With the same assumption as in Theorem 1.6 we have*

- For each $i \in \{1, \dots, n\}$, we have

$$|\mathbf{P}(w_i = 0) - 1/p| \leq O(\exp(-n^{c'})).$$

- For each $i \neq j$, and for any $a \in \mathbb{F}_p$ we have

$$|\mathbf{P}(\exists \mathbf{w} = (w_1, \dots, w_n) \in W_{n-1}^\perp : w_i = a \wedge w_j = 1) - 1/p| \leq O(\exp(-n^c)).$$

Proof. (of Proposition 8.1) We prove the first item of Proposition 8.1. It suffices to show this for $i = 1$. Fix $i = 1$. We seek to bound the probability of the event that our normal vector \mathbf{v} has $v_1 = 0$ under the condition that our first $n - 1$ columns achieve full rank, i.e. $\text{rank}(M_{n \times (n-1)}) = n - 1$. Suppose we are given such a normal vector. Then restricting to the bottom $n - 1$ rows, we see that this is equivalent to the event that the submatrix $M_{(n-1) \times (n-1)}$ has a nontrivial nullspace. So we rewrite $\mathbf{P}(v_1 = 0 \mid \text{rank}(M_{n \times (n-1)}) = n - 1)$ as $\mathbf{P}(M_{(n-1) \times (n-1)} \text{ is singular} \mid \text{rank}(M_{n \times (n-1)}) = n - 1)$. We can simply view this as $\mathbf{P}(\text{rank}(M_{(n-1) \times (n-1)}) = n - 2 \mid \text{rank}(M_{n \times (n-1)}) = n - 1) := \mathbf{P}(A|B) = \mathbf{P}(A \cap B)/P(B)$.

By Theorem 1.4 (see also [27, Theorem A.4]), we know that

$$\mathbf{P}(B) = \prod_{i=2}^{\infty} (1 - p^{-i}) + O(e^{-n^c}).$$

Now consider the event $A \cap B$. This is the event that rows $\mathbf{r}_2, \dots, \mathbf{r}_n$ span a subspace H of dimension $n - 2$ and \mathbf{r}_1 is not in the span of H , which can be expressed as $\mathbf{P}(A' \cap B') = \mathbf{P}(A')\mathbf{P}(B'|A')$. For $\mathbf{P}(A')$, we again use Theorem 1.4,

$$\mathbf{P}(A') = \frac{1}{p} \prod_{i=2}^{\infty} \frac{(1 - p^{-i})}{(1 - p^{-1})} + O(e^{-cn}).$$

For $\mathbf{P}(B'|A')$, our previous section tells us that if we condition on rows $\mathbf{r}_2, \dots, \mathbf{r}_n$ having rank equal to $n - 2$, then our normal vector \mathbf{v}' exists and has large **ULCD**, i.e. $\rho(\mathbf{v}') \leq \exp(-c\kappa^2)$. So the probability that \mathbf{r}_1 is in the span of H under this condition is

$$\mathbf{P}((B')^c | A') = 1/p + O(\exp(-n^c)).$$

Putting this all together, we have

$$\begin{aligned} \mathbf{P}(A|B) &= \frac{\mathbf{P}(A \cap B)}{\mathbf{P}(B)} \\ &= \frac{\mathbf{P}(A')\mathbf{P}(B'|A')}{\mathbf{P}(B)} \\ &= \frac{1}{p} + O(e^{-n^c}). \end{aligned}$$

Now we prove the second item. It suffices to assume $(i, j) = (1, 2)$. The event that $w_1 = a, w_2 = 1$ is equivalent to the event that $a\mathbf{r}_1 + \mathbf{r}_2 + \mathbf{r}_3 w_3 + \dots + \mathbf{r}_n w_n = 0$, where \mathbf{r}_i is the i -th row of our matrix. If a is zero, we are done via the previous argument, so assume a is nonzero.

Let H be the span of rows $\mathbf{r}_3, \dots, \mathbf{r}_n$, which has full rank $n - 2$ by our rank assumption on $M_{n \times (n-1)}$ and the fact that $a\mathbf{r}_1 + \mathbf{r}_2 + \mathbf{r}_3 w_3 + \dots + \mathbf{r}_n w_n = 0$. Further, let π be the projection to the orthogonal complement H^\perp . For each evaluation of rows $\mathbf{r}_3, \dots, \mathbf{r}_n$, π is deterministic and $\pi(\mathbf{r}) = \langle \mathbf{r}, \mathbf{n} \rangle$, where \mathbf{n} is the deterministic normal vector. Applying this projection to the linear combination, we have

$$a\langle \mathbf{r}_1, \mathbf{n} \rangle + \langle \mathbf{r}_2, \mathbf{n} \rangle = 0.$$

Since \mathbf{n} is deterministic, each inner product takes values $b, c \in \mathbb{F}_p$ with probability uniformly $1/p$ with error $O(\exp(-n^c))$ by Theorem 6.3. This means that a , as the ratio of the inner products, is also uniformly distributed with probability $1/p$ and similar error. \square

We next prove the second part of Theorem 1.6, restated for convenience.

Proposition 8.2. *Assume that $p \lesssim n/\log n$. Let n_a denotes the number of w_i such that $w_i = a$. Then for any $\delta < 1$ which might depend on n such that $\delta^{-2}p = o(n/\log n)$. We then have*

$$\mathbf{P}(\wedge_{a=0}^{p-1} (|n_a/n - 1/p| \leq \delta/p) \geq 1 - e^{-c\delta^2 n/p}.$$

Proof. (of Proposition 8.2) Let \mathcal{E} denote the set of vectors under consideration up to scaling, and $\bar{\mathcal{E}}$ be the complement. We first have the following elementary fact.

Fact 8.3. *We have*

$$|\bar{\mathcal{E}}| \leq 2p^n e^{-c\delta^2 n/p}.$$

Proof. First, we note that each n_a has distribution $\text{Bin}(n, \frac{1}{p})$ with variance

$$n\left(\frac{1}{p}\right)\left(1 - \frac{1}{p}\right) = \frac{n(p-1)}{p^2}.$$

Letting $0 < \delta < 1$ and μ denote the mean of this distribution, the upper-tail and lower-tail Chernoff inequalities combine to form the following bound:

$$\mathbf{P}(|n_a - \mu| \geq \delta\mu) \leq 2e^{-c\mu\delta^2}.$$

For each i in $\{0, 1, \dots, p-1\}$, let F_a denote the event that $|n_a - \frac{n}{p}| < \delta n/p$. Then trivial union bound gives

$$\mathbf{P}(F_0 \cap \dots \cap F_{p-1}) \geq 1 - 2pe^{-c\delta^2 n/p}.$$

Since there are p^n different choices for \mathbf{v} , the number of non-equidistributed vectors \mathbf{v} is at most $p^n(2pe^{-c\delta^2 n/p})$. \square

Now we complete our result. Let \mathbf{w} be an arbitrary vector in \mathbf{F}_p^n . We seek to upper bound $\mathbf{P}(\mathbf{w}$ is normal and $\mathbf{w} \in \bar{\mathcal{E}})$. Immediately we have $\mathbf{P}(\mathbf{w}$ is normal and $\mathbf{w} \in \bar{\mathcal{E}})$ is bounded above by

$$\sum_{\mathbf{w} \in \bar{\mathcal{E}}} \mathbf{P}(\mathbf{w} \perp X_1, \dots, X_{n-1}) \leq \sum_{\mathbf{w} \in \bar{\mathcal{E}}} (\rho(\mathbf{w}))^{n-1}.$$

Similar to our previous sections, we may decompose the sum into classes where \mathbf{w} is sparse and \mathbf{w} is non-sparse. By Lemma 6.1, the contribution over our sparse vectors is negligible. For our non-sparse vectors, we appeal to Theorem 6.3. We can now bound the sum via:

$$\begin{aligned} \sum_{\mathbf{w} \in (\bar{\mathcal{E}}), \text{non-sparse}} (\rho(\mathbf{w}))^{n-1} &\leq \frac{2p^n}{e^{\delta^2 n/3p}} (1/p + e^{-n^c})^{n-1} \\ &= \frac{2p}{e^{\delta^2 n/3p}} (1 + pe^{-n^c})^{n-1} \\ &\leq \frac{4p}{e^{c\delta^2 n/p}} \\ &= O(e^{-c\delta^2 n/2p}), \end{aligned}$$

as long as $\delta^{-2}p = o(n/\log n)$, completing the proof. \square

9. PROOF OF THEOREM 1.7

It suffices to prove Theorem 9.1 below. Again, for simplicity we will assume M_n to be an iid Bernoulli matrix taking values ± 1 with probability $1/2$ and $p \geq 3$. We recall that $\phi(x)$ has degree d and p is sufficiently large and

$$p \leq n^{1/2-\varepsilon}.$$

Let α be a root of $\phi(\alpha) = 0$ and consider the field extension $\mathbb{F}_q = \mathbb{F}_p[\alpha]$. Notice that any element x of this field has form

$$x = \sum_{i=0}^{d-1} c_i \alpha^i.$$

More importantly, the event $\phi(x)|D_M(x)$ is equivalent to the event that $M_n - \alpha$ has rank at most $n - 1$ in this field \mathbb{F}_q . In other words, let W_{n-k} be the subspace in \mathbb{F}_q^n generated by the first $n - k$ columns of the matrix $M_n - \alpha$ (equivalently, the columns of $M_{[n] \times [n-k]} - \alpha$), then the event that $M_n - \alpha$ has rank at most $n - 1$ is the union of the (disjoint) events \mathcal{E}_k that W_{n-k} has rank $n - k$ and the $n - k + 1$ -th column $X_{n-k+1} - \alpha \mathbf{e}_{n-k+1}$ belongs to W_{n-k} . In what follows we will be mainly focusing on the case of \mathcal{E}_1 , treatments for $\mathcal{E}_2, \mathcal{E}_3, \dots$ will be discussed later, and summing over these events will imply Theorem 1.7.

Theorem 9.1. *There exists an absolute constant C such that*

$$|\mathbf{P}(\mathcal{E}_1) - \frac{1}{p^d}| = |\mathbf{P}(X_n - \alpha \mathbf{e}_n \in W_{n-1} | \text{rank}(W_{n-1}) = n - 1) - \frac{1}{p^d}| \leq C e^{-n^{1-\varepsilon}/p^2}.$$

Consider the normal vector $\mathbf{v} = (v_1, \dots, v_n)$ of W_{n-1} (i.e. the column space of the matrix $M_{[n] \times [n-1]} - \alpha$). This vector can be written as

$$\mathbf{v} = \sum_{i=0}^{d-1} \alpha^i \mathbf{u}_i,$$

where $\mathbf{u}_i = (u_{1i}, \dots, u_{ni})^T \in \mathbb{F}_p^n$. Notice that as for $1 \leq j \leq n - 1$ we have $\mathbf{v} \cdot (X_j - \alpha \mathbf{e}_j) = 0$. So we have that

$$\sum_{i=0}^{d-1} \alpha^i (\mathbf{u}_i \cdot X_j) = \alpha^{i+1} \mathbf{u}_i \cdot \mathbf{e}_j.$$

This implies that

$$\mathbf{u}_i \cdot X_j = u_{j(i-1)}. \quad (30)$$

Let

$$Q = M_{[n-1] \times [n-1]}^T. \quad (31)$$

By fixing the last coordinates $u_{in} = f_i \in \mathbb{F}_p$ of each \mathbf{u}_i (and with a loss of a multiplicative factor p^d in probability), and by fixing $X = \mathbf{r}_n(M_{[n] \times [n-1]})$ (i.e. X is the last row of $M_{[n] \times [n-1]}$), with \mathbf{v}_i be the truncated vectors $(u_{1i}, \dots, u_{(n-1)i})$ we can rewrite (30) as (with $\mathbf{v}_d = \mathbf{v}_0$)

$$Q \mathbf{v}_i + f_i X = \mathbf{v}_{i-1}, 1 \leq i \leq d. \quad (32)$$

In what follows we set

$$m := n^{1-\varepsilon/2}.$$

Conditioning on f_i, X , we will show the following key lemma.

Lemma 9.2. *With probability $\exp(-\Theta(n))$ with respect to the columns of the matrix M_n , for any vector \mathbf{v} that is orthogonal to the first $n - 1$ columns of $M_n - \alpha$ the subspace H generated by $\mathbf{v}_1, \dots, \mathbf{v}_d$ (defined as above) in \mathbb{F}_p^n cannot have m -sparse vector. In other words, there do not exist coefficients $\alpha_i \in \mathbb{F}_p$, not all zero, such that*

$$|\text{supp}(\sum_i \alpha_i \mathbf{v}_i)| \leq m.$$

We can actually prove a slightly more general version of this lemma, which will be used to control $\mathcal{E}_2, \mathcal{E}_3, \dots$

Lemma 9.3. *With probability at most $\exp(-\Theta(n))$ with respect to the columns of the matrix M_n , for any vector \mathbf{v} that is orthogonal to the first n' columns of $M_n - \alpha$ (where $n' = (1 - o(1))n$) there do not exist coefficients $\alpha_i \in \mathbb{F}_p$, not all zero, such that*

$$|\text{supp}(\sum_i \alpha_i \mathbf{v}_i)| \leq m.$$

We remark that the above lemmas are somewhat similar to Propositions 6.2, 6.3, 6.6, but the situation here is much more complicated as the relation between \mathbf{v}_i and $X_1, \dots, X_{n'}$ are non-trivial (for instance \mathbf{v}_i is not orthogonal to X_j), and also the diagonal entries are perturbed by α .

We postpone the proof of this lemma for a moment, and let us use it to prove the following result, which automatically implies Theorem 9.1.

Theorem 9.4. *On the event of Lemma 9.2 we have*

$$|\mathbf{P}_{X_n}((X_n - \alpha \mathbf{e}_n) \cdot \mathbf{v} = 0) - 1/p^d| \leq \exp(-cm/p^2).$$

Proof. (of Theorem 9.4) Notice that the event $(X_n - \alpha \mathbf{e}_n) \cdot \mathbf{v} = 0$ implies that (by (30), using the same notations for \mathbf{v}_i, f_i, x_n) for all $1 \leq i \leq d$

$$\mathbf{v}_i \cdot X_n|_{[n-1]} + f_i x_n = f_{i-1}.$$

In other words, conditioning on x_n , and by letting $Y_n = X_n|_{[n-1]}$ and by choosing deterministic numbers $g_i \in \mathbb{F}_p$ appropriately we have

$$Y_n \cdot \mathbf{v}_i = g_i, 1 \leq i \leq d. \quad (33)$$

$$\begin{aligned} \mathbf{P}(\wedge_i Y_n \cdot \mathbf{v}_i = g_i) &= p^{-d} \sum_{t_i \in \mathbb{F}_p} e_p(t_1(Y_n \cdot \mathbf{v}_1 - g_1) + \dots + t_d(Y_n \cdot \mathbf{v}_d - g_d)) \\ &= p^{-d} \sum_{t_i \in \mathbb{F}_p} \frac{1}{p} \sum_{t \in \mathbb{F}_p} e_p(t[t_1(Y_n \cdot \mathbf{v}_1 - g_1) + \dots + t_d(Y_n \cdot \mathbf{v}_d - g_d)]) \\ &= p^{-d} + p^{-d} \sum_{t_i \in \mathbb{F}_p, \text{ not all zero}} e_p(t_1(Y_n \cdot \mathbf{v}_1 - g_1) + \dots + t_d(Y_n \cdot \mathbf{v}_d - g_d)) \\ &= p^{-d} + p^{-d} \sum_{t_i \in \mathbb{F}_p, \text{ not all zero}} \frac{1}{p-1} \sum_{t \in \mathbb{F}_p, t \neq 0} e_p(t[Y_n \cdot \sum_i t_i \mathbf{v}_i - \sum_i t_i g_i]), \end{aligned}$$

Now as $\sum_i t_i \mathbf{v}_i$ is not very sparse for any non-trivial choice of (t_1, \dots, t_d) , by Corollary 4.6 we have

$$\left| \frac{1}{p} \sum_{t \in \mathbb{F}_p, t \neq 0} e_p(t[Y_n \cdot \sum_i t_i \mathbf{v}_i - \sum_i t_i g_i]) \right| \leq \exp(-cm/p^2).$$

Thus we have

$$|\mathbf{P}(\wedge_i Y_n \cdot \mathbf{v}_i = g_i) - p^{-d}| \leq \frac{p}{p-1} \exp(-cm/p^2).$$

□

Notice that in the above proof, with $Z_n = X_n - \alpha \mathbf{e}_n$, then the event $Z_n \cdot \mathbf{v} = 0$ can be written as

$$\mathbf{P}(Z_n \cdot \mathbf{v} = 0) = \frac{1}{q} \sum_{t \in \mathbb{F}_q} e_p(\text{tr}(t Z_n \cdot \mathbf{v})) = \frac{1}{q} + \frac{1}{q} \sum_{t \in \mathbb{F}_q, t \neq 0} e_p(\text{tr}(t Z_n \cdot \mathbf{v})),$$

where $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ is the field trace. We just showed that

$$\left| \mathbf{P}(Z_n \cdot \mathbf{v} = 0) - \frac{1}{q} \right| = \left| \frac{1}{q} \sum_{t \in \mathbb{F}_q, t \neq 0} e_p(\text{tr}(t Z_n \cdot \mathbf{v})) \right| \leq \exp(-cm/p^2). \quad (34)$$

In the same way, we show the following more general version of Theorem 9.1.

Theorem 9.5. *On the event of Lemma 9.3, as long as $k = o(n)$ we have*

$$|\mathbf{P}_{X_{n-k+1}}(X_{n-k+1} - \alpha \mathbf{e}_{n-k+1} \in W_{n-k} | \text{rank}(W_{n-k}) = n - k) - 1/p^{dk}| \leq \exp(-cm/p^2).$$

In particular,

$$|\mathbf{P}(\mathcal{E}_k) - \frac{1}{p^{dk}}| \leq \exp(-cm/p^2).$$

Proof. (of Theorem 9.5) Notice that the event $Z_{n-k+1} = X_{n-k+1} - \alpha \mathbf{e}_{n-k+1} \in W_{n-k}$ is equivalent with the event that this vector is orthogonal to the (orthogonal basis) $\mathbf{w}_1, \dots, \mathbf{w}_k$ of W_{n-k}^\perp in \mathbb{F}_q^n . We have

$$\begin{aligned} \mathbf{P}(\wedge_{i=1}^k Z_{n-k+1} \cdot \mathbf{w}_i = 0) &= q^{-k} \sum_{t_i \in \mathbb{F}_q} e_p(\text{tr}(t_1(Z_{n-k+1} \cdot \mathbf{w}_1)) + \dots + \text{tr}(t_k(Z_{n-k+1} \cdot \mathbf{w}_k))) \\ &= q^{-k} + q^{-k} \sum_{t_i \in \mathbb{F}_q, \text{ not all zero}} e_p(\text{tr}(Z_{n-k+1} \cdot \sum_i t_i \mathbf{w}_i)) \\ &= q^{-k} + q^{-k} \sum_{t_i \in \mathbb{F}_q, \text{ not all zero}} \frac{1}{q-1} \sum_{t \in \mathbb{F}_q, t \neq 0} e_p(\text{tr}(t Z_{n-k+1} \cdot \sum_i t_i \mathbf{w}_i)). \end{aligned} \quad (35)$$

Now observe that $\mathbf{v} = \sum_i t_i \mathbf{w}_i$ is a non-zero vector that is orthogonal to the first n' columns of $M_n - \alpha$. By Lemma 9.3 and by the proof of Theorem 9.4 (via Equation (34)) we have

$$\left| \frac{1}{q} \sum_{t \in \mathbb{F}_q, t \neq 0} e_p(\text{tr}(t Z_{n-k+1} \cdot \sum_i t_i \mathbf{w}_i)) \right| = \left| \frac{1}{q} \sum_{t \in \mathbb{F}_q, t \neq 0} e_p(\text{tr}(t Z_{n-k+1} \cdot \mathbf{v})) \right| \leq \exp(-cm/p^2).$$

Plugging this bound into Equation (35) for each non-zero tuple (t_1, \dots, t_d) we complete the proof. \square

For the rest of this section we will be focusing on Lemma 9.2. The proof of Lemma 9.3 can be done similarly. Indeed, assume that $\mathbf{w}_i = \sum_{k=0}^{d-1} \alpha^k \mathbf{v}_{ik}$ with $\mathbf{v}_{ik} \in \mathbb{F}_p^n$, then $\alpha_i \mathbf{w}_i$ can be expressed as $\sum_{k=0}^{d-1} \alpha^k \alpha_{ik} \mathbf{v}_{ik}$ for some $\alpha_{ik} \in \mathbb{F}_p$, one of which is non-zero if α_i is non-zero. Hence if $\sum_i \alpha_i \mathbf{w}_i = \sum_{k=0}^{d-1} \alpha^k (\sum_i \alpha_{ik} \mathbf{v}_{ik})$ is m -sparse in \mathbb{F}_q , then $\sum_i \alpha_{ik} \mathbf{v}_{ik}$ are m -sparse for any $0 \leq k \leq d-1$. Choose one index k where α_k is non-zero, and hence not all α_{ik} are zero.

In what follows we prove the key lemmas on non-sparsity. We will mainly focus on Lemma 9.2 because the proof for Lemma 9.3 is almost identical as long as $n' = (1 - o(1))n$.

9.6. Proof of Lemma 9.2. Let us assume that $\sum_i c_i \mathbf{v}_i$ is an m -sparse vector. We first note that by a proper ‘‘rotation’’, we can assume that this vector is \mathbf{v}_1 . This can be seen by, where \mathbf{v} and \mathbf{u}_i are as before,

$$\left(\sum_{i=0}^{d-1} c_i \alpha^i \right) \mathbf{v} = \left(\sum_{i=0}^{d-1} c_i \alpha^i \right) \sum_{i=0}^{d-1} \alpha^i \mathbf{v}_i = \sum_{i=0}^{d-1} \alpha^i \sum_{j=0}^{d-1} c_j \mathbf{u}_{i-j}.$$

By iterating (32) we have (with $\mathbf{g} = X$ and Q from (36), and t_i are deterministic, being determined by f_i from (32))

$$Q^d \mathbf{v}_1 + \sum_{j=0}^{d-1} t_j Q^j \mathbf{g} = \mathbf{v}_1. \quad (36)$$

Our goal is that, assuming that \mathbf{v}_1 is m -sparse, then conditioning on a realization of $\binom{n}{m} p^m = \exp(o(n))$ possible values of \mathbf{v}_1 , we show that the probability $\mathbf{P}(Q^d \mathbf{v}_1 + \sum_{j=0}^{d-1} t_j Q^j \mathbf{g} = \mathbf{v}_1)$ is very small, so that after taking union bound the probability is still negligible (where we will use the assumption that $p \leq n^{1/2-\varepsilon}$ and $m \leq n^{1-2\varepsilon}$).

We will estimate $\mathbf{P}(Q^d \mathbf{v}_1 + \sum_{j=0}^{d-1} t_j Q^j \mathbf{g} = \mathbf{v}_1)$ by a decoupling process, which roughly speaking allows us to pass from polynomials of Q to multilinear forms where the factors are sparser matrices than Q , but they are independent, and so that we can control the probability easier. This process, roughly speaking, can be described as follows: assume that M_i is a matrix obtained from Q by replacing all entries by zero, except the i -th block of rows (in general we decompose the rows of Q into 2^d groups, each with consecutive indices of size approximately $(n-1)/2^d$, and our matrices are formed by rows within a group). Then we can write

$$M_i = M_{i1} + M_{i2},$$

where M_{i1} and M_{i2} are submatrices obtained from M_i by dividing the i -th block of rows into two groups of (almost) equal size.

In general, in each step of our process, we decrease the polynomial degrees of a given matrix (the total degree remains the same), but double the number of matrices, and hence the probability. We will rely on the following well-known decoupling result (see for instance [7, 41]).

Claim 9.7. *Let X, Y be two random vectors in \mathbb{R}^k and \mathbb{R}^l , and let $f : \mathbb{R}^{k+l} \rightarrow \mathbb{R}$ be a function. Then for any a we have*

$$\begin{aligned} \mathbf{P}_{X,Y}(f(X,Y) = a)^4 &\leq (\mathbf{P}_{X,Y,Y'}(f(X,Y) - f(X,Y') = 0))^2 \\ &\leq \mathbf{P}_{X,X',Y,Y'}(f(X,Y) - f(X,Y') - f(X',Y) - f(X',Y') = 0), \end{aligned}$$

where X' is an independent copy of X , and Y' is an independent copy of Y .

In our application below X, Y, X', Y' , etc will be matrices. Now we describe the process in more details.

- We start by decomposing $Q = M_1 + M_2$ in (36). Factoring out, we will obtain a sum of many products of M_1 and M_2 . In the next step we will be using Claim 9.7 to remove M_1^d and M_2^d (i.e. the highest degree polynomial of M_1 and M_2) accordingly.
- In general, assume that we have $XZ_1XZ_2 \dots Z_kX$, where Z_i are products of matrices that do not contain X (it is possible that Z_i is just the identity matrix), and X appears k times; we then decompose $X = X' + X''$ into block matrices, expanding the products we obtain

$$(X' + X'')Z_1(X' + X'')Z_2 \dots Z_k(X' + X'') = X'Z_1X'Z_2 \dots Z_kX' + X''Z_1X''Z_2 \dots Z_kX'' + R,$$

where in R the total number of appearances of X' and X'' are at most $k-1$. We then keep X' , decouple X'' by another independent matrix Y'' of the same distribution to remove $X'Z_1X''Z_2 \dots Z_kX''$, and then keep X'' and Y'' , decouple X' by another independent matrix Y' of the same distribution to remove $X''Z_1X''Z_2 \dots Z_kX'' - Y''Z_1X''Z_2 \dots Z_kY''$. More precisely, by Claim 9.7 (with $\{\mathbf{z}_1, \mathbf{z}_2\} = \{\mathbf{f}, \mathbf{v}_1\}$)

$$\begin{aligned} &\mathbf{P}_{X',X'',\dots} \left(A(X', X'')_{\mathbf{z}_1} + (X' + X'')Z_1(X' + X'')Z_2 \dots Z_k(X' + X'')_{\mathbf{z}_2} = 0 \right)^4 \\ &= \mathbf{P}_{X',X'',\dots} \left(A(X', X'')_{\mathbf{z}_1} + (X'Z_1X'Z_2 \dots Z_kX' + X''Z_1X''Z_2 \dots Z_kX'' + R(X', X''))_{\mathbf{z}_2} = 0 \right)^4 \\ &\leq \mathbf{P}_{X',X'',Y'' \dots} \left([A(X', X'') - A(X', Y'')]_{\mathbf{z}_1} + (X''Z_1 \dots Z_kX'' - Y''Z_1 \dots Z_kY'' + R(X', X'') - R(X', Y''))_{\mathbf{z}_2} = 0 \right)^2 \\ &\leq \mathbf{P}_{X',Y',X'',Y'' \dots} \left([A(X', X'') - A(X', Y'') - A(Y', X'') + A(Y', Y'')]_{\mathbf{z}_1} \right. \\ &\quad \left. + (R(X', X'') - R(X', Y'') - R(Y', X'') + R(Y', Y''))_{\mathbf{z}_2} = 0 \right). \end{aligned}$$

It is crucial to note that by doing so, if the highest degree of X (which was decomposed into $X' + X''$) was also k , then the products having k factors of X' (and also Y', X'', Y'') are canceled out in $A(X', X'') - A(X', Y'') - A(Y', X'') + A(Y', Y'')$.

- In summary, after each round of the decoupling process, we will not create higher polynomials elsewhere but replace X which appears k times in the product form by four matrices X', X'', Y', Y'' which appear at most $k-1$ times. Hence, after 4^d steps of iterating the process, we will create a sum of many multilinear forms in which each matrix factor appears at most once. In other words they might have the form

$$\mathbf{P}(Q^d \mathbf{v}_1 + \sum_{j=0}^{d-1} t_j Q^j \mathbf{g} = \mathbf{v}_1)^{4^d} \leq \mathbf{P}((\sum_{\sigma} X_{\sigma(1)} X_{\sigma(2)} \dots X_{\sigma(d)} + R)_{\mathbf{z}_1} + S_{\mathbf{z}_2} = 0),$$

where R, S are also multilinear forms which might also contain X_1, \dots, X_d, \dots but the total degrees are smaller than d .

Notice that in the matrix X_i there are approximately $n/4^d$ non-zero rows.

Proof. (of Theorem 9.4) We have seen that

$$\mathbf{P}\left(Q^d \mathbf{v}_1 + \sum_{j=0}^{d-1} t_j Q^j \mathbf{g} = \mathbf{v}_1\right)^{4^d} \leq \mathbf{P}\left((X_1 X_2 \dots X_d \mathbf{v}_1 + R \mathbf{v}_1 + S \mathbf{g} = 0)\right). \quad (37)$$

Set

$$n' = n/4^d.$$

A simplified case. In order to motivate our next step, let us assume for now that our RHS (37) has only the term $X_1 \dots X_d$, that we are estimating the probability that $\mathbf{P}((X_1 X_2 \dots X_d \mathbf{v}_1 = 0))$.

Let $1 \leq m_0 \leq m$ be fixed. We will assume \mathbf{v}_1 to have exactly m_0 non-zero entries (noting that taking union bound over m_0 will not significantly change our bounds), then by the fact that $\sup_a \mathbf{P}(\sum_{i=1}^m \xi_i x_i = a) \leq 1 - c$ for some absolute constant c and by the fact that X_d has $C_d n$ iid row vectors (where $C_d \approx 1/4d$) we have that

$$\mathbf{P}(X_d \mathbf{v}_1 \text{ has at least } C_d n \text{ non-zero entries}) \geq 1 - c^{C_d n}. \quad (38)$$

In the next step, conditioning on this event of X_d , we consider the vector $X_{d-1}(X_d \mathbf{v}_1)$ and apply the following fact (by relying on Theorem 4.1)

Claim 9.8. *Assume that \mathbf{w} is not $C_d n$ -sparse, and X is a random matrix with n' iid rows as in M . Then for sufficiently large p , and for $p \lesssim \sqrt{n}$*

$$\mathbf{P}(X \mathbf{w} \text{ is } n'/3\text{-sparse}) \leq p^{-n'/2}.$$

Proof. Note that if \mathbf{w} is not $C_d n$ -sparse then by Theorem 4.1

$$\sup_{f_i \in \mathbb{F}_p} \mathbf{P}\left(\sum_i x_i w_i = f_i\right) \leq 1/p + 1/\sqrt{C_d n} \lesssim 1/p. \quad (39)$$

As such, as p is sufficiently large the probability under consideration is bounded by

$$(C/p)^{(1-1/3)n'} \binom{n'}{n'/3} \leq (C/p)^{n'/2},$$

where we take a union bound over all possible positions for the zero coordinates of $X \mathbf{w}$. □

We remark that the above might continue to hold for small p , but we will not be focusing on this case for simplicity.

We next iterate Claim 9.8, by taking union bound and with an assumption that $m \lesssim_d \sqrt{n}$ we obtain a bound

$$p^m (2/p)^{c'_d n} \leq (1/p)^{c'_d n}$$

for the event that $X_1 \dots X_d \mathbf{v}_1 = 0$ (or $X_1 \dots X_d \mathbf{v}_1$ is m -sparse).

General case. First let us record here a slightly more general variant of Claim 9.8. We say that a random vector \mathbf{w} is m -free if all but at most m coordinates of \mathbf{w} are determined. So for instance m -sparse vectors are m -free because all but at most m coordinates of \mathbf{w} are zero. By an identical proof to Claim 9.8, we have

Claim 9.9. *Assume that \mathbf{w} is not $C_d n$ -free, and X is a random matrix with n' iid rows as in M . Then for sufficiently large p , and for $p \lesssim \sqrt{n}$*

$$\mathbf{P}(X \mathbf{w} \text{ is } n'/3\text{-free}) \leq p^{-n'/2}.$$

To continue, recall that we would like to estimate $\mathbf{P}(\sum_{\sigma} X_{\sigma(1)} X_{\sigma(2)} \dots X_{\sigma(d)} + R) \mathbf{z}_1 + S \mathbf{z}_2 = 0$, and here we cannot expose X_d , and then X_{d-1} , etc one by one in order as in the simplified case above because X_i might not appear exactly in the i -th position of each multilinear forms. However we can adjust the process using the following observation.

Fact 9.10. *For any i , and for any vector \mathbf{u} , the vector $X_i \mathbf{u}$ of \mathbb{R}^n have non-zero entries only in the i -th block. In particular, if a vector $\sum_i X_i \mathbf{u}_i$ is n' -sparse, then $X_1 \mathbf{u}_1$ is also n' -sparse.*

Now we describe the method. First, basing on Fact 9.10 we just need to address all the multilinear forms beginning with X_1 . The vector obtained by summing over these forms is of type $X_1(\sum_{i=2}^d a_i X_i R_i \mathbf{w}_i)$. To estimate the probability that this vector is not m -free, we will focus only on the submatrix restricted by the columns of X_1 having the same index as the rows of X_2 , and condition on the remaining entries of X_1 . Only using the randomness from this submatrix X'_1 of X_1 , it suffices to show that $(X'_1 + F)(X_2 R_2 \mathbf{v})$ is not n' -free with high probability. To show this, assume that we already know that $X_2 R_2 \mathbf{v}$ is non-sparse, we then can use (39) (i.e. Claim 9.9), where f_i is allowed to depend on F . Now to show that $X_2 R_2 \mathbf{v}$ is not n' -free with high probability (where the randomness is on X_2, \dots, X_d), where R_2 is a sum of multilinear forms without X_1 and X_2 , we again focus on the submatrix X'_2 of X_2 restricted by the columns having the same indices as that of X_3 , and continue forward. So in the last step of our argument (or the first step if we go backward as in the simplified case above), we just need to show that $X_d \mathbf{v}_1$ is not n' -free with high probability with respect to the randomness of X_d and for some appropriate number $n' = \Theta_d(n)$, but this was exactly (38). \square

10. PROOF OF THEOREM 1.8

We are going to prove the following result.

Proposition 10.1 (asymptotically independence). *Let $d \geq 1$ be fixed. Then for any distinct numbers a_1, \dots, a_d in \mathbb{F}_p ,*

$$\mathbf{P}(\mathcal{E}_{a_d} \wedge \dots \wedge \mathcal{E}_{a_1}) = \frac{1}{p^d} + \exp(-c_d n/p^2),$$

where \mathcal{E}_a is the event that a is an eigenvalue of M .

Proof. (of Theorem 1.8) Let $X_{n,p}$ denote the random variable

$$X_{n,p} = \sum_{a \in \mathbb{F}_p} 1_{\mathcal{E}_a}.$$

By Proposition 10.1, one easily has $\mathbf{E}X_{n,p} = 1 + p \times \exp(-c_1 n/p^2) = 1 + o(1)$, and more generally for any fixed integer $d \geq 1$

$$\lim_{n \rightarrow \infty} \mathbf{E}X_{n,p}^d = \mathbf{E}X^d,$$

where $X \sim \text{Pois}(1)$. It thus follows that $X_{n,p}$ is asymptotically distributed as $\text{Pois}(1)$. In particular

$$\lim_{n,p \rightarrow \infty} \mathbf{P}(X_{n,p} = 0) = \mathbf{P}(X = 0) = e^{-1}.$$

\square

It remains to justify the above independence lemma.

10.2. Proof of Proposition 10.1. The event $\wedge \mathcal{E}_{a_i}$ is equivalent to the event that there exist $\mathbf{v}_i, 1 \leq i \leq d$ such that

$$M \mathbf{v}_1 = a_1 \mathbf{v}_1 \wedge \dots \wedge M \mathbf{v}_d = a_d \mathbf{v}_d.$$

We condition on $M_{[n] \times [n-1]}$. Let \mathbf{u}_i be a normal vector of $M_{[n] \times [n-1]} - a_i$. The event $\wedge \mathcal{E}_{a_i}$ then implies that

$$(X_n - a_i \mathbf{e}_n) \cdot \mathbf{u}_i = 0, 1 \leq i \leq d. \tag{40}$$

We are going to show that the probability of this event with the randomness on X_n is $\frac{1}{p^d}$ modulo a small error term for almost all realization of $M_{[n] \times [n-1]}$. To be more precise, we will restrict on the following event of probability close to 1.

Lemma 10.3. *Let c_d be a sufficiently small constant to be chosen later. With probability at least $1 - O(\exp(-\Theta(n)))$ with respect to $M_{[n] \times [n-1]}$, none of the vectors $\sum_u \beta_i \mathbf{u}_i$ for all $\beta_i \in \mathbb{F}_p$, not all zero, is $c_d n$ -sparse.*

Assuming this for now we can conclude our main result.

Proof. (of Proposition 10.1) Conditioning on the event consider in Lemma 10.3, we can then just follow the proof of Theorem 9.4 applied to the events in (40). More precisely, the estimates following Equation (33) hold with $g_i = a_i \mathbf{e}_n \cdot \mathbf{u}_i$ for $1 \leq i \leq d$. \square

10.4. Proof of Lemma 10.3. Set $m = c_d n$, for sufficiently small c_d . By taking union bound (with a loss of a multiplicative factor p^d in probability), it suffices to consider the probability that $\mathbf{w} = \sum_u \beta_i \mathbf{u}_i$ is m -sparse for a fixed choice of β_1, \dots, β_d .

Lemma 10.5. *With probability at least $1 - O(\exp(-\Theta(n)))$, \mathbf{w} cannot be m -sparse.*

As in the previous section, let Q denote the matrix $M_{[n-1] \times [n-1]}^T$. Our result says that the vectors \mathbf{w} can be viewed as null vector of a polynomial of degree d of Q . More specifically, let X be the last row of $M_{[n] \times [n-1]}$.

Claim 10.6. *There exist coefficients α_i and α'_i such that*

$$\sum_{i=0}^d \alpha_i Q^i \mathbf{w} + \sum_{i=0}^{d-1} \alpha'_i Q^i X = 0.$$

It is clear that, by using this claim, we can complete the proof of Lemma 10.3 by following exactly the decoupling process in the proof of Theorem 9.4 in the previous section (which in turns yield the bound $1 - \exp(-\Theta(n))$, obtained at the last step of the process). This bound is clearly strong enough to absorb all union bounds of type $p^{O(d)}$ given the range of p . It thus remains to justify the result above.

Proof. (of Claim 10.6) By fixing $f_i = u_{in}$ (and hence we lose another multiplicative factor of p^d in probability), and \mathbf{w}_i is the concatenation of \mathbf{u}_i , by $(M - a_i) \mathbf{u}_i = 0$ we have

$$(Q - a_i) \mathbf{w}_i = f_i X.$$

As such

$$(Q - a_1) \sum_i \beta_i \mathbf{w}_i = \beta_1 f_1 X + \sum_{i \geq 2} \beta_i f_i X + \sum_{i \geq 2} \beta_i (\alpha_i - \alpha_1) \mathbf{w}_i.$$

In other words, under the action by $Q - a_1$, we eliminate \mathbf{w}_1 (or we changed it to a deterministic vector). Iterating the process, we then obtain that

$$\sum_{i=0}^d \alpha_i Q^i \mathbf{w} + \sum_{i=0}^{d-1} \alpha'_i Q^i X = 0,$$

where $\alpha_d \neq 0$, α_i, α'_i depend on $\beta_1, \dots, \beta_d, a_1, \dots, a_d$ and X . \square

11. REMARKS

First, among the three characterizations provided, Theorem 3.1 was less effective in our current applications because of the polynomial restriction, but this result is expected to have other implications beyond random matrix theory because of its near optimality. The remaining two characterizations, Theorem 4.4 and Theorem 5.1, yield sub-exponential bounds in application. The later is more amenable to perturbations (that we don't have to assume $\|M\|_2 = O(\sqrt{n})$).

Second, we remark that the error bounds in Theorem 9.1 and in Proposition 10.1 are of the form $\exp(-n^{1-o(1)}/p^2)$, which were obtained by applying Corollary 4.6. Compared to the justification for the uniform model in Section 2, our approach seems to be natural and does explain the main terms in Theorem 1.7 (obtained from Theorem 9.1 and Theorem 9.5) and in Theorem 1.8 (obtained from Proposition 10.1). Following our treatment of Section 7, it is natural to expect that these error bounds can be made $\exp(-n^c)$, but for this improvement one has to show that the vectors \mathbf{v}_1 in (36) or \mathbf{w} in Claim 10.6 to have large ULCD or large R_k , but this task seems to be extremely challenging.

Universality is an extremely complicated phenomenon. While we have addressed only a few universal examples for random matrices in (prime) fields in the current note, there remains so many interesting and tantalizing questions. Beside the obvious (and doable) direction of extending the current results to general finite fields \mathbb{F}_q , we conjecture that the following statistics of the uniform model are universal in terms of iid random matrix model:

- the distributions of $\lambda_{\phi_1}, \dots, \lambda_{\phi_k}$ are asymptotically independent for different irreducible polynomials ϕ_1, \dots, ϕ_k (which would then generalize (5));
- the results of Stong and of Hansen and Schmutz [19] connecting the distribution of degrees of irreducible factors of the characteristic polynomial to the cycle lengths of a random permutation.

Lastly, we conjecture that for a fixed random matrix model (such as the Bernoulli $(0, 1)$ or $(-1, 1)$ model), the considered statistics over \mathbb{F}_p for different primes p are asymptotically independent.

Acknowledgements. The authors are thankful to J. Koenig for helpful comments. The first author is supported in part by the National Science Foundation postdoctoral fellowship DMS-1702533. The last two authors are partially supported by National Science Foundation grants DMS-1600782 and CAREER DMS-1752345.

APPENDIX A. TENSORIZATION LEMMA

The following is an analog of [32, Lemma 2.2].

Lemma A.1. *Let $K, \delta_0 \geq 0$ be given. Assume that ξ_1, \dots, ξ_n are iid real-valued random variable and that $\mathbf{P}(\|\xi_i\|_{\mathbb{R}/\mathbb{Z}} < \delta) \leq K\delta$ for all $\delta \geq \delta_0$. Then*

$$\mathbf{P}(\|\xi_1\|_{\mathbb{R}/\mathbb{Z}}^2 + \dots + \|\xi_n\|_{\mathbb{R}/\mathbb{Z}}^2 < \delta n) \leq (C_0 K \delta)^n,$$

where C_0 is absolute.

Proof. Assume that $\delta \geq \delta_0$. By Chebyshev's inequality

$$\mathbf{P}(\|\xi_1\|_{\mathbb{R}/\mathbb{Z}}^2 + \dots + \|\xi_n\|_{\mathbb{R}/\mathbb{Z}}^2 \leq \delta n) \leq \mathbf{E} \exp(n - \sum_{i=1}^n \|\xi_i\|_{\mathbb{R}/\mathbb{Z}}^2 / \delta) = \exp(n) \prod_{i=1}^n \mathbf{E} \exp(-\|\xi_i\|_{\mathbb{R}/\mathbb{Z}}^2 / \delta).$$

On the other hand,

$$\mathbf{E} \exp(-\|\xi_i\|_{\mathbb{R}/\mathbb{Z}}^2 / \delta) = \int_0^1 \mathbf{P}(\exp(-\|\xi_i\|_{\mathbb{R}/\mathbb{Z}}^2 / \delta) > s) ds = \int_0^\infty 2u \exp(-u^2) \mathbf{P}(\|\xi_i\|_{\mathbb{R}/\mathbb{Z}} < \delta u) du.$$

For $0 \leq u \leq 1$ we use $\mathbf{P}(\|\xi_i\|_{\mathbb{R}/\mathbb{Z}} \leq \delta u) \leq \mathbf{P}(\|\xi_i\|_{\mathbb{R}/\mathbb{Z}} \leq \delta) \leq K\delta$, while for $u \geq 1$ we have $\mathbf{P}(\|\xi_i\|_{\mathbb{R}/\mathbb{Z}} \leq \delta u) \leq K\delta u$. Thus

$$\mathbf{E} \exp(-\|\xi_i\|_{\mathbb{R}/\mathbb{Z}}^2/\delta) = \int_0^1 2u \exp(-u^2)K\delta du + \int_1^\infty 2u \exp(-u^2)K\delta u du \leq C_0K\delta,$$

as desired. □

REFERENCES

- [1] G. V. Balakin, The distribution of the rank of random matrices over a finite field (Russian, with English summary), *Teor. Veroyatn. Primen.* 13 (1968), 631-641.
- [2] J. Blomer, R. Karp, and E. Welzl, The rank of sparse random matrices over finite fields, *Random Structures Algorithms* 10 (1997), no. 4, 407-419.
- [3] R. P. Brent and B. D. McKay, Determinants and ranks of random matrices over \mathbb{Z}_m , *Discrete Math.* 66 (1987), no. 1-2, 35-49.
- [4] J. Bourgain, V. Vu and P. M. Wood, On the singularity probability of discrete random matrices, *Journal of Functional Analysis* 258 (2010), no.2, 559-603.
- [5] J. Clancy, T. Leake, N. Kaplan, S. Payne, and M. M. Wood. On a Cohen-Lenstra heuristic for Jacobians of random graphs, *Journal of Algebraic Combinatorics* 42 (2015), no. 3, 701-723.
- [6] C. Cooper, On the rank of random matrices, *Random Structures Algorithms* 16 (2000), no. 2, 209-232.
- [7] K. Costello, T. Tao, V. Vu, Random symmetric matrices are almost surely non-singular, *Duke Math. J.* 135 (2006), 395-413.
- [8] A. Ferber, V. Jain, K. Luh and W. Samotij, On the counting problem in inverse Littlewood–Offord theory, arxiv.org/abs/1904.10425.
- [9] J. Kahn, J. Komlós and E. Szemerédi, On the probability that a random ± 1 matrix is singular, *J. Amer. Math. Soc.* 8 (1995), 223-240.
- [10] J. Kahn and J. Komlós, Singularity probabilities for random matrices over finite fields. *Combin. Probab. Comput.*, 10(2):137-157, 2001.
- [11] M. V. Kozlov, On the rank of matrices with random Boolean elements, *Sov. Math. Dokl.* 7 (1966), 1048-1051.
- [12] L. S. Charlap, H. D. Rees, and D. P. Robbins, The asymptotic probability that a random biased matrix is invertible, *Discrete Math.* 82 (1990), no. 2, 153-163.
- [13] N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent. *Illinois J. Math.* 2 (1958).
- [14] E. Friedman and L. C. Washington. On the distribution of divisor class groups of curves over a finite field. In *Theorie des nombres* (Quebec, PQ, 1987), pages 227-239. de Gruyter, Berlin, 1989.
- [15] J. Fulman, Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms and cycle indices, Ph.D. Thesis, Harvard University, 1997.
- [16] J. Fulman, Random matrix theory over finite fields, *Bull. Amer. Math. Soc.* 39 (2002), 51-85.
- [17] J. Fulman and L. Goldstein, Stein’s method and the rank distribution of random matrices over finite fields, *Ann. Probab.* Volume 43, Number 3 (2015), 1274-1314.
- [18] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, *Period. Math. Hungar.* 8 (1977), no. 3-4, 197-211.
- [19] J. Hansen and E. Schmutz, How random is the characteristic polynomial of a random matrix?, *Math. Proc. Cambridge Philos. Soc.* 114 (1993), 507-515.
- [20] I. N. Kovalenko and A. A. Levitskaya, Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring (Russian), *Dokl. Akad. Nauk SSSR* 221 (1975), no. 4, 778-781.
- [21] I. N. Kovalenko, A. A. Levitskaya, and M. N. Savchuk, *Izbrannyye zadachi veroyatnostnoi kombinatoriki* (Russian), Naukova Dumka, Kiev, 1986.
- [22] J. Kung, The cycle structure of a linear transformation over a finite field, *Lin. Alg. Appl.* 36 (1981), 141-155.
- [23] K. Maples, Singularity of Random Matrices over Finite Fields, preprint, arxiv.org/abs/1012.2372.
- [24] K. Maples, Cokernels of random matrices satisfy the Cohen-Lenstra heuristics, preprint, arxiv.org/abs/1301.1239.
- [25] P.M. Neumann and C.E. Praeger, Derangements and eigenvalue-free elements in finite classical groups, *J. London Math. Soc.* (2) 58 (1998), 562-586.
- [26] P.M. Neumann and C.E. Praeger, Cyclic matrices in classical groups over finite fields, *J. Algebra* 234 (2000), 367-418.

- [27] H. Nguyen and E. Paquette, Surjectivity of near square matrices, submitted, accepted to *Combinatorics, Probability and Computing*, arxiv.org/abs/1802.00001.
- [28] H. Nguyen and V. Vu, Optimal inverse Littlewood-Offord theorems, *Advances in Mathematics*, Vol. 226 6 (2011), 5298-5319.
- [29] H. Nguyen and V. Vu, Normal vector of a random hyperplane, *International Mathematics Research Notices*, (2018) Issue 6, 1754-1778.
- [30] H. Nguyen and M. M. Wood, Random integral matrices: universality of surjectivity and the cokernel, submitted.
- [31] H. Nguyen and M. M. Wood, Cyclicity and rank evolution in random symmetric and alternating matrices, in preparation.
- [32] M. Rudelson and R. Vershynin, The Littlewood-Offord problem and invertibility of random matrices, *Advances in Mathematics* 218 (2008), 600-633.
- [33] M. Rudelson and R. Vershynin, Smallest singular value of a random rectangular matrix, *Communications on Pure and Applied Mathematics* 62 (2009), 1707-1739.
- [34] R. Stanley, Smith normal form in Combinatorics, *Journal of Combinatorial Theory, Series A* Volume 144, November 2016, Pages 476-495.
- [35] R. Stanley and Y. Wang, The Smith normal form distribution of a random integer matrix, *SIAM J. Discrete Math.*, 31 (3), 2017, 2247-2268.
- [36] R. Stong, Some asymptotic results on finite vector spaces, *Adv. Appl. Math.* 9 (1988), 167-199.
- [37] T. Tao and V. Vu, *Additive combinatorics*, Volume 105, Cambridge University Press, Cambridge, 2006.
- [38] T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, *Journal of the A. M. S* 20 (2007), 603-673.
- [39] T. Tao and V. Vu, John-type theorems for generalized arithmetic progressions and iterated sumsets, *Adv. Math.* 219 (2008), no. 2, 428-449.
- [40] T. Tao and V. Vu, Inverse Littlewood-Offord theorems and the condition number of random matrices, *Annals of Mathematics* (2) 169 (2009), no 2, 595-632.
- [41] R. Vershynin, Invertibility of symmetric random matrices, *Random Structures and Algorithms* 44 (2014), 135-182.
- [42] M. M. Wood, The distribution of sandpile groups of random graphs, *Journal of the A. M. S*, 30 (2017), pp. 915-958.
- [43] M. M. Wood, Random integral matrices and the Cohen-Lenstra Heuristics, *American Journal of Mathematics*, arxiv.org/abs/1504.04391.

CENTER OF MATHEMATICAL SCIENCES AND APPLICATIONS, HARVARD UNIVERSITY, 20 GARDEN ST., CAMBRIDGE, MA 02138 USA

Email address: kluh@cmsa.fas.harvard.edu

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, 231 W 18TH AVE, COLUMBUS, OH 43210 USA

Email address: meehan.73@buckeyemail.osu.edu

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, 231 W 18TH AVE, COLUMBUS, OH 43210 USA

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