Combinatorics, Probability and Computing (2020), **29**, pp. 267–292
doi:10.1017/S0963548319000348

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Surjectivity of near-square random matrices

Hoi. H. Nguyen*,† and Elliot Paquette

Department of Mathematics, The Ohio State University, 231 West 18th Avenue, Columbus, OH 43210, USA
*Corresponding author. Email: nguyen.1261@math.osu.edu

(Received 30 January 2018; revised 30 July 2019; first published online 6 November 2019)

Abstract

We show that a nearly square independent and identically distributed random integral matrix is surjective over the integral lattice with very high probability. This answers a question by Koplewitz [6]. Our result extends to sparse matrices as well as to matrices of dependent entries.

2010 MSC Codes: Primary 15B52; Secondary 20G40

1. Introduction

In this paper we study random rectangular matrices $M_{n\times(n+u)} = (M_{ij})$ of size $n \times (n+u)$, where $n \to \infty$ and $u \geqslant 0$, and the entries M_{ij} are independent and identically distributed (i.i.d.) copies of a random variable ξ taking integral values and such that, for any prime p,

$$\max_{x\in\mathbb{Z}/p\mathbb{Z}} \mathbb{P}(\xi = x) \leqslant 1 - \alpha_n, \tag{1.1}$$

where $\alpha_n > 0$ is a parameter allowed to depend on n. Such distributions are called α_n-*balanced*.

For random square matrices of random Bernoulli entries taking values 0 and 1 with probability 1/2, the problem of estimating the probability p_n of $M_{n\times n}$ being singular has attracted quite a lot of attention. In the early 1960s Komlós [5] showed $p_n = O(n^{-1/2})$. This bound was significantly improved by Kahn, Komlós and Szemerédi in the 1990s to $p_n \leqslant 0.999^n$. About ten years ago, Tao and Vu [16] improved the bound to $p_n \leqslant (3/4 + o(1))^n$. We also refer the reader to [13] by Rudelson and Vershynin for implicit bounds of type e^{-cn}. The most recent record is due to Bourgain, Vu and Wood [2], who show the following result.

Theorem 1.1.

$$p_n \leqslant \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

These results imply that with very high probability the linear map $M_{n\times n}$ is injective over $\mathbb{Z}^n$ (and hence the lattice $M_{n\times n}(\mathbb{Z}^n)$ has full rank in $\mathbb{Z}^n$). Another fundamental question of interest is the surjectivity onto $\mathbb{Z}^n$, more specifically:

Is it true that with high probability $M_{n\times n}$ is also surjective over $\mathbb{Z}^n$ (in other words, the quotient group $\mathbb{Z}^n/M_{n\times n}(\mathbb{Z}^n)$ is trivial)?

†The first author is supported by research grants DMS-1600782 and DMS-1752345.

© Cambridge University Press 2019

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Unfortunately, the answer to this question turns out to be negative: with high probability M is never surjective over $\mathbb{Z}^n$. To explain this at the heuristic level, assume that the vector $\mathbf{e}_1 = (1, 0, \dots, 0)$ is in the image space $M_{n\times n}(\mathbb{Z}^n)$, then (assuming that $M_{n\times n}$ is non-singular)

$$\mathbf{x} = M_{n\times n}^{-1}(\mathbf{e}_1) = ((M_{n\times n}^{-1})_{11}, \dots, (M_{n\times n}^{-1})_{1n})^T \in \mathbb{Z}^n.$$

However, we have

$$(M_{n\times n}^{-1})_{1i} = \frac{\det(M^{1i})}{\det(M_{n\times n})},$$

where M^{1i} is the matrix obtained from $M_{n\times n}$ by removing the first row and the ith column. By the co-factor expansion

$$\det(M_{n\times n}) = \sum_{i=1}^{n} (-1)^{i-1} M_{1i} \det(M^{1i}). \tag{1.2}$$

But as the M_{1i} are independent from the submatrices M^{1i}, $1 \leqslant i \leqslant n$, it is highly unlikely that the random sum $|\sum_{i=1}^{n} (-1)^{i-1} M_{1i} \det(M^{1i})|$ becomes smaller than all $|\det(M^{1i})|$ so that the components $(\det(M^{1i}))/(\det(M_{n\times n}))$ of $\mathbf{x}$ are all integral.

Having seen that $M_{n\times n} : \mathbb{Z}^n \to \mathbb{Z}^n$ is unlikely to be surjective, it is natural to think of rectangular matrices $M_{n\times(n+u)} : \mathbb{Z}^{n+u} \to \mathbb{Z}^n$ which might have a better chance of being surjective. In fact, in the past few years there have been exciting developments (see *e.g.* [7, 10, 18, 19]) in the study of $M_{n\times(n+u)}(\mathbb{Z}^{n+u})$ for various ensembles of $M_{n\times(n+u)}$. For instance, a special version of a recent result by Wood [19, Corollary 3.4] shows the following.

Theorem 1.2. *Let $u \geqslant 0$ be a fixed integer. Let $M_{n\times(n+u)}$ be a random matrix with entries being i.i.d. copies of an α_n-balanced random variable of fixed $\alpha_n > 0$. Let P be a finite set of primes, then*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{Coker}(M_{n\times(n+u)})_P \simeq \{\mathrm{id}\}) = \prod_{p\in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}),$$

where $G_P = \prod_{p\in P} G_p$ is the product of p-Sylow subgroups of G and the co-kernel $\operatorname{Coker}(M_{n\times m})$ *is the quotient group $\mathbb{Z}^n / M_{n\times m}(\mathbb{Z}^m)$.*

We remark that P is fixed and $n \to \infty$ in this result. However, as P increases, the probability on the right-hand side of the limit becomes arbitrarily small. Hence it follows that

$$\limsup_{n\to\infty} \mathbb{P}(\operatorname{Coker}(M_{n\times n}) \simeq \{\mathrm{id}\}) \leqslant \inf_P \lim_{n\to\infty} \mathbb{P}(\operatorname{Coker}(M_{n\times n})_P \simeq \{\mathrm{id}\}) = 0$$

which officially answers our question above.

In the opposite direction, the following has been conjectured by Koplewitz [6, 7].

Conjecture 1.1. *Let the matrix entries be i.i.d. copies of an α_n-balanced random variable of fixed $\alpha_n > 0$. Then, for any fixed constant $\varepsilon > 0$,*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{Coker}(M_{n\times\lfloor(1+\varepsilon)n\rfloor}) \simeq \{\mathrm{id}\}) = 1.$$

Also, with $u \to \infty$ together with n,

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{Coker}(M_{n\times(n+u)}) \simeq \{\mathrm{id}\}) = 1.$$

To support these conjectures, Koplewitz himself showed in [6, Theorem 1] (see also [7, Theorem 30]) that $\mathbb{P}(M_{n\times\lfloor(2+\varepsilon)n\rfloor} \simeq \{\mathrm{id}\}) \geqslant 1 - e^{-c_\varepsilon n}$. In the same paper he also confirmed

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Conjecture 1.1 for random matrices of entries distributed according to the Haar measure over the profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$.

In this paper we confirm the first conjecture. In fact we are able to extend the result to very sparse matrices. More specifically, we can assume ξ to take integer values as in (1.1) with

$$\alpha_n \geqslant \frac{C_0 \log n}{n} \tag{1.3}$$

for a sufficiently large constant C_0.

Theorem 1.3 (main result). *Let ξ be as in (1.3). Assume furthermore that ξ is bounded with probability one. Then, for every $A, \varepsilon_0 > 0$, there exist $B = B(A, C_0, \varepsilon_0)$ and an absolute constant c such that*

$$\mathbb{P}\left(\mathrm{Coker}\left(M_{n\times\left(n+\left\lfloor B\left(\frac{\log n}{\alpha_n}\log\left(\frac{\log n}{\alpha_n}\right)+\log n\right)\right\rfloor\right)}\right) \simeq \{\mathrm{id}\}\right) \geqslant 1 - O(n^{-A} + e^{-c\alpha_n n}).$$

In particular, if α_n is fixed then

$$\mathbb{P}(\ \mathrm{Coker}\ (M_{n\times\lfloor n+\log^{1+o(1)} n\rfloor}) \simeq \{\mathrm{id}\}) \geqslant 1 - O(n^{-\omega(1)}), \tag{1.4}$$

and if $\alpha_n \geqslant (\log^{O(1)} n)/n$ then

$$\mathbb{P}(\ \mathrm{Coker}\ (M_{n\times\lfloor(1+o(1))n\rfloor}) \simeq \{\mathrm{id}\}) \geqslant 1 - O(n^{-\omega(1)}). \tag{1.5}$$

Note that a balanced assumption on ξ is necessary as the results no longer hold, for instance, if we work with the Bernoulli ± 1 ensemble; in this case the matrix cannot be surjective modulo 2 for even n. Note also that by considering the $\{0, 1\}$ ensemble with $\alpha_n = \mathbb{P}(\xi = 1)$, we can see that roughly the stated number of additional columns is necessary up to multiplicative constants, just by considering rows that are identically 0.

We will also discuss an extension to a family of matrices of dependent entries; see Section 3. Our method is short and direct. We will first prove a slightly weaker version (Theorem 2.4) by relying on a totally elementary lemma by Odlyzko (Lemma 2.3). We then refine the method by using a more involved result by Maples from [8] (Theorem 2.7). However, as [8] appears to be slightly incomplete and contains several (minor) errors, we will take this opportunity to recast Maples' proof toward our sparsest settings. Along the way, we show that this approach also yields a completely new singularity bound for sparse integral matrices.

Theorem 1.4. *There exists an absolute constant $c > 0$ such that, as long as the entries of $M_{n\times n}$ are i.i.d. copies of ξ distributed as in (1.3) (which is not necessarily bounded), then*

$$p_n \leqslant e^{-c\alpha_n n}.$$

We note that the recent paper [1] by Basak and Rudelson addressed the singularity (and more generally the least singular value) for a general family of sparse matrices. Unfortunately, Theorem 1.4 does not seem to follow from [1] because we have no restriction on the spectral norm of $M_{n\times n}$.

2. Proof of Theorem 1.3

We assume that

$$\mathbb{P}(|\xi| \leqslant K_0) = 1$$

for some positive constant K_0. This assumption is only for Theorem 1.3 but not for Theorem 1.4.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

A natural approach is to show that the equation system

$$M_{n\times m}\mathbf{x} = \mathbf{e}_i,$$

has solutions $\mathbf{x} \in \mathbb{Z}^m$, for any standard unit vector $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$, $1 \leqslant i \leqslant n$. However, such an approach does not look simple, as we would have to prove cancellation of extremely large numbers involving determinants of minors (see also the discussion around (1.2)). Instead, we will prove surjectivity by reducing our matrices over finite fields via the following result.

Lemma 2.1 (Lemma 5 of [6]). *Let $m \geqslant n$. A matrix $M_{n\times m} : \mathbb{Z}^m \to \mathbb{Z}^n$ is surjective if and only if the modulo matrix $M_{n\times m}/p : \mathbf{F}_p^m \to \mathbf{F}_p^n$ is surjective for every prime p. Here $M_{n\times m}/p$ is the matrix over $\mathbf{F}_p$ given by $(M_{n\times m}/p)_{ij} = M_{ij} \pmod p$.*

Proof. Assume $M_{n\times m}/p : \mathbf{F}_p^m \to \mathbf{F}_p^n$ is surjective. Then $M_{n\times m}/p$ contains a submatrix $M'_{n\times n} = M'_{n\times n}(p)$ (depending on p) of size $n \times n$ such that $\det(M'_{n\times n}/p) \neq 0 \pmod p$. Thus $\det(M'_{n\times n}) \neq 0$. This implies that the columns of $M'_{n\times n}$ generate $\mathbb{Q}^n$, and hence $M'_{n\times n}(\mathbb{Z}^n)$ is a full-rank integer lattice, which therefore satisfies $|\det(M'_{n\times n})| = |\mathbb{Z}^n/M'_{n\times n}(\mathbb{Z}^n)|$. Moreover, the lattice co-volume $d = |\mathbb{Z}^n/M_{n\times m}(\mathbb{Z}^m)|$ divides $|\det(M'_{n\times n})|$ as $\mathbb{Z}^n/M_{n\times m}(\mathbb{Z}^m)$ is canonically isomorphic to a subgroup of $\mathbb{Z}^n/M'_{n\times n}(\mathbb{Z}^n)$. As p does not divide $|\det(M'_{n\times n})|$ and d does, it therefore follows that p does not divide d, as p is prime. As p is arbitrary, it follows that d has no prime divisors, so $d = 1$. □

By this lemma, for our problem we need to show that $M_{n\times m}/p : \mathbf{F}_p^m \to \mathbf{F}_p^n$ is surjective (or equivalently, $M_{n\times m}/p$ has rank n in $\mathbf{F}_p^n$) for *every* prime p. This does not seem to be an easier task, but in what follows we show that there is a way to restrict the treatment to a set of only a few primes.

Our first ingredient is the following simple bound (see [12, Lemma 3.9]).

Lemma 2.2 (quadratic estimate). *Let p be a prime. Let $0 < \varepsilon_n < 1$ be a given parameter that might depend on n. Let $M_{n\times n}$ be a matrix of size $n \times n$ whose entries are i.i.d. copies of a random variable ξ from (1.3). Then the probability that $M_{n\times n}$ has rank at most $(1 - \varepsilon_n)n$ in $\mathbf{F}_p^n$ is smaller than $e^{-\alpha_n \varepsilon_n^2 n^2 + n}$.*

To prove this result we rely on a useful result by Odlyzko [4].

Lemma 2.3. *Let H be a subspace of dimension $1 \leqslant d \leqslant n$ in $\mathbf{F}_p^n$. Then if X is a random vector whose entries are i.i.d. copies of a random variable ξ from (1.3), then*

$$\mathbb{P}(X \in H) \leqslant (1 - \alpha_n)^{n-d}.$$

We insert a proof of this well-known result here for completeness.

Proof of Lemma 2.3. Let $\{H_1, H_2, \dots, H_d\}$ be a basis for H. By permuting coordinates, we may assume without loss of generality that the restrictions $\tilde{H}_1, \tilde{H}_2, \dots, \tilde{H}_d$ of these vectors to the first d coordinates are again linearly independent. Consider the event

$$X = (\xi_1, \dots, \xi_d, \xi_{d+1}, \dots, \xi_n)^t \in H.$$

From the linear independence of $\{\tilde{H}_i\}_1^d$, there are unique $c_1, c_2, \dots, c_d \in \mathbf{F}_p$ such that

$$(\xi_1, \dots, \xi_d)^t = \sum_{i=1}^{d} c_i \tilde{H}_i.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Hence conditioning on $(\xi_1, \dots, \xi_d)$, if $X = (\xi_1, \dots, \xi_d, \xi_{d+1}, \dots, \xi_n)^t \in H$, then

$$X = \sum_{i=1}^{d} c_i H_i.$$

In particular, each value $\xi_{d+1}, \xi_{d+2}, \dots, \xi_n$ is determined. However, the probability of each of these events is at most $1 - \alpha_n$, so by independence the event $X \in H$ holds with probability at most $(1 - \alpha_n)^{n-d}$. □

Now we turn to the quadratic estimate.

Proof of Lemma 2.2. Let $d = \lfloor (1 - \varepsilon_n)n \rfloor$. Assume that the columns $X_{i_1}, \dots, X_{i_d}$ span the column space of $M_{n\times n}$. For now assume that $\{i_1, \dots, i_d\} = \{1, \dots, d\}$. Let H be the subspace spanned by $X_1, \dots, X_d$. We are considering the event $\mathcal{E}_{1,\dots,d}$ that $X_i \in H$, $d + 1 \leqslant i \leqslant n$. By Lemma 2.3, for any $i \geqslant d + 1$,

$$\mathbb{P}(X_i \in H) \leqslant (1 - \alpha_n)^{n-d} \leqslant e^{-\alpha_n \varepsilon_n n}.$$

Applying this bound for $d + 1 \leqslant i \leqslant n$ and using independence, we obtain

$$\mathbb{P}_{X_i, d+1 \leqslant i \leqslant n}(\mathcal{E}_{1,\dots,d} | X_1, \dots, X_d) = \mathbb{P}_{X_i, d+1 \leqslant i \leqslant n}(X_{d+1}, \dots, X_n \in H | H) \leqslant e^{-\alpha_n \varepsilon_n^2 n^2}.$$

Taking the union bound over at most 2^n choices of $\{i_1, \dots, i_d\}$, we conclude the proof. □

2.1 A simpler result

To get the main idea, in this subsection we show the following.

Theorem 2.4. *For every $A > 0$, there exists sufficiently large B such that*

$$\mathbb{P}(\text{ Coker } (M_{n\times(n+u)}) \simeq \{\text{id}\}) \geqslant 1 - n^{-A},$$

where

$$u = \left\lfloor B \frac{\log^2 n}{\alpha_n} + \sqrt{\frac{n \log n}{\alpha_n}} \right\rfloor.$$

Note that u does not drop below $\sqrt{n \log n}$.

In what follows we prove Theorem 2.4. The same argument will also be used to deal with matrices of dependent entries. Let $\mathcal{P}_n$ be the set of primes up to $(K_0 n)^{n/2}$:

$$\mathcal{P}_n := \{p \text{ prime }, p \leqslant (K_0 n)^{n/2}\}. \tag{2.1}$$

By taking the union bound, Lemma 2.2 then implies the following.

Corollary 2.5. *Let $\mathcal{E}$ be the event that the matrix $M_{n\times n}$ has rank at least $(1 - \varepsilon_n)n$ in $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$. Then*

$$\mathbb{P}(\mathcal{E}) \geqslant 1 - e^{-\alpha_n \varepsilon_n^2 n^2 + n \log n + n + n \log K_0/2}.$$

Set

$$\varepsilon_n := \sqrt{\frac{3 \log n}{\alpha_n n}}.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

With this value of $\varepsilon_n < 1$, Corollary 2.5 implies

$$\mathbb{P}(\mathcal{E}) \geqslant 1 - e^{-n \log n}.$$

Lemma 2.6 (surjectivity for small primes). *For any A there is a sufficiently large B so that with probability at least $1 - n^{-A}$, the random matrix $M_{n\times(n+u)}$ is surjective over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$ simultaneously, and $u = u(B)$ is as in Theorem 2.4.*

Proof of Lemma 2.6. It suffices to show that with high probability $M_{n\times(n+u)}$ has full rank in $\mathbf{F}_p^n$ (which would then imply surjectivity in $\mathbf{F}_p^n$).

We consider the submatrix $M_{n\times n}$, the restriction of $M_{n\times(n+u)}$ to the first n columns. Let $\mathcal{E}$ be the event defined in Corollary 2.5, *i.e.* that $M_{n\times n}$ has rank at least $(1-\varepsilon_n)n$ over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$. We thus have

$$\mathbb{P}_{M_{n\times n}}(\mathcal{E}) \geqslant 1 - e^{-n \log n}.$$

Consider also the event $\mathcal{E}_{\neq 0}$ that $\det(M_{n\times n}) \neq 0$, where by Theorem 1.4

$$\mathbb{P}(\mathcal{E}_{\neq 0}) \geqslant 1 - n^{-A},$$

provided that $(C_0 \log n)/n \leqslant \alpha$ for large C_0.

Now we condition on $M_{n\times n}$ satisfying $\mathcal{E}$ and $\mathcal{E}_{\neq 0}$ and show that, with high probability (with respect to the last u columns), $M_{n\times(n+u)}$ is surjective over all $\mathbf{F}_p^n$, $p \in \mathcal{P}_n$.

Let $\mathcal{P}^* = \mathcal{P}^*(M_{n\times n})$ be the collection of prime divisors of $\det(M_{n\times n})$. Because $|\det(M_{n\times n})| \leqslant (K_0 n)^{n/2}$ by the Hadamard bound, the random set $\mathcal{P}^*$ has small size, say

$$|\mathcal{P}^*| \leqslant n^2.$$

Case 1. When $p \in \mathcal{P}_n$ but $p \notin \mathcal{P}^*$, then $M_{n\times n}$ has full rank in $\mathbf{F}_p^n$, and so does $M_{n\times(n+u)}$.

Case 2. Consider $p \in \mathcal{P}^*$. We estimate the probability of the event $\mathcal{E}_p$ that $M_{n\times(n+u)}/p$ has full rank.

Let $H_0 \subset \mathbf{F}_p^n$ be the column subspace of $M_{n\times n}$, for which by assumption

$$d_0 := n - \dim(H_0) \leqslant n - (1-\varepsilon_n)n \leqslant \sqrt{\frac{3n\log n}{\alpha_n}}.$$

We next expose the remaining u vectors in groups. For $1 \leqslant i \leqslant d_0$, at step i we add k_i column vectors $X_{n+\sum_{l=1}^{i-1} k_l + j}$, $1 \leqslant j \leqslant k_i$ to the set of already exposed column vectors $X_1, \dots, X_{n+\sum_{l=1}^{i-1} k_l}$, where

$$k_i := \left\lceil \frac{B \log n}{\alpha d_{i-1}} \right\rceil,$$

and where d_{i-1} is the co-dimension of the subspace H_{i-1} generated by $\langle X_1, \dots, X_{n+\sum_{l=1}^{i-1} k_l}\rangle$. Note that in this exposing process the choice of k_i depends on d_{i-1}, a decreasing sequence throughout the process.

Next let $\mathcal{F}_i$ be the event that $\dim(H_i) \geqslant \dim(H_{i-1}) + 1$. In other words, $\mathcal{F}_i$ is the event that after adding the vectors of group i we have a strict decrease in the co-rank,

$$d_i \leqslant d_{i-1} - 1.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Assuming that $\dim(H_{i-1}) < n$, then by Lemma 2.3, and by independence of the column vectors,

$$\begin{aligned}\mathbb{P}(\mathcal{F}_i | \wedge_{j=0}^{i-1} \mathcal{F}_j \wedge \mathcal{E} \wedge \mathcal{E}_{\neq 0}, \dim(H_{i-1}) < n) &\geqslant 1 - ((1-\alpha_n)^{\operatorname{codim}(H_{i-1})})^{k_i} \\ &\geqslant 1 - ((1-\alpha_n)^{d_{i-1}})^{k_i} \\ &\geqslant 1 - n^{-B}.\end{aligned}$$

By Bayes' rule, with probability at least $(1-n^{-B})^{d_0} \geqslant 1 - n^{-B+1}$, after adding

$$\sum_i k_i \leqslant \sum_i \frac{B\log n}{\alpha_n d_i} + 1 \leqslant \frac{B\log n}{\alpha_n}\log d_0 + d_0$$

columns, the matrix

$$M_{n\times\left(n+\frac{B\log n}{\alpha_n}\log d_0 + d_0\right)}$$

has full rank in $\mathbf{F}_p^n$.

Taking the union bound over all primes $p \in \mathcal{P}^*$, we obtain that with probability at least $1 - n^{-B+3}$ the obtained matrix has full rank in $\mathbf{F}_p^n$ for all $p \in \mathcal{P}^*$.

By Case 1 and Case 2, we have seen that with $M_{n\times n}$ satisfying $\mathcal{E}$ and $\mathcal{E}_{\neq 0}$, the matrix $M_{n\times(n+u)}$ is surjective simultaneously over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$ with the desired probability. The proof is then complete after unfolding the conditioning on $M_{n\times n}$ (using Corollary 2.5). □

Proof of Theorem 2.4. We condition on the event $\mathcal{E}_{\neq 0}$. Note that with probability one

$$|\det(M_{n\times n})| \leqslant (K_0 n)^{n/2}.$$

This shows that with prime $p > (K_0 n)^{n/2}$, $\det(M_{n\times n}) \neq 0 \pmod p$. Hence on $\mathcal{E}_{\neq 0}$ the matrix $M_{n\times n}$ is surjective over $\mathbf{F}_p^n$ for all $p \geqslant (K_0 n)^{n/2}$.

Furthermore, Lemma 2.6 implies that with probability at least $1 - n^{-A}$, for all $p \in \mathcal{P}_n$ the random matrix $M_{n\times(n+u)}$ is surjective over $\mathbf{F}_p^n$. Hence altogether our matrix $M_{n\times(n+u)}$ is surjective in $\mathbb{Z}^n$ by Lemma 2.1. □

2.2 Proof of Theorem 1.3

Now we turn to our main theorem, where the proof is similar, but instead of Lemma 2.3 we will use the following result by Maples (see either [8, Theorem 1.2] or [10, Corollary 1.3]).

Theorem 2.7. *Let p be any prime. Assume that the entries of $M_{n\times n}$ are i.i.d. copies of ξ from (1.1) with α from (1.3). Then, for all $k \leqslant \eta n$ with a sufficiently small absolute constant η, we have*

$$\mathbb{P}(\operatorname{rank}(M_{n\times n}/p) = n - k) = O(n^k(p^{-k^2} + e^{-c\alpha n})). \tag{2.2}$$

In fact, [10, Corollary 1.3] says much more, that the bound is precisely

$$p^{-k^2}\prod_{i=1}^{k}(1-p^{-i})^{-1}\prod_{i=k+1}^{\infty}(1-p^{-i}) + O(e^{-c\alpha n}). \tag{2.3}$$

However, we will not need this later result (given that it has not been formally verified, especially for the sparse case). Note that (2.3), in its limit form ($n \to \infty$), is a simple consequence of the aforementioned paper [19, Corollary 3.5] by Wood. Back to [8], as this paper has some mistakes (*e.g.* [8, Proposition 2.3] is incorrect: see the Appendix for further discussion), for transparency

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

we will recast an almost complete proof of Theorem 2.7 in the Appendix. Theorem 2.7 and Theorem 1.4 will then follow as a byproduct.

Let $\mathcal{P}'_n$ be the set of primes up to $e^{c\alpha_n n/2}$, where c is the sufficiently small constant from Theorem 2.7, that is,

$$\mathcal{P}'_n := \{p \text{ prime}, p \leqslant e^{c\alpha_n n/2}\}.$$

Note that $\mathcal{P}'_n \subset \mathcal{P}_n$ (defined in (2.1)). By applying (2.2) with $k = C_1 \log n$ for a sufficiently large constant C_1 to each $p \in \mathcal{P}'_n$ and taking the union bound,

$$\sum_{p\in\mathcal{P}'_n} n^k(p^{-k^2} + O(e^{-c\alpha_n n})) = n^{-\omega(1)}.$$

Corollary 2.8. *Let $\mathcal{E}'$ be the event that the matrix $M_{n\times n}$ has rank at least $n - C_1 \log n$ in $\mathbf{F}_p^n$ for all $p \in \mathcal{P}'_n$. Then*

$$\mathbb{P}(\mathcal{E}') \geqslant 1 - n^{-\omega(1)}.$$

We next prove an analogue of Lemma 2.6. Set

$$u = \left\lfloor B \cdot \left(\frac{\log n}{\alpha_n} \log \frac{\log n}{\alpha_n} + \log n\right)\right\rfloor,$$

for a sufficiently large constant B.

Lemma 2.9. *With probability at least $1 - n^{-A}$, the random matrix $M_{n\times(n+u)}$ is surjective over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$ simultaneously.*

Proof of Lemma 2.9. Again, it suffices to show that with high probability $M_{n\times(n+u)}/p$ has full rank in each $\mathbf{F}_p^n$.

We consider the submatrix $M_{n\times n}$, the restriction of $M_{n\times(n+u)}$ to the first n columns. Let $\mathcal{E}'$ be the event implied by Corollary 2.8 that this matrix $M_{n\times n}$ has rank at least $n - C_1 \log n$ over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}'_n$. We thus have

$$\mathbb{P}_{M_{n\times n}}(\mathcal{E}') \geqslant 1 - n^{-\omega(1)}.$$

Consider also the event $\mathcal{E}_{\neq 0}$ that $\det(M_{n\times n}) \neq 0$ from Theorem 1.4. Conditioning on $M_{n\times n}$ satisfying $\mathcal{E}'$ and $\mathcal{E}_{\neq 0}$, we will show that, with high probability (with respect to the last u columns), $M_{n\times(n+u)}$ is surjective over all $\mathbf{F}_p^n$, $p \in \mathcal{P}_n$.

To do this, similarly to the proof of Lemma 2.6, let $\mathcal{P}^* = \mathcal{P}^*(M_{n\times n})$ be the collection of prime divisors of $\det(M_{n\times n})$. Then clearly the random set $\mathcal{P}^*$ has size at most n^2.

Case 1. When $p \in \mathcal{P}_n$ but $p \notin \mathcal{P}^*$, then $M_{n\times n}$ has full rank in $\mathbf{F}_p^n$, and so does $M_{n\times(n+u)}$.

Case 2. Consider $p \in \mathcal{P}^*$. We estimate the probability of the event $\mathcal{E}_p$ that $M_{n\times(n+u)}$ has full rank over $\mathbf{F}_p^n$. For this, first note that under $\mathcal{E}'$, if $p \in \mathcal{P}'_n$ (*i.e.* $p \leqslant e^{c\alpha_n n/2}$), then the co-rank of $M_{n\times n}$ over $\mathbf{F}_p^n$ is at most $C_1 \log n$. Now if $e^{c\alpha_n n/2} < p \leqslant (K_0 n)^{n/2}$, as $|\det(M_{n\times n})| \leqslant (K_0 n)^{n/2}$, the co-rank of $M_{n\times n}$ over $\mathbf{F}_p^n$ for these large p must be at most

$$\frac{\log(K_0 n)^{n/2}}{\log p} \leqslant (c\alpha_n)^{-1} \log(K_0 n).$$

So in either case the co-rank is at most $(c\alpha_n)^{-1} \log n + C_1 \log n$.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Let $H_0 \subset \mathbf{F}_p^n$ be the column subspace of $M_{n\times n}$, for which, by assumption,

$$d_0 := n - \dim(H_0) \leqslant (c\alpha_n)^{-1} \log n + C_1 \log n.$$

Similarly to the proof of Theorem 2.4, for $1 \leqslant i \leqslant d_0$, we will add

$$k_i = \left\lceil \frac{B \log n}{\alpha_n d_{i-1}} \right\rceil$$

column vectors $X_{n+\sum_{l=1}^{i-1} k_l + j}$, $1 \leqslant j \leqslant k_i$ to the already exposed column vectors $X_1, \dots, X_{n+\sum_{l=1}^{i-1} k_l}$, where d_{i-1} is the co-dimension of the subspace H_{i-1} generated by $\langle X_1, \dots, X_{n+\sum_{l=1}^{i-1} k_l} \rangle$.

Let $\mathcal{F}_i$ be the event that $\dim(H_i) \geqslant \dim(H_{i-1}) + 1$. By Lemma 2.3, and by independence of the column vectors,

$$\mathbb{P}(\mathcal{F}_i | \wedge_{j=0}^{i-1} \mathcal{F}_j \wedge \mathcal{E}' \wedge \mathcal{E}_{\neq 0}, \dim(H_{i-1}) < n) \geqslant 1 - ((1-\alpha)^{\operatorname{codim}(H_{i-1})})^{k_i} \geqslant 1 - n^{-B}.$$

By Bayes' rule, with probability at least $(1-n^{-B})^{d_0} \geqslant 1 - n^{-B+1}$, after adding

$$\sum_i k_i = O\left(\frac{\log n}{\alpha_n} \log d_0 + d_0 \right) := u$$

columns, the matrix $M_{n\times(n+u)}$ has full rank in $\mathbf{F}_p^n$. (It is possible to improve the total number of extra columns by a more careful analysis of the d_i, but we will not do so here for simplicity.)

Taking the union bound over all primes $p \in \mathcal{P}^*$, we obtain that with probability at least $1 - n^{-B+3}$ the matrix $M_{n\times(n+u)}$ has full rank in $\mathbf{F}_p^n$ for all $p \in \mathcal{P}^*$.

We have seen that with $M_{n\times n}$ satisfying $\mathcal{E}$ and $\mathcal{E}_{\neq 0}$, the matrix $M_{n\times(n+u)}$ is surjective simultaneously over $\mathbf{F}_p^n$ for all $p \in \mathcal{P}_n$ with the desired probability. The proof is then complete after unfolding the conditioning on $M_{n\times n}$, knowing that these events hold with very high probability. □

Finally, for Theorem 1.3, conditioning on the event $\mathcal{E}_{\neq 0}$, with prime $p > (K_0 n)^{n/2}$ we have $\det(M_{n\times n}) \neq 0 \pmod p$, and hence on $\mathcal{E}_{\neq 0}$ the matrix $M_{n\times n}$ is surjective over $\mathbf{F}_p^n$ for all $p \geqslant (K_0 n)^{n/2}$.

On the other hand, Lemma 2.9 implies that with probability at least $1 - n^{-A}$, for all $p \in \mathcal{P}_n$ the random matrix $M_{n\times(n+u)}$ is surjective over $\mathbf{F}_p^n$.

3. Some remarks

We have studied random matrices of independent entries. It is natural to consider Conjecture 1.1 for other families of matrices of dependent entries. Here we discuss one such model.

Let $M_{n\times n}$ be a random symmetric matrix, where for simplicity we assume that the entries $(M_{n\times n})_{ij}$, $1 \leqslant i \leqslant j \leqslant n$ are i.i.d. copies of a bounded random variable ξ from (1.1) with fixed α. It follows from [11, 17] that for this model the singularity probability can be bounded by

$$p_n = n^{-\omega(1)}. \tag{3.1}$$

Heuristically, arguing similarly to (1.2) (where we expose both columns and rows at the same time to obtain a quadratic variant of (1.2)), we can show that with high probability the matrix $M_{n\times n}$ is not surjective over $\mathbb{Z}^n$. In fact an analogue of Theorem 1.2 has been established in [10] for this model,[1] which confirms the above heuristic. However, we will show that by adding a couple more (say) independent rows, the matrix becomes surjective.

[1] To be more precise, M. M. Wood studied the Laplacian, but the result of [10] also covers the non-normalized ensemble.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Theorem 3.1. *Let $M_{n\times(n+u)}$ be a random matrix where its restriction $M_{n\times n}$ to the first n columns is a symmetric matrix as above, and the last u columns are independent with entries being i.i.d. copies of ξ. Then, for any $A > 0$, there exists B such that, for $u = \lfloor B\sqrt{n\log n}\rfloor$,*

$$\mathbb{P}(\text{ Coker }(M_{n\times(n+u)}) \simeq \{\text{id}\}) \geqslant 1 - n^{-A}.$$

To justify this result, we establish the following analogue of Lemma 2.2.

Lemma 3.2 (quadratic estimate). *Let p be a prime. Let $0 < \varepsilon_n < 1$ be a given parameter that might depend on n. Let $M_{n\times n}$ be a symmetric matrix where $(M_{n\times n})_{ij}, 1 \leqslant i \leqslant j \leqslant n$ are i.i.d. copies of a bounded random variable ξ from (1.1) with fixed α_n. Then the probability that $M_{n\times n}$ has rank at most $(1-\varepsilon_n)n$ in $\mathbf{F}_p^n$ is smaller than $e^{-\alpha_n\varepsilon_n^2 n^2/2+n}$.*

Proof. Let $d = \lfloor(1-\varepsilon_n)n\rfloor$. Assume that the columns $X_{i_1},\dots,X_{i_d}$ span the column space of $M_{n\times n}$. For now assume that $\{i_1,\dots,i_d\} = \{1,\dots,d\}$. Let H be the span of $X_1,\dots,X_d$. We are considering the event $\mathcal{E}_{1,\dots,d}$ that $X_i \in H, d+1 \leqslant i \leqslant n$. Now as X_i is dependent on H, we cannot estimate the probability of $X_i \in H$ directly by Odlyzko's bound. However, we can get rid of the dependence by deleting the corresponding common entries as below.

For $1 \leqslant j \leqslant n-d$ set

$$I_{d+j} := \{1,\dots,d+j\}.$$

For any $X \in \mathbf{F}_p^n$ and $J \subset [n]$ we denote $X|_J$ by the restriction of X over the components indexed by J. For convenience we also denote $H|_J$ by the subspace generated by $X_1|_J,\dots,X_d|_J$. Assume that $X_{d+1},\dots,X_n \in H$. Then the following holds:

- $X_{d+2}|_{I_{d+1}} \in H_{I_{d+1}}$, and more generally $X_{d+j+1}|_{I_{d+j}} \in H|_{I_{d+j}}, 1 \leqslant j \leqslant n-d-1$,
- the vector $X_{d+j+1}|_{I_{d+j}}$ is independent of $H|_{I_{d+j}}$,
- the vectors $X_{d+j+1}|_{I_{d+j}}, 1 \leqslant j \leqslant n-d-1$ are mutually independent.

Now as $H|_{I_{d+j}}$ has rank at most d in $\mathbf{F}_p^{d+j}$, by Lemma 2.3 we have

$$\mathbb{P}(X_{d+j+1}|_{I_{d+j}} \in H|_{I_{d+j}}) \leqslant (1-\alpha_n)^j.$$

Applying this bound for $1 \leqslant j \leqslant n-d-1$ and using the independence of $X_{d+j+1}|_{I_{d+j}}$, we obtain

$$\mathbb{P}_{X_i, d+1\leqslant i\leqslant n}(\mathcal{E}_{1,\dots,d}|X_1,\dots,X_d) \leqslant \prod_{j=1}^{n-d-1}(1-\alpha_n)^j \leqslant e^{-\alpha_n\varepsilon_n^2 n^2/2}.$$

Taking the union bound over at most 2^n choices of $\{i_1,\dots,i_d\}$, we conclude the proof. □

We can now complete the proof of Theorem 3.1 verbatim as in the proof of Theorem 2.4 with fixed α_n. Indeed, Corollary 2.5 follows from Lemma 3.2, and Lemma 2.6 can be justified similarly (conditioning on (3.1)) because the last u columns are mutually independent, and are independent from $M_{n\times n}$.

Acknowledgement

The authors thank Kyle Luh for helpful comments. They are also thankful to the anonymous referees whose suggestions have helped us to improve the presentation of the paper substantially.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

References

[1] Basak, A. and Rudelson, M. (2017) Invertibility of sparse non-Hermitian matrices. *Adv. Math.* **310** 426–483.
[2] Bourgain, J., Vu, V. and Wood, P. M. (2010) On the singularity probability of discrete random matrices. *J. Funct. Anal.* **258** 559–603.
[3] Halász, G. (1977) Estimates for the concentration function of combinatorial number theory and probability. *Periodica Math. Hungar.* **8** 197–211.
[4] Kahn, J., Komlós, J. and Szemerédi, E. (1995) On the probability that a random ±1 matrix is singular. *J. Amer. Math. Soc.* **8** 223–240.
[5] Komlós, J. (1967) On the determinant of (0 − 1) matrices. *Studia Sci. Math. Hungar.* **2** 7–22.
[6] Koplewitz, S. (2016) The corank of a rectangular random integer matrix. arXiv:1611.06441
[7] Koplewitz, S. (2017) Random graphs, sandpile groups, and surjectivity of random matrices. PhD thesis, Yale University.
[8] Maples, K. (2010) Singularity of random matrices over finite fields. arXiv:1012.2372
[9] Maples, K. (2011) Arithmetic properties of random matrices. PhD thesis, University of California, Los Angeles.
[10] Maples, K. (2013) Cokernels of random matrices satisfy the Cohen–Lenstra heuristics. arXiv:1301.1239
[11] Nguyen, H. (2012) Inverse Littlewood–Offord problems and the singularity of random symmetric matrices. *Duke Math. J.* **161** 545–586.
[12] Nguyen, H. (2018) Random matrices: Overcrowding estimates for the spectrum. *J. Funct. Anal.* **275** 2197–2224.
[13] Rudelson, M. and Vershynin, R. (2008) The Littlewood–Offord problem and invertibility of random matrices. *Adv. Math.* **218** 600–633.
[14] Stanley, R. (1997) *Enumerative Combinatorics*, Vol. 1, Cambridge University Press.
[15] Tao, T.and Vu, V. (2006) *Additive Combinatorics*, Vol. 105, Cambridge University Press.
[16] Tao, T. and Vu, V. (2007) On the singularity probability of random Bernoulli matrices. *J. Amer. Math. Soc.* **20** 603–673.
[17] Vershynin, R. (2014) Invertibility of symmetric random matrices. *Random Struct. Alg.* **44** 135–182.
[18] Wood, M. M. (2017) The distribution of sandpile groups of random graphs. *J. Amer. Math. Soc.* **30** 915–958.
[19] Wood, M. M. (2019) Random integral matrices and the Cohen–Lenstra heuristics. *Amer. J. Math.* **141** 383–398.

Appendix. The co-rank estimate: proof of Theorem 2.7

We will work in a more general setting. Let $q = p^f$ be a prime power and $\mathbf{F}_q$ be the finite field with q elements. We say that a probability distribution μ in $\mathbf{F}_q$ is α_n-*balanced* (for some $0 < \alpha_n < 1$) if, for every additive subgroup T in $\mathbf{F}_q$ and $s \in \mathbf{F}_q$,

$$\mu(s + T) \leqslant 1 - \alpha_n.$$

In the general finite field setting, we will assume

$$\alpha_n \geqslant n^{-1/2+\varepsilon} \quad \text{for any } \varepsilon > 0\,. \tag{A.1}$$

In the more specific setting when $q = p$ (which is the setting of Theorem 2.7), as there is no non-trivial additive subgroup in $\mathbf{F}_p$, we will assume

$$\max_{x \in \mathbf{F}_p} \mu(x) = 1 - \alpha_n,$$

where

$$\alpha_n \geqslant \frac{C_0 \log n}{n} \quad \text{for a sufficiently large constant } C_0. \tag{A.2}$$

In what follows $M_{n\times n}$ is a random matrix, where the entries are i.i.d. according to an α_n-balanced μ from either (A.1) or (A.2), and $n \to \infty$. Note that, in either case, we do not assume the support of μ is bounded. Recall that $X_1, \dots, X_n$ are the columns of $M_{n\times n}$ and W_{n-k} is the subspace $\langle X_1, \dots, X_{n-k}\rangle$ generated by $X_1, \dots, X_{n-k}$. Our first goal is to re-prove the following variant of [8, Proposition 2.1] and [9, Proposition 2.1.1].

Theorem A.1. *Assume that μ is distributed according to either (A.1) or (A.2) depending on q. Then there exist positive constants c, η such that the following holds for $1 \leqslant k \leqslant \eta n$: there exists an event*

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

$\mathcal{E}_{n-k}$ on the σ-algebra generated by $X_1, \dots, X_{n-k}$ of probability at least $1 - e^{-c\alpha_n n}$ such that, for any $k \leqslant k_0 \leqslant \eta n$,

$$\mathbb{P}_{X_{n-k+1}}(X_{n-k+1} \in W_{n-k} \mid \mathcal{E}_{n-k} \wedge \operatorname{codim}(W_{n-k}) = k_0) = q^{-k_0} + O(e^{-c\alpha_n n}).$$

Note that there are some modifications of this result compared to the original statement by Maples in [8, Proposition 2.1] or [9, Proposition 2.1.1] that:

(i) the statement also holds when the co-dimension of W_{n-k} is not necessarily k,
(ii) the statement also holds for sparse settings such as (A.1) and (A.2).

Note that (i) is not new as it also appeared in a subsequent (unpublished) preprint by Maples ([10, Proposition 3.1]). We then deduce Theorem 2.7 restated here for the finite field.

Corollary A.2. *Assume that μ is distributed according to either (A.1) or (A.2). Assume that $k \leqslant \eta n$ for some sufficiently small η. Then*

$$\mathbb{P}(\operatorname{rank}(M_{n\times n}) = n - k) = O(n^k(q^{-k^2} + e^{-c\alpha n})). \tag{A.3}$$

It seems plausible to get rid of the factor n^k here (especially for fixed α), but we do not attempt to do so, as the reader can check that any improvement along these lines has little effect on the bounds in Theorem 1.3.

Proof. The event $\operatorname{rank}(M_{n\times n}) = n - k$ implies that there exist k column vectors $X_{i_1}, \dots, X_{i_k}$ which belong to the subspace of dimension $n - k$ generated by the remaining column vectors $X_i, i \neq i_1, \dots, i_k$. With a loss of a factor of n^k in probability, we can assume that $\{i_1, \dots, i_k\} = \{n - k + 1, \dots, n\}$. We then use Theorem A.1 to show

$$\begin{aligned}
&\mathbb{P}(X_{n-k+1}, \dots, X_n \in W_{n-k} \wedge \operatorname{codim}(W_{n-k}) = k)\\
&\quad = \mathbb{P}(X_{n-k+1}, \dots, X_n \in W_{n-k} \wedge \mathcal{E}_{n-k} \wedge \operatorname{codim}(W_{n-k}) = k) + O(e^{-c\alpha_n n})\\
&\quad \leqslant \mathbb{P}(X_{n-k+1}, \dots, X_n \in W_{n-k} \mid \mathcal{E}_{n-k} \wedge \operatorname{codim}(W_{n-k}) = k) + O(e^{-c\alpha_n n})\\
&\quad \leqslant (q^{-k} + O(e^{-c\alpha_n n}))^k + O(e^{-c\alpha_n n})\\
&\quad = O(q^{-k^2} + e^{-c\alpha_n n}).
\end{aligned}$$

□

Taking $k = 1$ and $q = p \to \infty$ in Corollary A.2, we then obtain Theorem 1.4.

Corollary A.3. *Assume that the entries of $M_{n\times n}$ are i.i.d. copies of a discrete random variable ξ taking integer values such that*

$$\max_{x\in\mathbb{Z}} \mathbb{P}(\xi = x) \leqslant 1 - \frac{C_0 \log n}{n} \quad \text{for a sufficiently large constant } C_0.$$

Then the matrix $M_{n\times n}$ is non-singular with probability at least $1 - e^{-c\alpha_n n}$.

Proof. Choose a prime p to be large such that $p \geqslant \max\{n^{2n}, |\det(M_{n\times n})|\}$ and $\operatorname{supp}(\xi) \subset (-p, p)$. It then suffices to show that $M_{n\times n}/p$ has full rank with probability at least $1 - e^{-c\alpha_n n}$. To this end, and by Corollary A.6 (to be discussed below), it suffices to bound the probability that $M_{n\times n}/p$ has co-rank k between 1 and ηn, but then the statement follows from Corollary A.2 (stated for μ distributed according to (A.2)) by taking the union bound. □

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Note that the trick to pass the singularity problem over $\mathbb{Z}$ to over $\mathbf{F}_p$, and let $p \to \infty$, is not new. See for instance [2, 16] and the references therein.

Finally, we will also show the following more general variant of Theorem A.1 for rectangular matrices $M_{n\times(n+u)}$ where $W_k = \langle X_{k+1}, \dots, X_{n+u}\rangle$.

Theorem A.4. *Assume that μ is distributed according to either (A.1) or (A.2) depending on q. Then there exist positive constants c, η such that the following holds. Let $0 \leqslant u \leqslant \eta n$ be given. Then, for $k \leqslant \eta n$, there exists an event $\mathcal{E}_{n+u-k}$ on the σ-algebra generated by $X_1, \dots, X_{n+u-k}$ of probability at least $1 - e^{-c\alpha_n n}$ such that, for any $(k-u)^+ \leqslant k_0 \leqslant \eta n$,*

$$\mathbb{P}_{X_{n+u-k+1}}(X_{n+u-k+1} \in W_{n+u-k} \mid \mathcal{E}_{n+u-k} \wedge \operatorname{codim}(W_{n+u-k}) = k_0) = q^{-k_0} + O(e^{-c\alpha_n n}).$$

The rest of the Appendix is mainly dedicated to verifying Theorem A.1. The proof of Theorem A.4 will be deduced shortly. As already mentioned, our approach mainly follows [8].

Part I. Proof of Theorem A.1

In what follows, the constants η, β, δ, d are sufficiently small but fixed (see *e.g.* (A.16) for a choice of d), and α_n is allowed to depend on n as from (A.1) or (A.2) for sufficiently large constant C_0. The only place we have to treat (A.1) and (A.2) separately is in the proof of Proposition A.7 below.

We first note that Odlyzko's lemma in fact holds in any finite field.

Lemma A.5. *For a deterministic subspace V of $\mathbf{F}_q^n$ and a random vector X of i.i.d. entries from an α_n-balanced distribution*

$$\mathbb{P}(X \in V) \leqslant (1-\alpha_n)^{\operatorname{codim}(V)}.$$

Corollary A.6. *Let $X_1, \dots, X_{n-k}$ be the columns of $M_{n\times n}$. Then the probability that $X_1, \dots, X_{n-k}$ are linearly independent in $\mathbf{F}_q^n$ is at least $1 - n(1-\alpha_n)^k$.*

Proof. Let $0 \leqslant i \leqslant n-k-1$ be minimal such that $X_{i+1} \in \operatorname{Span}(X_1, \dots, X_i)$. By Lemma 2.3, this event is bounded by $(1-\alpha_n)^{n-i}$. Summing over $0 \leqslant i \leqslant n-k-1$, the probability under consideration is bounded by $n(1-\alpha_n)^k$. □

A.1. Sparse subspace.

Let $0 < \delta, \eta$ be small constants (independently from α_n). Given a vector space $H \subset \mathbf{F}_q^n$, we say that H is *δ-sparse* if there is a non-zero vector w with $|\operatorname{supp}(w)| \leqslant \delta n$ (*i.e.* w is *δ-sparse*) such that $w \perp H$, where $\operatorname{supp}(w)$ is the set of non-zero coordinates of w.

Proposition A.7 (random subspaces are not sparse). *Let $0 < \varepsilon_0 < 1/2$ be any fixed constants. Then, for any $0 \leqslant \delta, \eta$ such that $\delta + \eta \leqslant \varepsilon_0$, and with α_n from (A.1) or (A.2), the following holds for $0 \leqslant k < \eta n$: with probability at least $1 - e^{-c\alpha_n n}$ with respect to $X_1, \dots, X_{n-k}$, the random subspace W_{n-k} is not δ-sparse. Here $c = c(\varepsilon_0)$ is an absolute constant.*

Proof. For $\sigma \subset [n]$ with $1 \leqslant t = |\sigma| \leqslant \delta n$, let $\mathcal{E}_\sigma$ be the event that W_{n-k} is orthogonal to a vector w with $\operatorname{supp}(w) = \sigma$, but is not orthogonal to any vector w' with $|\operatorname{supp}(w')| \leqslant t-1$. Note that in this case the σ-restricted vector $w|_\sigma$ is orthogonal to the σ-restricted column vectors $X_1|_\sigma, \dots, X_{n-k}|_\sigma$.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

The dimension of the annihilator of W_{n-k} in $\mathbf{F}_q^\sigma$ and the dimension of Span $(X_1|_\sigma, \dots, X_{n-k}|_\sigma)$ sum to t. If the annihilator were more than one-dimensional, there would necessarily exist a non-zero linear combination of annihilators with support strictly contained in σ. Hence it follows that the column vectors $X_1|_\sigma, \dots, X_{n-k}|_\sigma$ span a subspace of dimension $t-1$, and there are $t-1$ linearly independent column vectors $X_{i_1}|_\sigma, \dots, X_{i_{t-1}}|_\sigma$ in $\mathbf{F}_q^\sigma$.

We therefore define the event $\mathcal{E}_{\sigma,i_1,\dots,i_{t-1}}$ to be that

(1) $X_{i_1}|_\sigma, \dots, X_{i_{t-1}}|_\sigma$ are linearly independent,
(2) $X_i|_\sigma \in$ Span $(X_{i_1}|_\sigma, \dots, X_{i_{t-1}}|_\sigma)$ for all $1 \leqslant i \leqslant n-k$,
(3) the annihilator of Span $(X_{i_1}|_\sigma, \dots, X_{i_{t-1}}|_\sigma)$ in $\mathbf{F}_q^\sigma$ contains no non-zero vectors with support begin a proper set of σ,

and observe that $\mathcal{E}_\sigma$ is a union over all such $\mathcal{E}_{\sigma,i_1,\dots,i_{t-1}}$.

Case 1. If $144\alpha_n^{-1} \leqslant t \leqslant \delta n$, then by Theorem A.15 (whose proof is given in Part II),

$$\mathbb{P}(\mathcal{E}_{\sigma,i_1,\dots,i_{t-1}}) \leqslant \left(\frac{1}{q} + \frac{2}{\sqrt{\alpha_n t}}\right)^{n-k-t+1} \leqslant \left(\frac{1}{q} + \frac{2}{\sqrt{\alpha_n t}}\right)^{(1-\varepsilon_0)n} \leqslant \left(\frac{2}{3}\right)^{n/2}.$$

Thus

$$\mathbb{P}(\mathcal{E}_\sigma) \leqslant \sum_{i_1,\dots,i_{t-1}} \mathbb{P}(\mathcal{E}_{\sigma,i_1,\dots,i_{t-1}}) \leqslant \binom{n-k}{t-1}\left(\frac{2}{3}\right)^{n/2}.$$

So

$$\sum_{\sigma,|\sigma|\geqslant 144\alpha_n^{-1}} \mathbb{P}(\mathcal{E}_\sigma) \leqslant \sum_{144\alpha_n^{-1}\leqslant t\leqslant \delta n} \binom{n}{t}\binom{n-k}{t-1}\left(\frac{2}{3}\right)^{n/2} \leqslant \left(\frac{2}{3}\right)^{n/4},$$

provided that ε_0 (and hence δ) are sufficiently small.

Case 2. If $1 \leqslant t \leqslant 144\alpha_n^{-1}$. We use the simple bound

$$\mathbb{P}(X_i|_\sigma \in \text{Span}\,(X_{i_1}|_\sigma, \dots, X_{i_{t-1}}|_\sigma)) \leqslant 1-\alpha_n.$$

Hence

$$\mathbb{P}(\mathcal{E}_\sigma) \leqslant \sum_{i_1,\dots,i_{t-1}} \mathbb{P}(\mathcal{E}_{\sigma,i_1,\dots,i_{t-1}}) \leqslant \binom{n-k}{t-1}(1-\alpha_n)^{(1-\delta-\eta)n} \leqslant \binom{n-k}{t-1}(1-\alpha_n)^{(1-\varepsilon_0)n}.$$

Consequently,

$$\sum_{\sigma,|\sigma|\leqslant 144\alpha_n^{-1}} \mathbb{P}(\mathcal{E}_\sigma) \leqslant \sum_{t\leqslant 144\alpha_n^{-1}} \binom{n}{t}\binom{n-k}{t-1}(1-\alpha_n)^{(1-\varepsilon_0)n}.$$

Subcase 2.1. Assume that α_n is from (A.1). Then, as $\alpha_n \geqslant n^{-1/2+\varepsilon}$, the above can be easily bounded by

$$\sum_{\sigma,|\sigma|\leqslant 144\alpha_n^{-1}} \mathbb{P}(\mathcal{E}_\sigma) \leqslant (1-\alpha_n)^{\varepsilon_0 n/2}.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Subcase 2.2. Assume that α_n is from (A.2):

$$\frac{C_0 \log n}{n} \leqslant \alpha_n = 1 - \max_x \mu(x) \leqslant n^{-1/2+\varepsilon}.$$

We will rely on the following observation, which is a simple variant of [1, Lemma 3.2].

Claim A.8. *The following holds with probability at least* $1 - e^{-c\alpha_n n}$ *with respect to* $X_1, \dots, X_{n-k}$. *For any* $1 \leqslant t \leqslant 144\alpha_n^{-1}$ *and any* $\sigma \in \binom{[n]}{t}$, *there are at least two columns* X_i, X_{i+1} *whose restriction* $(X_{i+1} - X_i)|\sigma$ *has exactly one non-zero entry.*

Suppose that $w \in \mathbf{F}_q^n$ has support σ of size $t = |\sigma| = |\operatorname{supp}(w)| \leqslant 144\alpha_n^{-1}$. Then, conditioning on the event in the lemma, there is some $1 \leqslant i \leqslant n-k-1$ such that $(X_{i+1} - X_i)|_\sigma$ has exactly one non-zero entry, and hence $w|\sigma$ is not orthogonal to it. Hence, it cannot be simultaneously orthogonal to all X_i, $1 \leqslant i \leqslant n-k$. Thus, it suffices to prove the claim.

Proof of Claim A.8. For each $i \in \{1, 3, \dots, 2\lfloor (n-k-1)/2 \rfloor + 1\}$, consider the vectors $Y_i = X_{i+1} - X_i$. The entries of this vector are i.i.d. copies of the symmetrized random variable $\psi = \xi - \xi'$, where ξ', ξ are independent and have distribution μ. With $1 - \alpha_n' = \mathbb{P}(\psi = 0)$, then we have

$$\alpha_n \leqslant \alpha_n' \leqslant 2\alpha_n,$$

as this can be seen by

$$(1-\alpha_n)^2 \leqslant \max_x \mathbb{P}(\xi = x)^2 \leqslant \sum_x \mathbb{P}(\xi = x)^2 = \mathbb{P}(\psi = 0) \leqslant \max_x \mathbb{P}(\xi = x) = 1 - \alpha_n.$$

Now let p_σ be the probability that all $Y_i|_\sigma$, $i \in \{1, 3, \dots, 2\lfloor (n-k-1)/2 \rfloor + 1\}$ fail to have exactly one non-zero entry. Then, by independence of the columns and of the entries,

$$p_\sigma = (1 - t\alpha_n'(1-\alpha_n')^{t-1})^{(n-k)/2} \leqslant (1 - t\alpha_n' e^{-t\alpha_n'})^{n-k} \leqslant e^{-nt\alpha_n' e^{-t\alpha_n'}/2}.$$

Note that as $1 \leqslant t \leqslant 8^{3/\varepsilon_0}\alpha_n^{-1}$, $e^{-t\alpha_n'}/2 \geqslant c$ for some positive constant c, and hence

$$e^{-nt\alpha_n' e^{-t\alpha_n'}/2} \leqslant (e^{-cn\alpha_n'})^t \leqslant n^{-cC_0 t/2} e^{-cn\alpha_n/2}.$$

Thus

$$\begin{aligned}\sum_{1 \leqslant t \leqslant 144\alpha_n^{-1}} \sum_{\sigma \in \binom{[n]}{t}} p_\sigma &\leqslant \sum_{1 \leqslant t \leqslant 144\alpha_n^{-1}} \binom{n}{t} e^{-(n-k)t\alpha_n e^{-t\alpha_n}} \\ &\leqslant \sum_{1 \leqslant t \leqslant 144\alpha_n^{-1}} (n^t n^{-cC_0 t/2}) e^{-cn\alpha_n/2} \\ &< e^{-cn\alpha_n/2},\end{aligned}$$

provided that C_0 is sufficiently large. □

Our proof of Proposition A.7 is then complete by combining the cases considered above. □

Remark. Our treatment here is quite different from [8, Section 2.1] as there is no need to use [8, Proposition 2.3] (which states 'Let $Z_1, \dots, Z_r$ be non-trivial i.i.d. random vectors in $\mathbf{F}_q^n$, then $\mathbb{P}(Z_1, \dots, Z_r \in V \mid Z_1, \dots, Z_r$ are linearly independent$) \leqslant \mathbb{P}(Z \in V)^r$'). An elementary counter-example to this proposition is that Z_i are chosen uniformly at random from $\{a_1, 2a_1, 3a_1, a_2, a_3\}$,

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

where $a_1 \notin V$ and a_2, a_3 are linearly independent in V: in this case the left-hand side probability bound is larger than the right-hand side.[2] Also, Maples did not provide *any treatment* for the sparse case (Case 2) for Proposition A.7 in [8] or [9], which we have added. See also the remark after Lemma A.9 below.

To conclude, given constants η, δ and the parameter α_n from (A.1) or (A.2), let $\mathcal{E}_{n-k,\text{dense}}$ denote the event considered in Proposition A.7,

$$\mathbb{P}(\mathcal{E}_{n-k,\text{dense}}) \geqslant 1 - e^{-c\alpha_n n}. \tag{A.4}$$

We next turn to another type of subspace.

A.2. Semi-saturated subspace.

Given $0 < \alpha_n, \delta, d < 1$, we call a subspace V of co-dimension k_0 *semi-saturated* (or *semi-sat* for short), where $k_0 \leqslant \eta n$, if V is not δ-sparse and

$$e^{-d\alpha_n n} < \left| \mathbb{P}(X \in V) - \frac{1}{q^{k_0}} \right| \leqslant \frac{16}{q^{k_0}}. \tag{A.5}$$

Here we assume

$$e^{-d\alpha_n n} < \frac{16}{q^{k_0}}.$$

If this condition is not satisfied (such as when q is sufficiently large), then the semi-saturated case can be omitted.

Lemma A.9 (Proposition 2.5 of [8]). *For all $\beta > 0$ and $\delta > 0$, there exists $0 < d = d(\beta, \delta) < 1$ in the definition of semi-saturation and a deterministic set $\mathcal{R} \subset \mathbf{F}_q^n$ of non-δ-sparse vectors and of size $|\mathcal{R}| \leqslant (2\beta^\delta)^n q^n$ such that every semi-saturated V is orthogonal to a vector $R \in \mathcal{R}$. In fact the conclusion holds for any subspace V satisfying the left-hand side of (A.5).*

In short, semi-saturated subspaces are necessarily orthogonal to one of a small number of non-sparse vectors in $\mathbf{F}_q^n$. A proof of this result will be given in Part II, where we emphasize that α_n can be as small as (A.2), in contrast to the proof of [8, Proposition 2.5], where α_n was treated as a constant.

Let $\mathcal{F}_{n-k,k_0,\text{semi-sat}}$ be the event that codim $(W_{n-k}) = k_0$ and W_{n-k} is semi-saturated.

Proposition A.10. *Let $\beta, \delta > 0$ be parameters such that $\beta^\delta < 17^{-2}/2$. With $d = d(\beta, \delta)$, from Lemma A.9 we have*

$$\mathbb{P}(\mathcal{F}_{n-k,k_0,\text{semi-sat}}) \leqslant e^{-n}.$$

In particular, with $\mathcal{E}_{n-k,\text{semi-sat}}$ being the event $\wedge_{k \leqslant k_0 \leqslant \eta n} \overline{\mathcal{F}}_{n-k,k_0,\text{semi-sat}}$ in the σ-algebra generated by $X_{k+1}, \ldots, X_n$, then

$$\mathbb{P}(\mathcal{E}_{n-k,\text{semi-sat}}) \geqslant 1 - e^{-n/2}. \tag{A.6}$$

Proof of Proposition A.10. We have

$$\mathbb{P}(\mathcal{F}_{n-k,k_0,\text{semi-sat}}) = \sum_{V \text{semi-sat}} \mathbb{P}(W_{n-k} = V) \leqslant \sum_{V \text{semi-sat}} \mathbb{P}(X_1, \ldots, X_{n-k} \in V).$$

[2] We thank M. M. Wood for pointing out the mistake, as well as for supplying a counterexample.

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Now, for each fixed V that is semi-saturated of co-dimension $k_0 \geqslant k$, by definition $\mathbb{P}(X \in V) \leqslant 17q^{-k_0}$. So

$$\mathbb{P}(X_1, \dots, X_{n-k} \in V) \leqslant 17^{n-k} q^{-k_0(n-k)}.$$

We next use Lemma A.9 to count the number $N_{\text{semi-sat}}$ of semi-saturated subspaces V. Each V is determined by its annihilator $V^\perp$ (of cardinality q^{k_0}). To count $V^\perp$, we first choose a vector $v \in \mathcal{R}$, and then another $(k_0 - 1)$-dimensional subspace that is linearly independent of v. The number of ways to complete this space equals the number of ways to pick a $(k_0 - 1)$-dimensional space from $\mathbf{F}_q^{n-1}$. The number of such subspaces is given by the well-known (see [14, Proposition 1.3.18]) exact formula

$$\prod_{j=0}^{k_0-2} \frac{q^{n-1-j} - 1}{q^{k_0-1-j} - 1} \leqslant C q^{(k_0-1)(n-k_0)}$$

for some absolute constant $C > 0$. Hence

$$N_{\text{semi-sat}} \leqslant C(2\beta^\delta)^n q^{nk_0 - k_0^2 + k_0}.$$

Therefore

$$\begin{aligned}
\mathbb{P}(\mathcal{F}_{k,k_0,\text{semi-sat}}) &\leqslant \sum_{V \text{semi-sat}} \mathbb{P}(X_1, \dots, X_{n-k} \in V) \\
&= O((2\beta^\delta)^n q^{nk_0 - k_0^2 + k_0} 17^{n-k} q^{-k_0(n-k)}) \\
&= O(17^{n-k}(2\beta^\delta)^n q^{k_0} q^{k_0(k-k_0)}) \\
&= O(17^{n-k}(2\beta^\delta)^n q^{k_0}).
\end{aligned}$$

Now recall that $e^{-d\alpha_n n} \leqslant 16q^{-k_0}$, and hence

$$\mathbb{P}(\mathcal{F}_{n-k,k_0,\text{semi-sat}}) = O(17^{n-k}(2\beta^\delta)^n q^{k_0}) = O(17^{n+1-k}(2\beta^\delta)^n e^{d\alpha_n n}).$$

We then choose β so that $2\beta^\delta < 17^{-2}$, and with $d < 1$ we have $\mathbb{P}(\mathcal{F}_{n-k,k_0,\text{semi-sat}}) \leqslant e^{-n}$. □

A.3. Unsaturated subspace.

Recall that $k \leqslant \eta n$ for sufficiently small η. Let V be a subspace of co-dimension $k_0 \geqslant k$ in $\mathbf{F}_q^n$. We say that V is *unsaturated* if V is not δ-sparse and

$$\max\left(e^{-d\alpha_n n}, 16q^{-k_0}\right) < |\mathbb{P}(X \in V) - q^{-k_0}|.$$

In particular, this implies that

$$\mathbb{P}(X \in V) \geqslant \max\left\{17q^{-k_0}, \frac{16}{17} e^{-d\alpha_n n}\right\}.$$

The following is from [8, Lemma 2.8].

Lemma A.11. *There is an α_n'-balanced probability distribution ν on $\mathbf{F}_q$ with $\alpha_n' = \alpha_n/64$ such that if $Y \in \mathbf{F}_q^n$ is a random vector with i.i.d. coefficients distributed according to ν, then, for any unsaturated proper subspace V,*

$$\left|\mathbb{P}(X \in V) - \frac{1}{q^{k_0}}\right| \leqslant \left(\frac{1}{2} + o(1)\right)\left|\mathbb{P}(Y \in V) - \frac{1}{q^{k_0}}\right|.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

A proof of this lemma will be given in Part II. By definition, if V is unsaturated then

$$\mathbb{P}(Y \in V) \geqslant (2 - o(1))\left(\mathbb{P}(X \in V) - \frac{1}{q^{k_0}}\right) + \frac{1}{q^{k_0}} > \frac{3}{2}\mathbb{P}(X \in V).$$

Definition. Let V be a subspace in $\mathbf{F}_q^n$. Let $d_{\text{comb}} \in \{1/n, \dots, n^2/n\}$. We say that V has combinatorial co-dimension d_{comb} if

$$(1 - \alpha_n)^{d_{\text{comb}}} \leqslant \mathbb{P}(X \in V) \leqslant (1 - \alpha_n)^{d_{\text{comb}} - 1/n}.$$

Now as we are in the unsaturated case, $\mathbb{P}(X \in V) \geqslant \frac{16}{17} e^{-d\alpha_n n}$, so

$$d_{\text{comb}} \leqslant 2dn.$$

In what follows we will fix d_{comb} from the above range, noting that d is sufficiently small, and there are only $O(n^2)$ choices of d_{comb}.

Fix any $0 < \delta_1 < \delta_2 < 1/3$ such that

$$16(\delta_2 - \delta_1)\left(1 + \log \frac{1}{\delta_2 - \delta_1}\right) < \delta_1. \tag{A.7}$$

Set

$$r := \lfloor \delta_1 n \rfloor \text{ and } s := n - k - \lfloor \delta_2 n \rfloor.$$

Let $Y_1, \dots, Y_r$ be random vectors with entries distributed by ν obtained by Lemma A.11, and let $Z_1, \dots, Z_s$ and $X_{r+s+1}, \dots, X_{n-k}$ be random vectors with entries distributed by μ.

Proposition A.12. *Let $W = \text{Span}\{X_1, \dots, X_{n-k}\}$. We have*

$$\mathbb{P}(r + s \leqslant \dim(W) \leqslant n - k, W \textit{unsaturated}) \leqslant \frac{3}{2}^{-r/2} \binom{n-k}{r+s} \leqslant \frac{3}{2}^{-\delta_1 n/4}.$$

The second inequality follows directly from (A.7) and the standard bound

$$\binom{n}{k} \leqslant \left(\frac{en}{n-k}\right)^{n-k}.$$

Note that we do not require $\{X_i\}$ to be linearly independent. In other words, let $\mathcal{E}_{n-k,\text{unsat}}$ denote the complement of the event above in the σ-algebra generated by $X_1, \dots, X_{n-k}$. Then

$$\mathbb{P}(\mathcal{E}_{n-k,\text{unsat}}) \geqslant 1 - \frac{3}{2}^{-\delta_1 n/4}. \tag{A.8}$$

To prove Proposition A.12 we show the following.

Theorem A.13. *Let V be any subspace of dimension between $r + s$ and $n - k$ and having $d_{\text{comb}} \leqslant 2dn$. Then we have*

$$\mathbb{P}(\text{Span}\{X_1, \dots, X_{n-k}\} = V) \leqslant \frac{3}{2}^{-r/2} \binom{n-k}{r+s} \mathbb{P}(\text{Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V).$$

To conclude Proposition A.12 we then just use

$$\sum_{\substack{V \leqslant \mathbf{F}_q^n \\ \text{codim}(V) \geqslant k}} \mathbb{P}(\text{Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V) = 1. \tag{A.9}$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Proof of Theorem A.13. First of all, by independence between X_i, Y_j, Z_l,

$$\begin{aligned}&\mathbb{P}(\text{ Span}\{X_1,\dots,X_{n-k}\}=V)\times\mathbb{P}(Y_1,\dots,Y_r,Z_1,\dots,Z_s\text{ linearly independent in }V)\\&\quad=\mathbb{P}(\text{ Span}\{X_1,\dots,X_{n-k}\}=V\wedge Y_1,\dots,Y_r,Z_1,\dots,Z_s\text{ linearly independent in }V).\end{aligned}\tag{A.10}$$

We next estimate $\mathbb{P}(Y_1,\dots,Y_r,Z_1,\dots,Z_s$ linearly independent in $V)$. By conditioning,

$$\begin{aligned}&\mathbb{P}(Z_1,\dots,Z_s,Y_1,\dots,Y_r\text{ linearly independent in }V)\\&\quad=\mathbb{P}(Y_r\in V)\mathbb{P}(Y_{r-1}\in V,Y_{r-1}\notin\langle Y_r\rangle\mid Y_r\in V)\\&\qquad\times\cdots\times\mathbb{P}(Y_1\in V,Y_1\notin\langle Y_2,\dots,Y_r\rangle\mid Y_2,\dots,Y_r\text{ lin. in }V)\\&\qquad\times\cdots\times\mathbb{P}(Z_1\in V,Z_1\notin\langle Z_2,\dots,Z_r,Y_1,\dots,Y_r\rangle\mid Z_2,\dots,Z_s,Y_1,\dots,Y_r\text{ lin. in }V).\end{aligned}$$

We first estimate the terms involving Y_i. By Lemma 2.3

$$\begin{aligned}&\mathbb{P}(Y_i\in V,Y_i\notin\langle Y_{i+1},\dots,Y_r\rangle\mid Y_{i+1},\dots Y_r\text{ lin. in }V)\\&\quad\geqslant\mathbb{P}(Y_i\in V)-(1-\alpha')^{n-(r-i)}\\&\quad\geqslant\frac{3}{2}\mathbb{P}(X_i\in V)-(1-\alpha_n')^{n-(r-i)}\\&\quad\geqslant\frac{3}{2}(1-\alpha_n)^{d_{\text{comb}}}-(1-\alpha_n')^{n-(r-i)}\\&\quad\geqslant\frac{3}{2}(1-\alpha_n)^{d_{\text{comb}}}(1-(1-\alpha_n)^{n/256-d_{\text{comb}}}),\end{aligned}$$

where we used that $\alpha_n'=\alpha_n/64$ and $n-r\geqslant(1-\delta_1)n\geqslant n/2$.

Similarly, the terms involving Z_i can be estimated as

$$\begin{aligned}&\mathbb{P}(Z_i\in V,Z_i\notin\langle Z_{i+1},\dots,Z_s,Y_1,\dots,Y_r\rangle\mid Z_{i+1},\dots,Z_s,Y_1,\dots,Y_r)\\&\quad\geqslant\mathbb{P}(Z_i\in V)-(1-\alpha_n')^{n-(r+s-i)}\\&\quad\geqslant(1-\alpha_n)^{d_{\text{comb}}}-(1-\alpha_n')^{n-(r+s-i)}\\&\quad\geqslant(1-\alpha_n)^{d_{\text{comb}}}-(1-\alpha_n)^{n/256},\end{aligned}$$

where we used that $r+s=n-k-(\lfloor\delta_2 n\rfloor-\lfloor\delta_1 n\rfloor)\geqslant n/2$. So

$$\begin{aligned}&\mathbb{P}(Y_1,\dots,Y_r,Z_1,\dots,Z_s\text{ linearly independent in }V)\\&\quad\geqslant\frac{3}{2}^r(1-\alpha_n)^{(r+s)d_{\text{comb}}}(1-(1-\alpha_n)^{n/256-d_{\text{comb}}})^{r+s}\\&\quad\geqslant\frac{3}{2}^{r-1}(1-\alpha_n)^{(r+s)d_{\text{comb}}},\end{aligned}\tag{A.11}$$

where we used $d_{\text{comb}}\leqslant 2dn$ and d is sufficiently small.

Now we estimate the probability

$$\mathbb{P}(\text{ Span}\{X_1,\dots,X_{n-k}\}=V\wedge Y_1,\dots,Y_r,Z_1,\dots,Z_s\text{ linearly independent in }V)$$

in (A.10). Since $Y_1,\dots,Y_r,Z_1,\dots,Z_s$ are linearly independent in V and $\text{Span}\{X_1,\dots,X_{n-k}\}=V$, there exist $n-k-r-s$ vectors $X_{i_1},\dots,X_{i_{n-k-r-s}}$ which together with $Y_1,\dots,Y_r,Z_1,\dots,Z_s$ are a basis for V. With a loss of a factor $\binom{n-k}{r+s}$ in probability, we can assume that

$$\text{Span}\{\{Y_i\}_1^r,\{Z_i\}_1^s,\{X_i\}_{r+s+1}^{n-k}\}=V,$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

and the remaining vectors $X_1, \dots, X_{r+s}$ belong to V. Thus,

$$\begin{aligned}
&\mathbb{P}(\text{ Span}\{X_1, \dots, X_{n-k}\} = V \wedge Y_1, \dots, Y_r, Z_1, \dots, Z_s \text{ linearly independent in } V) \\
&\quad \leqslant \binom{n-k}{r+s} \mathbb{P}(\text{ Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V \wedge X_1, \dots, X_{r+s} \in V) \\
&\quad \leqslant \binom{n-k}{r+s} \mathbb{P}(\text{ Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V) \mathbb{P}(X_1, \dots, X_{r+s} \in V) \\
&\quad \leqslant \binom{n-k}{r+s} \mathbb{P}(\text{ Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V)(1-\alpha_n)^{(r+s)(d_{\text{comb}}-1/n)}. \qquad \text{(A.12)}
\end{aligned}$$

Putting (A.10), (A.11) and (A.12) together,

$$\begin{aligned}
&\mathbb{P}(\text{ Span}\{X_1, \dots, X_{n-k}\} = V) \\
&\quad = \frac{\mathbb{P}(\text{ Span}\{X_1, \dots, X_{n-k}\} = V \wedge Y_1, \dots, Y_r, Z_1, \dots, Z_s \text{ linearly independent in } V)}{\mathbb{P}(Y_1, \dots, Y_r, Z_1, \dots, Z_s \text{ linearly independent in } V)} \\
&\quad \leqslant \frac{3}{2}^{-r+1} (1-\alpha_n)^{-(r+s)d_{\text{comb}}} \binom{n-k}{r+s} \\
&\qquad \times \mathbb{P}(\text{ Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V)(1-\alpha_n)^{(r+s)(d_{\text{comb}}-1/n)} \\
&\quad \leqslant \frac{3}{2}^{-r/2} \binom{n-k}{r+s} \mathbb{P}(\text{ Span}\{\{Y_i\}_1^r, \{Z_i\}_1^s, \{X_i\}_{r+s+1}^{n-k}\} = V).
\end{aligned}$$

□

We remark that our proof above follows [16, Section 4]. The treatment of [8] is similar but the author oversimplified the process by relying on the aforementioned incorrect result [8, Proposition 2.3]. We now conclude the main result.

Proof of Theorem A.1. Let $\mathcal{E}_{n-k,\text{dense}}, \mathcal{E}_{n-k,\text{semi-sat}}, \mathcal{E}_{n-k,\text{unsat}}$ be the events introduced in (A.4), (A.6) and (A.8). By definition, on these events, if $\text{codim}\,(W_{n-k}) = k_0$, then

$$\left| \mathbb{P}(X \in W_{n-k}) - \frac{1}{q^{k_0}} \right| \leqslant e^{-d\alpha_n n}.$$

□

Next we give a proof of Theorem A.4. The statement is clearly equivalent to Theorem A.1 if $k > u$. In what follows we assume $k \leqslant u$.

Proof of Theorem A.4. By Proposition A.7, with probability at least $1 - e^{-c\alpha_n n}$, the subspace $\langle X_1, \dots, X_{n-k} \rangle$ is not δ-sparse, and hence $\langle X_1, \dots, X_{n+u-k} \rangle$ is also not δ-sparse on this event.

For the semi-saturated subspace, the conclusion of Proposition A.10 continues to hold using Lemma A.9. Indeed, with the same choice of parameters, by the proof of Proposition of A.10,

$$\begin{aligned}
\mathbb{P}(\mathcal{F}_{n+u-k,k_0,\text{semi-sat}}) &= \sum_{V \text{semi-sat}} \mathbb{P}(W_{n+u-k} = V) \\
&\leqslant \sum_{V \text{semi-sat}} \mathbb{P}(X_1, \dots, X_{n+u-k} \in V) \\
&\leqslant \sum_{V \text{semi-sat}} \mathbb{P}(X_1, \dots, X_{n-k} \in V) \\
&\leqslant e^{-n}.
\end{aligned}$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Finally, for unsaturated subspaces, by the same method we can show the following analogue of Proposition A.12 with the same parameters

$$\mathbb{P}(\text{ Span}\{X_1,\dots,X_{n+u-k}\} \text{ unsaturated and of dim. between } r+s \text{ and } n) \leqslant \frac{3}{2}^{-r/2}\binom{n+u-k}{r+s}. \tag{A.13}$$

Indeed, to justify this result we just use the same swapping method of Theorem A.13; the only difference is that there are $\binom{n+u-k}{r+s}$ ways to choose the $X_1,\dots,X_{r+s}$ in (A.12). The bound (A.13) is again smaller than $(3/2)^{-\delta_1 n/4}$ if $u \leqslant \eta n$ with η sufficiently small compared to δ_1. □

Part II. Proofs of the lemmas

Here we sketch the proof of Lemma A.9, Lemma A.11 and Theorem A.15 by following [8].

Recall that $\mathrm{tr} : \mathbf{F}_q \to \mathbf{F}_p$ is the field trace, which gives rise to the isomorphism between $\mathbf{F}_q$ and $\widehat{\mathbf{F}}_q$ by $x \to e_p(\mathrm{tr}(tx)) = \exp(2\pi i \mathrm{tr}(tx)/p)$ (so we will identify $\widehat{\mathbf{F}}_q$ with $\mathbf{F}_q$). Let μ be a probability measure on $\mathbf{F}_q$. The Fourier transform of μ is

$$\widehat{\mu}(x) = \sum_{t\in\mathbf{F}_q} \mu(t) e_p(\mathrm{tr}(xt)) = \mathbb{E} e_p(\mathrm{tr}(x\xi)), \quad \text{where } \xi \text{ has distribution } \mu.$$

We define the additive spectrum by

$$\mathrm{Spec}_{1-\varepsilon}\,\mu := \{x \in \mathbf{F}_q, |\widehat{\mu}(x)| \geqslant 1-\varepsilon\}.$$

We will be using the following two important results.

Theorem 3.3 (Kneser, Theorem 5.5 of [15]). *Let $A, B \subset Z$ be finite subsets of an abelian group Z. Then*

$$|A+B| + |\,\mathrm{Sym}\,(A+B)| \geqslant |A| + |B|,$$

where $\mathrm{Sym}\,(X) = \{h \in Z : h + X = X\}$.

Note that $\mathrm{Sym}\,(X)$ is a symmetric additive subgroup of Z. As $\mathrm{Sym}\,(A_1+\cdots+A_k)$ is increasing in k, iterating the result we obtain

Corollary A.14.

$$|A_1+\cdots+A_k| + (k-1)|\,\mathrm{Sym}\,(A_1+\cdots+A_k)| \geqslant |A_1| + \cdots + |A_k|.$$

To start with, we prove the following version of the classical Erdős–Littlewood–Offord result in the finite field, which was used in the proof of Proposition A.7.

Theorem A.15 (Theorem 2.4 of [8]). *Let $X \in \mathbf{F}_q^n$ be a random vector with i.i.d. entries taken from an α-balanced distribution. Suppose $w \in \mathbf{F}_q^n$ has at least m non-zero coefficients. Then we have*

$$\left|\mathbb{P}(X\cdot w = r) - \frac{1}{q}\right| \leqslant \frac{2}{\sqrt{\alpha m}}.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Proof. Let $\xi_1, \dots, \xi_n$ denote the entries of X, and let $w_1, \dots, w_n$ denote the components of w. By $\mathbf{F}_p$-linearity of the field trace, we can write

$$1_{X\cdot w=r} = \frac{1}{q}\sum_{t\in\mathbf{F}_q} e_p\left(\mathrm{tr}\left(\sum_l \xi_l w_l\right)\right) e_p(-\mathrm{tr}(rt)).$$

By independence of the $\{\xi_i\}_1^n$, we can therefore write

$$\mathbb{P}(X\cdot w = r) = \mathbb{E}(1_{X\cdot w=r}) = \frac{1}{q}\sum_{t\in\mathbf{F}_q}\prod_{l=1}^{n}\mathbb{E}e_p(\mathrm{tr}(\xi_l w_l t))e_p(-\mathrm{tr}(rt)).$$

By the triangle inequality,

$$\left|\mathbb{P}(X\cdot w = r) - \frac{1}{q}\right| \leqslant \frac{1}{q}\sum_{t\in\mathbf{F}_q, t\neq 0}\prod_{l=1}^{n}|\mathbb{E}e_p(\mathrm{tr}(\xi_l w_l t))| = \frac{1}{q}\sum_{t\in\mathbf{F}_q, t\neq 0}\prod_{l=1}^{n}|\widehat{\mu}(w_l t)|.$$

Define $\psi(t) = 1 - |\widehat{\mu}(t)|^2$. Using $|x| \leqslant \exp(-(1-x^2)/2)$ for $|x| \leqslant 1$,

$$\left|\mathbb{P}(X\cdot w = r) - \frac{1}{q}\right| \leqslant \frac{1}{q}\sum_{t\in\mathbf{F}_q, t\neq 0}\exp\left(-\frac{1}{2}\sum_{l=1}^{n}\psi(w_l t)\right).$$

Set $f(t) = \sum_l \psi(w_l t)$. Then

$$\left|\mathbb{P}(X\cdot w = r) - \frac{1}{q}\right| \leqslant \frac{1}{2}\int_0^\infty \frac{1}{q}|\{t\neq 0, f(t)\leqslant v\}|e^{-v/2}dv = \frac{1}{2}\int_0^\infty \frac{1}{q}|T'(v)|e^{-v/2}dv, \tag{A.14}$$

where the level sets are defined as

$$T(v) := \{t, f(t)\leqslant v\} \quad \text{and} \quad T'(v) = T(v)\backslash\{0\}.$$

Claim A.16. *For any $v > 0$ we have*

$$kT(v) = T(v) + \cdots + T(v) \subset T(k^2 v).$$

Proof. It suffices to show that for any $\beta_1, \dots, \beta_k \in \mathbf{F}_q$

$$\psi(\beta_1 + \cdots + \beta_k) \leqslant k(\psi(\beta_1) + \cdots + \psi(\beta_k)).$$

Indeed, by definition of ψ, after squaring, the above is equivalent to

$$1 - \sum_{t_1,t_2\in\mathbf{F}_q}\mu(t_1)\mu(-t_2)\cos\left(\frac{2\pi}{p}\mathrm{tr}((t_1+t_2)(\beta_1+\cdots+\beta_k))\right)$$
$$\leqslant k^2 - k\sum_i\sum_{t_1,t_2\in\mathbf{F}_q}\mu(t_1)\mu(-t_2)\cos\left(\frac{2\pi}{p}\mathrm{tr}((t_1+t_2)\beta_i)\right).$$

Hence it suffices to observe that, for all real numbers $(\beta_i)_1^k$,

$$\cos(\beta_1 + \cdots + \beta_k) \geqslant k\sum\cos\beta_i - k^2 + 1,$$

which we justify now. If, for even a single β_i, $\cos(\beta_i) \leqslant 0$, then the largest value that can be attained on the right-hand side is $1-k$, from which it follows that the equality holds. Hence by periodicity, we may assume that all these $\beta_i \in (-\pi/2, \pi/2)$. The function

$$(\beta_i)_1^k \mapsto \cos(\beta_1 + \cdots + \beta_k) - k\sum\cos(\beta_i)$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

is smooth and its only local minimum in the domain considered can be checked to occur at 0, at which value equality is attained. □

By Corollary A.14,

$$kT(v) \leqslant |T(k^2 v)| + (k-1)\,\mathrm{Sym}\,(T(v) + \cdots + T(v)). \tag{A.15}$$

We next claim that if $k^2 v < \alpha_n m$, *i.e.* $k < \sqrt{\alpha_n m / v}$, then $T(k^2 v)$ contains no non-trivial additive subgroup H of $\mathbf{F}_q$, so $|\,\mathrm{Sym}\,(T(v) + \cdots + T(v))| = 1$. Indeed, fix a subgroup H. Then

$$|H|^{-1} \sum_{t \in H} f(t) = \sum_{l=1}^{n} |H|^{-1} \sum_{t \in H} \psi(w_l t) = \sum_{l=1}^{n} |H|^{-1} \sum_{t \in H} (1 - |\widehat{\mu}(w_l t)|^2).$$

By the Fourier inversion formula, and by the α-balanced assumption on the distribution μ,

$$|H|^{-1} \sum_{t \in H} (1 - |\widehat{\mu}(w_l t)|^2) = \sum_{s_1, s_2 \in \mathbf{F}_q} \mu(s_1)\mu(s_2) 1_{H^\perp}(w_l(s_1 - s_2)) \leqslant 1 - \alpha_n.$$

Since at least m of the choices w_l are non-zero,

$$|H|^{-1} \sum_{t} f(t) \geqslant \alpha_n m.$$

Thus there exists $t \in H$ such that $f(t) \geqslant \alpha_n m$, so $H \not\subset T(k^2 v)$. So by (A.15) we have

$$|T'(v)| \leqslant \sqrt{\frac{v}{\alpha_n m}} |T'(\alpha_n m)| \leqslant \sqrt{\frac{v}{\alpha_n m}} q \quad \text{for all } v \leqslant \alpha_n m.$$

Substitute back to (A.14). We obtain

$$\left| \mathbb{P}(X \cdot w = r) - \frac{1}{q} \right| \leqslant \frac{1}{2} \frac{1}{\sqrt{\alpha_n m}} \int_0^\infty \sqrt{v} e^{-v/2} dv + e^{-\alpha_n m/2}.$$ □

Now we prove the other lemmas that were used in the treatment of semi-saturated and unsaturated subspaces.

Proof of Lemma A.9. Note that V is not δ-sparse. Let $k_0 = \mathrm{codim}\,(V)$, and let $\xi_1, \ldots, \xi_n$ denote the entries of X. We have

$$\mathbb{P}(X \in V) = \mathbb{E} q^{-k_0} \sum_{t \in V^\perp} e_p\left(\mathrm{tr}\left(\sum_l \xi_l t_l\right)\right) = q^{-k_0} \sum_{t \in V^\perp} \prod_{l=1}^{n} \mathbb{E} e_p(\mathrm{tr}(\xi_l t_l)) = q^{-k_0} \sum_{t \in V^\perp} \prod_{l=1}^{n} \widehat{\mu}(t_l),$$

where $t_1, \ldots, t_n$ denote the entries of t, and where we used the fact that

$$\sum_{t \in V^\perp} e_p\left(\mathrm{tr}\left(\sum_l \xi_l t_l\right)\right) = 0 \quad \text{if and only if } X \notin V.$$

By the triangle inequality,

$$|\mathbb{P}(X \in V) - q^{-k_0}| \leqslant q^{-k_0} \sum_{t \in V^\perp, t \neq 0} \prod_{l=1}^{n} |\widehat{\mu}(t_l)|.$$

By the pigeonhole principle, for some $t \in V^\perp$, $t \neq 0$,

$$e^{-d\alpha_n n} \leqslant |\mathbb{P}(X \in V) - q^{-k_0}| \leqslant \prod_{l=1}^{n} |\widehat{\mu}(t_l)|.$$

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Again, using

$$|x| \leqslant \exp\left(-\frac{1}{2}(1-x^2)\right) \quad \text{for } |x| \leqslant 1,$$

we have

$$\sum_{l=1}^{n} 1 - |\widehat{\mu}(t_l)|^2 \leqslant 2d\alpha_n n.$$

By averaging, there exists an index set $\sigma \subset [n]$ with $|\sigma| \geqslant (1-\delta/2)n$ and $|\widehat{\mu}(t_l)| \geqslant 1 - 10d\delta^{-1}\alpha_n$ for $l \in \sigma$. In other words, for all $l \in \sigma$,

$$t_l \in \mathrm{Spec}_{1-10d\delta^{-1}\alpha_n}\, \mu.$$

Claim A.17. *The set* $\mathrm{Spec}_{1-\alpha_n/2}$ *does not contain any non-trivial additive subgroup* H *of* $\mathbf{F}_q$.

Proof. By Fourier's inversion formula,

$$(1-\alpha_n/2)^2 |H \cap \mathrm{Spec}_{1-\alpha_n/2}(\mu)| \leqslant \sum_{s\in H} |\widehat{\mu}(s)|^2 \leqslant |H|(1-\alpha_n),$$

where in the last estimate we used the fact that μ is α_n-balanced. □

Set $k := \lfloor \beta^{-1} \rfloor$ and choose d so that

$$d \leqslant k^{-2}\delta/5. \tag{A.16}$$

Then

$$\mathrm{Spec}_{1-10d\delta^{-1}\alpha_n} \subset \mathrm{Spec}_{1-2k^{-2}\alpha_n}(\mu) := A.$$

We next claim that

$$|A\backslash\{0\}| \leqslant \beta q. \tag{A.17}$$

Indeed, this is because by applying Cauchy–Schwarz,

$$kA \subset \mathrm{Spec}_{1-2\alpha_n}(\mu).$$

Furthermore,

$$\mathrm{Sym}(kA) \subset (kA) - (kA) = 2kA \subset \mathrm{Spec}_{1-\alpha_n/2}(\mu).$$

By Claim A.17, $\mathrm{Sym}(kA)$ is trivially $\{0\}$. So by Corollary A.14

$$k|A| \leqslant |kA| + (k-1) \leqslant q + (k-1),$$

proving (A.17).

Finally, let $\mathcal{R}$ be the set of non-zero t in $\mathbf{F}_q^n$ which have at least $(1-\delta/2)n$ components t_l in $\mathrm{Spec}_{1-10d\delta^{-1}\alpha}$. By (A.17), as $t \perp V$ and V is not δ-sparse, at least $\delta/2$ of the components ξ_l are non-zero, so that

$$|\mathcal{R}| \leqslant 2^n(\beta q)^{\delta n/2} q^{n-\delta n/2} \leqslant (2\beta^{\delta/2}q)^n.$$

□

To prove Lemma A.11, we use the following rather standard Halász-type construction from [8, Proposition 3.6] (see also [16, Lemma 7.1] or [3]).

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Proposition A.18. *There is a probability distribution $\nu : \mathbf{F}_q \to [0,1]$ depending on μ and α such that the following properties hold with $t = (t_1, \dots, t_n)$ and*

$$f(t) := \prod_{l=1}^{n} |\widehat{\mu}(t_l)|, g(t) := \prod_{l=1}^{n} |\widehat{\nu}(t_l)|.$$

- *For all $0 < u < 1$ we have $4F(u) \subset G(u)$, where*

$$F(u) = \{t \in \mathbf{F}_q^n, |f(t)| > u\} \quad \text{and} \quad G(u) = \{t \in \mathbf{F}_q^n, |g(t)| > u\}.$$

- *For all $t \in V^{\perp}$,*

$$f(t) \leqslant g^{16}(t).$$

- *For all t,*

$$\widehat{\nu}(t) \geqslant 0.$$

- *ν is α_n'-balanced with $\alpha_n' = \alpha_n/64$.*

Proof of Lemma A.11. Note that

$$\mathbb{P}(Y \in V) - q^{-k} = q^{-k} \sum_{t \in V^{\perp}, t \neq 0} \prod_{l=1}^{n} \widehat{\nu}(t_l) = q^{-k} \sum_{t \in V^{\perp}, t \neq 0} g(t).$$

Thus, to show

$$|\mathbb{P}(X \in V) - q^{-k}| \leqslant \left(\frac{1}{2} + o(1)\right) |\mathbb{P}(Y \in V) - q^{-k}| \quad \text{as } \widehat{\nu} \geqslant 0,$$

it suffices to show that

$$\sum_{t \in V^{\perp}, t \neq 0} f(t) \leqslant \left(\frac{1}{2} + o(1)\right) \sum_{t \in V^{\perp}, t \neq 0} g(t).$$

Let $\varepsilon > 0$ be a parameter to be sent to 0. We write

$$\sum_{t \in V^{\perp}, t \neq 0} f(t) = \sum_{t \in V^{\perp}, t \neq 0, f(t) < \varepsilon} f(t) + \sum_{t \in V^{\perp}, t \neq 0, f(t) \geqslant \varepsilon} f(t) := \sum_{< \varepsilon} (f) + \sum_{\geqslant \varepsilon} (f).$$

As $f(t) \leqslant g(t)^{16}$, we have

$$\sum_{< \varepsilon} (f) \leqslant \varepsilon^{15/16} \sum_{< \varepsilon} (g) < \left(\frac{1}{2} + o(1)\right) \sum_{< \varepsilon} (g).$$

We also write

$$\sum_{\geqslant \varepsilon} (f) = \int_{\varepsilon}^{\infty} |F'(u)| du + \varepsilon |F'(\varepsilon)|,$$

where

$$F'(u) = F(u) \backslash \{0\} = \{t \in V^{\perp}, t \neq 0, |f(t)| > u\}.$$

Claim A.19. *With $\varepsilon = \exp(-\frac{1}{2}\alpha_n' \delta n)$, the set $G(\varepsilon)$ does not contain any non-trivial additive subgroup $H \leqslant V^{\perp}$. In particular, as $G(u)$ is decreasing, the same happens for any $u \geqslant \varepsilon$.*

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press

Proof. Clearly we can assume $H \cong \mathbb{Z}/p\mathbb{Z}$. Suppose $w = (w_1, \dots, w_n) \in V^\perp$ generates H. Since V is unsaturated (and hence not δ-sparse), w has at least δn non-zero components. Define

$$h(t) := \sum_{l=1}^{n} 1 - |\widehat{\nu}(t_l)|^2, \quad t \in H.$$

We can also write

$$h(t) := \sum_{i=1}^{k} 1 - |\widehat{\nu}(tw_{l_i})|^2, \quad t \in \mathbb{Z}/p\mathbb{Z},$$

where w_{l_i} are non-zero. By Fourier's inversion formula, and as ν is α_n'-balanced,

$$\sum_{t \in \mathbb{Z}/p\mathbb{Z}} |\widehat{\nu}(tw_{l_i})|^2 \leqslant p(1 - \alpha_n').$$

So

$$\sum_{t \in H} h(t) \geqslant p\alpha_n' k \geqslant p\alpha_n' \delta n.$$

By the pigeonhole principle, there exists $t \in H$ such that $h(t) \geqslant \alpha_n' \delta n$. On the other hand,

$$g(t) = \prod_{l=1}^{n} |\widehat{\nu}(t_l)| \leqslant \exp\left(-\frac{1}{2}\sum_{l=1}^{n} 1 - |\widehat{\nu}(t_l)|^2\right) = \exp\left(-\frac{1}{2}h(t)\right) \leqslant \exp\left(-\frac{1}{2}\alpha_n'\delta n\right) = \varepsilon.$$

We have thus found an element $t \in H$ which lies outside $G(\varepsilon)$. □

Let $u \geqslant \varepsilon$. By Proposition A.18, $\mathrm{Sym}\,(2F(u)) \subset 4F(u) \subset G(u)$. Thus, by Claim A.19, the additive subgroup $\mathrm{Sym}\,(2F(u))$ must be trivial, so by Corollary A.14

$$2|F(u)| \leqslant |\,\mathrm{Sym}\,(F(u) + F(u))| + |F(u) + F(u)| \leqslant 1 + |G(u)|.$$

It thus follows that for all $u \geqslant \varepsilon$ we have $2|F'(u)| \leqslant |G'(u)|$. So

$$\int_{\varepsilon}^{\infty} |F'(u)|du + \varepsilon|F'(\varepsilon)| \leqslant \frac{1}{2}\left(\int_{\varepsilon}^{\infty} |G'(u)|du + \varepsilon|G'(\varepsilon)|\right),$$

completing the proof of Lemma A.11. □

Cite this article: Nguyen HH and Paquette E (2020). Surjectivity of near-square random matrices. *Combinatorics, Probability and Computing* **29**, 267–292. https://doi.org/10.1017/S0963548319000348

https://doi.org/10.1017/S0963548319000348 Published online by Cambridge University Press