APPROXIMATELY HADAMARD MATRICES AND RIESZ BASES IN RANDOM FRAMES

XIAOYU DONG AND MARK RUDELSON

ABSTRACT. An $n \times n$ matrix with ± 1 entries which acts on $\mathbb{R}^n$ as a scaled isometry is called Hadamard. Such matrices exist in some, but not all dimensions. Combining number-theoretic and probabilistic tools we construct matrices with ± 1 entries which act as approximate scaled isometries in $\mathbb{R}^n$ for all $n \in \mathbb{N}$. More precisely, the matrices we construct have condition numbers bounded by a constant independent of n.

Using this construction, we establish a phase transition for the probability that a random frame contains a Riesz basis. Namely, we show that a random frame in $\mathbb{R}^n$ formed by N vectors with independent identically distributed coordinate having a non-degenerate symmetric distribution contains many Riesz bases with high probability provided that $N \geq \exp(Cn)$. On the other hand, we prove that if the entries are subgaussian, then a random frame fails to contain a Riesz basis with probability close to 1 whenever $N \leq \exp(cn)$, where $c < C$ are constants depending on the distribution of the entries.

1. Introduction and main results

Let $n < N$ be natural numbers. A set of vectors $X_1, \dots, X_N \in \mathbb{R}^n$ is called a *frame* if

$$K(n,N) \|x\|_2^2 \leq \sum_{j=1}^{N} \langle x, X_j \rangle^2 \leq RK(n,N) \|x\|_2^2 \tag{1.1}$$

for all $x \in \mathbb{R}^n$. Here $R \geq 1$ is an absolute constant called the frame constant, and $K(n,N) > 0$ is some function of n and N. The notation $\|x\|_2$ stands for the Euclidean norm of the vector $x = (x_1, \dots, x_n)$:

$$\|x\|_2 = \left(\sum_{j=1}^{n} x_j^2 \right)^{1/2}.$$

In the last 40 years, frame theory became a well-developed area of applied mathematics, see [4], [5], [6], and the references therein. A frame can intuitively be regarded as overcomplete basis in $\mathbb{R}^n$. Because of this property, frames became a valuable tool in signal transmission. A signal which is viewed as an

Date: March 23, 2023.

2000 *Mathematics Subject Classification.* 60B20.

Research supported in part by NSF grant DMS 2054408 and by a fellowship from the Simons Foundation.

n-dimensional vector can be encoded by the sequence of its inner products with the frame vectors. If this sequence is transmitted over a communication line, then the original signal can be reconstructed even if part of the coefficients is lost or corrupted in the process of transmission. Moreover, this encoding is robust, which means that if the inner products are evaluated with some noise, then the reconstructed version will be close to the original one with the error depending on the noise magnitude.

One of the most popular classes of frames in algorithmic applications is the set of random frames. Such frames became also the method of choice in compressed sensing where one needs to reconstruct a low complexity signal from a small number of linear measurements, see, e.g., [21]. For example, if complexity is measured as the size of the support, and the support itself is unknown, the random frames provide robust recovery with optimal or almost optimal theoretical guarantees.

To construct a random frame, consider a random vector $X \in \mathbb{R}^n$ with centered uncorrelated coordinates of unit variance. In other words, assume that $\mathbb{E}\, X = 0$ and $\mathbb{E}\, XX^\top = I_n$. Let vectors $X_1, \dots, X_N$ be independent copies of X. The Law of Large Numbers implies that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} X_j X_j^\top = I_n \quad \text{a.s.}$$

and thus, with probability close to 1,

$$(1-\varepsilon)\,\|x\|_2^2 \le \sum_{j=1}^{N} \langle x, X_j\rangle^2 \le (1+\varepsilon)\,\|x\|_2^2$$

for all $x \in \mathbb{R}^n$ provided that $N = N(\varepsilon)$ is sufficiently large.

Another, trivial way to construct a frame is to take several bases in $\mathbb{R}^n$ and concatenate them. This allows an exact reconstruction of the transmitted signal if the number of corrupted coordinates is relatively small. Indeed, one can reconstruct the original vector from the set of transmitted coordinates for each basis separately and keep the copy which is repeated many times. While in practice the random frames perform better than such concatenated bases, it leads to a question whether a random frame contains a copy or copies of a nice basis. More precisely, a sequence of n vectors $v_1, \dots, v_n \in \mathbb{R}^n$ is called a Riesz basis if it possesses the frame property (1.1). This property ensures that the reconstruction is robust, i.e., that the reconstructed vector is close to the original one if the coordinates are distorted by adding a small noise. These considerations lead to a natural question of determining the values of N for which a random frame $\{X_1, \dots, X_N\} \subset \mathbb{R}^n$ contains one or many Riesz bases with high probability.

This problem can be conveniently translated to the language of random matrices. Namely, for an $n \times N$ matrix A, define its singular values as

$$s_{\max}(A) = s_1(A) \ge s_2(A) \ge \cdots \ge s_n(W) = s_{\min}(A) \ge 0,$$

where $s_j(A) = \sqrt{\lambda_j(AA^\top)}$, and $\lambda_1(AA^\top), \dots, \lambda_n(AA^\top)$ are eigenvalues of $AA^\top$ arranged in the decreasing order. Also, define the condition number of A as

$$\kappa(A) = \frac{s_{\max}(A)}{s_{\min}(A)}$$

using the convention that $\kappa(A) = \infty$ whenever $s_{\min}(A) = 0$. With this notation, the frame property (1.1) can be rewritten as $\kappa(A_{n,N}) \le C$ where $A_{n,N}$ is the $n \times N$ matrix with columns $X_1, \dots, X_N$. Thus, the problem of existence of a Riesz basis in a random frame can be recast as the question of existence of one or many well-conditioned square $n \times n$ submatrices of an $n \times N$ random matrix $A_{n,N}$ with i.i.d. entries. Our first main result shows that the probability of finding such a submatrix undergoes a phase transition when N is exponential in terms of n. Since the upper and the lower bound hold under somewhat different assumptions, we formulate them separately.

Denote by $[N]$ the set $\{1, \dots, N\}$. Let A be an $n \times N$ matrix. If $I \subset [N]$, denote by A_I the submatix of A whose columns belong to I. The following theorem shows that if N is exponential in n, then with high probability, the $n \times N$ random matrix has many square submatrices with uniformly bounded condition numbers. In the language of frames, it means that a random frame with exponentially many vectors contains a large number of Riesz bases whose frame constants are uniformly bounded.

Theorem 1.1. *Let A be an $n \times N$ matrix with i.i.d. symmetric non-degenerate entries. Then there exist constants $c, C, \alpha, \beta > 0$ depending on the distribution of entries of A with the following property.*
Assume that

$$N \ge \exp(Cn).$$

Then there exists

$$L \ge \exp(cn)$$

such that

$$\begin{aligned} &\mathbb{P}\big(\text{exist disjoint subsets } I_1, \dots, I_L \text{ of } [N] \text{ with} \\ &\qquad |I_j| = n \text{ and } \kappa(A_{I_j}) < \alpha \text{ for all } j \in [L]\big) \\ &\ge 1 - \exp\left(-\exp(\beta n)\right). \end{aligned}$$

The strategy of proving Theorem 1.1 relies on using a certain deterministic $n \times n$ matrix V having a bounded condition number. Denote by $\mathrm{Col}_j(M)$ the j-th column of the matrix M. We partition the set of integers $[N]$ into n subsets $I_1, \dots, I_n$ of approximately the same size and show that with high probability, the set $\{\mathrm{Col}_i(A)\}_{i \in I_j}$ contains many columns close to $\mathrm{Col}_j(V)$. Condition on the event that such columns exist and form an $n \times n$ matrix B taking one column from each set. Then conditionally this matrix can be viewed as a noisy version of the matrix V. This allows to show that with high probability, the matrix B has a bounded condition number as well.

The key to this strategy is a successful choice of the pattern matrix V. Since we strive to prove Theorem 1.1 under minimal assumptions, the choice of V becomes a non-trivial task. Indeed, the requirement that a column of A can be close to a column of V with a non-negligible probability forces us to look for matrices V whose entries are in the support of the distribution of an entry of A. The latter can be as small as two points, a and $-a$ because of the symmetry assumption. Thus, we need to to construct V as a scaled copy of a matrix with ± 1 entries. Such matrices are known in some cases. For instance, the condition number of any Hadamard matrix is one. An $n \times n$ matrix H is called Hadamard if $n^{-1/2}H$ is an isometry. The earliest result on the existence of Hadamard matrices was probably proved by Sylvester [20] who showed that Hadamard matrices exist for dimension 2^k where k is any nonnegative integer (these matrices are now called Wash since their rows are Walsh functions). Hadamard matrices is a well-studied subject, and a number of constructions of such matrices are available, see e.g., the books [1], [12], and the references therein. In particular, Wallis [23] proved that if $p > 3$ is an integer, then there exists an Hadamard matrix of order $2^t p$, where $t = \lfloor 2\log_2(p-3) \rfloor$. Craigen [7] improved Wallis's result by showing that for any odd number p, there exists an Hadamard matrix of order $2^t p$, where $t = 4\left\lceil \frac{1}{6}\log_2((p-1)/2) \right\rceil + 2$. Recently, de Launey [10] studied the asymptotic existence of Hadamard matrices and concluded that for any $\epsilon > 0$, the set of odd numbers k for which there is a Hadamard matrix of order $k2^{2+[\epsilon \log_2(k)]}$ always has positive density in the set of natural numbers. Yet, the dimensions in which Hadamard matrices were constructed are rare.

This leads us to a task of constructing *approximately Hadamard matrices*, i.e., matrices with ± 1 entries and bounded condition numbers. Some constructions of matrices with properties simlar to Hadamard's are available. For example, Banica, Nechita, and Życzkowski [2] defined an almost Hadamard matrix to be a N dimensional real square matrix H, such that $H/\sqrt{N}$ is orthogonal, and is a local maximum of the ℓ_1-norm of the entries on the orthogonal group $O(N)$. They showed the existence of almost Hadamard matrices under some special assumptions. There is also a notion of quasi-Hadamard matrix [2, 15], which is defined as a square matrix with $\{-1, 1\}$ entries that maximizes the absolute value of the determinant, but there are only very limited results on the existence of those matrices. In summary, no existing construction is directly related to our purpose.

The second main result of the paper is the following theorem asserting the existence of an approximately Hadamard matrix in all dimensions.

Theorem 1.2. *There exist constants $0 < c < C$ such that for any $n \in \mathbb{N}$, one can find an $n \times n$ matrix V with ± 1 entries satisfying*

$$c\sqrt{n} \le s_{\min}(V) \le s_{\max}(V) \le C\sqrt{n}.$$

The proof of Theorem 1.2 relies on Vinogradov's theorem from analytic number theory and combines number-theoretic and probabilistic ideas. The

details are presented in Section 2. After Theorem 1.2 is proved, we prove Theorem 1.1 in Section 3.

The conclusion of Theorem 1.1 holds under minimal assumptions on the distribution of entries. If we assume that the entries of the matrix are subgaussian, then the bound of Theorem 1.1 becomes sharp. Recall that a random variable X is called subgaussian if there is $a > 0$ such that

$$\mathbb{E} \exp\left(\frac{X^2}{a^2}\right) \leq 2.$$

If X is subgaussian then the smallest number a having this property is called the subgaussian norm of X and denoted $\|X\|_{\psi_2}$. Subgaussian random variables form a large family containing many naturally arising ones, see, e.g. [22].

The next theorem shows that finding a submatrix with a bounded condition number requires an exponential number of columns for matrices with subgaussian entries.

Theorem 1.3. *Let X be a centered subgaussian random variable. Then there exist $C, c, \tilde{c}, t_0 > 0$ depending only on $\frac{\|X\|_{\psi_2}}{\|X\|_2}$ with the following property. Let $t > t_0$, and assume that*

$$N \leq \exp\left(\frac{\tilde{c}}{t^4} n\right).$$

Let A be an $n \times N$ matrix whose entries are independent copies of X. Then

$$\mathbb{P}\left(\exists I \subset [N] \ |I| = n \text{ and } \kappa(A_I) < t\right) \leq \exp\left(-c\frac{n^2}{t^4}\right).$$

We prove Theorem 1.3 in Section 4. Its proof is easier than that of Theorem 1.1 and relies on the Hanson-Wright inequality [19].

Acknowledgment. The second author is grateful to Marcin Bownik for helpful discussions and bringing his attention to the problem. Part of this work was done when the second author visited the Weizmann Institute of Science. He is grateful to the Institute for its hospitality. The authors thank a referee for thoroughly checking the manuscript and correcting many typos.

2. Approximately Hadamard matrices

In this section we construct an $n \times n$ matrix with ± 1 entries whose scaled copy acts on $\mathbb{R}^n$ as an approximate isometry. More precisely, for any sufficiently large n, we construct an $n \times n$ matrix V such that its condition number $\kappa(V)$ is bounded by an absolute constant.

We use standard matrix norms below. Namely, $\|A\|$ stands for the operator norm of an $n \times m$ matrix $A = (a_{i,j})$, and $\|A\|_{\mathrm{HS}}$ stands for its Hilbert-Schmidt or Frobenius norm:

$$\|A\| = \max_{\|x\|_2 = 1} \|Ax\|_2, \quad \text{and} \quad \|A\|_{\mathrm{HS}} = \left(\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^2\right)^{1/2}.$$

We will apply an above mentioned result of Wallis [23] showing that Hadamard matrices exist in dimensions close to n^3.

Lemma 2.1. *There is $l_0 \in \mathbb{N}$ such that for any $l > l_0$, there exists an Hadamard matrix of dimension $m(l)$ with*

$$m(l) = 2^{2\lceil \log_2(l-3)\rceil} l.$$

We will need the following corollary.

Corollary 2.2. *For any $\varepsilon > 0$, there exists $N(\varepsilon)$ such that for any $n > N_0(\varepsilon)$, one can find an even number $m \in [(1-\varepsilon)n, (1+\varepsilon)n]$ for which there exists an Hadamard matrix of size $m \times m$.*

Proof. For any $n > 12$, there exists a unique $k \in \mathbb{N}$ such that $2^{2k}(2^{k-1}+3) < n \le 2^{2(k+1)}(2^k+3)$. Assume first that $2^{2k}(2^{k-1}+3) < n \le 2^{2k}(2^k+3)$. Set

$$m = 2^{2k}\left\lceil \frac{n}{2^{2k}} \right\rceil.$$

By Lemma 2.1, there exists an Hadamard matrix of size $m \times m$. Since

$$1 \le \frac{m}{n} = \frac{\lceil 2^{-2k} n \rceil}{2^{-2k} n},$$

and $2^{-2k} n \ge 2^{k-1} + 3 > (n/2)^{1/3}$, the result follows if we choose $N(\varepsilon)$ sufficiently large.

Since the tensor product of Hadamard matrices is an Hadamard matrix, and there are Hadamard matrices of sizes 2×2 and 4×4, there exist Hadamard matrices of sizes $2m(l)$ and $4m(l)$ for all $l > l_0$. This allows completing the proof of the corollary in the remaining cases when $2^{2k+1}(2^{k-1}+3) < n \le 2^{2k+1}(2^k+3)$ and $2^{2k+2}(2^{k-1}+3) < n \le 2^{2k+2}(2^k+3)$. □

The aim of this section is to construct *approximately Hadamard* matrices in any dimension, i.e. matrices whose condition number is $O(1)$. To this end, we use a construction of approximately Hadamard matrices of a prime size.

Let $q \in \mathbb{N}$ be an odd prime number. For $k \in \mathbb{Z}_q$, denote

$$e_q(k) = \exp\left(2\pi i \frac{k}{q}\right).$$

Define the Fourier transform on $\mathbb{Z}_q$ setting

$$\hat{v}(j) = \sum_{k \in \mathbb{Z}_q} v(k) e_q(jk)$$

for a vector $v \in \mathbb{C}^{\mathbb{Z}_q}$ and $j \in \mathbb{Z}_q$.

Lemma 2.3. *Let q be an odd prime number. Then there exists a vector $u_q \in \{-1,1\}^{\mathbb{Z}_q}$ such that*

$$\left| |\hat{u}_q(j)| - \sqrt{q} \right| \le \sqrt{q}\delta_q \quad \text{for any } j \in \mathbb{Z}_q$$

with $\delta_q = Cq^{-1/4}\sqrt{\log q}$.

Proof. The construction closely follows the one in [14, Proposition 3.2], which in turn originates in [16, Theorem 9.2].

Let $v : \mathbb{Z}_q \to \{-1, 1\}$ be the Legendre symbol (quadratic character mod q). More precisely, let

$$Q = \{k \in \mathbb{Z}_q : \ k = j^2 (\mathrm{mod}\ q) \text{ for some } j \in \mathbb{Z}_q\} \setminus \{0\}$$

be the set of quadratic residues, and set

$$v(k) = \begin{cases} 1, & \text{if } k \in Q; \\ -1, & \text{if } k \in \mathbb{Z}_q \setminus (Q \cup \{0\}); \\ 0, & \text{if } k = 0. \end{cases}$$

Then by a standard result on the Gauss sum, see e.g., [13, Proposition 6.3.2.; p.71], we have

$$|\hat{v}(j)| = \begin{cases} \sqrt{q}, & \text{if } j \in \mathbb{Z}_q \setminus \{0\} \\ 0, & \text{if } j = 0. \end{cases}$$

The difference between v and the desired function u_q is that $v(0) = 0$ and $\hat{v}(0) = 0$. We will perturb v replacing some of its coordinates by -1 to change the value of $\hat{v}(0)$ as required while keeping the other Fourier coefficients close to their original values. To this end, consider a sequence of i.i.d. random variables $\{X_k\}_{k \in Q}$ such that

$$\mathbb{P}(X_k = -1) = q^{-1/2} \quad \text{and} \quad \mathbb{P}(X_k = 1) = 1 - q^{-1/2}.$$

Set

$$u_q(k) = \begin{cases} X_k, & \text{if } k \in Q; \\ -1, & \text{if } k \in \mathbb{Z}_q \setminus Q; \end{cases}$$

Then $u_q : \mathbb{Z}_q \to \{-1, 1\}$, so we only have to check the values of the Fourier coefficients. Let us start with the expectations. We have

$$\begin{aligned} \mathbb{E}\, \hat{u_q}(0) = \mathbb{E}\, \hat{u_q}(0) - \hat{v}(0) &= \sum_{k \in Q} (\mathbb{E}\, X_k - 1) - 1 = -2q^{-1/2}|Q| - 1 \\ &= q^{-1/2} - q^{1/2} - 1, \end{aligned}$$

and

$$\mathbb{E}\, \hat{u_q}(j) - \hat{v}(j) = \sum_{k \in Q} (\mathbb{E}\, X_k - 1) e_q(jk) - 1 = \sum_{k \in Q} (-2q^{-1/2}) e_q(jk) - 1$$

for all $j \in \mathbb{Z}_q \setminus \{0\}$. Evaluation of the last sum is standard, see [8, Ch. 2], or [13, Ch. 6]. Namely,

$$\begin{aligned} \left| 1 + 2 \sum_{k \in Q} e_q(jk) \right|^2 = \left| \sum_{k \in \mathbb{Z}_q} e_q(jk^2) \right|^2 &= \sum_{k,l \in \mathbb{Z}_q} e_q(jk^2) \overline{e_q(jl^2)} \\ &= \sum_{k,l \in \mathbb{Z}_q} e_q\big(j(k+l)(k-l)\big) = q, \end{aligned}$$

where the last equality follows if we fix $k+l$ and sum over $k-l$ first. Thus,

$$|\mathbb{E}\,\hat{u_q}(j) - \hat{v}(j)| \le 2 + q^{-1/2} \quad \text{for any } j \in \mathbb{Z}_q \setminus \{0\},$$

and so $\big|\,|\,\mathbb{E}\,\hat{u_q}(j)| - \sqrt{q}\big| \le 3$ for all $j \in \mathbb{Z}_q$.

The quantity $\hat{u_q}(j) - \mathbb{E}\,\hat{u_q}(j)$ is a linear combination of i.i.d. centered random variables $X_k - \mathbb{E}\,X_k$, $k \in Q$ with coefficients $e_q(jk)$ whose absolute value is bounded by 1. Therefore, Bernstein's inequality yields

$$\mathbb{P}\left(|\hat{u_q}(j) - \mathbb{E}\,\hat{u_q}(j)| > t\right) \le 2\exp\left(-c\min(t^2 q^{-1/2}, t)\right)$$

for all $t > 0$ and $j \in \mathbb{Z}_q$. Setting $t = Cq^{1/4}\sqrt{\log q}$ and taking the union bound over $j \in \mathbb{Z}_q$, we obtain

$$\mathbb{P}\left(|\hat{u_q}(j) - \mathbb{E}\,\hat{u_q}(j)| \le Cq^{1/4}\sqrt{\log q} \text{ for all } j \in \mathbb{Z}_q\right) \ge 1 - q^{-1} > 0$$

if the constant $C > 0$ is chosen sufficiently large. The lemma follows. □

Corollary 2.4. *Let q be an odd prime number. There exists a $q \times q$ matrix U_q with ± 1 entries such that*

$$\sqrt{q}(1 - \delta_q) \le s_{\min}(U_q) \le s_{\max}(U_q) \le \sqrt{q}(1 + \delta_q)$$

with $\delta_q = Cq^{-1/4}\sqrt{\log q}$.

Proof. Represent $\mathbb{Z}_q$ as $\{1, \dots, q\}$, and let $u_q : \{1, \dots, q\} \to \{-1, 1\}$ be the vector defined in Lemma 2.3. Let U_q be the circulant matrix with the first row u_q. A circulant matrix is diagonal in the Fourier basis, see e.g., [9, Theorem 3.2.1; p. 72]. Therefore, the singular values of U_q are the absolute values of its eigenvalues which are the Fourier coefficients of the generating vector u_q. The result follows from Lemma 2.3. □

Remark 2.5. Corollary 2.4 implies that the matrix U_q satisfies

$$\left\|U_q (U_q)^\top - qI_q\right\| \le 3\delta_q q. \tag{2.1}$$

Inequality (2.1) will be used later in the proof of Theorem 1.2.

With this auxiliary construction in place, we can prove the main result of this section, namely Theorem 1.2.

Proof of Theorem 1.2. The proof of this theorem combines a deterministic construction of number-theoretic nature with a probabilistic argument. Without loss of generality, we can assume that n is larger than some number n_0 chosen in advance. Indeed, after the statement of the theorem is proved for $n \ge n_0$, we can adjust the constants c and C appropriately to make it hold for all $n \in \mathbb{N}$.

We start with the case when n is even. Let $\varepsilon > 0$ be a number to be chosen later. A combination of the Prime Number Theorem and Vinogradov's sum of three primes theorem [18], yields that there exists $N = N(\varepsilon)$ such that any even $n > N$ has a decomposition

$$n = q_1 + q_2 + q_3 + q_4 \text{ with } (1-\varepsilon)\frac{n}{4} \le q_j \le (1+\varepsilon)\frac{n}{4}, \tag{2.2}$$

where $q_1, \dots, q_4$ are prime numbers. Indeed, by the Prime Number Theorem, there exists a prime number q_1 such that $(1-\varepsilon/2)\frac{n}{4} \le q_1 \le (1+\varepsilon/2)\frac{n}{4}$. Then $m = n - q_1$ is odd, and thus by a stronger version of Vinogradov's theorem, it can be decomposed as

$$m = q_2 + q_3 + q_4, \text{ where } (1-\varepsilon/2)\frac{m}{3} \le q_j \le (1+\varepsilon/2)\frac{m}{3}, \tag{2.3}$$

and q_2, q_3, q_4 are primes. This immediately implies (2.2). Actually, decompositions with bounds tighter than (2.3) are available. More precisely, one can find a representations such as (2.3) with $|q_j - m/3| < m^\theta$ for some $\theta \in (0,1)$, see e.g., [3, 11, 17]. However, the weaker version presented above will be sufficient for our purposes.

Without loss of generality, assume that $q_1 \ge \dots \ge q_4 =: q$. We will consider the case $q_3 > q_4$ first. This is the most non-trivial case, and the other ones will be treated in the same way after obvious modifications. For $j = \{1, \dots, 4\}$, let U_j be the matrix U_{q_j} constructed in Corollary 2.4, and denote by U_j^{top} the submatrix formed by the q top rows of U_j. For $j \in \{1,2,3\}$, denote by U_j^{bottom} the submatrix of U_j formed by its $q_j - q$ bottom rows. We will construct the matrix $W = V^\top$ in the following block form:

$$W = \begin{pmatrix} W_{1,1} & W_{1,2} & W_{1,3} & W_{1,4} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ W_{4,1} & W_{4,2} & W_{4,3} & W_{4,4} \\ W_{5,1} & W_{5,2} & W_{5,3} & W_{5,4} \\ W_{6,1} & W_{6,2} & W_{6,3} & W_{6,4} \\ W_{7,1} & W_{7,2} & W_{7,3} & W_{7,4} \end{pmatrix} = \begin{pmatrix} W^{top} \\ W^{bottom} \end{pmatrix},$$

where the matrix W^{top} consists of the upper 4 block rows of W, and W^{bottom} consists of the lower three. Here $W_{j,k}$ is a $q \times q_k$ matrix if $1 \le j,k \le 4$ and a $(q_{j-4} - q) \times q_k$ matrix if $j = 5,6,7,\ 1 \le k \le 4$.

Let us define the matrices $W_{j,k}$. The matrix W^{top} will be deterministic, and the matrix W^{bottom} will consist of deterministic and random blocks. For $1 \le j,k \le 4$, set $W_{j,k} = \varepsilon_{j,k} U_k^{top}$, where $\varepsilon_{j,k},\ j,k \in \{1,\dots,4\}$ form a 4×4 Walsh matrix:

$$\begin{pmatrix} \varepsilon_{1,1} & \varepsilon_{1,2} & \varepsilon_{1,3} & \varepsilon_{1,4} \\ \varepsilon_{2,1} & \varepsilon_{2,2} & \varepsilon_{2,3} & \varepsilon_{2,4} \\ \varepsilon_{3,1} & \varepsilon_{3,2} & \varepsilon_{3,3} & \varepsilon_{3,4} \\ \varepsilon_{4,1} & \varepsilon_{4,2} & \varepsilon_{4,3} & \varepsilon_{4,4} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Now, let us define the matrices $W_{j,k}$ for $j = 5,6,7$. Set $W_{j,j-4} = U_{j-4}^{bottom}$. For $j = 5,6,7$ and $k \ne j-4$, let $W_{j,k}$ be a random matrix with i.i.d. Rademacher entries.

Consider the $(4q) \times (4q)$ matrix $W^{top}(W^{top})^\top$ first. The diagonal blocks of this matrix are close to nI_q. More precisely, for any $j \in \{1, \dots, 4\}$,

$$\begin{aligned}\left\| \sum_{k=1}^4 W_{j,k} W_{j,k}^\top - nI_q \right\| &= \left\| \sum_{k=1}^4 \left(U_k^{top} (U_k^{top})^\top - q_k I_q \right) \right\| \le \sum_{k=1}^4 \left\| U_k (U_k)^\top - q_k I_{q_k} \right\| \\ &\le 12 \delta_q n,\end{aligned}$$

where the first inequality follows since $U_k^{top}(U_k^{top})^\top$ is a submatrix of $U_k(U_k)^\top$ and the second one from (2.1).

Let us consider the off-diagonal blocks now. If $i \neq j,\ i, j \in \{1, \dots, 4\}$ then similarly

$$\begin{aligned}\left\| \sum_{k=1}^4 W_{j,k} W_{i,k}^\top \right\| &= \left\| \sum_{k=1}^4 \varepsilon_{i,k} \varepsilon_{j,k} U_k^{top} (U_k^{top})^\top \right\| \\ &\le \left\| \sum_{k=1}^4 \varepsilon_{i,k} \varepsilon_{j,k} \left(U_k^{top} (U_k^{top})^\top - q_k I_q \right) \right\| + \left| \sum_{k=1}^4 \varepsilon_{j,k} \varepsilon_{i,k} q_k \right| \\ &\le 12 \delta_q n + \varepsilon n,\end{aligned}$$

where the first estimate follows from the triangle inequality, and the second one from $q_k \in [(1-\varepsilon)\frac{n}{4}, (1+\varepsilon)\frac{n}{4}]$. Combining the two inequalities, we obtain

$$\left\| W^{top}(W^{top})^\top - nI_{4q} \right\| \le 12\delta_q n + 12(12\delta_q n + \varepsilon n) \le 13 \varepsilon n \tag{2.4}$$

for all sufficiently large n.

Let us introduce auxiliary $(n - 4q) \times n$ matrices S and R defined by

$$S = \begin{pmatrix} U_1^{bottom} & 0 & 0 & 0 \\ 0 & U_2^{bottom} & 0 & 0 \\ 0 & 0 & U_3^{bottom} & 0 \end{pmatrix} \qquad R = W^{bottom} - S.$$

In other words, R is the random part of the matrix W^{bottom}, i.e.,

$$R = \begin{pmatrix} 0 & W_{5,2} & W_{5,3} & W_{5,4} \\ W_{6,1} & 0 & W_{6,3} & W_{6,4} \\ W_{7,1} & W_{7,2} & 0 & W_{7,4} \end{pmatrix}$$

is an $(n - 4q) \times n$ matrix with zeros along the block diagonal corresponding to the positions of U_1^{bottom}, U_2^{bottom}, and U_3^{bottom} and i.i.d. Rademacher entries elsewhere.

Recall that $n - 4q \le 4\varepsilon n$. In view of Corollary 2.4 and inequality (2.1),

$$\begin{aligned}\|S\| \le \sqrt{\frac{n}{4}}(1 + \delta_q), \qquad \left\| S(W^{top})^\top \right\| \le 12 \delta_q n, \\ \|S\|_{\mathrm{HS}}^2 \le 3\varepsilon n \cdot (1+\varepsilon)\frac{n}{4} \le \varepsilon n.\end{aligned} \tag{2.5}$$

Also,

$$\begin{aligned}\left\|SS^\top - \frac{n}{4} I_{n-4q}\right\| &\le \max_{j=1,2,3} \left\|U_j^{bottom} (U_j^{bottom})^\top - q_j I_{q_j - q}\right\| + \varepsilon \frac{n}{4} \\ &\le \varepsilon \frac{n}{2}.\end{aligned}$$

Let $\tilde{R}$ be an $(n-4q) \times n$ matrix with i.i.d. Rademacher entries. Then a simple symmetrization argument yields

$$\mathbb{P}\left(\left\|SR^\top\right\| \ge C\sqrt{\varepsilon} n\right) \le 2\mathbb{P}\left(\left\|S\tilde{R}^\top\right\| \ge (C/2)\sqrt{\varepsilon} n\right)$$

which in combination with [19, Theorem 3.2] implies that

$$\mathbb{P}\left(\left\|SR^\top\right\| \le C\sqrt{\varepsilon} n\right) \ge 1 - \exp(-c\varepsilon n).$$

Another application of symmetrization yields

$$\mathbb{P}(\|R\| \ge 4\sqrt{n}) \le 2\mathbb{P}(\|\tilde{R}\| \ge 2\sqrt{n}) \le \exp(-cn).$$

Fix a matrix R for which

$$\left\|SR^\top\right\| \le C\sqrt{\varepsilon} n \quad \text{and} \quad \|R\| \le 4\sqrt{n} \tag{2.6}$$

at the same time.

Let $x \in S^{n-1}$. Following the previous convention, we write

$$x = \begin{pmatrix} x^{top} \\ x^{bottom} \end{pmatrix},$$

where $x^{top} \in \mathbb{R}^{4q}$ and $x^{bottom} \in \mathbb{R}^{n-4q}$. Assume first that $\left\|x^{bottom}\right\|_2 \ge \eta$, where the constant $\eta > 0$ will be chosen below. Then

$$\begin{aligned}\left\|W^\top x\right\|_2 &\ge \frac{1}{\|S\|} \cdot \left\|SW^\top x\right\|_2 \\ &\ge \frac{1}{\|S\|} \cdot \left(\left\|S(W^{bottom})^\top x^{bottom}\right\|_2 - \left\|S(W^{top})^\top x^{top}\right\|_2\right) \\ &\ge (1 - 2\delta_n)\sqrt{\frac{4}{n}} \cdot \\ &\qquad \left(\left\|SS^\top x^{bottom}\right\|_2 - \left\|SR^\top x^{bottom}\right\|_2 - \left\|S(W^{top})^\top x^{top}\right\|_2\right) \\ &\ge (1 - 2\delta_n)\sqrt{\frac{4}{n}} \cdot \\ &\qquad \left((1-2\varepsilon)\frac{n}{4}\left\|x^{bottom}\right\|_2 - \left\|SR^\top\right\| - \left\|S(W^{top})^\top\right\|\right) \\ &\ge (1 - 4\delta_n)\sqrt{\frac{n}{4}} \cdot \left((1-2\varepsilon)\left\|x^{bottom}\right\|_2 - C_1\sqrt{\varepsilon}\right) \\ &\ge \frac{\eta}{4}\sqrt{n}\end{aligned}$$

if η and ε are chosen so that $(1-2\varepsilon)\eta - C_1\sqrt{\varepsilon} > \eta/2$.

Assume now that $\|x_{bottom}\|_2 < \eta$. Then $\|x_{top}\|_2 > 1 - \eta$, and (2.4) yields

$$\begin{aligned}\left\|W^\top x\right\|_2 &\geq \left\|(W^{top})^\top x^{top}\right\|_2 - \left\|(W^{bottom})^\top\right\| \cdot \left\|x^{bottom}\right\|_2 \\ &\geq (1-7\varepsilon)\sqrt{n} \cdot \left\|x^{top}\right\|_2 - C_2\sqrt{n} \cdot \left\|x^{bottom}\right\|_2 \\ &\geq (1-7\varepsilon)\sqrt{n} \cdot (1-\eta) - C_2\sqrt{n} \cdot \eta \\ &\geq \frac{1}{2}\sqrt{n}\end{aligned}$$

if η is chosen so that $C_2\eta < \frac{1}{4}$. Choosing the parameters ε and η sufficiently small, we can reconcile the two restrictions, i.e., select ε, η so that the inequalities

$$(1-2\varepsilon)\eta - C_1\sqrt{\varepsilon} > \eta/2 \quad \text{and} \quad C_2\eta < \frac{1}{4}$$

hold at the same time. With this choice, the previous argument shows that

$$\left\|W^\top x\right\|_2 \geq \min\left(\frac{\eta}{4}, \frac{1}{2}\right)\sqrt{n}$$

for all $x \in S^{n-1}$, which means that

$$s_{\min}(W^\top) \geq c\sqrt{n}.$$

Obtaining a bound for $s_{\max}(W)$ is easier. Inequalities (2.4) and (2.5) imply

$$\left\|W^{top}\right\| \leq 2\sqrt{n} \quad \text{and} \quad \|S\| \leq \sqrt{n}.$$

This in combination with (2.6) yields

$$s_{\max}(W^\top) \leq C\sqrt{n},$$

which proves the theorem in the case $q_3 > q$.

If $q_j = q$ for some $j \in \{1,2,3\}$, then we repeat the same argument with the block rows of W containing $q_j - q = 0$ rows removed. For instance, if $q_1 > q$ and $q_2 = q_3 = q$, then we consider the $n \times n$ matrix W with W^{top} being the same as in the previous case and $W^{bottom} = (W_{5,1} \cdots W_{5,4})$ which is a $(q_1 - q) \times n$ matrix.

This completes the proof of the theorem in the case when n is even.

Assume that n is odd. By Corollary 2.2, if n is sufficiently large, then we can find an even number

$$m \in \left[\left(1 - \frac{\varepsilon}{2}\right)\frac{n}{4}, \left(1 + \frac{\varepsilon}{2}\right)\frac{n}{4}\right]$$

for which there exists an Hadamard matrix V of size $m \times m$. Note that $n - m$ is odd and

$$n - m \in \left[\left(1 - \frac{\varepsilon}{2}\right)\frac{3n}{4}, \left(1 + \frac{\varepsilon}{2}\right)\frac{3n}{4}\right],$$

so using Vinogradov's theorem again, we obtain a decomposition

$$n - m = q_1 + q_2 + q_3,$$

where q_1, q_2, q_3 are prime numbers and $\frac{1-\varepsilon}{4}n \leq q_j \leq \frac{1+\varepsilon}{4}n$. At this point we can apply the same argument we used in the case of an even n with one

of the matrices $U_1, \dots, U_4$ replaced by V. This completes the proof of the theorem. □

3. Submatrices with a small condition number

In this section we prove Theorem 1.1. As was explained in the Introduction, the proof relies on finding columns of A which are close to columns of a scaled copy of the matrix V constructed in the previous section. Conditioned on the event that such selection is possible, we prove that with high probability, the constructed submatrix has a bounded condition number. We start with the latter task, namely with analyzing a random matrix close to V.

Lemma 3.1. *Let V be an $n \times n$ matrix with ± 1 entries such that*

$$c_{3.1}\sqrt{n} \le s_{\min}(V) \le s_{\max}(V) \le C_{3.1}\sqrt{n}$$

for some $0 < c_{3.1} \le C_{3.1}$.

There exists $\delta \in (0,1)$ for which any $n \times n$ matrix Y with i.i.d. entries $Y_{i,j}$ such that

$$\mathbb{E}\, Y_{i,j} = 0 \quad \text{and } |Y_{i,j}| \le \delta \text{ a.s.}$$

satisfies

$$\mathbb{P}\left(\kappa(V+Y) \le 4\frac{C_{3.1}}{c_{3.1}}\right) \ge 1 - \exp(-cn).$$

Proof. The proof of Lemma 3.1 uses the basic net argument, see e.g., [22]. Since Y has i.i.d. centered subgaussian entries with $\|Y_{i,j}\|_{\psi_2} \le \|Y_{i,j}\|_\infty \le \delta$,

$$\mathbb{P}(\|Y\| \ge C\sqrt{\delta n}) \le \exp(-cn).$$

Therefore,

$$\mathbb{P}(s_{\max}(V+Y) \ge 2C_{3.1}\sqrt{n}) \le \mathbb{P}(\|V\| + \|Y\| \ge 2C_{3.1}\sqrt{n}) \le \exp(-cn),$$

as we can always assume that $C_{3.1} \ge 1$ and choose δ sufficiently small. Similarly,

$$\mathbb{P}(s_{\min}(V+Y) \le \frac{1}{2}c_{3.1}\sqrt{n}) \le \mathbb{P}(s_{\min}(V) - \|Y\| \le \frac{1}{2}c_{3.1}\sqrt{n}) \le \exp(-cn),$$

where as before, the last inequality holds for any sufficiently small δ. The result follows by combining the two bounds above. □

We now proceed to proving the main result, Theorem 1.1.

Proof ot Theorem 1.1. Since the distribution of entries of A is non-degenerate, there exists $a > 0$ such that for any $\nu > 0$

$$\mathbb{P}\left(|a_{i,j} - a| < \nu\right) > 0.$$

By the symmetry of distribution, we also have the same property for $-a$ in place of a.

Let $\delta > 0$ be as in Lemma 3.1, and denote $\nu = \frac{a}{4}\delta$. Let Z be a random variable having the same distribution as $a_{i,j}$ conditioned on the event that $|a_{i,j} - a| \le \nu$. More precisely, for a Borel set $E \subset \mathbb{R}$, set

$$\mathbb{P}(Z \in E) = \frac{1}{\mathbb{P}(|a_{i,j} - a| \le \nu)} \mathbb{P}(a_{i,j} \in E \ \& \ |a_{i,j} - a| \le \nu).$$

Set

$$R = \frac{Z - \mathbb{E}\, Z}{\mathbb{E}\, Z}.$$

Then R is a centered random variable such that

$$|R| \le \frac{2\nu}{(1 - \delta/4)a} \le \delta \ \text{ a.s.}$$

Let $C > 0$ be a constant to be chosen later, and assume that $N \ge \exp(2Cn)$. Partition $[N]$ into a union of sets $I_1, \dots, I_n$ such that

$$|I_j| \ge \left\lfloor \frac{N}{n} \right\rfloor \ge \exp(Cn).$$

Let V be the $n \times n$ matrix with ± 1 entries constructed in Theorem 1.2. Denote its columns by $V_1, \dots, V_n$ and the columns of A by $A_1, \dots, A_N$. Let M be a number to be chosen later. Let $\mathcal{E}$ be the event that for any $j \in [n]$, there exist at least M numbers $k \in I_j$ with

$$\|A_k - aV_j\|_\infty \le \nu.$$

If $\mathcal{E}$ occurs, denote by $k(j,1), \dots, k(j,M)$ the first M numbers $k \in I_j$ having this property. Then conditioned on $\mathcal{E}$, for any $m \in [M]$, the matrix $A_{\mathcal{E},m}$ with columns $A_{k(1,m)}, \dots, A_{k(n,m)}$ has the same distribution as $\mathbb{E}\, Z \cdot (V + Y)$, where Y is an $n \times n$ random matrix whose entries have the form $Y_{i,j} = V_{i,j} R_{i,j}$, where $R_{i,j}$ are independent copies of R. In view of Lemma 3.1, this implies that for any $m \in [M]$,

$$\mathbb{P}\left(\kappa(A_{\mathcal{E},m}) \le 4 \frac{C_{3.1}}{c_{3.1}} \mid \mathcal{E} \right) \ge 1 - \exp(-cn).$$

Since conditionally on $\mathcal{E}$, the matrices $A_{\mathcal{E},1}, \dots, A_{\mathcal{E},M}$ are independent, Bernstein's inequality allows to conclude that

$$\mathbb{P}\left(\kappa(A_{\mathcal{E},m}) \le 4 \frac{C_{3.1}}{c_{3.1}} \text{ for at least } M/2 \text{ numbers } m \in [M] \mid \mathcal{E} \right) \ge 1 - \exp(-c'M).$$

To complete the proof, we have to show that the probability of $\mathcal{E}^c$ is small. To this end, denote $\eta = \mathbb{P}(|a_{i,j} - a| \le \nu)$. Then by the symmetry of distribution of the entries of A, $\mathbb{P}(|a_{i',j'} - aV_{i,j}| \le \nu) = \eta$ for any i', j'. Let $j \in [n]$. For any $k \in I_j$,

$$\mathbb{P}(\|A_k - aV_j\|_\infty \le \nu) = \eta^n.$$

Set

$$M = \frac{N}{2} \cdot \eta^n = \frac{1}{2} \exp\left(Cn - \log\left(\frac{1}{\eta}\right) \cdot n \right) \ge \exp\left(\frac{Cn}{2}\right)$$

where the last inequality holds if $C = C(\eta)$ is chosen sufficiently large. Note that the events $\|A_k - aV_j\|_\infty \le \nu$ are independent for all $k \in I_j$. At this point, Bernstein's inequality yields

$$\mathbb{P}(\|A_k - aV_j\|_\infty \le \nu \text{ for less than } M \text{ numbers } k \in I_j) \le \exp(-c''M) \le \exp\left[-\exp\left(\frac{Cn}{4}\right)\right].$$

Therefore,

$$\begin{aligned}\mathbb{P}(\mathcal{E}^c) &\le \sum_{j=1}^{n} \mathbb{P}(\|A_k - aV_j\|_\infty \le \nu \text{ for less than } M \text{ numbers } k \in I_j) \\ &\le n \cdot \exp\left[-\exp\left(\frac{Cn}{4}\right)\right] \le \exp\left[-\exp\left(\frac{Cn}{8}\right)\right].\end{aligned}$$

Let $L = M/2$, and $\alpha = 4\frac{C_{3.1}}{c_{3.1}}$. Combining the previous inequalities, we obtain that

$$\begin{aligned}&\mathbb{P}\big(\text{exist disjoint subsets } I_1, \dots, I_L \text{ of } [N] \text{ such that} \\ &\qquad |I_j| = n \text{ and } \kappa(A_{I_j}) < \alpha \text{ for all } j \in [L]\big) \\ &\ge \mathbb{P}\left(\kappa(A_{\mathcal{E},m}) < \alpha \text{ for at least } M/2 \text{ numbers } m \in [M] \mid \mathcal{E}\right) \cdot (1 - \mathbb{P}(\mathcal{E}^c)) \\ &\ge 1 - \exp(-c'M) - \exp\left[-\exp\left(\frac{Cn}{8}\right)\right] \\ &\ge 1 - \exp\left(-\exp(\beta n)\right)\end{aligned}$$

for an appropriate $\beta > 0$. This completes the proof of the theorem. □

4. No submatrices with a small condition number

In this section, we prove Theorem 1.3.

Proof. Without loss of generality, we can assume that $\|X\|_2 = (\mathbb{E}\, X^2)^{1/2} = 1$. Throughout the proof, we denote by C, c, c', etc. constants depending only on $\|X\|_{\psi_2}$.

Consider an $n \times n$ random matrix B whose entries are independent copies of X. We claim that

$$\mathbb{P}(\|B\| \le c\sqrt{n}) \le \exp(-c'n^2). \tag{4.1}$$

Indeed, denoting the columns of B by $B_1, \dots, B_n$, and applying the Hanson-Wright inequality [19, Theorem 2.1], we get

$$\begin{aligned}\mathbb{P}(\|B\| \le \frac{1}{2}\sqrt{n}) &\le \mathbb{P}(\|B_j\|_2 \le \frac{1}{2}\sqrt{n} \text{ for all } j \in [n]) \\ &\le \left(\mathbb{P}\left[\mathbb{E}\,\|B_j\|_2^2 - \|B_j\|_2^2 \ge \frac{1}{2}n\right]\right)^n \le \exp(-c'n^2).\end{aligned}$$

Furthermore, we assert that

$$\mathbb{P}(s_n(B) \ge 2\sqrt{\varepsilon n}) \le \exp(-c'\varepsilon^2 n^2) \tag{4.2}$$

for any $\varepsilon > 0$. Proving (4.2) relies on a standard fact from linear algebra.

Lemma 4.1. *Let M be an $n \times n$ matrix. Let $k < n$, and denote $H = \operatorname{span}(Me_{k+1}, \dots, Me_n)$, where $e_1, \dots, e_n$ is the standard basis of $\mathbb{R}^n$. Then*

$$s_n(M) \le \min_{j=1,\dots,k} \|P_{H^\perp} M e_j\|_2 ,$$

where $P_{H^\perp}$ is the orthogonal projection on $H^\perp$.

Proof. Without loss of generality, we can assume that the matrix M is invertible. Let $j \in [k]$. Choosing an appropriate $u \in \operatorname{span}(e_{k+1}, \dots, e_n)$, we obtain

$$1 \le \|e_j - u\|_2 \le \left\|M^{-1}\right\| \cdot \|Me_j - Mu\|_2 = s_n^{-1}(M) \cdot \|P_{H^\perp} M e_j\|_2 ,$$

where the equality holds after optimization over u. The lemma follows. □

To prove (4.2), we apply Lemma 4.1 to B setting $k = \lfloor \varepsilon n \rfloor$. It yields

$$\mathbb{P}(s_n(B) \ge 2\sqrt{\varepsilon n}) \le \mathbb{P}(\|P_{H^\perp} B e_j\|_2 \ge 2\sqrt{\varepsilon n} \text{ for all } j \in [k]).$$

Conditioning on $B_{k+1}, \dots, B_n$, we can rewrite the right hand side ov the above inequality as

$$\begin{aligned} &\mathbb{E}\left(\mathbb{P}\big[\, \|P_{H^\perp} B e_j\|_2 \ge 2\sqrt{\varepsilon n} \text{ for all } j \in [k] \mid B_{k+1}, \dots, B_n \big]\right) \\ =&\,\mathbb{E}\left(\mathbb{P}\big[\, \|P_{H^\perp} B e_1\|_2 \ge 2\sqrt{\varepsilon n} \mid B_{k+1}, \dots, B_n \big]\right)^k \end{aligned}$$

using independence of the columns of B. The conditional probability can be estimated by applying the Hanson-Wright inequality again. Applying [19, Theorem 2.1] to the vector $B_1 = Be_1$ having i.i.d. centered subgaussian coordinates, we get

$$\begin{aligned} &\mathbb{P}\big[\, \|P_{H^\perp} B e_1\|_2 \ge 2\sqrt{\varepsilon n} \mid B_{k+1}, \dots, B_n \big] \\ \le\, &\mathbb{P}\big[\, \|P_{H^\perp} B e_1\|_2 - \|P_{H^\perp}\|_{\mathrm{HS}} \ge \sqrt{\varepsilon n} \mid B_{k+1}, \dots, B_n \big] \\ \le\, &\exp(-c\varepsilon n). \end{aligned}$$

Taking the expectation with respect to $B_{k+1}, \dots, B_n$ and combining it with the previous inequality completes the proof of (4.2).

Using (4.2) with $\varepsilon = t^{-2}/4$ together with (4.1), we derive

$$\mathbb{P}(\kappa(B) < t) \le \exp\left(-c' \frac{n^2}{t^4}\right).$$

The proposition follows by using this inequality for $B = A_I$ and taking the union bound over $I \subset [N]$:

$$\begin{aligned} \mathbb{P}\left(\exists I \subset [N] \ |I| = n \text{ and } \kappa(A_I) < t\right) &\le \binom{N}{n} \exp\left(-c' \frac{n^2}{t^4}\right) \\ &\le \exp\left(n \log\left(\frac{eN}{n}\right) - c' \frac{n^2}{t^4}\right) \\ &\le \exp\left(-(c' - \tilde{c}) \frac{n^2}{t^4}\right), \end{aligned}$$

where the last inequality follows from the assumption on N. Setting $\tilde{c} = c'/2$ completes the proof. □

References

[1] S. S. Agaian, Hadamard matrices and their applications. Lecture Notes in Mathematics, 1168. Springer-Verlag, Berlin, 1985.

[2] T. Banica, I. Nechita, K Życzkowski *Almost Hadamard matrices: general theory and examples,* Open Systems & Information Dynamics 19 (2012), no.04 1250024 pp.

[3] R.C. Baker, G. Harman, *The three primes theorem with almost equal summands,* Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 356 (1998), no. 1738, 763–780 pp.

[4] P. Casazza, G. Kutyniok, F.Philipp, Introduction to finite frame theory. Finite frames, 1–53, Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York, 2013.

[5] O. Christensen, Frames and bases. An introductory course. Applied and Numerical Harmonic Analysis. Birkhäuser Boston, Inc., Boston, MA, 2008.

[6] O. Christensen, An introduction to frames and Riesz bases. Second edition. Applied and Numerical Harmonic Analysis. Birkhäuser/Springer, 2016.

[7] R. Craigen, *Signed groups, sequences, and the asymptotic existence of Hadamard matrices,* Journal of Combinatorial Theory, Series A 71 (1995), no.2 241–254 pp.

[8] H. Davenport, Multiplicative number theory. Second edition. Revised by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980.

[9] P. J. Davis, Circulant matrices. A Wiley-Interscience Publication. Pure and Applied Mathematics. John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[10] W. de Launey, *On the asymptotic existence of Hadamard matrices,* Journal of Combinatorial Theory, Series A 116 (2009), no.4 1002–1008.

[11] C. B. Haselgrove, *Some theorems in the analytic theory of numbers*, J. London Math. Soc. 26 (1951), 273–277.

[12] K. J. Horadam, Hadamard matrices and their applications. Princeton University Press, Princeton, NJ, 2007.

[13] K. Ireland, M. Rosen, A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[14] Ph. Jaming, M. Matolcsi, *On the existence of flat orthogonal matrices,* Acta Math. Hungar. 147 (2015), no. 1, 179–188.

[15] P. Ki-Hyeon, H. Song, *Quasi-hadamard matrix,* 2010 IEEE International Symposium on Information Theory (2020), 1243–1247 pp.

[16] M. Matolcsi, I. Z. Ruzsa, *Difference sets and positive exponential sums I. General properties,* J. Fourier Anal. Appl. 20 (2014), no. 1, 17–41.

[17] K. Matomäki, J. Maynard, X. Shao, *Vinogradov's theorem with almost equal summands,* Proceedings of the London Mathematical Society 115 (2017), no. 2, 323–347 pp.

[18] M. B. Nathanson, Additive number theory. The classical bases. Graduate Texts in Mathematics, 164. Springer-Verlag, New York, 1996.

[19] M. Rudelson, R. Vershynin, *Hanson-Wright inequality and sub-Gaussian concentration,* Electron. Commun. Probab. 18 (2013), no. 82, 9 pp.

[20] J. Sylvester, *LX. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers.,* The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science 34 (1867), no.232 461–475 pp.

[21] R. Vershynin, Estimation in high dimensions: a geometric perspective. Sampling theory, a renaissance, 3–66, Appl. Numer. Harmon. Anal., Birkhäuser/Springer, 2015.

[22] R. Vershynin, High-dimensional probability. An introduction with applications in data science. With a foreword by Sara van de Geer. Cambridge Series in Statistical and Probabilistic Mathematics, 47. Cambridge University Press, Cambridge, 2018.
[23] J.S.Wallis, *On the existence of Hadamard matrices,* J. Combinatorial Theory Ser. A 21 (1976), no. 2, 188–195.

Department of Mathematics, University of Michigan, 530 Church St., Ann Arbor, MI 48109, U.S.A.
Email address: {xydong, rudelson}@umich.edu