Asymptotically optimal approximate Hadamard matrices

Boris Alexeev John Jasper* Dustin G. Mixon†‡

Abstract

In this paper, we study approximate Hadamard matrices, that is, well-conditioned $n \times n$ matrices with all entries in $\{\pm 1\}$. We show that the smallest-possible condition number goes to 1 as $n \to \infty$, and we identify some explicit infinite families of approximate Hadamard matrices.

1 Introduction

Given a real matrix A, let $\kappa(A) \in [1, \infty]$ denote the *condition number* of A:

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

where $\sigma_{\min}(A)$ and $\sigma_{\max}(A)$ denote the smallest and largest singular values of A, respectively. (If $\sigma_{\min}(A) = 0$, we put $\kappa(A) = \infty$.) For each positive integer n, let $\kappa(n)$ denote the smallest possible condition number of an $n \times n$ matrix with all entries in $\{\pm 1\}$, that is,

$$\kappa(n) := \min_{A \in \{\pm 1\}^{n \times n}} \kappa(A).$$

Observe that $\kappa(n) \geq 1$, with equality precisely when there exists a Hadamard matrix of order n.

Recently, Dong and Rudelson [10] showed that the sequence $\kappa(n)$ is uniformly bounded, and Steinerberger [18] later showed this still holds when restricting to circulant matrices. Steinerberger has since promoted this problem of *approximate Hadamard matrices*, for example, in [14, 19]. (In fact, he personally introduced the third author to the problem over a drink at the 5th Biennial Meeting of the Pacific Northwest Section of SIAM.) Here are the two main questions posed by Steinerberger:

1. Does it hold that $\lim_{n \to \infty} \kappa(n) = 1$?

2. Are there explicit infinite families of approximate Hadamard matrices?

In this paper, we resolve both questions in the affirmative, and we pose a few follow-up questions.

In the next section, we establish that there exists $\alpha > 0$ such that $\kappa(n) \leq 1 + \frac{1}{n^\alpha}$ for all sufficiently large n. As part of our proof, we resolve a 10-year-old problem of Jaming and Matolcsi [12] concerning flat orthogonal matrices. Next, Section 3 uses ideas from Ramsey theory to obtain a lower bound of the form $\kappa(n) \geq 1 + \frac{c \log n}{n}$ for all sufficiently large $n \not\equiv 0 \bmod 4$. In Section 4, we identify a few infinite families of approximate Hadamard matrices, we describe our (shockingly productive) use of AI in Section 5, and we conclude with a discussion in Section 6.

*Department of Mathematics and Statistics, Air Force Institute of Technology, Wright-Patterson AFB, Ohio, USA
†Department of Mathematics, The Ohio State University, Columbus, Ohio, USA
‡Translational Data Analytics Institute, The Ohio State University, Columbus, Ohio, USA

2 Upper bound

In this section, we construct approximate Hadamard matrices of order n with condition number approaching 1 as $n \to \infty$. Our approach follows the schematic

$$\boxed{\begin{array}{c}\text{known}\\ \text{Hadamard}\\ \text{matrices}\end{array}} \xrightarrow[]{\substack{\text{submatrix}\\ \text{orthogonalization}}} \boxed{\begin{array}{c}\text{flat}\\ \text{orthogonal}\\ \text{matrices}\end{array}} \xrightarrow[]{\substack{\text{random}\\ \text{rounding}}} \boxed{\begin{array}{c}\text{approximate}\\ \text{Hadamard}\\ \text{matrices}\end{array}}$$

and the result is the following:

Theorem 1. *There exists $\alpha > 0$ such that $\kappa(n) \le 1 + \frac{1}{n^\alpha}$ for all sufficiently large n.*

As we will see, with known constructions of Hadamard matrices, we can take $\alpha = \frac{17}{92} - \delta$ for any small $\delta > 0$, while conditioned on the Hadamard conjecture, we can take $\alpha = \frac{1}{4} - \delta$.

First, we explain the second arrow of the above schematic. In particular, we identify the related problem of *flat orthogonal matrices*, introduced by Jaming and Matolcsi in [12]. In particular, for each positive integer n, let $u(n)$ denote the smallest possible entry-wise infinity norm of an $n \times n$ orthogonal matrix:

$$u(n) := \min_{M \in O(n)} \|M\|_{\max}.$$

Observe that $u(n) \ge 1/\sqrt{n}$, with equality precisely when there exists a Hadamard matrix of order n. It turns out that $u(n)$ approaches this lower bound when n gets large, thereby resolving Problem 1.2 of [12] in the affirmative:

Theorem 2. *There exists $\epsilon \in (0, \frac{1}{2})$ such that $u(n) \le \frac{1}{\sqrt{n - n^\epsilon}}$ for all sufficiently large n.*

As we will see, with known constructions of Hadamard matrices, we can take $\epsilon = \frac{3}{23} + \delta$ for any small $\delta > 0$, while conditioned on the Hadamard conjecture, we can take $\epsilon > 0$ arbitrarily small.

Before proving this theorem, we first show that it implies Theorem 1. (As suggested by our schematic, the main idea is that randomly rounding a flat orthogonal matrix results in an approximate Hadamard matrix.)

Proof of Theorem 1. Select $M \in O(n)$ with $\|M\|_{\max} = u(n)$, and let X denote the random matrix with independent entries in $\{\pm 1\}$ such that $\mathbb{E}X = M/\|M\|_{\max}$. Put $E := X - \mathbb{E}X$. We will use the matrix Bernstein inequality to show that

$$\mathbb{E}\|E\|_{\text{op}} \le \sqrt{2(n - \tfrac{1}{u(n)^2}) \log(2n)} + \tfrac{2}{3}\log(2n) =: e(n). \tag{1}$$

For now, we assume (1) holds. Fix a sample point ω with $\|E(\omega)\|_{\text{op}} \le \mathbb{E}\|E\|_{\text{op}}$. Then Weyl's inequality gives

$$\sigma_{\min}(X(\omega)) \ge \sigma_{\min}(\mathbb{E}X) - \|E(\omega)\|_{\text{op}} \ge \frac{1}{u(n)} - e(n),$$
$$\sigma_{\max}(X(\omega)) \le \sigma_{\max}(\mathbb{E}X) + \|E(\omega)\|_{\text{op}} \le \frac{1}{u(n)} + e(n),$$

and so

$$\frac{\sigma_{\max}(X(\omega))}{\sigma_{\min}(X(\omega))} \le \frac{1 + u(n)e(n)}{1 - u(n)e(n)} = 1 + 2u(n)e(n) + o\big(u(n)e(n)\big).$$

Meanwhile, Theorem 2 implies

$$u(n)e(n) \leq \frac{\sqrt{4n^{1/2+\epsilon}\log(2n)} + \frac{2}{3}\log(2n)}{\sqrt{n} - n^{\epsilon}} = \big(1 + o(1)\big) \cdot \frac{\sqrt{4\log n}}{n^{1/4-\epsilon/2}}.$$

The result then follows by taking $\alpha < 1/4 - \epsilon/2$.

It remains to establish (1). We shall follow Theorem 6.1.1 in Tropp's *An Introduction to Matrix Concentration Inequalities* [21], which in turn requires us to identify a boundedness parameter L and a variance parameter v in our use case. Let E_{ij} denote the (i,j) entry of the random matrix E, let e_i denote the ith standard basis element, and put $S_{ij} := E_{ij}e_ie_j^\top$ so that $E = \sum_{i,j\in[n]} S_{ij}$. Since $|E_{ij}| \leq 2$ almost surely, we have $\|S_{ij}\|_{\mathrm{op}} \leq 2 =: L$ almost surely. Next,

$$\sum_{i,j\in[n]} \mathbb{E}[S_{ij}S_{ij}^\top] = \sum_{i,j\in[n]} \mathrm{Var}(X_{ij}) \cdot e_ie_i^\top = \sum_{i,j\in[n]} \big(1 - (\mathbb{E}X_{ij})^2\big) \cdot e_ie_i^\top = (n - \tfrac{1}{u(n)^2}) \cdot I_n,$$

and similarly, $\sum_{i,j\in[n]} \mathbb{E}[S_{ij}^\top S_{ij}] = (n - \frac{1}{u(n)^2}) \cdot I_n$. It follows that

$$v := \max\left\{\Bigg\|\sum_{i,j\in[n]} \mathbb{E}[S_{ij}S_{ij}^\top]\Bigg\|_{\mathrm{op}}, \Bigg\|\sum_{i,j\in[n]} \mathbb{E}[S_{ij}^\top S_{ij}]\Bigg\|_{\mathrm{op}}\right\} = n - \frac{1}{u(n)^2}.$$

Thus, taking $d_1 := n$ and $d_2 := n$, Theorem 6.1.1 in [21] gives

$$\mathbb{E}\|E\|_{\mathrm{op}} \leq \sqrt{2v\log(d_1+d_2)} + \tfrac{1}{3}L\log(d_1+d_2) = \sqrt{2(n - \tfrac{1}{u(n)^2})\log(2n)} + \tfrac{2}{3}\log(2n)$$

i.e., (1) holds. □

It remains to prove Theorem 2. Here's our approach: Given a positive integer n, find a Hadamard matrix H of order $m \geq n$ (with m not much larger than n), and then "orthogonalize" an $n \times n$ submatrix of H. The following lemma explains this latter step:

Lemma 3 (submatrix orthogonalization)**.** *Given an orthogonal matrix* $\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$ *with* $I - A$ *invertible, it holds that* $D + C(I-A)^{-1}B$ *is also orthogonal.*

Proof. We will show that $M := D + C(I-A)^{-1}B$ satisfies $\|Mu\| = \|u\|$ for every u. Fix u. Since $I - A$ is invertible, there is a unique x such that $x = Ax + Bu$, namely, $x = (I-A)^{-1}Bu$. Then

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}\begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} Ax + Bu \\ Cx + Du \end{bmatrix} = \begin{bmatrix} x \\ C(I-A)^{-1}Bu + Du \end{bmatrix} = \begin{bmatrix} x \\ Mu \end{bmatrix}.$$

Since $\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$ is orthogonal, the result follows by taking the norm of both sides. □

Conveniently, running submatrix orthogonalization on a Hadamard matrix results in a *flat* orthogonal matrix, provided A has relatively few rows and columns:

Lemma 4. *Given an* $m \times m$ *Hadamard matrix* H*, select* $k < \sqrt{m}$ *and consider the block decomposition* $\frac{1}{\sqrt{m}}H = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$ *with* $A \in \mathbb{R}^{k\times k}$*. Then* $I - A$ *is invertible and* $\|D + C(I-A)^{-1}B\|_{\max} \leq \frac{1}{\sqrt{m}-k}$*.*

Proof. First, $\|A\|_{\mathrm{op}}^2 \leq \|A\|_F^2 = k^2/m < 1$. As such, $I - A$ is invertible and the Neumann series

$$(I-A)^{-1} = \sum_{n=0}^{\infty} A^n$$

converges. Put $M := D + C(I-A)^{-1}B$. The size of the (i,j) entry of M is

$$|D_{ij} + e_i^\top C(I-A)^{-1}Be_j| \le |D_{ij}| + \|e_i^\top C\|_2 \|(I-A)^{-1}\|_{\mathrm{op}} \|Be_j\|_2 = \frac{1}{\sqrt{m}} + \frac{k}{m} \cdot \|(I-A)^{-1}\|_{\mathrm{op}}.$$

Next, we apply the triangle inequality over the Neumann series:

$$\|(I-A)^{-1}\|_{\mathrm{op}} \le \sum_{n=0}^{\infty} \|A\|_{\mathrm{op}}^n \le \sum_{n=0}^{\infty} \left(\frac{k}{\sqrt{m}}\right)^n = \frac{1}{1-k/\sqrt{m}}.$$

All together, we have

$$\|M\|_{\max} \le \frac{1}{\sqrt{m}} + \frac{k}{m} \cdot \frac{1}{1-k/\sqrt{m}} = \frac{1}{\sqrt{m}-k}. \qquad \square$$

Finally, the plethora of known Hadamard matrices allows us to select m close to n:

Lemma 5. *Fix positive integers a, b, and c with the property that for every positive integer s, there exists a Hadamard matrix of order $2^t(2s+1)$, where $t = t(s) = a\lfloor \frac{1}{b}\log_2 s\rfloor + c$. Then for every sufficiently large integer n, there exists a Hadamard matrix of order m such that*

$$n \le m < n + 2 \cdot 2^{\frac{b(a+c+1)}{a+b}} \cdot n^{\frac{a}{a+b}}.$$

Notably, the hypothesis of Lemma 5 was proven by Craigen [7] in 1995 with $a = 4$, $b = 6$, and $c = 6$, resulting in an exponent of $\frac{a}{a+b} = \frac{2}{5} < \frac{1}{2}$. More recently, Du and Jiang [11] obtained $a = 6$, $b = 40$, and $c = 10$, resulting in a smaller exponent of $\frac{a}{a+b} = \frac{3}{23}$. (See [11] for a discussion of the history of such results.)

Proof of Lemma 5. By iteratively taking Kronecker products with a Hadamard matrix of order 2, we have Hadamard matrices of order $2^t(2s+1)$ for every $t \ge t(s)$. Notably, $t(s)$ is monotonically increasing in s. Given an integer $t \ge c$, let $s(t)$ denote the largest integer s for which $t \ge t(s)$. Then we have Hadamard matrices of order $2^t(2s+1)$ for every $s \le s(t)$. This gives an arithmetic progression of Hadamard matrix orders with common difference 2^{t+1}. Given a positive integer n, find the smallest $t \ge c$ for which $n \le 2^t(2s(t)+1)$. Then the smallest $m \ge n$ in this arithmetic progression satisfies

$$n \le m < n + 2^{t+1}.$$

It remains to bound 2^{t+1} in terms of a, b, and c.

First, we observe that $s(t) \ge 2^{b\lfloor\frac{t-c}{a}\rfloor}$ for $t \ge c$. Indeed, this follows from the easily verified fact that $t(2^{b\lfloor\frac{t-c}{a}\rfloor}) \le t$. Next, since t was selected to be minimal, it either holds that $t = c$ or

$$n > 2^{t-1}(2s(t-1)+1) \ge 2^t \cdot 2^{b\lfloor\frac{t-1-c}{a}\rfloor} \ge 2^t \cdot 2^{b(\frac{t-1-c}{a}-1)} = 2^{\frac{t(a+b)}{a}} \cdot 2^{-\frac{b(a+c+1)}{a}},$$

which rearranges to $2^t < 2^{\frac{b(a+c+1)}{a+b}} \cdot n^{\frac{a}{a+b}}$. Since n is sufficiently large, this latter bound is greater than 2^c, and the result follows. $\square$

Proof of Theorem 2. Put $a = 6$, $b = 40$, and $c = 10$, and fix $\epsilon \in (\frac{a}{a+b}, \frac{1}{2})$. Given a sufficiently large integer n, then the main result in [11] combined with Lemma 5 gives a Hadamard matrix H of order $m \in [n, n+n^\epsilon)$. Put $k := m - n$, and consider the block decomposition $\frac{1}{\sqrt{m}}H = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$ with $A \in \mathbb{R}^{k\times k}$. By Lemma 4, $I - A$ is invertible, and $M := D + C(I-A)^{-1}B$ satisfies $\|M\|_{\max} \le \frac{1}{\sqrt{m}-k}$. Furthermore, M is orthogonal by Lemma 3, and so

$$u(n) \le \|M\|_{\max} \le \frac{1}{\sqrt{m}-k} \le \frac{1}{\sqrt{n}-n^\epsilon}. \qquad \square$$

3 Lower bound

In this section, we use ideas from Ramsey theory to obtain a lower bound on $\kappa(n)$:

Theorem 6. *There exists $c > 0$ such that $\kappa(n) \geq 1 + \dfrac{c \log n}{n}$ for all sufficiently large $n \not\equiv 0 \bmod 4$.*

Our approach is to identify a poorly conditioned principal submatrix of $A^\top A$ for any given $A \in \{\pm 1\}^{n \times n}$. The following lemma indicates the sort of submatrix we target:

Lemma 7. *Fix positive integers k and $n \geq k$, and suppose $M \in \mathbb{R}^{k \times k}$ is positive semidefinite with n's on the diagonal and positive integers on the off-diagonal. Then $\kappa(M) \geq 1 + \frac{k}{n-1}$, with equality precisely when $M = (n-1)I_k + J_k$.*

Proof. In the case where $M = M_0 := (n-1)I_k + J_k$, it holds that $n-1$ is an eigenvalue with multiplicity $k-1$, and $n-1+k$ is an eigenvalue with multiplicity 1. As such, $\kappa(M) = 1 + \frac{k}{n-1}$. Now suppose $M \neq M_0$. Then $k > 1$ and

$$\lambda_{\max}(M) \geq \frac{\mathbf{1}_k^\top M \mathbf{1}_k}{\mathbf{1}_k^\top \mathbf{1}_k} > \frac{kn + k(k-1)}{k} = \lambda_{\max}(M_0),$$

and so

$$\lambda_{\min}(M) \leq \frac{1}{k-1}\Big(\operatorname{tr}(M) - \lambda_{\max}(M)\Big) < \frac{1}{k-1}\Big(\operatorname{tr}(M_0) - \lambda_{\max}(M_0)\Big) = \lambda_{\min}(M_0).$$

Thus, $\kappa(M) > \kappa(M_0)$. $\square$

A similar proof gives the following:

Lemma 8. *Fix positive integers k and $n \geq k$, and suppose $M \in \mathbb{R}^{k \times k}$ is positive semidefinite with n's on the diagonal and negative integers on the off-diagonal. Then $\kappa(M) \geq 1 + \frac{k}{n+1-k}$, with equality precisely when $M = (n+1)I_k - J_k$.*

Finally, it will be useful to recall the following classic result, which in turn implies the famous necessary condition on Hadamard matrices:

Proposition 9. *There exist three orthogonal vectors in $\{\pm 1\}^n$ if and only if n is a multiple of 4.*

Proof of Theorem 6. In the case where n is odd, let k denote the largest positive integer such that $n \geq R(k,k)$, where $R(k,k)$ denotes the kth diagonal Ramsey number. Then the signs of the entries of $A^\top A$ determine a 2-coloring of the edges of K_n. (Here, the colors are "positive" and "negative".) Since there is necessarily a monochromatic clique of size k, this determines a principal $k \times k$ submatrix M of $A^\top A$ such that all off-diagonal entries have the same sign. Thus, Lemmas 7 and 8 together give

$$\kappa(A) = \sqrt{\kappa(A^\top A)} \geq \sqrt{\kappa(M)} \geq \sqrt{1 + \frac{k}{n-1}}. \tag{2}$$

In the case where n is even, let k denote the largest positive integer such that $n \geq R(3,k,k)$, where $R(3,k,k)$ denotes the appropriate multicolor Ramsey number. Then the signs of the entries of $A^\top A$ determine a 3-coloring of the edges of K_n. (Here, the colors are "zero", "positive", and "negative".) There is either a triangle of color "zero" or a size-k clique of color "positive" or "negative". However, since n is not a multiple of 4, Proposition 9 rules out the first possibility. As such, there is a principal $k \times k$ submatrix M of $A^\top A$ such that all off-diagonal entries have the same sign, and so the bound (2) holds.

In both cases, known bounds on Ramsey numbers give $k \geq \Omega(\log n)$. $\square$

4 Explicit approximate Hadamard matrices

We say $C \in \mathbb{R}^{n\times n}$ is a *conference matrix* if C has 0's on the diagonal, ± 1's on the off-diagonal, and satisfies $C^\top C = (n-1)I$. Delsarte, Goethals, and Seidel [9] showed that, for every conference matrix, one may apply signed permutations to the rows and columns to obtain a conference matrix C that is symmetric (when $n \equiv 2 \bmod 4$) or skew-symmetric (when $n \equiv 0 \bmod 4$). In the latter case, it holds that $C + I$ is a Hadamard matrix; in fact, all *skew Hadamard* matrices arise in this way, and they are conjectured to exist for every $n \equiv 0 \bmod 4$ [22]. When $n \equiv 2 \bmod 4$, it is natural to consider $\kappa(C + I)$.

Lemma 10. *Given a symmetric conference matrix $C \in \mathbb{R}^{n\times n}$, it holds that $\kappa(C + I) = \frac{\sqrt{n-1}+1}{\sqrt{n-1}-1}$.*

Proof. Since $C^2 = C^\top C = (n-1)I$, the eigenvalues of C reside in $\{\pm\sqrt{n-1}\}$. Next, $\operatorname{tr}(C) = 0$ implies that both numbers are eigenvalues with multiplicity $n/2$. Then the eigenvalues of $C+I$ are $\sqrt{n-1}+1$ and $-\sqrt{n-1}+1$, and so the singular values are the absolute values of these: $\sqrt{n-1}+1$ and $\sqrt{n-1}-1$. The quotient is the desired condition number. $\square$

Notably, this implies $\kappa(n) = 1+O(\frac{1}{\sqrt{n}})$ whenever there exists a symmetric conference matrix of order n. This occurs if $n-1 \equiv 1 \bmod 4$ is a prime power, and only if $n-1$ is a sum of two perfect squares [5, 4].

Next, we take inspiration from yet another relaxation of the Hadamard matrix problem, namely, Hadamard's maximal determinant problem; see [6] for a recent survey. One family of matrices $A \in \{\pm 1\}^{n\times n}$ that emerges in this problem satisfies $A^\top A = (n-1)I + J$. These are known as *Barba matrices*. Then $\lambda_{\max}(A^\top A) = 2n-1$ and $\lambda_{\min}(A^\top A) = n-1$, and so

$$\kappa(A) = \sqrt{\kappa(A^\top A)} = \sqrt{\frac{2n-1}{n-1}} = \sqrt{2} + o(1).$$

Such matrices exist, for example, whenever $n = 2(q^2 + q) + 1$ for some odd prime power q; see Theorem A in [16]. Notably, this implies $n \equiv 1 \bmod 4$.

Another important family arises from *supplementary difference sets (SDSs)*. Specifically, when $n \equiv 2 \bmod 4$, suppose there exist circulant matrices $R, S \in \mathbb{R}^{n/2\times n/2}$ that satisfy the autocorrelation identity $R^\top R + S^\top S = (n-2)I + 2J$. Then the matrix

$$A = \begin{bmatrix} R & S \\ S^\top & -R^\top \end{bmatrix}$$

satisfies $A^\top A = I_2 \otimes ((n-2)I_{n/2} + 2J_{n/2})$. As such, $\lambda_{\max}(A^\top A) = 2n-2$ and $\lambda_{\min}(A^\top A) = n-2$, and so

$$\kappa(A) = \sqrt{\kappa(A^\top A)} = \sqrt{\frac{2n-2}{n-2}} = \sqrt{2} + o(1).$$

Furthermore, such matrices exist whenever $n/2 = q^2 + q + 1$ for some odd prime power q; see Theorem 1 in [17].

We conclude this section by discussing Table 1, which reports putative values of $\kappa(n)$ for $n \leq 30$ (in cases other than 1, 2, and multiples of 4). In addition to the first 10 digits of the condition number, we supply its minimal polynomial. By exhaustive search, the reported condition numbers are known to equal $\kappa(n)$ for $n \leq 6$. Interestingly, for smaller values of n, matrices that appear to minimize condition number also maximize the determinant (in absolute value). Also, when n is even, we found a lot of success with circulant $n/2 \times n/2$ blocks, much like the SDS construction. (Each matrix appears as an ancillary file of the arXiv version of this paper.)

Table 1: Putatively minimal condition numbers

n	condition number	minimal polynomial	comments
3	2.000000000	$-2+t$	circulant, symmetric, max determinant
5	1.500000000	$-3+2t$	Barba, circulant, symmetric, max determinant
6	1.581138830	$-5+2t^2$	SDS, circulant 3×3 blocks, symmetric, max determinant
7	1.732050808	$-3+t^2$	symmetric, max determinant
9	1.850781059	$-5-t+2t^2$	symmetric
10	1.500000000	$-3+2t$	SDS, circulant 5×5 blocks, max determinant
11	1.767766953	$-25+8t^2$	symmetric, max determinant
13	1.443375673	$-25+12t^2$	Barba, symmetric, max determinant
14	1.471960144	$-13+6t^2$	SDS, circulant 7×7 blocks, max determinant
15	1.527525232	$-7+3t^2$	symmetric, max determinant
17	1.700930833	$256-1152t^2+1661t^4-936t^6+169t^8$	symmetric
18	1.457737974	$-17+8t^2$	SDS, circulant 9×9 blocks, max determinant
19	1.662877383	$-77+288t^2-307t^4+77t^6$	circulant
21	1.732050808	$-3+t^2$	circulant core
22	1.511424872	$-3719+21191t^2-45561t^4+45825t^6-21466t^8+3719t^{10}$	circulant 11×11 blocks
23	1.702109681	$-6029+40001t^2-93367t^4+93950t^6-40331t^8+6029t^{10}$	circulant core
25	1.428869017	$-49+24t^2$	Barba, max determinant
26	1.329508134	$3-7t^2+3t^4$	circulant 13×13 blocks
27	1.603484352	$-271+1029t^2-1056t^4+271t^6$	block circulant with circulant 9×9 blocks
29	1.666939342	$354061-1045624t^2+1266560t^4-806784t^6+285440t^8-53248t^{10}+4096t^{12}$	circulant core
30	1.379101101	$59-109t^2+41t^4$	circulant 15×15 blocks

5 Comments on AI

N.B.: The content of this section is most naturally presented as a first-person account, so it is written from the perspective of the third author.

For the first month, this project did not involve any AI. We had two main ideas:

1. Inspired by the known circulant approximate Hadamard matrices obtained by randomly perturbing the Legendre symbol, we figured out a non-circulant analogue: Given a Hadamard matrix of order $n+1$, normalize the first row and column before discarding them, and then randomly flip a few -1's to $+1$'s to get condition number $1 + c \cdot n^{-1/4}\sqrt{\log n}$.

2. Inspired by how John and I have studied projective codes [13], we ran a bunch of computer experiments to minimize the condition number for $n \leq 30$, with the intent of hunting for emergent combinatorial structure that would then lead to infinite families.

We wanted to extend our first idea in a way that starts with an approximate Hadamard matrix, thereby giving an inductive construction of approximate Hadamard matrices of order $m-k$ whenever there's a Hadamard matrix of order m. We expected to be able to get k up to $\sqrt{m}$ or so since each random perturbation would increase the fraction of +1s by about $1/\sqrt{m}$. We also knew from ChatGPT (the free version) that Hadamard gaps are currently known to be much smaller than $\sqrt{m}$, so this would be a route to prove $\kappa(n) = 1 + o(1)$. However, we didn't have a clear picture of how the induction would work, so we hesitated to write the details.

Recently, I had upgraded to GPT-5 Pro. I was throwing big open problems at it, but the problems were too hard (or I was bad at prompting), and frustratingly, Pro tended to push back on thinking about famous open problems. (Maybe it was trained to save on compute?) Finally, it occurred to me that I should have Pro write exploratory code in support of our second main idea. After all, this is an intended use case of Pro.

5.1 Exploratory code

About a month prior, we launched a private table of putatively optimal approximate Hadamard matrices. My only surviving contributions were for $n \in \{3, 5, 6, 9\}$. But then I ran some code written by Pro, and it improved the $n = 13$ case from 1.7677 to 1.4433. (!) Notably, I didn't tell Pro how it should perform the optimization (and I never bothered to find out what it did); it just selected an approach and then outperformed about a month's worth of expert searching. Sadly, the code didn't improve any other entries, so perhaps this was just a weak point in the table.

The drop from 1.7677 to 1.4433 was so big that we expected some hidden combinatorial structure in the matrix. So I asked Pro for an explanation involving combinatorial design, and it provided a plausible explanation in terms of the projective plane $\mathrm{PG}(2, 3)$. At this point, I was hoping for an infinite family, so I asked Pro, but other constructions involving projective planes have larger condition numbers; this was a fluke. After more back and forth, Pro realized this matrix achieves equality in the *Barba bound* for Hadamard's maximal determinant problem. By consulting a recent survey on this problem [6] (also pointed to by Pro), we identified the infinite family in Section 4 with condition number $\sqrt{2} + o(1)$ and improved the $n = 25$ entry in our table.

(I wouldn't have expected any relationship between Hadamard's maximal determinant problem and approximate Hadamard matrices, but in hindsight, there's a nice analogy with energy minimization on the sphere. In particular, there are special configurations of points that simultaneously minimize a diverse family of energies [8]. So while I can't prove a strong relationship between the determinant and the condition number, it still makes sense to evaluate the condition number of determinant maximizers on the off chance they're sufficiently universally optimal.)

5.2 Proof discovery

Part of me was hoping the exploratory code would inspire enough infinite families to render our first main idea moot. But after exhausting that avenue, it was time to return to the induction. Since it wasn't clear to us how the induction should go, I expected it to take a full day to work out one approach, only to see how it breaks. Maybe Pro could help navigate this for me?

I started by telling Pro a sketch of the result we already had, and I asked it to flesh out the details. I actually forgot to mention that we used matrix Bernstein, but it figured it out. A perfect reconstruction of the proof on the first try. So then I explained how we wanted to extend this result to get even smaller approximate Hadamard matrices, and I told it my vague concepts of a plan of how an induction might go. And it responded with a proof! But the proof was wrong. After lots of back and forth, it started to push back on the inductive approach entirely. Instead, it wanted to push towards a "one-shot" approach, but I wasn't convinced.

I asked how the one-shot approach would treat the $k = 1$ case we already understood, and it described an expected matrix that was a rank-1 perturbation (involving the discarded row and column vectors) of the surviving $n \times n$ matrix (before normalization). But in general, we want this expected matrix to be a multiple of an orthogonal matrix, and that seemed difficult to me, so I asked a more general question (paraphrased):

> Given an orthogonal matrix with block decomposition $\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$, how can you use A, B, C, and D to construct an orthogonal matrix of the same size as D?

After some thought, it came up with

$$D + C(I - A)^{-1}B.$$

I didn't believe it. I asked for a proof, and it gave a full page of calculations that I wasn't interested in checking. So I punched the formula into MATLAB with a random orthogonal matrix, and the result was orthogonal!

Where did this formula come from? Pro points to references from linear system theory, scattering theory, and operator theory (e.g., [3]), but I would never have thought to consult these corners of the literature. Case in point, this exact formula for submatrix orthogonalization is the subject of a reference request on MathOverflow [20], but no one offers a pointer to the existing literature.

Once I had this submatrix orthogonalization formula (see Lemma 3), I was able to sketch a "one-shot" proof of the desired result to Pro, and it responded with all the details fleshed out (much like my experience with the original $k = 1$ case). It's clear that Pro is much better at writing a proof from a sketch than from scratch. (Aren't we all?) But here's the most humbling thing about this experience: I don't know if I could've proven this result without the submatrix orthogonalization formula, and I don't think I would've come up with that formula on my own.

(More generally, how many open problems could be solved today if the experts knew the relevant results from other communities? I'm optimistic that AI will help to close this gap.)

5.3 Formalization

The only theoretical component of this paper that came from AI is submatrix orthogonalization (Lemma 3). Out of an abundance of caution, we decided to formalize the proof of this result in Lean [15]. Instead of vibe coding a proof with ChatGPT as in [2], we adopted a much more user-friendly auto-formalization workflow. Boris asked Pro to state the result in Lean, with a couple pointers to block matrix concepts like `fromBlocks`. After 9 minutes of thinking, it responded with a formal statement that looked very clean and clearly corresponded exactly to the intended result.

Boris then asked Aristotle [1] to prove the result, offering no hints whatsoever. After 13 minutes, it responded with a formal proof, and it type-checked with no issues. (The Lean code appears as an ancillary file of the arXiv version of this paper.)

At this point, we've verified Lemma 3 in four independent ways: (1) we checked it in MATLAB with random orthogonal matrices, (2) we identified references in the literature that state the result, (3) we wrote out a human-readable proof, and (4) we auto-formalized a proof in Lean. The result is legit. I have no intuition for it, but I know it's true.

6 Discussion

In this paper, we showed that the smallest-possible condition number of $n \times n$ approximate Hadamard matrices approaches 1 as $n \to \infty$, and we presented some explicit constructions. Several open problems remain, and in this section, we highlight a few of them. Our first problem asks for the rate at which the best condition number approaches 1:

Problem 11. What is the largest α for which $\kappa(n) = 1 + \dfrac{f(n)}{n^\alpha}$ for some subpolynomial f?

We currently know that $\frac{17}{92} \leq \alpha \leq 1$. Better upper bounds on gaps between Hadamard matrices will increase this lower bound, but with our proof technique, the Hadamard conjecture only increases the lower bound to $\frac{1}{4}$. Meanwhile, our explicit construction involving symmetric conference matrices suggests taking α to be $\frac{1}{2}$.

Next, we are interested in the optimal version of Dong and Rudelson's original result in [10]:

Problem 12. What is $\sup_n \kappa(n)$?

Of course, our result $\kappa(n) \to 1$ reduces this to a finite problem. Sadly, it's not all that finite: even assuming the Hadamard conjecture, a refinement of our upper bound on $\kappa(n)$ establishes that $\kappa(n) < 2$ for every $n > 3.11 \times 10^6$. For the record, the authors believe $\sup_n \kappa(n) = 2$, and to prove this, it suffices to treat odd n, since taking a Kronecker product with a 2×2 Hadamard matrix would cover the even case. For larger values of n that are not resolved by the asymptotic result, it might suffice to find circulant approximate Hadamard matrices, considering Steinerberger's main result in [18].

Unfortunately, we didn't find many explicit examples to help close this gap. At the moment, we observe a "$\sqrt{2}$ bottleneck" in the case where n is odd:

Problem 13. Is there an explicit infinite family of approximate Hadamard matrices of odd order with condition number less than $\sqrt{2}$?

Strangely, none of the condition numbers in Table 1 are less than $\sqrt{2}$ for odd n.

Acknowledgments

DGM thanks Stefan Steinerberger for introducing him to this problem. BA and DGM thank OpenAI for access to GPT-5 Pro, and Harmonic for access to Aristotle. JJ was supported by NSF DMS 2220320. DGM was supported by NSF DMS 2220304. The views expressed are those of the authors and do not reflect the official guidance or position of the United States Government, the Department of Defense, the United States Air Force, or the United States Space Force.

References

[1] T. Achim, et al., Aristotle: IMO-level automated theorem proving, arXiv:2510.01346 (2025).

[2] B. Alexeev, D. G. Mixon, Forbidden Sidon subsets of perfect difference sets, featuring a human-assisted proof, arXiv:2510.19804 (2025).

[3] D. Alpay, J. A. Ball, Y. Peretz, System theory, operator models and scattering: The time-varying case, J. Oper. Theory 47 (2002) 245–286.

[4] N. A. Balonin, J. Seberry, A review and new symmetric conference matrices, `ro.uow.edu.au/cgi/viewcontent.cgi?article=3757&context=eispapers`, retrieved November 14, 2025.

[5] V. Belevitch, Theorem of $2n$-terminal networks with application to conference telephony, Electr. Commun. 27 (1950) 231–244.

[6] P. Browne, R. Egan, F. Hegarty, P. Ó. Catháin, A survey on the Hadamard maximal determinant problem, Electron. J. Combin. 28 (2021).

[7] R. Craigen, Signed groups, sequences, and the asymptotic existence of Hadamard matrices, J. Combin. Theory Ser. A 71 (1995) 241–254.

[8] H. Cohn, A. Kumar, Universally optimal distribution of points on spheres, J. Amer. Math. Soc. 20 (2007) 99–148.

[9] P. Delsarte, J. M. Goethals, J. J. Seidel, Orthogonal matrices with zero diagonal II, Can. J. Math. 33 (1971) 816–832.

[10] X. Dong, M. Rudelson, Approximately Hadamard matrices and Riesz bases in random frames, Int. Math. Res. Not. IMRN 2024 (2024) 2044–2065.

[11] C. Du, Y. Jiang, Golay complementary sequences of arbitrary length and asymptotic existence of Hadamard matrices, arXiv:2401.15381 (2024).

[12] P. Jaming, M. Matolcsi, On the existence of flat orthogonal matrices, Acta Math. Hungar. 147 (2015) 179–188.

[13] J. Jasper, E. J. King, D. G. Mixon, Game of Sloanes: Best known packings in complex projective space, Proc. SPIE 11138 (2019) 416–425.

[14] M. Manskova, Open problems UP24, arXiv:2504.04845 (2025).

[15] L. de Moura, S. Ullrich, The Lean 4 theorem prover and programming language, CADE 2021, 625–635.

[16] M. G. Neubauer, A. J. Radcliffe, The maximum determinant of ± 1 matrices, Linear Algebra Appl. 257 (1997) 289–306.

[17] E. Spence, Skew-Hadamard matrices of the Goethals-Seidel type, Canad. J. Math. 27 (1975) 555–560.

[18] S. Steinerberger, A note on approximate Hadamard matrices, Des. Codes Cryptogr. 92 (2024) 3125–3131.

[19] S. Steinerberger, Some open problems, `faculty.washington.edu/steinerb/openproblems.pdf`, retrieved November 14, 2025.

[20] B. Terrell, Reduction of size of orthogonal matrices, `https://mathoverflow.net/questions/112430/reduction-of-size-of-orthogonal-matrices`, retrieved November 14, 2025.

[21] J. A. Tropp, An Introduction to Matrix Concentration Inequalities, Found. Trends Machine Learn. 8 (2015) 1–230.

[22] J. Wallis, Some $(1, -1)$ matrices, J. Combin. Theory Ser. B 10 (1971) 1–11.