A Comment on the Hadamard Conjecture

Warwick de Launey

Center for Communications Research
4320 Westerra Court
San Diego, California, CA92121
E-mail: warwick@ccrwest.org

and

Daniel M. Gordon

Center for Communications Research
4320 Westerra Court
San Diego, California, CA92121
E-mail: gordon@ccrwest.org

Fix n. Let $\boldsymbol{r}(n)$ denote the largest number r for which there is an $r \times n$ $(1, -1)$-matrix H satisfying the matrix equation $HH^\top = nI_r$. The Hadamard conjecture states that for n divisible by 4 we have $\boldsymbol{r}(n) = n$. Let $\epsilon > 0$. In this paper, we show that the Extended Riemann Hypothesis and recent results on the asymptotic existence of Hadamard matrices imply that for n sufficiently large $\boldsymbol{r}(n) > \left(\frac{1}{2} - \epsilon\right) n$.

Key Words: Hadamard matrices, Extended Riemann Hypothesis, orthogonal arrays

1. OVERVIEW

The following theorem was proved in [4].

Theorem 1.1. *There is an absolute positive integer c_1 and an integer N such that for all $t > N$, we have $\boldsymbol{r}(4t) \geq \frac{4}{3}t - 2(2t-3)^{\frac{2}{3}} \log^{c_1}(2t-3)$.*

Thus for sufficiently large $n = 4t$, there is about one third of a Hadamard matrix. Standard arguments (described in [4]) show that for all $t > 1$, there exists a two level, strength two, orthogonal array $\mathrm{OA}_t(\boldsymbol{r}(4t) - 1, 2)$ with $\boldsymbol{r}(4t) - 1$ constraints and index t. Therefore Theorem 1.1 leads to lower bounds on the size of several interesting combinatorial objects. These include transversal designs, resolvable transversal designs, high distance binary error correcting block codes and sets of mutually orthogonal F-squares. Except in the case of F-squares, the ratio between the lower bound given by Theorem 1.1 and the well established upper bound is asymptotic to one third. For the F-squares the ratio is asymptotic to one ninth.

The approach taken in [4] was to concatenate three Hadamard matrices derived from Paley's conference matrices with orders close to $2t/3$ and summing to $2t$. Clearly, the best one could hope to prove by concatenating Hadamard matrices is that $\boldsymbol{r}(4t)/4t \to 1/2$ as t grows. However, even though experiments (see [5]) suggest that there are sufficiently many Paley conference matrices to imply that $\boldsymbol{r}(4t)/4t \to 1/2$ as $t \to \infty$, proving this is true would imply that every even number is the sum of two prime powers a proposition which is very close to the Goldbach conjecture. So even though this approach might be of practical interest, it seems a rigorous proof would require some new deep mathematics.

The goal of this paper is to prove the following result.

Theorem 1.2. *Let $\epsilon > 0$. If the Extended Riemann Hypothesis is true, then for every sufficiently large $n \equiv 0 \pmod 4$*

$$\boldsymbol{r}(n) \geq \frac{n}{2} - n^{\frac{17}{22}+\epsilon}.$$

Hence provided the Extended Riemann Hypothesis is true, there is for every sufficiently large $n = 4t$ about one half of a Hadamard matrix. The ratios between the lower bounds implied by Theorem 1.2 and the standard upper bounds on the size of the related combinatorial designs are asymptotic to one half and one quarter instead of one third and one ninth. So the conclusion of Theorem 1.2 is much stronger than that of Theorem 1.1.

Theorem 1.2 is proved by concatenating a type I Paley Hadamard matrix with a Hadamard matrix whose existence is guaranteed by recent results on the asymptotic existence of Hadamard matrices. The argument depends on there being a prime power in a short arithmetic progression. Unfortunately, we cannot prove the existence of such a prime power without recourse to the Extended Riemann Hypothesis. It is noteworthy that our argument would not have succeeded without Craigen's recent improvements of Seberry's original result on the asymptotic existence of Hadamard matrices.

2. PROOF OF THE THEOREM

To prove Theorem 1.2, we prove the following lemma. Its proof is given in Section 3.

Lemma 2.1. *Let a be any positive real number. Suppose that for some absolute positive constant c_2, there is a Hadamard matrix of order $2^t r$ when-*

ever

$$2^t \geq c_2 r^a. \tag{1}$$

Let $\epsilon > 0$. *If the Extended Riemann Hypothesis is true, then for every sufficiently large* $n \equiv 0 \pmod 4$ *we have*

$$\boldsymbol{r}(n) \geq \frac{n}{2} - n^{\frac{1}{2}+\frac{a}{1+a}+\epsilon}. \tag{2}$$

Proof (Proof of Theorem 1.2). In 1993, Craigen's result in [2] shows that we can take $c_2 = 2^{\frac{16}{5}}$ and $a = 4/6$, and a later result [1, Theorem 24.27(3)] implies that we may take $c_2 = 2^{\frac{26}{16}}$ and $a = 3/8$. Using the latter values in the lemma gives the theorem. ▮

Remark 2. 1. In the lemma, note that the best deviation we can hope for is the square root of n, and that the smaller the value of a the closer one comes to achieving this deviation. In the mid 1970's, Seberry [6] showed that we may take $c_2 = 1$ and $a = 2$. However, the lemma is vacuous for $a \geq 1$. So Craigen's advances are essential.

3. PROOF OF THE LEMMA

Proof (Proof of Lemma 2.1). By Remark 2.1, we may suppose that $a < 1$. It is sufficient to prove the result for ϵ in the open interval $(0, \frac{1}{1+a} - \frac{1}{2})$. Choose $\delta \in (0, \epsilon)$, and set $\gamma = \frac{1}{1+a} - \frac{1}{2} - (\epsilon - \delta)$. Then $\gamma \in (\delta, \frac{1}{1+a} - \frac{1}{2})$. Let 2^t be the smallest power of two not smaller than $n^{\frac{a}{1+a}+\delta}$; let $r = [n/2^{t+1}]$; and let $y = [n^b]$, where $b = \frac{1}{1+a} - \gamma$. Hence

$$b = \frac{1}{2} + (\epsilon - \delta) > \frac{1}{2} \tag{3a}$$

$$n^{\frac{a}{1+a}+\delta} \leq 2^t < 2n^{\frac{a}{1+a}+\delta} \tag{3b}$$

$$\frac{n}{2} \geq 2^t r > \frac{n}{2} - 2^t > \frac{n}{2} - 2n^{\frac{a}{1+a}+\delta} \tag{3c}$$

$$2^t(r+y) < \frac{n}{2} + 2^t n^{\frac{1}{1+a}-\gamma} \leq \frac{n}{2} + 2n^{1+\delta-\gamma} = \frac{n}{2} + 2n^{\frac{a}{1+a}+\delta+b}. \tag{3d}$$

So for the arithmetic progression

$$\mathcal{S} = \{n - 2^t r - 1, n - 2^t(r+1) - 1, \ldots, n - 2^t(r+y) - 1\},$$

we have by equations (3c) and (3d)

$$\mathcal{S} \subseteq [\frac{n}{2} - 2n^{\frac{a}{1+a}+\delta+b} - 1, \frac{n}{2} + 2n^{\frac{a}{1+a}+\delta+b} - 1]. \tag{4}$$

In particular, for n sufficiently large $\mathcal{S}$ contains only positive integers. Moreover (since $y \leq n^b$ and $\delta < \gamma$) for sufficiently large n we have by the inequalities (3b) and (3c)

$$\begin{aligned} c_2(r+y)^a \leq c_2(\frac{n}{2^{t+1}} + n^b)^a &\leq c_2(\frac{1}{2}n^{\frac{1}{1+a}-\delta} + n^{\frac{1}{1+a}-\gamma})^a \\ &\leq c_2(n^{\frac{a}{1+a}-a\delta}) \leq n^{\frac{a}{1+a}+\delta} \leq 2^t. \end{aligned}$$

So by equation (1) for sufficiently large n there is a Hadamard matrix of order $2^t k$ for $k = r, r+1, \ldots, r+y$.

Now suppose there is a prime power $p = n - 2^t k_0 - 1$ in the sequence $\mathcal{S}$. Then, since $n \equiv 0 \pmod 4$, for n sufficiently large, we must have $p \equiv 3 \pmod 4$. Hence, we can combine Paley's type I Hadamard matrix of order $p+1$ with the Hadamard matrix of order $2^t k_0$ to prove that $\boldsymbol{r}(n) \geq \min\{n - 2^t k_0, 2^t k_0\}$. By the containment (4), we therefore have

$$\boldsymbol{r}(n) \geq \frac{n}{2} - 2n^{\frac{a}{1+a}+\delta+b}. \tag{5}$$

To show that the sequence $\mathcal{S}$ contains a prime power (given the Extended Riemann Hypothesis), consider the quantity

$$\psi(x;q,d) \quad = \sum_{\substack{k \leq x \\ k \equiv d \pmod q}} \Lambda(k)$$

where von Mangoldt's function $\Lambda(k)$ equals $\log p$ if k is a power of the prime p and zero otherwise. Note that the number $\Pi(x;q,d)$ of prime powers $p^t \leq x$ congruent to d modulo q satisfies

$$\psi(x;q,d) \geq \Pi(x;q,d) \geq \psi(x;q,d)/\log x.$$

Let d be the non-negative integer less than 2^t such that $d \equiv n-1 \pmod{2^t}$. By the Extended Riemann Hypothesis [3, equation (14) of Chapter 20]),

$$\begin{aligned} &\psi(n - 2^t r - 1; 2^t, d) - \psi(n - 2^t(r+y) - 1; 2^t, d) \\ = &\ \frac{2^t y}{\phi(2^t)} + \mathrm{O}((n - 2^t r - 1)^{\frac{1}{2}}(\log(n - 2^t r - 1))^2) \\ = &\ 2y + \mathrm{O}((n - 2^t r - 1)^{\frac{1}{2}}(\log(n - 2^t r - 1))^2). \end{aligned}$$

Now by the inequalities (3c) we have $2^t r/n \to 1/2$ as $n \to \infty$; so to guarantee the sequence $\mathcal{S}$ contains a prime power, we need

$$\frac{n^b}{n^{1/2}(\log n)^3} \to \infty \qquad \text{as } n \to \infty.$$

This happens if and only if $b > \frac{1}{2}$. By equation (3a), this inequality holds. Therefore the inequality (5) applies and we have (since $b = \frac{1}{2} + \epsilon - \delta$)

$$\boldsymbol{r}(n) > \frac{n}{2} - 2n^{\frac{a}{1+a}+\delta+\frac{1}{2}+\epsilon-\delta} = \frac{n}{2} - 2n^{\frac{1}{2}+\frac{a}{1+a}+\epsilon}.$$

Since this holds for all ϵ in the open interval $(0, \frac{1}{1+a} - \frac{1}{2})$, we may absorb the factor 2 appearing in the last term into the ϵ in the exponent. This completes the proof of the lemma. ▌

REFERENCES

1. Craigen, R., "Hadamard matrices and Designs," *The CRC Handbook of Combinatorial Designs*, Ed.s C. J. Colbourne and J. H. Dinitz, CRC Press, 1995.
2. Craigen, R., "Signed Groups, Sequences, and the Asymptotic existence of Hadamard matrices," *J. Combin. Th. Ser. A* **71** (1995), 241–254.
3. Davenport, H., "Multiplicative Number Theory," Second Edition, Springer-Verlag, New York Berlin Heidelberg, 1980.
4. de Launey, Warwick, "On the Asymptotic Existence of Partial Complex Hadamard Matrices and Related Combinatorial Objects," *Discrete Applied Mathematics*, to appear.
5. de Launey, Warwick and Gordon, D. M., "A remark on Plotkin's bound," preprint.
6. Seberry-Wallis, J., "On the existence of Hadamard matrices," *J. Combin. Th. Ser. A* **21** (1976), 188–195.