ON THE ASYMPTOTIC EXISTENCE OF HADAMARD MATRICES

WARWICK DE LAUNEY

Abstract. It is conjectured that Hadamard matrices exist for all orders $4t$ ($t > 0$). However, despite a sustained effort over more than five decades, the strongest overall existence results are asymptotic results of the form: for all odd natural numbers $k$, there is a Hadamard matrix of order $k2^{[a+b \log_2 k]}$, where $a$ and $b$ are fixed non-negative constants. To prove the Hadamard Conjecture, it is sufficient to show that we may take $a = 2$ and $b = 0$. Since Seberry’s ground-breaking result, which showed that we may take $a = 0$ and $b = 2$, there have been several improvements where $b$ has been by stages reduced to $3/8$. In this paper, we show that for all $\epsilon > 0$, the set of odd numbers $k$ for which there is a Hadamard matrix of order $k2^{2+\epsilon \log_2 k}$ has positive density in the set of natural numbers. The proof adapts a number-theoretic argument of Erdos and Odlyzko to show that there are enough Paley Hadamard matrices to give the result.

1. Overview

As noted in the abstract, there have been incremental improvements in the power of known asymptotic existence results for Hadamard matrices [1 2 7]. These theorems all have the form: For all positive odd integers $k$, there is a Hadamard matrix of order $k2^{[a+b \log_2 k]}$, where $a$ and $b$ are fixed non-negative real numbers. The strength of the result depends on how close $b$ is to zero, and then on how close $a$ is to zero. In this paper, we adapt a number-theoretic argument of Erdos and Odlyzko [5] to prove the following theorem.

Theorem 1.1. Let $\epsilon > 0$. Let $H(x)$ denote the number of odd positive integers $k \leq x$ for which there is a Hadamard matrix of order $2^\ell k$, for some positive integer $\ell \leq 2 + \epsilon \log_2 k$. Then there is a constant $c_1(\epsilon)$, dependent only on $\epsilon$, such that, for all sufficiently large $x$, $H(x) > c_1(\epsilon)x$.

Key words and phrases. Hadamard matrices, asymptotic existence, cocyclic Hadamard matrices, relative difference sets, Riesel numbers, Extended Riemann Hypothesis.

Work by a Contractor to the US Government.
Our approach is to prove the following number-theoretic result.

**Theorem 1.2.** Let $\epsilon > 0$. Let $M_\epsilon(x)$ denote the number of odd positive integers $k \leq x$ for which $2^mk - 1$ is prime for some positive integer $m \leq \epsilon \log_2 k$. Then there is a constant $c_2(\epsilon)$, dependent only on $\epsilon$, such that for all sufficiently large $x$, $M_\epsilon(x) > c_2(\epsilon)x$.

Since there is a Paley Hadamard matrix of order $q + 1$, when $q \equiv 3 \pmod{4}$ is prime, and of order $2(p+1)$, when $p \equiv 1 \pmod{4}$ is prime, taking a Kronecker product with the Sylvester Hadamard matrix of appropriate order, we have, for any odd prime $p$, a Hadamard matrix of order $2^m(p+1)$, where

$$m \geq \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

So, for $k$ odd, when $2^mk - 1$ equals a prime $p$, for some positive integer $m < \epsilon \log_2 k$, there is a Hadamard matrix of order $2^mk$ if $m > 1$, and of order $2^2k$ if $m = 1$. So, in either case, there is a Hadamard matrix of order $2^\ell k - 1$, for some positive integer $\ell \leq 2 + \epsilon \log_2 k$. Therefore, Theorem 1.2 certainly implies Theorem 1.1 with $c_1(\epsilon) = c_2(\epsilon)$.

**Remark 1.1.** 1. Since the Hadamard matrices used above are all cocyclic (see [4] for this fact and a discussion of cocyclic Hadamard matrices), Theorem 1.1 also holds for cocyclic Hadamard matrices. Thus we have an asymptotic existence result for a certain class of relative difference sets.

2. Since there is a Sylvester matrix of order 4, there is a constant $c'_1(\epsilon)$ dependent only on $\epsilon$, such that $H(x) \geq c'_1(\epsilon)x$ for all $x \geq 1$.

There are inherent limitations to our approach. The Hadamard Conjecture implies that we may take $c_1(\epsilon) = 1/2$. However, the following holds.

**Proposition 1.3.** There is a positive number $\delta_0$, such that, for all $\epsilon > 0$, there are infinitely many $x \geq 0$ for which $M_\epsilon(x) \leq \frac{1}{2}(1 - \delta_0)x$. Moreover, if the Extended Riemann Hypothesis holds, then for all $\epsilon, \delta > 0$, we have $M_\epsilon(x) \leq x2(1 + \delta)\log_2(1 + \epsilon)$ for all sufficiently large $x$.

The part concerning the Extended Riemann Hypothesis will be proved in Section 3. We explain now why the first part of the proposition holds. H. Riesel [6] showed that there are infinitely many odd numbers $k$ for which $2^mk - 1$ is always composite. The smallest known such number is 509203. Indeed, it can be shown that for any $m \geq 0$, at least one of the primes 3, 5, 7, 13, 17 or 241 divides $2^mk - 1$, where $k = 509203 + 11184810r$, and $r$ is any non-negative integer. Consequently, for any $\epsilon > 0$, there are infinitely many $x \geq 0$ such that
M_1(x) \leq x(1 - 1/11184810)/2. This proves the first part of the proposition, and shows that the approach to \( c_1(\epsilon) \) via \( c_2(\epsilon) \) will fail once \( c_1(\epsilon) \) becomes close enough to 1/2. Indeed, the proposition says that if the Extended Riemann Hypothesis holds, then the approach will fail once we ask that \( c_1(\epsilon) \) exceed 2 log_2(1 + \epsilon), a number which, when \( \epsilon \) is small, is far less than 1/2.

On the other hand, by using more involved number-theoretic arguments to explore the scope of known constructions for Hadamard matrices, one might be able to show that \( c_1(\epsilon) \) can be taken very close to 1/2. Aside from offering us a way to prove strong asymptotic existence results for Hadamard matrices, this approach has the advantage of giving us a measure of how far we have come towards proving the Hadamard Conjecture. We now describe a replacement constant \( c_3(\epsilon) \) for \( c_2(\epsilon) \).

Notice that if there is a Hadamard matrix of order \( k_i 2^{[\epsilon \log_2 k_i]} \) for \( i = 1, 2, \ldots, n \), then there is a Hadamard matrix of order \( k 2^{\epsilon \log_2 k} \) for \( k = k_1 k_2 \ldots k_n \). So define \( M'_i(x) \) to be the number of odd positive integers \( k \) with the property P, say, that \( k = k_1 k_2 \ldots k_n \) where, for \( i = 1, 2, \ldots, n \), there are \( m_i \leq \epsilon \log_2 k_i \) such that \( k_i 2^{m_i} - 1 \) is prime for \( i = 1, 2, \ldots, n \). Clearly, Theorem 1.2 implies that there is a constant \( c_3(\epsilon) > 0 \) such that \( M'_i(x) \geq c_3(\epsilon) x \) for all sufficiently large \( x \). Notice that, by the Prime Number Theorem for primes in arithmetic progression, there are infinitely many Riesel numbers which are prime. Therefore there are infinitely many numbers which do not have property P. However, notice that if \( k_1 \) and \( k_2 \) have property P, then so does \( k = k_1 k_2 \), and, since most large numbers \( k \) can be written in the form \( k_1 k_2 \) in many ways, it seems likely that almost all numbers have property P. So more complicated counting arguments along the lines of those described in this paper might be used to prove that \( c_1(\epsilon) \) can be taken very close to 1/2.

The rest of this paper is organized as follows. In Section 2, we prove Theorem 1.2. Then in Section 3, assuming a lemma concerning the Extended Riemann Hypothesis, we prove Proposition 1.3. Finally, in Section 4, we prove the lemma needed in Section 3.

2. Proof of Theorem 1.2

We adapt an argument of Erdos and Odlyzko [5] to prove the following lemma. The lemma and our comments about how large one can take \( c_1(\epsilon) \) is of independent number-theoretic interest.

**Lemma 2.1.** Let \( \epsilon > 0 \). Let \( N_\epsilon(x) \) denote the number of positive integers \( k \leq x \) for which \( 2^m k - 1 \) is prime for some positive integer
\[ m < \epsilon \log_2 x. \text{ Then there is a constant } c_4(\epsilon), \text{ dependent only on } \epsilon, \text{ such that, for all sufficiently large } x, N_\epsilon(x) > c_4(\epsilon)x. \]

Before we prove this lemma, we confirm that it implies Theorem 1.2. In fact, we prove the following stronger result.

**Lemma 2.2.** Lemma 2.1 and Theorem 1.2 are equivalent. Under this equivalence, the constants \( c_4(\epsilon) \) and \( c_2(\epsilon) \) are related as follows:

\[ c_4(\epsilon) = c_2(\epsilon) > (1 - \delta)c_4(\epsilon/A), \quad (1) \]

for all \( A > 1 \) and \( \delta > 0 \).

**Proof.** First notice that Theorem 1.2 implies Lemma 2.1 with \( c_4(\epsilon) = c_2(\epsilon) \). So it is sufficient to prove that Lemma 2.1 implies Theorem 1.2 with \( c_2(\epsilon) > (1 - \delta)c_4(\epsilon/A) \) for all \( A > 1 \) and \( \delta > 0 \).

Fix \( x \). Then, for all \( A > B > 1 \),

\[ M_\epsilon(x) > N_\epsilon(x) - N_{\epsilon A}(x^{1/A}) > c_4(\epsilon)x - x^{1/B} = c_4(\epsilon)(1 - x^{-1+1/B})x. \]

So, for all \( A > B > 1 \) and \( \delta > 0 \),

\[ M_\epsilon(x) > x(1 - \delta)c_4(\epsilon/A), \]

for all \( x > \delta^{B/(1-B)} \). Consequently, we may take \( c_2(\epsilon) > (1 - \delta)c_4(\epsilon/A) \), for all \( A > 1 \) and \( \delta > 0 \). This completes the proof of the lemma. □

Therefore, since Theorem 1.2 implies Theorem 1.1 with \( c_1(\epsilon) = c_2(\epsilon) \), Lemma 2.1 implies Theorem 1.1 with

\[ c_1(\epsilon) > (1 - \delta)c_4(\epsilon/A), \]

for all \( A > 1 \) and \( \delta > 0 \).

We now prove Lemma 2.1. Fix \( \epsilon > 0 \), an integer \( x \geq 4^{1/\epsilon} \), and set \( L = \lfloor \epsilon \log_2 x \rfloor - 1 \). So \( L \geq 1 \), and \( L + 1 \) is the largest integer less than or equal to \( \epsilon \log_2 x \). In particular,

\[ x \geq (2^{L+1})^{1/\epsilon}, \quad (2) \]

and

\[ L = \epsilon \log_2 x - \alpha \quad \text{where } 2 > \alpha \geq 1. \quad (3) \]

For odd \( k \leq x \), let \( S(k, x) \) denote the number of primes of the form \( 2^\ell k - 1 \) where \( \ell = 1, 2, \ldots, L \). Then

\[ N_\epsilon(x) \geq \sum_{k \leq x \atop odd} 1\{S(k, x) > 0\}. \]

We show that the variance of \( S(k, x) \) is quite small. We have the following analog to a special case of Lemma 2 of [5].
Lemma 2.3. There exists a constant $c_5(\epsilon)$, dependent on $\epsilon$ only, such that, for all sufficiently large $x$,

$$\sum_{k \leq x \text{ odd}} S^2(k, x) \leq c_5(\epsilon)x.$$ \hfill (5)

Proof. In their paper [5], Erdos and Odlyzko fix $r$ base primes $p_1, p_2, \ldots, p_r$, and, for each positive integer $k \leq x$ coprime to $p_1p_2\ldots p_r$, define the quantity $R(k, x)$ to be the number of $r$-tuples $(a_1, a_2, \ldots, a_r)$ $(a_i = 1, 2, \ldots, N)$ such that $1 + k \prod_{a_i}^{N} a_i^{p_i}$ is prime. Here $N \sim c' \log x$, where $c'$ is a fixed constant. They assert that there is a constant $c''$, which depends only on the choice of base primes and $c'$, such that

$$\sum_{k \leq x \text{ odd}} R^2(k, x) \leq c''x(\log x)^{2r-2}. \hfill (4)$$

Our quantity $S(k, x)$ is analogous to their quantity $R(k, x)$ with $r = 1$, $p_1 = 2$, $N = L$, and $c' = \epsilon/\log 2$. With these settings, their quantity $R(k, x)$ is defined for odd $k \leq x$ and counts the number of integers $\ell \in \{1, 2, \ldots, L\}$ for which $2^\ell k+1$ is prime. On the other hand, our quantity $S(k, x)$ is defined for odd $k \leq x$ and counts the number of integers $\ell \in \{1, 2, \ldots, L\}$ such that $2^\ell k - 1$ is prime. As pointed out at the end of the introduction to their paper, their techniques handle primes of the form $2^\ell k - 1$ in the same way as they set out for primes of the form $2^\ell k + 1$. In particular, equation (4) also holds for $r = 1$, and $p_1 = 2$, when our quantity $S(k, x)$ replaces the analogous quantity $R(k, x)$.

Following Erdos and Odlyzko, we have by the Cauchy-Schwarz inequality

$$N_\epsilon(x) \geq \left(\sum_{k \leq x \text{ odd}} S(k, x)\right)^2 / \sum_{k \leq x \text{ odd}} S^2(k, x) \geq \frac{1}{c_5(\epsilon)x} \left(\sum_{k \leq x \text{ odd}} S(k, x)\right)^2.$$ \hfill (6)

To prove the lemma, it is therefore sufficient to show there is a constant $c_6(\epsilon)$ dependent only on $\epsilon$, such that for all sufficiently large $x$

$$\sum_{k \leq x \text{ odd}} S(k, x) \geq c_6(\epsilon)x. \hfill (5)$$

For then we may take

$$c_4(\epsilon) = c_6(\epsilon)^2/c_5(\epsilon). \hfill (6)$$

Let $\pi(x; q, a)$ denote the number of primes $p \leq x$ such that $p \equiv a \pmod{q}$. Then, since $\pi(2^\ell x - 1; 2^{\ell+1}, 2^\ell - 1) = \pi(2^{\ell} x; 2^{\ell+1}, 2^{\ell} - 1)$,
and, since \( p = 2^\ell k - 1 \) is prime for some odd positive integer \( k \leq x \) if and only if \( p \leq 2^\ell x \) is a prime congruent to \( 2^\ell - 1 \) modulo \( 2^{\ell + 1} \), we have

\[
\sigma_\epsilon(x) = \sum_{\substack{k \leq x \ \text{odd} \ \text{for all } \ell \leq x}} S(k, x) = \sum_{\ell=1}^L \pi(2^\ell x; 2^{\ell + 1}, 2^\ell - 1). \]

To estimate the sum on the right, we use the following lemma which is a special case of Lemma 1 of Erdos and Odlyzko [5].

**Lemma 2.4.** There exist constants \( c_7 \) and \( c_8 \) such that, for all integers \( \ell \geq 1 \),

\[
\pi(x; 2^{\ell + 1}, 2^\ell - 1) \geq \frac{c_7 x}{2^\ell \log x}, \quad \text{for all } x \geq (2^{\ell + 1})^{c_8}.
\]

Now by the inequality (2), for \( \epsilon \leq 1/c_8 \), we have

\[
x \geq (2^{\ell + 1})^{1/\epsilon} \geq (2^{L + 1})^{c_8} \geq (2^{\ell + 1})^{c_8},
\]

for all \( \ell = 1, 2, \ldots, L \). Therefore, for \( \epsilon \leq 1/c_8 \), we may use Lemma 2.4 to bound \( \sigma_\epsilon(x) \) below. We obtain

\[
\sigma_\epsilon(x) \geq \sum_{\ell=1}^L \frac{c_7 x}{\log 2^\ell x} = c_7 x \sum_{\ell=1}^L \frac{a}{1 + \ell a},
\]

where \( a = (\log_2 x)^{-1} \). Now, for \( L \geq M \geq 1 \), define

\[
I(M, L, a) = \int_M^L \frac{a}{1 + \ell a} d\ell.
\]

Then

\[
I(M, L, a) = \log \left( \frac{1 + La}{1 + Ma} \right),
\]

and, since, for all \( a > 0 \), the function \( f_a(\ell) = a/(1 + \ell a) \) is monotonic decreasing in the region \( \ell \geq 0 \), we have, for all \( L \geq M \geq 1 \),

\[
I(M - 1, L - 1, a) > \sum_{\ell=M}^L \frac{a}{1 + \ell a} > I(M, L, a).
\]

So,

\[
\sigma_\epsilon(x) > x \frac{c_7}{\log 2} \log \left( \frac{1 + L(\log_2 x)^{-1}}{1 + (\log_2 x)^{-1}} \right).
\]

Now, by equation (3), \( L(\log_2 x)^{-1} = \epsilon - \alpha(\log_2 x)^{-1} \), where \( 2 \geq \alpha > 1 \). So, for some \( \beta \in [2, 3) \),

\[
\sigma_\epsilon(x) > x \frac{c_7}{\log 2} \log \left( 1 + \frac{\epsilon - \beta(\log_2 x)^{-1}}{1 + (\log_2 x)^{-1}} \right),
\]
and, for all \( \delta > 0 \),

\[
\sigma_\epsilon(x) > x(1 - \delta)c_7 \log_2(1 + \epsilon)
\]

for all sufficiently large \( x \). Thus we have proved the inequality (5) for all \( c_6(\epsilon) < c_7 \log_2(1 + \epsilon) \). Therefore, by equation (6), Lemma 2.1 holds for all \( c_4(\epsilon) < (c_7 \log_2(1 + \epsilon))^2/c_5(\epsilon) \).

3. Proof of the Proposition

It will be sufficient to prove that, for all sufficiently large \( x \), for all \( \delta > 0 \),

\[
N_\epsilon(x) \leq 2x(1 + \delta) \log_2(1 + \epsilon).
\]

(10)

Notice that, since, by definition, \( N_\epsilon(x) \leq \frac{1}{2}(1 + \frac{1}{x})x \), the above inequality (10) holds trivially when \( \epsilon > 2^\frac{1}{4} - 1 \). So we may certainly suppose that \( \epsilon < 1 \).

Now, since \( S(k, x) > 0 \) implies \( S(k, x) \geq 1 \), we have

\[
N_\epsilon(x) < \sum_{k \leq x \text{ odd}} S(k, x) = \sigma_\epsilon(x).
\]

We will use the following technical lemma to be proved in the next section.

**Lemma 3.1.** Suppose the Extended Riemann Hypothesis holds. Then there is a constant \( A > 0 \) such that, for all positive coprime non-negative integers \( q \) and \( a < q \),

\[
\pi(x; q, a) < \frac{2x}{\phi(q) \log x} + Ax^{1/2} \log x.
\]

Assuming this lemma, we have

\[
\sigma_\epsilon(x) = \sum_{\ell=1}^{L} \pi(2^\ell x; 2^{\ell+1}, 2^\ell - 1)
\]

\[
< LA(2^L x)^{1/2} \log(2^L x) + \sum_{\ell=1}^{L} \frac{2x}{\log 2^\ell x}.
\]

By the inequalities (2) and (3), \( 2^L x < x^{1+\epsilon} \) and \( L < \epsilon \log_2 x \). So the first term is less than \( \epsilon(1+\epsilon)Ax^{1+\epsilon/2}(\log_2 x)^2 \), which is negligible since we have supposed that \( \epsilon < 1 \). Moreover, the second term is the sum in equation (7) with \( c_7 = 2 \). This sum is handled as before, except we
use the upper bound in the inequalities (9). Therefore, for \( \epsilon < 1 \), any \( \delta > 0 \), and all sufficiently large \( x \),

\[
N_\epsilon(x) < \sigma_\epsilon(x) \\
< (1 + \delta) \frac{2x}{\log 2} I(0, L - 1, (\log_2 x)^{-1}) \\
= x 2(1 + \delta) \log_2 (1 + \epsilon - \beta (\log_2 x)^{-1}) \\
\leq x 2(1 + \delta) \log_2 (1 + \epsilon).
\]

4. Proof of Lemma 3.1

To prove the lemma, we consider the familiar number-theoretic function

\[
\psi(x; q, a) = \sum_{k \leq x \atop k \equiv a \pmod{q}} \Lambda(k),
\]

where \( \Lambda(k) \) is the von Mangoldt function defined as follows:

\[
\Lambda(k) = \begin{cases} 
\log p & \text{if } k \text{ is a power of the prime } p, \\
0 & \text{if } k \text{ is not a prime power.}
\end{cases}
\]

Now

\[
\pi(x; q, a) = \sum_{k \leq x \atop k \equiv a \pmod{q}} 1\{k \text{ is prime}\},
\]

and

\[
\psi(x; q, a) = \sum_{k \leq x \atop k \equiv a \pmod{q}} 1\{k \text{ is prime}\} \lfloor \log_k x \rfloor \log k \\
= \sum_{\sqrt{x} < k \leq x \atop k \equiv a \pmod{q}} 1\{k \text{ is prime}\} \log k \\
+ \sum_{k \leq \sqrt{x} \atop k \equiv a \pmod{q}} 1\{k \text{ is prime}\} \lfloor \log_k x \rfloor \log k.
\]

Since \( \lfloor \log_k x \rfloor \log k \leq \log x \), we therefore have

\[
\sum_{\sqrt{x} < k \leq x \atop k \equiv a \pmod{q}} 1\{k \text{ is prime}\} \log k = \psi(x; q, a) + O(\phi(q)^{-1}x^{1/2} \log x).
\]

So, there is a constant \( c > 0 \) such that

\[
\frac{1}{2}(\pi(x; q, a) - \pi(x^{1/2}; q, a)) \log x < \psi(x; q, a) + c\phi(q)^{-1}x^{1/2} \log x,
\]
and hence, for some constant $c' > 0$,

$$
\pi(x; q, a) < \frac{2\psi(x; q, a)}{\log x} + c' \phi(q)^{-1} x^{1/2}.
$$

Now, by [3, equation (14) of Chapter 20], the Extended Riemann Hypothesis implies that for $(a, q) = 1$,

$$
\psi(x; q, a) = \frac{x}{\phi(q)} + O(x^{1/2} (\log x)^2).
$$

So, for some constant $A > 0$, we have

$$
\pi(x; q, a) < \frac{2x}{\phi(q) \log x} + Ax^{1/2} \log x.
$$

REFERENCES

[1] Craigen, R., “Signed Groups, Sequences, and the Asymptotic existence of Hadamard matrices,” J. Combin. Th. Ser. A 71 (1995), 241–254.
[2] Craigen, R., Holzmann, W. H., and Kharaghani, H., “On the asymptotic existence of complex Hadamard matrices,” J. Combin. Des. 5 (1997), 319–327.
[3] Davenport, H., “Multiplicative Number Theory,” Second Edition, Springer-Verlag, New York Berlin Heidelberg, 1980.
[4] de Launey, W. R., Flannery D. H. and Horadam, K. J., “Cocyclic Hadamard matrices and difference sets,” Disc. Appl. Math. 102 (2000), 47–61.
[5] Erdos, P. and Odlyzko, A. M., “On the Density of Odd Integers of the Form $(p - 1)2^{-n}$ and Related Questions,” J. Numb. Th. 11 (1979), 257–263.
[6] Riesel, H., “Naagra stora primtal,” Elementa 39 (1956), 258–260.
[7] Seberry-Wallis, J., “On the existence of Hadamard matrices,” J. Combin. Th. Ser. A 21 (1976), 188–195.

CENTER FOR COMMUNICATIONS RESEARCH, INSTITUTE FOR DEFENSE ANALYSES, 4320 WESTERRA COURT, SAN DIEGO, CALIFORNIA, CA92121
E-mail address: warwick@ccrwest.org
E-mail address: warwickdelauney@earthlink.net