The Impact of Number Theory and Computer Aided Mathematics on Solving the Hadamard Matrix Conjecture

Jennifer Seberry
Centre for Computer and Information Security Research, SCSSE,
University of Wollongong, NSW 2522, Australia
Email: j.seberry@uow.edu.au

In memory of Alf van der Poorten

Abstract

The Hadamard Conjecture has been studied since the pioneering paper of J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions, tessellated pavements in two or more colours, with applications to Newtons rule, ornamental tile work and the theory of numbers", *Phil Mag*, 34 (1867), 461–475 first appeared.

We review the importance of primes on those occasions that the conjecture, that for every odd number t there exists an Hadamard matrix of order $4t$, is confirmed. Although substantial advances have been made into the question of the density of this odd number t it has still not been shown to have positive density.

We survey the results of some computer aided construction algorithms for Hadamard matrices.

Keywords: Hadamard matrix, skew-Hadamard matrix, symmetric Hadamard matrix, asymptotic Hadamard matrices, prime number theorem, Extended Riemann Hypothesis, computer aided construction.

AMS Subject Classification: 20B20.

1 Introduction

The Hadamard conjecture, attributed to R.E.A.C.Paley in 1933 is that "an Hadamard matrix exists for every order 1, 2 and $4t$, t a non-negative integer". This question has attracted research for over 110 years. In the early 1970's orthogonal designs were introduced to further their study. We do not cover orthogonal designs but refer the reader to Geramita and Seberry [16]. Hadamard matrices themselves have many applications: they give codes to correct the maximum number of errors in electromagnetic signals, they allow for the best possible weights to be obtained for

tiny objects (eg jewels, chemicals, drugs), they allow the most exact spectral analysis of the content of solutions, they give the binary functions with highest non-linearity for cryptographic primitives, ...

Amicable orthogonal designs derived from Hadamard matrices have led to the best CDMA (code division multiple access) codes for mobile communications.

Number theory has been extensively used by Yamada and Yamamoto [39, 40] of Japan, Ming Yuan Xia [33, 35] and his team in China, A. L Whiteman [32] and Warwick de Launey [9]. The constructions use Legendre characters, Gaussian sums and relative Gauss sums, Jacobi sums, the theory of cyclotomy, quadratic forms, to name a few.

However, Hadamard matrices also come with a very curious property, while most of the constructions that give infinite families of orders which satisfy the Hadamard conjecture are based on primes, other constructions seem to hit a solid wall concerning upper sizes when computer aided searches are undertaken to look for them.

We give a small taste of the problems with computer assisted research.

2 Definitions and Basics

An Hadamard matrix, H, of order h is a square matrix with entries ± 1, in which any pair of distinct rows (or columns) are orthogonal, that is $HH^T = hI_h$ where I is the identity matrix.

We first consider some results about non prime orders, then prime orders and then computer aided construction.

We believe that orders of Hadamard matrices $4p$, $p \equiv 3 (\text{mod } 4)$ are the toughest to find.

3 Why are the primes so important for the Hadamard conjecture?

3.1 Multiplying Hadamard Matrices

Hadamard matrices can be multiplied together to give new Hadamard matrices using the Kronecker product. However this increases the power of two. Summarizing

Matrix sizes	Multiplication Size	Reference
$4a$, $4b$	2^4ab	Classical Result due to Sylvester [27]
$4a$, $4b$	2^3ab	Agayan [1]
$4a$, $4b$, $4c$, $4d$	2^5abcd	Agayan [1]
$4a$, $4b$, $4c$, $4d$	2^4abcd	Craigen, Seberry, Zhang [4]
$4a_1, \cdots, 4a_{12}$	$2^{10}\prod_{i=1}^{12} a_i$	Previous methods
$4a_1, \cdots, 4a_{12}$	$2^9\prod_{i=1}^{12} a_i$	de Launey [6]

3.2 Asymptotic Existence of Hadamard Matrices

The Asymptotic Form of the Hadamard Conjecture

In 1975 Seberry [25] and in 1995 Craigen [2] had found some asymptotic type existence theorems for Hadamard matrices but were unable to establish that their results had positive density in the set of natural numbers $4t$.

Let $S(x)$ be the number $n \leq x$ for which an Hadamard matrix of order n exists. Then the Hadamard conjecture states that $S(x)$ is about $\frac{x}{4}$.

Then in a ground breaking paper de Launey and Gordon [10] increased the bound for the density from Paley's constructions ($O(\pi(x))$ by a factor of $\exp((\log\log\log x)^2)$, but this bound is still $o(x)$. The question of whether $S(x)$ has positive density is still open. Their lovely theorem is

Theorem 1 de Launey and Gordon *For all $\epsilon > 0$, there is a natural number x_ϵ such that, for all $x \geq x_\epsilon$,*

$$S(x) \geq \frac{x}{logx} \exp((C+\epsilon)(\log\log\log x)^2)$$

for $C = 0.8178....$

de Launey and Gordon's original insights [7, 9] were derived under the extended Riemann hypothesis, using the multiplication theorem of the type in subsection 3.1 and the Paley theorems of section 4. Later results by a number of authors including Kevin Ford, David Levin, H Iwaniec, Sidney Graham and Igor Shparlinski [18] meant that the extended Riemann hypothesis was not required for the proof.

Looking at these results in a slightly different way de Launey and Gordon [11] say: "Let a be any positive real number. Then for some absolute positive constant c_2 there is a Hadamard matrix of order 2^{tr} whenever $2^t \geq c_2 r^a$".

In 1975 Seberry [25] had proved this fact for the first time for $c_2 = 1$ and $a = 2$. In 1995 R. Craigen [2] improved Seberry's result to $c_2 = 2^{\frac{13}{8}}$ and $a = \frac{3}{8}$. de Launey and Gordon now had the $a < 1$ they needed to remove the assumption of the Extended Riemann Hypothesis for their result in [9].

These were summarized by Daniel M. Gordon [11]. "For g odd, the fraction of orders $2^t g$ with orders $2^t > c_2 g^a$ is at least

author	a	c_2	fraction
Seberry	2	1	1
Craigen	$\frac{3}{8}$	$2^{13/8}$	1
Livinski	$\frac{1}{5}$		1
deLauney andGordon	$\epsilon > 0$	1	$c(\epsilon) > 0$

".

Craigen, de Launey, Holzmann, Kharaghani and Smith have also been involved in other wonderful asymptotic results [3, 5, 14, 8, 12].

3.3 Multiplication and Asymptotics

Since we can always multiply orders of Hadamard matrices together even though we get higher powers of two and the asymptotic results mean that we can always get an Hadamard matrix of order $2^t n$ for any odd n provided we have all the factors of n.

This means we need to concentrate on looking for those orders $4p$ where p is a prime, even though the primes are not dense in the positive integers. Thus we first confine ourselves to the primes.

4 Constructions using Primes

The earliest construction were based on primes or ad hoc constructions. We discuss computer aided construction of ad hoc orders in the next section.

Author	Year	Constructions
Sylvester	1867	orders 2^t
Hadamard	1893	orders 12, 20
Paley	1933	orders $p^r + 1$, $p \equiv 3 (\mathrm{mod}\ 4)$ a prime
		orders $2(q^s + 1)$, $q \equiv 1 (\mathrm{mod}\ 4)$ a prime

Mieko Yamada [37] has given a taste of the importance of primes to resolving the Hadamard conjecture:

Theorem 2 Yamada 1 *If $q \equiv 1 (\mathrm{mod}\ 8)$, is a prime power and there exists an Hadamard matrix of order $(q-1)/2$, then we can construct an Hadamard matrix of order $4q$.*

Theorem 3 Yamada 2 *If $q \equiv 5 (\mathrm{mod}\ 8)$, is a prime power and there exists a skew-Hadamard matrix of order $(q+3)/2$, then we can construct an Hadamard matrix of order $4(q+2)$.*

Theorem 4 Yamada 3 *If $q \equiv 1 (\mathrm{mod}\ 8)$, is a prime power and there exists a conference matrix of order $(q+3)/2$, then we can construct an Hadamard matrix of order $4(q+2)$.*

Zuo and Xia introduced a special class of T-matrices in Zuo and Xia [41] which relies on primes. Xia and Colleagues also showed that

Theorem 5 Xia, Xia, Seberry and Zuo [34] *There exists an infinite family of T-matrices of order q^2 with q prime power $q \equiv 3 (\mathrm{mod}\ 8)$.*

5 By Hand and Computer Aided Construction of Hadamard Matrices

5.1 Williamson matrices (or zero periodic autocorrelation function)

In 1944 Williamson [31] gave a beautiful method to construct most orders ≤ 200 by hand. The only infinite families which suits this construction method were found by

Turyn [29] and Yamada [36] but they give no new Hadamard matrix orders beyond those given by Paley.

However this led many of us to conjecture that "Williamson's method can be used to construct all Hadamard matrices of order $4n$ for n odd."

Alas this is not true. In 1993 Djokovic [15] showed, by complete search, that there were matrices of this kind for order $4n$, $n = 33$, 39 and none of order 35. 35 being a composite number, some thought that it may be true that such matrices exist of order $4n$, n a prime number. Then in 2008 Holzmann, Kharaghani and Tayfeh-Rezaie, [20] dashed hopes by using an exhaustive computer search to show none of this kind exist for $n = 47,\ 53$ or 59.

Some researchers now conjecture (verbally) that "Williamson's method can be used to construct Hadamard matrices of order $4n$ for n odd $n \leq 45$, $n \neq 35$, and orders $4n$, for some primes $n \equiv 1 (\text{mod } 4)$ and no other primes". Multiples of known orders have not been settled.

5.2 Constructions using other sequences with zero autocorrelations function

We refer our patient reader to Geramita and Seberry [16] and Seberry and Yamada [26] for any terms we do not now explain and for examples of the types of constructions we now describe.

Williamson's method inspired many authors to look for 1, 2, 3, 4, 6 and 8 matrices (or sequences which are their first rows) with elements $\{0, \pm 1\}$ and zero auto correlation functions that might be used to find Hadamard matrices. The limit of 8 is related to the algebra of the quaternions. The methods found have been beautiful, clever and very inventive. They include Golay sequences, T-matrices, base sequences, Yang sequences, Turyn sequences, good matrices and Turyn 6-sequences. Often they give many new Hadamard matrices but in the cases where computer searches have been undertaken we have usually found that after a certain length n (the length seems to depend on the method) no more of that kind exist. Many construction results have the proviso that no prime p, $p \equiv 3 (\text{mod } 4)$ divides the length n.

6 Equivalence of Hadamard Matrices by Computer

Two Hadamard matrices are said to be equivalent to each other if one can be obtained from the other by a series of operations of the type (a) interchange any pair of rows (or columns), and/or type (b) multiply any row or column by -1. The results in the following table were found by hand upto order 20 and with computer assistance for higher orders:

Order	Number Inequivalent	Authors
4, 8, 12	Unique	
16	5	Marshall Hall Jr
20	3	Marshall Hall Jr
24	60	Ito
28	487	Kimura
32	13,710,027	Many *
36	>30,000,000	Many *

* Among the authors are: Holtzman, Kharaghani, Tayfeh-Rezaie, Koukouvinos, Orrick.

7 The Future

Thanks to de Launey we now know more regarding the known orders for Hadamard matrices in the natural number $4t$: but this set has not yet been shown to have positive density. However we have merely scratched the surface of how important Number Theory is to solving the Hadamard conjecture which remains unresolved. A search (unpublished) for existence orders upto 40,000 showed that some kind of construction, including the multiplicative constructions gave some result for 80-90% of the odd numbers but in the cases where the asymptotic results had to be invoked it was usually a prime $p > 3$, $p \equiv 3 (\mathrm{mod}\ 4)$ that was involved.

8 Acknowledgements

The author sincerely thanks Professor Igor Shparlinski and Dr Daniel Gordon for alerting her to her confusion in Section 3.2 and pointing out pertinent references.

References

[1] S.S. Agayan, *Hadamard Matrices and Their Applications*, Lecture Notes in Mathematics, vol 1168, Springer-Verlag, New York-Heidelberg, 1985.

[2] R. Craigen, Signed groups, sequences and the asymptotic existence of Hadamard matrices, *J. Combin. Theory,* 71 (1995), 241-254.

[3] R. Craigen, W. H. Holzmann and H. Kharaghani, On the asymptotic existence of complex Hadamard matrices. *J. Combin. Des.,* 5 (1997), 319-327.

[4] R. Craigen, Jennifer Seberry and Xian-Mo Zhang, Product of four Hadamard matrices, *J. Combin. Theory (Ser A)*, 59, (1992), 318-320.

[5] W. de Launey, On the asymptotic existence of partial complex Hadamard matrices and related combinatorial objects. *Conference on Coding, Cryptography and Computer Security*, (Lethbridge, AB, 1998). *Discrete Appl. Math.,* 102 (2000), 37-45,

[6] W. de Launey, A product for twelve Hadamard matrices. *Australas. J. Combin.*, 7 (1993), 123-127.

[7] W. de Launey, On the asymptotic existence of Hadamard matrices. *J. Combin. Theory (Ser A)*, 116 (2009), 1002-1008.

[8] W. de Launey and J. Dawson, An asymptotic result on the existence of generalised Hadamard matrices. *J. Combin. Theory (Ser A)*, 65 (1994), 158-163.

[9] W. de Launey and D. M. Gordon, A comment on the Hadamard conjecture, *J. Combin. Theory (Ser A)*, 95 (2001), 180-184.

[10] W. de Launey and D. M. Gordon, On the density of the set of known Hadamard orders, *Cryptography and Communications*, 2 (2010), 233-246.

[11] W. de Launey and D. M. Gordon, Should we believe the Hadamard conjecture? *Conference in Honor of Warwick de Launey, IDA/CCR*, La Jolla, CA, 16 May 2011.

[12] W. de Launey and H. Kharaghani, On the asymptotic existence of cocyclic Hadamard matrices. *J. Combin. Theory (Ser A)*, 116 (2009), 1140-1153.

[13] W. de Launey and D. A Levin, A Fourier analytic approach to counting partial Hadamard matrices, *arXiv:1003.4003v1 [math.CO]*, 21 March 2010.

[14] W. de Launey and M. Smith, Cocyclic orthogonal designs and the asymptotic existence of cocyclic Hadamard matrices and maximal size relative difference sets with forbidden subgroup of size 2. *J. Combin. Theory (Ser A)*, 93 (2001), 37-92.

[15] D. Z Djokovic, Williamson matrices of order $4n$ of order $n = 33, 35, 39$. *Discrete Math* 115 (1993), 267-271.

[16] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard matrices*, Marcel Dekker, Boston, 1969.

[17] G. M'. Edmonson, J. Seberry and M. Anderson, On the existence of Turyn sequences of length less than 43, *Mathematics of Computation*, 62 (1994), 351–362.

[18] S. W Graham and I. E Shparlinski, On RSA moduli with almost half of the bits prescribed, *Discrete Applied Math.*, 156 (2008), 3150–3154.

[19] M. Hall, Jr., *Combinatorial Theory*, 2nd ed., John Wiley & Sons, New York, 1986.

[20] W. H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson matrices up to order 59, *Designs, Codes and Crypto.*, 46 (2008), 343–352.

[21] K. J Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, 2007.

[22] I. Livinski, *Asymptotic Existence of Hadamard Matrices*, Master of Science Thesis, University of Manitoba, 2012.

[23] J. Horton, C. Koukouvinos and J. Seberry, A search for Hadamard matrices constructed from Williamson matrices, *Bull. Inst. Combin. Appl.* 35 (2002), 75–88.

[24] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* 12 (1933), 311–320.

[25] J. Seberry Wallis, On Hadamard matrices, *J. Combinatorial Theory, Ser. A.*, 18 (1975), 149–164.

[26] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, eds., John Wiley and Sons, Inc., 1992, 431–560.

[27] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile work and the theory of numbers, *Phil. Mag.*, 34 (1867), 461–475.

[28] R. Turyn, Character sums and difference sets, *Pacific J. Math.*, 15 (1965), 319–346.

[29] R. Turyn, An infinite class of Hadamard matrices, *J. Combin. Theory (Ser. A)* 12 (1972), 319–321.

[30] J. Seberry Wallis, Hadamard matrices, in W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets and Hadamard Matrices,* Lecture Notes in Mathematics, Springer Verlag, Berlin, 1972.

[31] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, 11 (1944), 65–81.

[32] A. L Whiteman, An infinite family of Hadamard matrices of Williamson type, *J. Combin. Theory (Ser A)*, 14 (1972), 334–340.

[33] M. Y. Xia, Some infinite families of Williamson matrices and difference sets, *J. Combin. Theory (Ser A)*, 61 (1992), 230–242.

[34] M. Y. Xia, T. B. Xia, J. Seberry, and G. X. Zuo, A new method for constructing T-matrices, *Aust. J. Combin.*, 32 (2005), 61–78.

[35] Ming Yuan Xia, Tianbing Xia and Jennifer Seberry, A new method for constructing Williamson matrices, *Designs, Codes and Crypto.* 35 (2005), 191–209.

[36] M. Yamada, On the Williamson type j matrices of orders $4 \cdot 29$, $4 \cdot 41$ and $4 \cdot 37$, *J. Combin. Theory (Ser A)*, 27 (1979), 378–381.

[37] M. Yamada, Some new series of Hadamard matrices, *Proc. Japan Acad. (Ser. A)*, 63, (1987), 86–89.

[38] M. Yamada, Hadamard matrices generated by an adaptation of generalized quaternion type array. *Graphs and Combinatorics*, 2 (1986), 179–187.

[39] K. Yamamoto and M. Yamada, Williamson Hadamard matrices and Gauss sums. *J. Math. Soc. Japan*, 37 (1985), 703–717.

[40] K. Yamamoto, On congruences arising from relative Gauss sums. *Number Theory and Combinatorics,* Japan 1984, World Scientific Publ., Singapore, (1985), 423–446.

[41] G. X. Zuo and M. Y. Xia, A special class of T-matrices, *Designs, Codes and Crypto.*, 54 (2010), 21–28.