C1.1 Project Title: New constructions for Hadamard matrices

C1.2 Aims and Background

Aims. The aim of this project is to to study new ways of constructing *Hadamard matrices* using sums of *Kronecker products*, and to understand the structure of the class of matrices that can be obtained by this construction.

Background. The *Hadamard maximal determinant problem* is: "given n, what is the largest possible determinant of an $n \times n$ matrix R with elements ± 1?". Hadamard's problem has many applications to signal processing, error-correcting codes, experimental design theory, and cryptography, as described in more detail in §C1.3 below.

Hadamard [15] established an upper bound $n^{n/2}$, which is only attainable if the order n equals $1, 2$, or a multiple of 4, and which only occurs when the rows of the matrix R are orthogonal. It is a famous open problem whether a *Hadamard matrix* (a matrix attaining the Hadamard bound) exists for each order a multiple of 4. The conjecture that this is true is known as the *Hadamard conjecture*, actually conjectured by Paley [43]. Although the conjecture is known to be true for all orders $n = 4k < 668$ [22], it is not yet known if the set of such orders has positive density. The best results known in this direction are due to de Launey and Gordon [9, 10]; see also Horadam [20], Seberry [52], and Craigen and Kharaghani [7, 8].

There has been much work on the number of *equivalence classes* of Hadamard matrices of a given order, for a natural definition of equivalence, and small order ($n \leq 36$). The sequence grows very rapidly, and is difficult to calculate, requiring a means of (at least implicitly) generating a complete set of Hadamard matrices of fixed order, and an algorithm to decide equivalence (in general a difficult problem, although no more difficult than the graph isomorphism problem [28]). The largest case for which an answer is published is $n = 32$, where there are 13 710 072 equivalence classes of Hadamard matrices [23, 24].

The *switching operations* introduced by Denniston [11] enable us to produce many new (inequivalent) Hadamard matrices from a given starting matrix. PI Orrick [37, 38] has discovered several new switching operations and has used them to give lower bounds on the number of equivalence classes of Hadamard matrices of certain orders, including 36. Switching operations have also been used by Holzmann, Kharaghani and PI Orrick [17] to find the first triple of real mutually unbiased bases for $n = 36$, the only $n \neq 2^k$ for which this has been achieved.

Many infinite families of Hadamard matrices are known, including those of Sylvester [51] and Paley [43]. This project focuses on generalizations of the *Williamson construction* [53], which constructs Hadamard matrices of order $n = 4k$, given four matrices of order k satisfying certain conditions. These matrices are called "suitable matrices" in [48], but we use the more descriptive term *ingredient matrices*. They are often chosen to be circulant, but this is not necessary and is usually done simply to restrict the size of the search space. Unfortunately, it is not easy to find the ingredients, so the Williamson construction is incomplete. In a sense, it is half of a construction, with the other half (the ingredient matrices) missing. The Williamson construction is an example of a "plug-in" method [48]: one needs to know the ingredient matrices and plug them in. Despite this difficulty, the Williamson construction has proved very useful for finding Hadamard matrices whose orders do not lie in known infinite families, e.g. $n = 92$ [1] and $n = 172$ [53]. For further discussion of the Williamson construction, see Horadam [19, §4.1.4] and Xia *et al* [54, 55].

The Williamson construction is closely related to the multiplication table of the quaternions, and a generalized Williamson construction known as *8-Williamson* is similarly related to the octonions [41, 47]. Both the Williamson and the 8-Williamson constructions use orthogonal designs [14].

In applications the cases of the Hadamard maximum determinant problem where the order $n \neq 0 \bmod 4$ are also important, and much less is known about them than the case $n = 0 \bmod 4$. In a recent arXiv preprint [2], CI Brent, PI Orrick and PI Osborn, with Zimmermann, showed that for order 19, certain matrices with determinant 833×2^{30}, found previously by Smith [50], Cohn [5], Orrick and Solomon [40], are indeed maximal. The paper also proves that the maximal determinant for order 37 is $2^{39} \times 3^{36}$. The techniques described in the paper included the enumeration of candidate Gram matrices, and the use of switching operations and McKay's *nauty* program [27, 29, 30] to determine equivalence classes.

C1.3 Research Project

Significance. The Hadamard maximal determinant problem is a fascinating combinatorial optimisation problem with many applications to signal processing, error-correcting codes, experimental design theory [16], and cryptography.

Applications to signal processing include both the Walsh-Hadamard transform and the fast Hadamard transform [19, §3.1] [26, Ch. 14].

Error-correcting codes derived from Hadamard matrices include the binary Golay codes, the Reed-Muller codes [26, 44] and quantum error-correcting codes [3, 34]. The Golay codes and the Reed-Muller codes have been used in deep space communications [19, pp. 40-42]. Codes based on Hadamard matrices are also used for CDMA wireless schemes to separate channels in mobile telephony [19, pp. 43-47].

Applications to experimental design theory include orthogonal designs [14] and orthogonal arrays [16].

The Walsh-Hadamard transform has applications to cryptography because of the connection with *bent functions* [19, §3.5]. Bent functions were introduced by Rothaus [45], and are Boolean functions whose Walsh-Hadamard transform coefficients have constant absolute value. In a sense, they are as far from linear as possible, so provide maximal resistance against linear attacks.

There is a continuing and renewed interest in the structure of the set of Hadamard matrices of small order, including those obtainable by specific constructions, as evidenced by recent papers [23, 24] on the equivalence classes of the Hadamard matrices of order 32, and the theses of Ó Catháin [35, 36], which include the classification of *cocyclic* Hadamard matrices [19, Part 2] of order less than 40.

National Research Priorities. The project is directly relevant to the National Research Priority: *Frontier Technologies*, most specifically to the goal of *Breakthrough sciences*. The immediate results of this project are intended to be breakthroughs in our understanding of Hadamard matrices, whose study is a topic in Combinatorics and Discrete Mathematics. The methods developed to obtain these results will have direct relevance to the goal of *Smart information use*, specifically, new and improved algorithms for use in the study of Hadamard matrices and similar investigations in the area of combinatorics.

As outlined in "Significance" immediately above, Hadamard matrices are ubiquitous in signal processing, coding theory and cryptography, as well as in their more classical application to the design of experiments. Thus, the project is also indirectly relevant to the National Research Priority *Safeguarding Australia* (Critical infrastructure, such as communications).

The project will also benefit Australia by increasing scientific collaboration between Australia, Canada, Ireland, Spain and especially the USA, and raising the profile of Australian research in this area, leading to a probable increase in future collaborations between Australian and overseas researchers on related projects.

The techniques, algorithms and software developed in the course of the project, including parallel computation, are also likely to be useful in other applications.

Innovation. The innovative aspects of the project include:

- A program of research into the properties of a class of Hadamard matrices given by new generalization of the Williamson construction, recently introduced by CI Leopardi [32].
- The use of properties of the smaller matrices within this class, recently discovered by CI Osborn [42], to gain an understanding of how to proceed in determining the structure of the class for larger matrices.
- The use of algorithms for smaller matrices within this class, recently developed by CI Osborn and CI Brent [42], as the basis for developing more efficient algorithms for use with larger matrices.

For a detailed explanation of each of these points, see the paragraphs immediately below.

Conceptual framework and summary of recent work.

Our sum-of-Kronecker-products construction [32] is a plug-in construction that generalizes of the Williamson construction [53]. In this construction, we aim to find

$$A_k \in \{-1, 0, 1\}^{n \times n}, \quad B_k \in \{-1, 1\}^{p \times p}, \quad k \in \{1, \ldots, n\},$$

and construct

$$H := \sum_{k=1}^{n} A_k \otimes B_k, \tag{H0}$$

such that

$$HH^T = npI_{(np)}. \tag{H1}$$

Due to well-known and easily verified properties of the Kronecker product (e.g. [33, (2.8)],) if the order of the products in (H0) is reversed to yield the construction

$$G := \sum_{k=1}^{n} B_k \otimes A_k, \tag{G0}$$

we obtain the equivalent result,

$$GG^T = npI_{(np)}. \tag{G1}$$

It is not clear how to find a set of $2n$ ingredient matrices $(A_1,\ldots,A_n)$, $(B_1,\ldots,B_n)$, which simultaneously satisfy conditions (H1) other than by a brute force search. We therefore impose the stronger conditions

$$\begin{aligned} A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1,1\}^{n\times n}, \\ A_k A_k^T = I_{(n)}, \\ A_j A_k^T + \lambda_{j,k} A_k A_j^T = 0 \quad (j \neq k), \\ B_j B_k^T - \lambda_{j,k} B_k B_j^T = 0 \quad (j \neq k), \\ \lambda_{j,k} \in \{-1,1\}, \\ \sum_{k=1}^{n} B_k B_k^T = npI_{(p)}, \end{aligned} \tag{2}$$

where $*$ is the Hadamard matrix product.

It is straightforward to check that if the conditions (2) apply, then constructions (G0) and (H0) yield Hadamard matrices [32, Theorem 1].

The coupling between the $\{-1,0,1\}$ and $\{-1,1\}$ ingredient matrices is mediated by the λ parameters. If we find an n-tuple of $\{-1,0,1\}$ ingredient matrices $(A_1,\ldots,A_n)$ satisfying the conditions (2), we can then use the resulting λ values to search for an n-tuple of $\{-1,1\}$ ingredient matrices $(B_1,\ldots,B_n)$ satisfying the conditions (2) with the same λ values, to complete the sums (G0) and (H0).

A pair of matrices M, N are called *amicable* if $MN^T = NM^T$ and *anti-amicable* if $MN^T = -NM^T$. In his recent paper [32], CI Leopardi showed how certain sets of n "basis" matrices of type $\{-1,0,1\}$ and order $n = 2^m$ are pair-wise either amicable or anti-amicable. This gives a method of constructing the required n-tuples of $\{-1,0,1\}$ matrices satisfying the conditions (2). The paper includes an account of an exhaustive search of the $\{-1,1\}$ matrices of order $p = 2$, for multisets of size $n = 2$ and $n = 4$ satisfying the *Gram matrix* condition:

$$\sum_{k=1}^{n} B_k B_k^T = npI_{(p)}, \tag{3}$$

and also satisfying the condition that each pair in the multiset is either amicable or anti-amicable. The paper also states that pairs of anti-amicable $\{-1,1\}$ matrices exist only for even orders.

If the order is odd, then only mutually amicable pairs of $\{-1,1\}$ matrices exist. In this case, each pair of corresponding $\{-1,0,1\}$ matrices must be mutually anti-amicable. Such sets of $\{-1,0,1\}$ matrices exist only for orders $n = 2$, $n = 4$ and $n = 8$, with orders 4 and 8 corresponding to the Williamson and 8-Williamson constructions. CI Osborn, with the assistance of CI Brent [42], has conducted searches in the matrices of type $\{-1,1\}$ and orders $p = 3$ and $p = 5$ for pair-wise amicable multisets of size 2, 4 and 8, satisfying the Gram matrix condition (3).

CI Leopardi's paper [32] gives one construction for the $\{-1,0,1\}$ ingredient matrices, but an exhaustive search can also be carried out to find all sets of these matrices for small values of n, to study the structure of the class of these sets. The theory of these sets of $\{-1,0,1\}$ ingredient matrices is essentially the same as the theory of *systems* of orthogonal designs and *quasi-Clifford* algebras, as studied by Gastineau Hills [12, 13]. The number of candidate n-tuples, that is n-tuples of $\{-1,0,1\}$ matrices $(A_1,\ldots,A_n)$ satisfying

$$A_j * A_k = 0 \quad (j \neq k), \quad \sum_{k=1}^{n} A_k \in \{-1,1\}^{n\times n},$$
$$A_k A_k^T = I_{(n)}$$

grows rapidly with n. For order $n = 2^m$, the number of candidate n-tuples is the number of Latin squares of order n ([49, Sequence A002860] [31]) divided by $n!$ (the number of permutations on n symbols), multiplied by 2^{n^2} (the number of possible sign patterns).

The recent paper of CI Osborn [42] describes the searches conducted for the Williamson and 8-Williamson constructions for order $p = 5$, and gives the structure of the class of matrices obtained, including results on the Hadamard equivalence classes. A naive search for multisets of 8 $\{-1,1\}$ ingredient matrices of order $p = 5$ would involve in the order of 2^{200} 8-tuples of such matrices (2^{200} is about 10^{60}), and is therefore completely infeasible. CI Osborn therefore used a number of techniques both to cut down the search space required and to speed up the evaluation of each case. CI Brent provided special algorithms and techniques to make the searches faster still.

Specifically, for order $p = 5$, the 2^{25} members of the full set of $\{-1,1\}$ matrices were first paired as $B, -B$, since for any third $\{-1,1\}$ matrix C, the matrix B is amicable with C if and only if $-B$ is amicable with C. The analysis of the *amicability graph* with these pairs as nodes, and edges between amicable pairs B, C, revealed 16 isomorphic components. The remainder of the search was conducted in only one component, containing 2^{20} pairs. The pairs within this component were then divided into 949 disjoint subsets, each corresponding to a different Gram matrix. For size $n = 4$ (the Williamson case), for each multiset of size 4 of Gram matrices, corresponding to a solution to the Gram matrix condition (3), the corresponding sets of ingredient matrices were searched for a pairwise amicable multiset. This search resulted in the construction of matrices from 2 of the 3 equivalence classes of Hadamard matrices of order 20.

For size $n = 8$ (the octonion case), a *meet in the middle* algorithm was used, a simplified version of which combines two pairwise amicable multisets of size 4 [42] whenever the resulting multiset of size 8 satisfies the both pairwise amicability condition and the Gram matrix condition (3). This search resulted in the construction of matrices from 72 of the equivalence classes of Hadamard matrices of order 40.

Approach and Methodology. The project will proceed in two phases. In the first phase, we will concentrate on small matrices and small multisets, and build on our recent work and our recently developed methods. In the second phase, we will use the results of the first phase to attack larger matrices.

First phase.

Initially we will search the $\{-1,1\}$ ingredient matrices of orders 4 and 6, by applying the ideas used by CI Osborn and refined by CI Brent in the cases of orders 3 and 5 [42], but modified to take into account the possible occurrence of different graphs of amicability and anti-amicability. Order 6 is larger than anything tried so far, and new techniques may be needed to speed up the search. We also intend to study the $\{-1,0,1\}$ ingredient matrices of order 4.

We will use a combination of techniques to speed up the searches for $\{-1,1\}$ ingredient matrices including:

1. All known symmetries and other relevant properties will be used to cut down the search space. The idea is to search through a transversal of equivalence classes, rather than exhaustively.

2. The search space will be partitioned into independent parts and those parts will be searched in parallel.

3. Each check will be made as fast as possible. This means avoiding full matrix multiplications whenever the Gram or amicability conditions can be established more cheaply. We will continue to hash matrices via the first row of the Gram matrix.

4. One straightforward algorithm searches for sets of size 2^m satisfying the Gram matrix condition (3). Within each set, the algorithm then determines the amicability graph. If a pair is found which is neither amicable or anti-amicable, then the algorithm tries to find subsets of size 2^j (for $1 \leqslant j < m$) which do not contain that pair, and which satisfy both the Gram matrix condition and the amicability conditions.

5. We will also try a random sampling approach, first to see how well this characterizes the smaller orders (2 to 5), then to try sampling orders 6 before performing an exhaustive search.

6. If possible, we will identify some characteristic subsets with known properties and see how these vary as the order increases from 2 to 5, to see if searching within the corresponding subsets for order 6 yields useful information before performing an exhaustive search.

Second phase

Through the first phase we will have accumulated enough experience with $\{-1, 1\}$ ingredient matrices of orders 2 to 6 to try larger orders. We will also examine the $\{-1, 0, 1\}$ ingredient matrices of order 8. There will be four approaches, used in combination:

1. Use ideas from the first phase. We will again try the ideas used in the first phase, retaining those which still work efficiently for larger orders.

2. New and improved theory. If we better understand the classes of ingredient matrices of smaller orders, we may be able to cut down the search space by ruling out subclasses or by exploiting the properties of characteristic subclasses of ingredient matrices of larger orders.

   A better understanding of ingredient matrices is also valuable in its own right. As a radical example, if we can show that for any even order a pair (either amicable or anti-amicable) always exists satisfying the Gram property, then this proves the Hadamard conjecture. As a possibly more modest example, it is known that the Williamson construction with symmetric circulant $\{-1, 1\}$ ingredient matrices fails for orders 35, 47, 53, and 59 [18]. If we can demonstrate the existence of a 4-tuple of pairwise amicable $\{-1, 1\}$ ingredient matrices $(B_1, \ldots, B_4)$ satisfying the Gram condition (3), for one of these orders, then we will have demonstrated that our constructions (G0) and (H0) can produce Hadamard matrices with orders where the Williamson construction fails.

3. New and improved algorithms. Our experience of ingredient matrices of smaller orders may suggest improvements in the low-level algorithms used, or in the ways that we can exploit parallelism, or both.

4. Improved hardware. Some or all of the search for larger orders could be conducted on petascale hardware, including the use of GPUs. Note here that we will be doing essentially integer computations, but current GPU hardware includes efficient integer arithmetic. Similar issues arise in the use of GPUs to implement random number generators, since most of these generators use integer arithmetic and arithmetic in finite fields. As such, there is a known set of techniques on GPUs which can be adapted for use in this project.

C1.4 Research Environment

ANU has an active world-class research environment in Pure Mathematics, as evidenced by its scoring 5 in the recent ARC ERA exercise. In addition, Computational Mathematics and High Performance Computing are key developing areas for ANU in the near future.

The University of Newcastle hosts CARMA, the Priority Research Centre for Computer-Assisted Research Mathematics and its Applications. CARMA specializes in the development and use of techniques and tools for computer-assisted research and discovery in mathematics. Research areas include computation analysis, number theory and discrete mathematics.

There are essentially three types of university facilities needed for this project, computing, information and collaboration.

Available computing facilities at ANU include workstations, the Orac research cluster, and the Pi teaching cluster. The University of Newcastle has similar facilities, including a small Linux cluster run by Academic Research Computing Services.

Large-scale computation will be conducted via the National Computation Infrastructure (NCI) through the ANU Supercomputer Time Allocation Scheme and the separate NCI Merit Allocation Scheme. There may also be an opportunity to perform scalability testing of some of the algorithms on the Fujitsu hardware associated with the separate ARC Linkage Project LP110200410.

Information facilities at ANU include the ANU Library, ANU Library access to electronic sources, interlibrary loans and Article Reach. The library at the University of Newcastle offers similar services.

Collaboration at ANU would include collaboration within the Computational Mathematics group (especially M. Hegland, S. Roberts, L. Stals). Collaboration at the University of Newcastle would include collaboration within CARMA (especially J. Borwein, M. Elder). External collaboration is described in more detail in the Budget Justification.

Communication of Results The results will be communicated in several ways:

- Publication of major results in relevant high quality refereed journals.
- Presentation of results at well recognized national and international conferences.
- Via a website which will be set up to provide information about the project and its progress.
- If appropriate, by adding new data to the Online Encyclopedia of Integer Sequences [49] and incorporating it in computer algebra packages such as Sage [46] and Magma [4]. CI Brent has a close and long-standing connection with the Magma group.

C1.5 Role of Personnel

- *CI Leopardi:*
  - Overall project lead.
  - Investigation of the cases where one or more pairs of $\{-1, 1\}$ ingredient matrices are anti-amicable.
  - Development and implementation of parallel algorithms.

- *CI Osborn:*
  - Investigation of the cases where all pairs of $\{-1, 1\}$ ingredient matrices are amicable.
  - Study of the structure of equivalence classes and methods of pruning searches, via automorphisms and otherwise.
  - Collaboration with CI Brent and CI Leopardi on the development of faster algorithms.
- *CI Brent:*
  - Development of algorithms that take advantage of automorphisms to prune the search.
  - Refinement of algorithms.
  - Advice on implementation.
- *PI Orrick:*
  - Study of the structure of equivalence classes, especially with respect to switching operations.
  - Collaboration with CI Osborn on the study of structure and the development of theory for use in pruning searches.

The Team: The backgrounds of members of our proposed team are complementary. CI Leopardi is an expert on Clifford algebras, devised the generalization of the Williamson construction outlined in §1.3 [32], and has a solid background in programming, including the implementation of parallel algorithms. CI Osborn wrote her Honours thesis on generalizations of the Williamson construction for Hadamard matrices, and has a remarkable knowledge of the subject dating from her Honours thesis and past collaboration with PI Orrick (since 2002) and CI Brent (since 2007) [2, 42]. CI Brent is well-known for his research on the design and implementation of efficient algorithms. PI Orrick is one of the world's leading experts on the Hadamard maximal determinant problem, and (with Kharaghani, Solomon and others) has several recent publications in this area [39, 37, 38, 17, 2]. Thus, as a team we have both the theoretical and practical knowledge required to attack the problem.

References

[1] L. Baumert, S.W. Golomb, and M. Hall, Jr., Discovery of an Hadamard Matrix of Order 92. *Bulletin of the American Mathematical Society* **68** (1962), 237–238.

[2] **R. P. Brent, W. P. Orrick, J. Osborn**, and P. Zimmermann, Maximal determinants and saturated D-optimal designs of orders 19 and 37, arXiv:1112.4160v1 [math.CO], (2011).

[3] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor, N. J. A. Sloane, A group-theoretic framework for the construction of packings in Grassmannian spaces *J. Algebraic Combin.* 9 (1999), no. 2, 129–140.

[4] J. J. Cannon et al, *MAGMA Computational Algebra System*, `http://magma.maths.usyd.edu.au/magma/` (as at 2012).

[5] J. H. E. Cohn, Almost D-optimal designs, *Utilitas Math.* **57** (2000), 121–128.

[6] C. J. Colbourn and J. H. Dinitz, eds., *The CRC Handbook of Combinatorial Designs*, second edition, CRC Press, Boca Raton, 2006.

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

[8] R. Craigen and H. Kharaghani, Hadamard matrices and Hadamard designs, in [6, Chapter V.1, 273–279], 2006.

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

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

[11] R. H. F. Denniston, Enumeration of symmetric designs $(25, 9, 3)$, in *Algebraic and Geometric Combinatorics*, volume 65 of *North-Holland Math. Stud.*, North-Holland, Amsterdam, 1982, 111–127.

[12] H. M. Gastineau-Hills. *Systems of orthogonal designs and quasi-Clifford algebras.* PhD thesis, University of Sydney, 1980.

[13] H. M. Gastineau-Hills. Quasi-Clifford algebras and systems of orthogonal designs. *J. Austral. Math. Soc. Ser. A*, **32** (1):1–23, 1982.

[14] A. V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York, 1979.

[15] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sci. Math.* **17** (1893), 240–246.

[16] A. S. Hedayet, N. J. A. Sloane and J. Stufken, *Orthogonal Arrays, Theory and Applications*, Springer, New York, 1999.

[17] W. H. Holzmann, H. Kharaghani and **W. Orrick**, On the real unbiased Hadamard matrices, *Contemporary Mathematics, Combinatorics and Graphs*, **531** (2010), 243-250.

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

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

[20] K. J. Horadam, Hadamard matrices and their applications: Progress 20072010, *Cryptogr. Commun.* (2010) 2, 129–154.

[21] H. Kharaghani and **W. Orrick**, *D-optimal designs*, in [6, Chapter V.3, 295–297].

[22] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *Journal of Combinatorial Designs* **13** (2004), 435–440.

[23] H. Kharaghani and B. Tayfeh-Rezaie, On the classication of Hadamard matrices of order 32, *Journal of Combinatorial Designs* **18** (2010), 328336.

[24] H. Kharaghani and B. Tayfeh-Rezaie, Hadamard matrices of order 32, `http://math.ipm.ac.ir/tayfeh-r/Hadamard32.htm` (as at 2012).

[25] E. S. Lander, *Symmetric Designs: an Algebraic Approach*, LMS Lecture Note Series **74**, Cambridge University Press, 1983.

[26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, ninth impression, 1996.

[27] B. D. McKay, Computing autmorphisms and canonical labellings of graphs, *Combinatorial Mathematics: Lecture Notes in Mathematics* **686**, Springer Verlag, Berlin, 1978.

[28] B. D. McKay, Hadamard equivalence via graph isomorphism, *Discrete Mathematics* **27** (1979), 213–214.

[29] B. D. McKay, Practical graph isomorphism, *Congressus Numerantium* **30** (1981), 45–87.

[30] B. D. McKay, *nauty*, `http://cs.anu.edu.au/~bdm/nauty/` (as at 2012).

[31] B. D. McKay and I. M. Wanless, On the number of Latin squares, *Ann. Combinat.* **9** (2005), 335–344.

[32] **P. Leopardi**, Constructions for Hadamard matrices, Clifford algebras, and their relation to amicability - anti-amicability graphs, submitted to the *Australian Journal of Combinatorics* for a special issue on Hadamard matrices to honour Kathy Horadam, 2011.

[33] E. C. MacRae. Matrix derivatives with an application to an adaptive linear decision problem. *Ann. Statist.*, 2:337–346, 1974.

[34] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[35] P. Ó Catháin, *Group actions of Hadamard matrices*, Masters Thesis, NUI Galway, 2008.

[36] P. Ó Catháin, *Automorphisms of Pairwise Combinatorial Designs* PhD Thesis, NUI Galway, 2011.

[37] **W. P. Orrick**, Switching operations for Hadamard matrices, *SIAM J. Discrete Math.* **22** (2008), 31–50.

[38] **W. P. Orrick**, On the enumeration of some D-optimal designs, *J. Statist. Plann. Inference*, **138** (2008), 286–293.

[39] **W. Orrick** and B. Solomon, Large-determinant sign matrices of order $4k + 1$, *Discrete Math.* **307** (2007), 226–236.

[40] **W. Orrick** and B. Solomon, *The Hadamard maximal determinant problem*, `http://www.indiana.edu/~maxdet/` (as at 2012).

[41] **J. H. Osborn**, *The Hadamard Maximal Determinant Problem*, Honours thesis, University of Melbourne, 2002.

[42] **J. H. Osborn**, On Williamson and octonion matrices with ingredients not necessarily circulant: classification results for order 5 ingredients, submitted to the *Australian Journal of Combinatorics* for a special issue on Hadamard matrices to honour Kathy Horadam, 2011.

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

[44] V. S. Pless and W. C. Huffman, eds., *Handbook of Coding Theory*, North-Holland, Amsterdam, 1998.

[45] O. S. Rothaus, On "bent" functions, *J. Combin. Theory A* **20** (1976), 300–305.

[46] *Sage: open source mathematics software*, `http://www.sagemath.org/` (as at 2012).

[47] A. G. Sarukhanyan, Generalized Williamson type matrices, *Uch. Zap. Erevan Gos. Univ.* **2** (1978), 3–11.

[48] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson (eds.), Wiley, New York, 1992.

[49] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, `http://oeis.org/` (as at 2012).

[50] W. D. Smith, *Studies in Computational Geometry Motivated by Mesh Generation*, PhD dissertation, Princeton University, 1988.

[51] J.J. Sylvester, 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, *Philosophical Magazine* **34** (1867), 461–475.

[52] J. S. Wallis (J. Seberry), On the existence of Hadamard matrices, *J. Combin. Theory A* **21** (1976), 188–195.

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

[54] M. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory A* **61** (1992), 230–242.

[55] M. Xia, T. Xia and J. Seberry, A new method for constructing Williamson matrices, *Designs, Codes and Cryptography* **35** (2005), 191–209.