# ABSTRACTS

Workshop on Algebraic Design Theory and Hadamard Matrices (ADTHM) 2014
University of Lethbridge
Lethbridge, Alberta
July 8 – 11, 2014

Invited and Plenary Speakers (in alphabetical order by speaker name)

## *A cocyclic approach to some families of Hadamard matrices*

*Victor Alvarez*
*Universidad de Sevilla, Seville, Spain*

In this talk we will describe a cocyclic approach to some families of Hadamard matrices. This will support the fact that the cocyclic approach might be the most uniform construction technique for Hadamard matrices currently known.

This is a joint work with J.A. Armario, R.M. Falcn, M.D. Frau, F. Gudiel, M.B. Güemes and A. Osuna.

## *Maximal determinants and cocyclic matrices*

*José Andrés Armario*
*Universidad de Sevilla, Seville, Spain*

The maximal determinant problem asks for the largest possible $n \times n$ determinant with entries $\pm 1$. It is well-known that Hadamard matrices give the solution to this question when $n = 1, 2$ or a multiple of 4. Since the 90's, cocyclic matrices have been successfully used for constructing Hadamard matrices. Recently, the cocyclic approach has been extended to finding matrices with large determinant in the case $n \equiv 2 (\mod 4)$. In this talk, we will show some results that we have obtained as a consequence of this approach, among them: a method for embedding cocyclic matrices with large determinant in Hadamard matrices and a connection with matrices of the conference type with large determinant.

This is joint work with V. Álvarez, M.D. Frau and F. Gudiel.

# *Hadamard Matrices and Covering Arrays*

*Charlie Colbourn*

*Arizona State University, Tempe, Arizona*

Covering arrays are employed in applications in which experimental factors interact. When applied in testing, columns correspond to experimental *factors*, and the symbols in the column form *values* or *levels* for the factor. Each row specifies the values to which to set the factors for an experimental run.

Let $N$, $k$, $t$, and $v$ be positive integers with $k \geq t$. Let $C$ be an $N \times k$ array with entries from an alphabet $\Sigma$ of size $v$; we typically take $\Sigma = \{0, \ldots, v-1\}$. Choose a $t$-tuple $(\nu_1, \ldots, \nu_t)$ with $\nu_i \in \Sigma$ for $1 \leq i \leq t$ and a tuple of $t$ columns $(c_1, \ldots, c_t)$ with $c_i \in \{1, \ldots, k\}$, and $c_i \neq c_j$. Then $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ is a *$t$-way interaction*. The array *covers* the $t$-way interaction $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ if, in at least one row $\rho$ of $C$, the entry in row $\rho$ and column $c_i$ is $\nu_i$ for $1 \leq i \leq t$. Array $C$ is a *covering array* $\mathrm{CA}(N; t, k, v)$ of *strength $t$* if every $t$-way interaction is covered. We denote by $CAN(t, k, v)$ the minimum $N$ for which a $CA(N; t, k, v)$ exists. To facilitate testing, the goal is to determine the exact value of, or a useful upper bound on, $CAN(t, k, v)$.

Existence results for covering arrays are still quite incomplete, even for small values of $t$. In this talk, we explore the use of Hadamard matrices in the construction of covering arrays. These existence results motivate powerful algebraic constructions for covering arrays, which we also explore.

# *On some codes and divisible designs constructed from Hadamard matrices*

*Dean Crnkovic*

*University of Rijeka, Rijeka, Croatia*

In this talk we present a construction of a class of regular Hadamard matrices. From orbit matrices of the corresponding Menon designs we construct classes of self-orthogonal or self-dual codes. Further, we describe construction of divisible design graphs using Hadamard matrices. Divisible design graphs have been introduced in 2011 by W. H. Haemers, H. Kharaghani and M. A. Meulenberg.

# 3.5 *years of periodic complementary sequences*

*Dragomir Z. Djokovic and Ilias S. Kotsireas*

*University of Waterloo, Waterloo, Ontario, and*

*Wilfrid Laurier University, Waterloo, Ontario*

We discuss our new results on periodic complementary sequences used to construct Hadamard and skew-Hadamard matrices, D-optimal matrices, periodic Golay pairs and weighing matrices. The main new tool employed in these constructions is the method of compression, which is applicable when the length of sequences is a composite number. Another crucial concept is furnished by necklaces and bracelets, namely combinatorial objects that allow one to systematically account for symmetries. For instance we use compression by a factor of 2 and bracelets of balanced content to find a periodic Golay pair of length $2 \cdot 29 = 58$. As another example, we constructed Hadamard matrices of orders $4 \cdot 251$ and $4 \cdot 631$ (new orders) and skew-Hadamard matrices of orders $4 \cdot 213$ and $4 \cdot 631$. Part of this work has been published in joint papers with Oleg Golubitsky (Google Inc.), Daniel Recoskie (University of Guelph), Joe Sawada (University of Guelph).

# *On linear shift representations*

*Dane Flannery (and Ronan Egan)*

*National University of Ireland, Galway, Ireland*

We introduce and develop the concept of ‘shift representation’. This derives from a certain action on 2-cocycle groups preserving both orthogonality and cohomological equivalence, discovered by Horadam in the context of relative difference sets. Detailed results about complete reducibility and fixed points are provided. We also describe some computational applications.

# *Orthogonal designs, the Kharaghani array and applications to other fields*

*Stelios Georgiou*

*RMIT University, Melbourne, Australia*

Orthogonal designs are proved to be an important combinatorial tool. The use of orthogonal designs and combinatorial structures, such as the Kharaghani array, found many applications in a number of different fields, such as coding theory, cryptography, statistics, and many more. This talk briefly presents some applications, suggestions and constructions, that significantly improved on know methods and gave a number of new results.

## *Hadamard matrices and complex equiangular lines*

*Jonathan Jedwab*

*Simon Fraser University, Burnaby, British Columbia*

Equiangular lines in complex space have been studied for nearly forty years. Renewed interest was sparked by Zauner's 1999 thesis on quantum designs, and since then there has been intense effort by mathematicians and physicists to determine the maximum number of equiangular lines in complex d-dimensional space. I shall describe a simple construction for maximum-sized sets of complex equiangular lines in dimensions 2, 3 and 8 from Hadamard matrices.

This is joint work with Amy Wiebe.

## *Nice Euclidean configurations from incidence matrices and characters of designs*

*William Martin*

*Worcester Polytechnic Institute, Worcester, Massachusetts*

A number of constructions have recently emerged in communications and quantum information theory which employ designs in an interesting way. The aim of this talk will be to survey these applications, the tools involved, and the properties of designs which will allow us to push these constructions further. Examples include MUBs, SIC-POVMs, ETFs, and almost orthogonal vectors.

## *A new approach to the circulant Hadamard conjecture with Walsh-Fourier analysis*

*Mate Matolcsi*

*Rényi Institute, Budapest, Hungary*

I will present an approach to the circulant Hadamard conjecture based on Walsh-Fourier analysis. The conjecture will be shown to be equivalent to a linear system of equations having full rank. One philosophical advantage of the approach is that the non-existence of a circulant Hadamard matrix of size $n$ can be shown by exhibiting a 'witness' $w_n$. We will show some witnesses in low dimensions, and contemplate on how such witnesses may be produced for general $n$.

# *Generalized tensor products and related constructions*

*Akihiro Munemasa*

*Tohoku University, Sendai, Japan*

Generalized tensor products, weaving, and strong Kronecker products are well-known techniques for constructing new matrices from old. In this talk, we point out relationships between them. We also point out less well-known objects called Jones graphs and Nomura algebras, through which generalized tensor products can be recognized.

# *Lander chains and structure of Hadamard matrices*

*William Orrick*

*Indiana University, Bloomington, Indiana*

A fruitful approach to understanding the structure of designs has been to study the linear code $\mathcal{C}$ constructed from the incidence matrix of the design by taking the span of the matrix rows over a suitable finite field. For some purposes, it is better to look at the dual of this code, $\mathcal{C}^{\perp}$. Eric Lander discovered that, for certain design parameters, a deeper understanding can be obtained by forming the **Z**-module—that is, the integer span—of the rows. Relative to a suitable prime, there is an interesting chain of submodules, from which Lander formed a chain of linear codes. At one end of the chain is the code $\mathcal{C}$; at the other, is its dual, $\mathcal{C}^{\perp}$. But there may be additional codes, interpolating between $\mathcal{C}$ and its dual.

Peter Cameron suggested to me that Lander's idea could be applied to Hadamard matrices. In this talk I will give an introduction to Lander's chain and its application to Hadamard matrices. In the case of $32 \times 32$ Hadamard matrices, Lander's chain contains, in addition to $\mathcal{C}$ and $\mathcal{C}^{\perp}$, a third code which is self-dual, contains $\mathcal{C}$, and is contained in $\mathcal{C}^{\perp}$. I will describe what is known about the codes in Lander's chain, and what the open questions are. As an application, I will look at switchable structures in Hadamard matrices—structures with two or more alternative forms—and what Lander's chain of codes has to say about such structures.

# *A new family of Alltop functions*

*Asha Rao*

*RMIT University, Melbourne, Australia*

Sequences with optimal correlation properties are much sought after for applications in communication systems. In 1980, Alltop (IEEE Trans. Inf. Theory 26(3):350–354, 1980) described a set of sequences based on a cubic function and showed that these sequences were optimal with respect to the known bounds on auto and crosscorrelation. Subsequently these sequences were used to construct mutually unbiased bases (MUBs), a structure of importance in quantum information theory. The key feature of this cubic function is that its difference function is a planar function. We call functions with planar difference functions, Alltop functions.

I will first show that Alltop functions cannot exist in fields of characteristic 3 and that for a known class of planar functions, $x^3$ is the only Alltop function. I will then construct a new family of Alltop functions that are EA-inequivalent to $x^3$ and establish the use of Alltop functions in the construction of sequence sets and MUBs.

This is joint work with Joanne Hall, Stephen Gagola and Diane Donovan.

# *Some Thoughts on Symmetric Conference Matrices*

*Jennifer Seberry (talk given by Gene Awyzio)*

*University of Wollongong, Wollongong, Australia*

# *Circulant Hadamard Matrices and Barker Sequences*

*Bernhard Schmidt*
*Nanyang Technological University, Singapore*

A **circulant Hadamard matrix of order** $v$ is a Hadamard matrix of the form

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}.$$

A **Barker sequence of length** $v$ is a sequence $a_1, \ldots, a_v$ with $a_i = \pm 1$ and

$$\left| \sum_{j=1}^{v-k} a_j a_{j+k} \right| \leq 1$$

for $k = 1, \ldots, v-1$. Barker sequences and circulant Hadamard matrices are closely connected, as the existence of a Barker sequence of length $v > 13$ implies the existence of a circulant Hadamard matrix of order $v$.

In his 1963 book *Combinatorial Mathematics*, H. J. Ryser stated the conjecture that there is no circulant Hadamard matrix of order larger than 4. This conjecture is still unresolved despite frequently appearing claims to the contrary. In fact, there are only a few publications which contain results relevant to the conjecture. We will give an overview of the status of the conjecture and present some new results.

# *New Results on Binary Frameproof Codes*

*Doug Stinson*
*University of Waterloo, Ontario*

We give some new results on $w$-frameproof codes, which are equivalent to $\{1,w\}$-separating hash families. Let $h$ be a function from a set $X$ of size $n$ to a set $Y$ of size $q$. Let $C$, $D$ be disjoint subsets of $X$, where $|C| = 1$ and $|D| = w$. We say that $h$ separates $(C,D)$ if $h(C)$ is disjoint from $h(D)$. A set of $N$ functions from $X$ to $Y$ is an $(N;n,q,\{1,w\})$-separating hash family, denoted by $SHF(N;n,q,\{1,w\})$, if for all disjoint subsets $C$, $D$ of $X$, where $|C| = 1$ and $|D| = w$, there exists at least one of the $N$ specified functions that separates $(C,D)$.

Our results concern binary codes, which are defined over an alphabet of two symbols. For all $w \geq 3$, and for $w+1 \leq N \leq 3w$, we show that an $SHF(N;n,2,\{1,w\})$ exists only if $n \leq N$ and an $SHF(N;N,2,\{1,w\})$ must be a permutation matrix of order $N$. We also obtain some results concerning when the incidence matrix of a symmetric BIBD is an $SHF(N;N,2,\{1,3\})$ (i.e., a 3-frameproof code).

This talk is based on joint work with Chuan Guo and Tran van Trung.

## *Mutually unbiased weighing matrices and their generalization*

*Sho Suda*

*Aichi University of Education, Kariya, Aichi, Japan*

Mutually unbiased bases play a role in the quantum information theory. This concept is regarded as a finite subset in the real unit sphere with some conditions. From the view point of algebraic combinatorics on the unit sphere, they provide a nice algebraic structure which is called an association scheme.

Recently Holzmann, Kharaghani and Orrick introduced the concept of mutually unbiased weighing matrices as a generalization of MUBs. Also a very recent work of Best, Kharaghani and Ramp studied MUWMs further and posed a problem on MUWMs which asks us to construct MUWMs with some parameters. In this talk we give an affirmative answer to Best, Kharaghani and Ramp's question to use coding theory. Also we introduce a generalization of MUWMs and show how it connects to MUWMs. Finally we provide a sufficient condition for MUWMs to give association schemes, which is closely related to works of Brouwer or Haemers-Tonchev on strongly regular graphs with spreads.

## *Modular combinatorial designs and Hadamard matrices modulo 5*

*Ferenc Szöllősi*

*Tohoku University, Sendai, Japan*

We introduce modular combinatorial designs and study them to obtain new modular Hadamard matrices. We prove that there exist 5-modular Hadamard matrices of order $n$ if and only if $n \neq 6$, 11 and $n \not\equiv 3, 7 \pmod{10}$. In particular, this solves the 5-modular version of the Hadamard conjecture.

## *Classification of Hadamard matrices of small orders*

*Behruz Tayfeh-Rezaie*

*Institute for Fundamental Research, Tehran, Iran*

All equivalence classes of Hadamard matrices of order at most 28 have been found by 1994. Order 32 is where a combinatorial explosion occurs on the number of Hadamard matrices. Recently, using an exhaustive computer search we showed that there are exactly $13,710,027$ Hadamard matrices of order 32. In this talk we present our approach and also report partial results on the classification in order 36.

# *Cyclotomic orthomorphisms*

*Ian Wanless*
*School of Mathematical Sciences, Monash University, Clayton, Victoria, Australia*

An orthomorphism of a finite field $F$ is a permutation $\theta : F \to F$ such that the map $x \to \theta(x) - x$ is also a permutation. The orthomorphism $\theta$ is cyclotomic of index $k$ if $\theta(0) = 0$ and $\theta(x)/x$ is constant on the cosets of a subgroup of index $k$ in the multiplicative group $F^*$. In this talk I will explain briefly why cyclotomic orthomorphisms are a particularly good way of building orthogonal Latin squares. I will then focus on two problems posed by Tony Evans about the existence of cyclotomic orthomorphisms. We can solve one completely and provide an asymptotic answer to the other.

# *Menon-Hadamard difference sets obtained from a local field by natural projections*

*Mieko Yamada*
*Tokyo Woman's Christian University, Tokyo, Japan*

We know there exists a family of Menon-Hadamard difference sets over Galois rings of characteristic of an ever power of 2 and of an odd extension degree, which has an embedded structure. As the projective limit of Galois rings is a variation ring of a local field, the projective limit of these Menon-Hadamard difference sets is a non-empty subset of a variation ring of a local field.

Conversely, does there exist a subset of a local field whose image by the natural projection always gives a difference set over a Galois ring?

We will show an example answer to this problem in this talk. A family of Menon-Hadamard difference sets is obtained from a subgroup of a variation ring of a local field by natural projections. Furthermore this family also has an embedded structure. The formal group and the $p$-adic logarithm function serve an important role.

# *Quantum information processing, combinatorics and Hadamard matrices*

*Karol Życzkowski*
*Jagiellonian University, Kraków, Poland*

# Contributed Talks (in alphabetical order by speaker name)

## *Mutually unbiased bases, Hadamard matrices and symplectic spreads*

*Kanat Abdukhalikov*
*UAE University, Al Ain, UAE*

The notion of mutually unbiased bases (MUBs) is one of the basic concepts of quantum information theory. MUBs have very close relations to other problems in various parts of mathematics, such as Lie algebras, theory of Hadamard matrices, algebraic combinatorics, finite geometry, coding theory and spherical codes. All these branches have problems similar to MUBs, and all these problems were developed independently from others. In this talk we will discuss relations of MUBs and Hadamard matrices, give explicit descriptions of complete sets of MUBs and orthogonal decompositions of special Lie algebras $sl_n(\mathbb{C})$ obtained from commutative and symplectic semifields, and from some other non-semifield symplectic spreads. We show that automorphism groups of complete sets of MUBs and corresponding orthogonal decompositions of Lie algebras $sl_n(\mathbb{C})$ are isomorphic, and in case of symplectic spreads these automorphism groups are determined by automorphism groups of those spreads. Planar functions over fields of odd characteristics also lead to constructions of MUBs. There are no planar functions over fields of characteristic two satisfying the traditional definition. However, by using new notion of pseudo-planar functions over fields of characteristic two we give new explicit constructions of complete sets of MUBs.

## *Automorphisms of the Sylvester matrix and related designs*

*Ronan Egan*
*National University of Ireland, Galway*

We review the notions of regular and centrally regular group actions for pairwise combinatorial designs. Motivated by de Launey and Stafford's classification of the centrally regular subgroups for the Paley matrices, we discuss some (old and new) results in this area concerning the Sylvester Hadamard matrix and an equivalent design introduced by Kantor.

# *Entropy Optimal Orthogonal Matrices*

*Jacob Erickson*
*Wright State University, Dayton, Ohio*

The entropy of an orthogonal matrix follows naturally from the standard definition of entropy from information theory. In this talk, the maximization of entropy over orthogonal matrices is discussed. This maximization process has an intriguing connection to Hadamard matrices. Following the result on Hadamard matrices, several related results will be discussed.

# *Instantaneously estimating quantum channels through linear codes*

*Yuichiro Fujiwara*
*California Institute of Technology, Pasadena, California*

We present an on-the-spot method for reliably and instantly estimating the noise level during quantum information processing protected by quantum error-correcting codes. As preprocessing of quantum error correction, our scheme estimates the current noise level through a negligible amount of classical computation with syndromes from linear codes, and updates the decoder's knowledge on the spot before inferring the locations of errors. The estimation requires no additional quantum circuits. The estimate can be of higher quality than the maximum likelihood estimate based on perfect knowledge of channel parameters, thereby eliminating the need of the unrealistic assumption that the decoder accurately knows the channel parameters a priori.

# *Signed group orthogonal designs and their applications*

*Ebrahim Ghaderpour*
*York University, Toronto, Ontario*

A *signed group* $S$ is a group with a distinguished central element of order two. The trivial signed group $S_{\mathbb{R}} = \{\pm 1\}$ and the complex signed group $S_{\mathbb{C}} = \{\pm 1, \pm i\}$ are examples of two signed groups in which $-1$ is their distinguished central element of order two.

A *signed group orthogonal design*, SOD, of type $(u_1, \ldots, u_k)$, where $u_1, \ldots, u_k$ are positive integers, and of order $n$, is a square matrix $X$ of order $n$ with entries from $\{0, \varepsilon_1 x_1, \ldots, \varepsilon_k x_k\}$, where the $x_i$'s are variables and $\varepsilon_j \in S$, $1 \leq j \leq k$, for some signed group $S$, that satisfies

$$XX^* = \left(\sum_{i=1}^{k} u_i x_i^2\right) I_n,$$

where $X^*$ is the conjugate transpose of $X$. We call an SOD with no zero entries a full SOD.

Equating all variables to 1 in any full SOD of order $n$ results in a signed group Hadamard matrix of order $n$. R. Craigen introduced and studied signed group Hadamard matrices and using these matrices, he eventually improved the asymptotic existence of Hadamard matrices.

An SOD over the trivial signed group $S_{\mathbb{R}}$ results in an orthogonal design, OD.

In this talk, the asymptotic existence of ODs will be discussed using SODs; more precisely, for any $k$-tuple $(u_1, u_2, \ldots, u_k)$ of positive integers, there is an integer $N = N(u_1, u_2, \ldots, u_k)$ such that for each $n \geq N$, a full OD (no zero entries) of type $(2^n u_1, 2^n u_2, \ldots, 2^n u_k)$ exists. Depending on the purposes and sequences used to create SODs, the following two upper bounds are obtained for the asymptotic existence of ODs:

$$N \leq \frac{3}{13} \sum_{i=1}^{k} \log(u_i) + 8k + 4 \quad \text{and} \quad N \leq \frac{1}{5} \sum_{i=1}^{k} \log(u_i) + 10k + 4.$$

This is a joint work with H. Kharaghani.

## *Designing MIMO antenna systems*

*Pekka H. J. Lampio*

*Aalto University, Finland*

Multiple-Input and Multiple-Output, or MIMO, is the use of multiple antennas at both the transmitter and receiver to improve performance of wireless communications. It offers significant increases in data throughput and link range without additional bandwidth or increased transmit power.

In this work we describe how the problem of designing precoding codebooks for MIMO systems can be solved by reducing it to two problems in discrete mathematics. We first show how the original design problem defined in a continuous space can be formulated with discrete orthogonal matrices that are generalizations of Butson-type Hadamard matrices. This reformulation leads to a maximum clique problem in a simple graph which in turn is solved with an exhaustive computer search. We give some preliminary results for systems with 4 transmit and 2 receive antennas.

This is joint work with Patric R.J. Östergård, Renaud-Alexander Pitaval, and Olav Tirkkonen.

## *Twin bent functions and Clifford algebras*

*Paul Leopardi*

*Australian National University, Acton ACT, Australia*

It is known that the function $f$ defined on an ordering of the $4^n$ monomial basis matrices of the real representation of the Clifford algebra $Cl(n,n)$, where $f(M) = 0$ if $M$ is symmetric, $f(M) = 0$ if $M$ is skew, is a bent function. It is perhaps less well known that the function $g$ where $g(M) = 0$ if $M$ is diagonal or skew, $g(M) = 1$ otherwise, is also a bent function, with the same parameters as $f$. The talk will describe these functions and their relation to constructions for Hadamard matrices.

## *Combinatorial designs and compressed sensing*

*Padraig Ó Catháin*

*University of Queensland, Brisbane, Queensland*

Compressed sensing is a technique used in signal processing to reconstruct under-sampled data, subject to some assumptions. It has been intensively studied in the past fifteen years or so, and lies at the interface of mathematics, statistics and electrical engineering. One of the main challenges is the construction of good matrices for use in compressed sensing. In this talk, we will give an introduction to compressed sensing, emphasizing the relation with well-known concepts in linear algebra. We then describe a new construction for compressed sensing matrices using pairwise balanced designs and Hadamard matrices. This construction generalises and unifies a number of results in the literature. Using results on the asymptotic existence of certain designs, we obtain new asymptotic existence results on compressed sensing matrices.

# *Some families of $1\frac{1}{2}$-difference set in elementary abelian p-groups*

*Oktay Olmez*
*Ankara University, Tandogan, Ankara, Turkey*

Let $T = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a tactical configuration with parameters $(v, b, k, r)$. For every point $x \in \mathcal{P}$ and every block $B \in \mathcal{B}$, let $\phi(x, B)$ be the number of flags $(y, C) \in \mathcal{I}$ such that $y \in B \setminus \{x\}$, $x \in C$ and $C \neq B$. A $1\frac{1}{2}$-design with parameters $(v, b, k, r; \alpha, \beta)$ is a tactical configuration $T$ such that

$$\phi(x, B) = \begin{cases} \alpha, & x \notin B; \\ \beta, & x \in B. \end{cases}$$

Well-studied examples of $1\frac{1}{2}$-designs include 2-designs, transversal designs, and partial geometries. In this talk, we will introduce a new construction method called the $1\frac{1}{2}$-difference set for symmetric $1\frac{1}{2}$-designs. This new construction produces a $1\frac{1}{2}$-design whose automorphism group has a subgroup that is transitive on blocks and points of the incidence structure. We will provide preliminary results concerning $1\frac{1}{2}$-difference sets and the group rings. We will also provide examples of $1\frac{1}{2}$-difference sets in elementary abelian $p$-groups.

# *Solving Open Cases of Circulant Weighing Matrices*

*Ming Ming Tan*
*Nanyang Technological University, Singapore, Singapore*

A **circulant weighing matrix**, denoted by $CW(v, n)$, is a square matrix of order $v$ of the form

$$M = \begin{pmatrix} a_1 & a_2 & \dots & a_v \\ a_v & a_1 & \dots & a_{v-1} \\ \dots & \dots & \dots & \dots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$$

with $a_i \in \{0, \pm 1\}$ for all $i$ and

$$MM^T = nI.$$

Circulant weighing matrices serve as one of the main tools in constructing Hadamard matrices and for the study of Lander's conjecture.

We study the existence problem of circulant weighing matrices, i.e., for what values of $v$ and $n$ does a $CW(v, n)$ exist? Strassler's table listed the existence status of $CW(v, n)$'s with $v \leq 200$ and $n \leq 100$. Despite many recent results, there are still numerous open cases.

We employ various algebraic techniques in an attempt to tackle some remaining open cases. Though some of the open cases can be solved theoretically, some require partial computer searches. We will present the algebraic approaches and explain how they can be incorporated in efficient computer searches.

This is joint work with Bernhard Schmidt.

# *A 4-dimensional family of generalized Hadamard matrices*

*Ilya Zhdanovskiy*

*Moscow Institute of Physics and the Technology State University, Moscow, Russia*

In my talk I will present 4-dimensional family of generalized Hadamard (or type-II) matrices of size 6. Using this construction, one can prove the existence of 4-dimensional complex Hadamard matrices of size 6.

# *Regular polyhedra and Hadamard matrices*

*Peter Zvengrowski*

*University of Calgary, Calgary, Alberta*

It's clear that by taking four vertices of a cube, in pairs that are diagonally opposite across each face, one obtains the vertices of a regular tetrahedron. This was known to Kepler (and probably much earlier), who also took the regular tetrahedron formed by the remaining four vertices and called the eight pointed star obtained by taking the two tetrahedra together a *stella octangula*.

One can ask this question more generally for convex regular polytopes in $n$-dimensional euclidean space: given such a regular polytope when is it possible for a proper subset of its vertices to also form a regular $n$-dimensional polytope? Here we only consider $n \geq 3$, the two dimensional case is rather trivial. In this talk we shall answer this question for all $n$, and see that in particular an $(n-1)$-cube admits a regular $(n-1)$-simplex among its vertices (as in the Kepler example above for $n = 3$) if an only if there exists a Hadamard matrix of degree $n$. We shall also talk about some of the history associated with these ideas, in particular Stringham and Schläfli in the nineteenth century and Boole-Stott, Coxeter, Paley, and Todd in the early twentieth century. The talk is based on joint work with J. Adams and P. Laird.