Searching for (cocyclic) (partial) Hadamard matrices

Víctor Álvarez

We describe a system of equations characterizing the set of cocyclic Hadamard matrices over a given group. Attending to this system, some upper and lower bounds are given on the number of elementary coboundary matrices to combine in order to form a cocyclic Hadamard matrix. We also prove that the cocyclic framework is not suitable for constructing partial Hadamard matrices. As an alternative, we describe a heuristic procedure to construct large partial Hadamard matrices, in terms of cliques of certain graphs.

On inequivalence criteria for cocyclic Hadamard matrices

José Andrés Armario

Given two Hadamard matrices of the same order, it can be quite difficult to decide whether or not they are equivalent. There are some criteria to determine Hadamard inequivalence. For instance, the profile criterion is a sufficient (but not necessary) condition for Hadamard inequivalence. In this talk, we give some ideas on how to adapt (rewrite) this criterion to determine inequivalence in the cocyclic framework.

New families of q-ary error correcting codes obtained from generalised Hadamard matrices

Carl Bracken

It is well known that a generalised Hadamard matrix can be used to construct an optimal q-ary error correcting code. We will demonstrate a special construction of generalised Hadamard matrices from which we obtain good q-ary codes by considering a subset of the columns of the matrix. The efficiency of these codes will be discussed with relation to the Griesmer bound and a generalisation of the Grey-Rankin bound.

Some aspects of codes over rings (especially the integers mod 4)

Peter J. Cameron

The study of codes over the integers mod 4 received a huge boost in the 1990s when Hammons et al. discovered that some famous non-linear binary codes (the Nordstrom-Robinson, Preparata and Kerdock codes) can be regarded as images under a non-linear isometry (the Gray map) of linear codes over the integers mod 4. Since then, codes over rings have been studied by various people. Josephine Kusuma recently extended the known connection (due to Delsarte) between strength (as orthogonal array) and minimum weight of the dual code over a field to arbitrary commutative rings with identity.

Since the ring of integers mod 4 is a non-split extension of the binary field by itself, it is natural that cohomology should enter the discussion of codes over this ring. Little has been done on this apart from recent work by Fatma Al Kharoosi. The problem of classifying the extensions of one binary code by another in this sense is an interesting and difficult one.

Codes over arbitrary quotients of the ring of integers arise in the earlier algebraic approach to symmetric designs by Eric Lander.

The talk will address some of the issues arising in this area.

A digraph construction for circulant partial Hadamard matrices

Rob Craigen

A question about stream cipher cryptanalysis leads to the following problem: For which positive n and k does there exist an nxn circulant (±1)-matrix whose first k rows are mutually orthogonal? Such matrices we call *partial circulant Hadamard matrices*. Their row sums are obviously constant; if the common row sum is r then we denote such a matrix by r-CPH(k x n). If the first k rows are orthogonal so are the first k−1, so the pertinent question becomes: “For given r, n, what is the maximum possible value of k?”

Remarkably, this initially obscure-sounding question provides a novel and promising approach to Ryser’s famous conjecture that there are no circulant Hadamard matrices of order > 4. Further, surprising connections have been found between these exotic rectangular matrices and better-known square types—such as negacyclic conference matrices. Extremal r-CPH(k x n)’s display an unexpected amount of regularity in their pattern of existence.

With two students I have developed a tool for the construction of these matrices, that is also useful for analyzing the general problem, that employs digraphs in a manner reminiscent of the famous construction for de Bruijn sequences, but far more general. I will explain how the method works, and discuss some recent results.

Warwick de Launey

TBA

Some REALLY beautiful Hadamard matrices

John F. Dillon

In honor of our friend and colleague Warwick de Launey we provide some “party decorations" in the way of some Hadamard matrices which arise from difference sets in a wide variety of groups. Along the way, we provide some background on their constructions . . . some old and some new . . . and point out some related open questions.

Algebra in Design Theory

Dane Flannery

A forthcoming book by Warwick de Launey and the speaker covers a wide range of topics under the above heading. In this talk we survey some of those topics, that fall under the subheading ‘Group Actions on Pairwise Combinatorial Designs’. Although the main problems arose in design theory, they are essentially algebraic problems that can be solved algorithmically i.e. using computational algebra.

A heuristic procedure with guided reproduction for constructing cocyclic Hadamard matrices over D_{4t}

V. Álvarez**, Maria Dolores Frau**, and A. Osuna

A genetic algorithm for constructing cocyclic Hadamard matrices over D_{4t} is described. The novelty of this algorithm is the guided heuristic procedure for reproduction, instead of the classical crossover and mutation operators used by the authors in an earlier performance. This has permitted to find larger cocyclic Hadamard matrices than before.

Daniel Gordon

TBA

Rooted trees searching for cocyclic Hadamard matrices over D_{4t}

V. Álvarez, J. A. Armario, M. D. Frau, **Félix Gudiel**, and A. Osuna

A new reduction on the size of the search space for cocyclic Hadamard matrices over dihedral groups D_{4t} is described, in terms of the so-called *central distribution*. This new search space adopt the form of a forest consisting of two rooted trees (the vertices representing subsets of coboundaries) which contains all cocyclic Hadamard matrices satisfying the constraining condition. Experimental calculations indicate that the ratio between the number of constrained cocyclic Hadamard matrices and the size of the constrained search space is greater than the usual ratio.

On cocyclic Hadamard matrices over $Z_t \times Z_2^2$

V. Álvarez, F. Gudiel, and **Belén Güemes**

We describe some nice properties on cocyclic Hadamard matrices over $Z_t \times Z_2^2$, which have led to the design of a new heuristic procedure for constructing cocyclic Hadamard matrices over this family of groups.

Hadamard matrices and their applications: an update

Kathy Horadam

I will give an overview of progress over the last two years, much of it due to Warwick and co-authors, on a selection of the problems listed in my book `Hadamard matrices and their applications'.

Unbiased bases and Hadamard matrices

Hadi Kharaghani

Two Hadamard matrices H and K of order n are called unbiased if the matrix HK^t has no zero entries. If the absolute value of all the entries equal $\sqrt{n}$, then the pair is called to be regularly unbiased. This is a survey talk on all which is known about these matrices. The relationship between mutually unbiased bases and regularly mutually unbiased Hadamard matrices will be discussed and some applications will be presented. (A joint work with W. Holzmann and W. Orrick).

Recent Advances in Weighing Matrices

Ilias Kotsireas

The weighing matrices tables contained in the second edition of the Handbook of Combinatorial Designs published in November 2006 are already obsolete. By employing an amalgamation of theoretical and computational techniques, old and new ideas, metaheuristics, code generation and
supercomputing we have found many new weighing matrices in a series of papers with K. T. Arasu, Christos Koukouvinos and Jennifer Seberry.

Classification of difference matrices over cyclic groups

Pekka Lampio

In this computer-aided work we investigate the existence of difference matrices over cyclic groups. Up to the computational limit, we determine the maximum values of the parameters for which difference matrices exist as well as the number of inequivalent difference matrices in each case. Several new difference matrices have been found in this manner. This is joint work with Patric Östergård."

Near-extremal matrices

David Asher Levin

We prove the existence of (-1,1)-matrices with near-extremal properties. In particular, we find matrices either having small inner products between all pairs of distinct rows, or having determinants approaching Hadamard's bound. In applications which call for Hadamard matrices, these matrices may be nearly as useful. Our approach is to study the random submatrices of Hadamard matrices, which may be of independent interest. Time permitting, I will also describe some work in progress on upper bounds on the number of Hadamard matrices.

This reports on joint work with Warwick de Launey.

The problem of mutually unbiased bases in dimension 6

Máté Matolcsi

Two orthonormal bases X, Y in $\mathbf{C}^d$ are called unbiased if $|\langle x_j, y_k\rangle| = 1/\sqrt{d}$ for all j, k. A collection of orthonormal bases $X_1, \ldots, X_r$ is mutually unbiased if any pair of them are unbiased. It is known that the maximal number of mutually unbiased bases in $\mathbf{C}^d$ is at most $d + 1$, and such maximal collection does exist if d is a prime power. However, the problem is still open for any composite dimensions, even for $d = 6$. The situation is similar in spirit to that of orthogonal Latin squares, and the two problems indeed have some mathematical connections. Mutually unbiased bases are naturally connected to complex Hadamard matrices, and in this talk we offer an approach that might lead to the solution via an exhaustive computer search.

Classification of cocyclic Hadamard matrices of order less than 40

Pádraig O'Catháin

The concept of cocyclic Hadamard matrix was introduced by Horadam and de Launey in seminal work in the early 1990s. This class of Hadamard matrices is a natural generalization of group-developed Hadamard matrices, without the restriction that the order of the matrix is square. In this talk we outline our recent classification of all cocyclic Hadamard matrices of order less than 40. Our techniques exploit

• the equivalence (discovered by Warwick de Launey) between cocyclic Hadamard matrices of order 4t, and relative difference sets with parameters (4t, 2, 4t, 2t)
• recent advances (due to Marc Röder) in the computer-aided construction and classification of relative difference sets.

We expand upon this equivalence, to show that a given relative difference set corresponds to at least one and at most two inequivalent Hadamard matrices. This result, combined with an exhaustive search for (4t, 2, 4t, 2t)-relative difference sets suffices to classify all cocyclic Hadamard matrices of order 4t.

We carried out this programme for $t \leq 9$. Our results were obtained using Röder's GAP package RDS. Complete and irredundant lists of the cocyclic Hadamard matrices of orders 32 and 36 are available at http://www.maths.nuigalway.ie/_padraig/research We have discovered many new classes of cocyclic Hadamard matrices, and also new classes of Hadamard matrices that are not cocyclic.

William Orrick

TBA

Two new honeycomb arrays

Anastasia Panoui

A honeycomb array of radius r is a set of n=2r+1 dots placed on the hexagonal grid in such a way that the distance of every dot from the centre is at most r. We also require that in each column and in each diagonal only one dot occurs and that the vector differences between all pairs of dots are distinct. Honeycomb arrays were first defined by S.W.Golomb and H.Taylor in 1984 and they are the natural hexagonal analogue of Costas arrays. In this talk we will give a brief description of how honeycomb arrays can be constructed using Costas arrays and we will present two new arrays of radius r=7.

MUBs and MOLS - similar in more than spirit

Asha Rao

Mutually Unbiased Bases (MUBs) are important in quantum information theory.
While constructions of complete sets of d+1 MUBs in $\mathbf{C}^d$ are known when d is a prime power, it is unknown if such complete sets exist in non-prime power dimensions.
It has been conjectured that sets of complete MUBs only exist in $\mathbf{C}^d$ if a maximal set of Mutually Orthogonal Latin Squares (MOLS) of side length d also exists.
Using known constructions of MUBs we construct maximal sets of MOLS in the prime case. This is a new construction is based on the inner product between pairs of vectors.

Sylvester Hadamard matrices

Jennifer Seberry

Since this is the first construction everyone meets and it is so elegant, we think we know it all. We will talk about "sign changes", the equivalence class, the strange submatrix properties, higher dimensional properties, Walsh functions and discrete Fourier transforms, counting for SNF. This family of Hadamard matrices undoubtedly has far more to offer than these aspects, and yet they are just orthogonal with +1 and -1 element.

The Paley matrices and their automorphism groups

Richard M. Stafford

The Paley matrices consist of the conference matrices of order q+1, where q is an odd prime, and two classes of Hadamard matrices: The type I Hadamard matrices of order q + 1 where q is a prime congruent to 3 modulo 4, and the type II Hadamard matrices of order 2(q + 1) where q is a prime congruent to 1 modulo 4. These matrices comprise the densest known classes of conference and Hadamard matrices. Moreover, they have a very rich algebraic structure. In particular, they are cocyclic.

It happens that the Paley matrices provide a very nice concrete setting for seeing how all the various aspects of the theory of cocyclic weighing matrices fit together. The series of papers [1], [2], and [3], building on the articles by Ito and Kantor, work out all the details. This talk takes the reader on a guided tour of this material.

References

[1] W. de Launey and R. M. Stafford, On cocyclic weighing matrices and the regular group actions of certain Paley matrices, Discrete Appl. Math. 102 (2000), no. 1-2, 63–101, Coding, cryptography and computer security (Lethbridge, AB, 1998).
[2] W. de Launey and R. M. Stafford, On the automorphisms of Paley's type II Hadamard matrix, Discrete Math. 308 (2008), 2910–2924.
[3] W. de Launey and R. M. Stafford, The regular subgroups of the Paley type II Hadamard matrix, preprint.
[4] N. Ito, Note on Hadamard matrices of type Q, Studia Sci. Math. Hungar. 16 (1981), no. 3-4, 389–393.
[5] N. Ito, Note on Hadamard groups of quadratic residue type, Hokkaido Math. J. 22 (1993), no. 3, 373–378.
[6] N. Ito, On Hadamard groups, J. Algebra 168 (1994), no. 3, 981–987.
[7] N. Ito, On Hadamard groups. II, J. Algebra 169 (1994), no. 3, 936–942.
[8] W. M. Kantor, Automorphism groups of Hadamard matrices, J. Combinatorial Theory 6 (1969), 279–281.

Exotic complex Hadamard matrices and their equivalence

Ferenc Szöllösi

We present some new constructions of complex Hadamard matrices of order n, the entries of which are in the quadratic fields $\mathbb{Q}(i\sqrt{n})$ and $\mathbb{Q}(i\sqrt{(n-4)})$ respectively. This approach unifies and extends some earlier results of Björck, de la Harpe-Jones and Munemasa-Watatani, who constructed circulant complex Hadamard matrices of prime orders. Our method gives a theoretical explanation for the existence of some sporadic examples of complex Hadamard matrices in the recent literature, which were found by means of computer. In order to justify that our matrices are essentially new, we introduce a new invariant, the *fingerprint* of Hadamard matrices.