Algebraic design theory with Hadamard matrices: applications, current trends and future directions [14w2199]

Robert Craigen (University of Manitoba), Dane Flannery (National University of Ireland, Galway), Hadi Kharaghani (University of Lethbridge)

12–13 July 2014

The meeting began 8.30am on 12 July 2014 and concluded at noon on 13 July. Invited and contributed lectures (of 50 and 20 minutes respectively) were delivered by leading experts, and a lengthy problem session ran on the second day. There were 32 participants from more than 25 institutions in Australia, Canada, Croatia, Hungary, Iran, Ireland, Japan, Poland, Singapore, Spain, Turkey, and the USA. Early stage researchers, especially graduate students, were well represented.

1 Overview of the Field

As formulated in [3, 4], algebraic design theory emphasizes the use of algebraic techniques and viewpoints to solve problems in combinatorial design theory. The focus is on 'pairwise combinatorial designs', such as Hadamard matrices and their generalizations; these are rich in applications to areas such as coding and communications theory, quantum physics and computing, to name just a few.

Several long-standing problems concern the existence question: whether for every allowable order there are any designs of the specified type. Perhaps the most famous of these is the existence conjecture for Hadamard matrices; and a special case for Hadamard matrices that are circulant type. B.Schmidt, a participant at the meeting, has made remarkable progress towards resolution of the circulant conjecture, and it seems likely that he will eventually settle it (in the negative) [5, 6].

Another important kind of problem is enumeration or classification. Typically these are most prominent in cases when existence is trivial or easily proved. Even here, however, sophisticated algebraic tools are required to produce manageable classifications. The use of modern computer algebra systems such as MAGMA [1] is vital in generating lists.

2 Recent Developments and Open Problems

Two of the foremost researchers on existence problems for Hadamard matrices, W. Orrick and B. Schmidt, delivered presentations and shared their expertise in numerous conversations with other participants. Classification problems for complex Hadamard matrices and generalized Hadamard

matrices over groups are powered by applications in quantum physics and computing; this area was represented by K. Życzkowski. Other very recent applications featured prominently: to coding theory (V. Tonchev) and compressed sensing (P. O Catháin).

3 Presentation Highlights

C. Colbourn outlined a general framework for permutation covering problems, and an algorithm for constructing them.

R. Craigen talked about constructions for circulant and group-developed generalized weighing matrices. This is work with Warwick de Launey, who is a founder of algebraic design theory and a continuing major influence on the subject.

W. Orrick spoke on Hadamard's maximal determinant problem—another major unsolved problem in the field. The question is: what is the largest determinant of a $\{\pm 1\}$-matrix of (arbitrary) order n? Much progress towards its solution has been made by Orrick and his co-authors. He surveyed various constructions and proofs of maximality.

Lander's conjecture states that if G is an abelian group of order v containing a difference set of order n, and p is a prime dividing v and n, then the Sylow p-subgroup of G must be non-cyclic. B. Schmidt discussed attempts to construct counterexamples to Lander's conjecture.

V. Tonchev spoke on special classes of Hadamard matrices, such as Bush-type matrices, and generalized Hadamard matrices over groups. He also described results on related combinatorial designs and codes.

Talks by early stage researchers included those by Darcy Best on parity of transversals in Latin squares, and by Ferenc Szöllősi, on the recent closure of the final existence questions for weighing matrices of weight 9.

4 Scientific Progress Made

The meeting culminated in a lively and highly productive problem session. Single-page writeups of new interesting problems arising out of the work presented at both this meeting and the preceding one in Lethbridge (ADTHM 2014) were compiled and discussed during this session. In no particular order, the following problems were raised.

- R. Craigen proposed a problem of studying $\bmod m$ Hadamard matrices of order 256 for $m \leq 256$ to produce helpful new insights about modular questions and potential progress toward the current smallest outstanding case of existence of Hadamard matrices. Known special cases and general approaches were discussed.

- P. Leopardi asked about graphs whose edge-sets can be partitioned into two or three strongly regular subgraphs, isomorphic via an isomorphism of the underlying graph. These correspond to an important class of combinatorial designs related to Hadamard matrices.

- D. Goyeneche and K. Życzkowski suggested that an Orthogonal Array OA(r, N, d, k) be called *irredundant* if, when any k columns are removed, all remaining r rows are distinct. They ask for a list and characterization of irredundant OAs at low orders, and for a characterization of "local equivalence" of orthogonal arrays corresponding to local equivalence of orthogonal states (a deep question arising from quantum information theory).

- M. Matolcsi and K. Życkowski define "Almost Hadamard matrices" (AHM), slightly perturbed from $\{\pm 1\}$-matrices (distance defined using matrix norms) and exhibiting orthogonality, i.e., $AA^\top = nI$. They pose four problems (much discussion ensued).
  - Find an infinite family of these in which the distance goes to 0 as $n \to \infty$.
  - Improve known numerical algorithms for AHM, particularly for large values of n.
  - Experiment with known and new techniques in order $n = 667$ and other small, likely difficult, orders.
  - When such a matrix can be 2-valued, explore replacement by 1 and -1 (heuristics suggest that previously unknown Hadamard matrices may arise in this way).
- A. Rao spoke on "Alltop functions", which provide powerful ways to construct difference sets, Hadamard matrices, and mutually unbiased bases (MUBs). She posed four problems: find new families (these are currently rare); identify whether certain classical families are equivalent; determine whether inequivalent Alltop functions generate inequivalent MUBs; and analyse the new Alltop functions discussed in her talk, relative to correlation measure.
- P. Ó Catháin gave a surprising lemma about the number of nonzero entries in linear combinations of rows of a complex Hadamard matrix. He asked for a description of (complex) Hadamard matrices with the property that no linear combination of t rows contains more than t zeros; or, failing that, contain no more than $f(t)$ rows where f is a slow-growth function.
- I. Wanless contributed a question informally raised at both meetings: what is the smallest number of nonzero entries in which two Butson-Hadamard matrices of order n can differ? A simple combinatorial argument shows that in the real case this is n; it is conjectured to be the same in the complex case. The Butson-Hadamard case appears to have no specific merit over the general "complex-Hadamard" case, suggesting that the question be asked generally.

  Wanless also posed a puzzle about the largest power of 2 dividing the permanent of a Hadamard matrix of order n, conjecturing that this is also the highest power of 2 dividing $n!$.
- R. Egan asked whether there is a central relative difference set with certain parameters in the dicyclic group of order $8t$. Such a set would imply the Hadamard matrix conjecture. This is a natural place to seek the elusive single, general class of Hadamard matrices in all orders $4t$, which lends itself to study via the nascent algebraic design theory and cocyclic development of designs. Egan provides a lemma suggesting an attack using two $\{\pm 1\}$-sequences with certain properties, and he asks when such pairs can be found beyond those already known, whether recursive constructions can be developed, and whether a probabilistic approach to construction will bear fruit.
- W. Martin asked for new examples of "linking systems" for difference sets in finite abelian groups. A construction discovered by Cameron and Seidel in 1973 suggested that there many be others. In 2014 Davis, Martin and Polhill succeeded in finding linking systems using Galois rings, but the call is for more constructions. Their result suggests the possibility of involving algebraic tools heretofore not brought to bear on the problem.

  Martin also asked for a proof that the existence of more than k mutually unbiased (real) Hadamard matrices of order n implies that $4^k | n$—even just for $k = 3$. Known partial results were given.

Some of these problems—notably those of Craigen, Matolcsi, Życkowski and Wanless—are well-suited for exploration by undergraduate and graduate students; indeed some were posed with that in mind, but simultaneously promise substantial progress on key gaps in our understanding.

5 Outcomes of the Meeting

Collaborations were initiated (e.g., between Flannery, Egan, and O Catháin on classifying cocyclic Butson matrices, prompted by K. Życzkowski's remarks about the dearth of libraries of complex Hadamard matrices; cf. [2]). Several preprints are in preparation.

Shortly after the meeting, R. Craigen visited D. Flannery and R. Egan at NUI Galway, Ireland for several months, to pursue foundational questions in algebraic design theory, and the specific problem posed by Egan at the BIRS meeting.

Planning of future conferences in algebraic design theory were initiated. M. Matolcsi undertook to organize the next meeting focused on Hadamard matrices and their generalizations at the Alfréd Rényi Institute of Mathematics, Hungary, in 3 years time.

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] W. Bruzda, W. Tadej and K. Życzkowski, `http://chaos.if.uj.edu.pl/karol/hadamard/`

[3] W. de Launey and D. L. Flannery, *Algebraic design theory*, Mathematical Surveys and Monographs vol. 175, American Mathematical Society, Providence, RI, 2011.

[4] K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007.

[5] K.H. Leung and B. Schmidt, New restrictions on possible orders of circulant Hadamard matrices, *Designs, Codes and Cryptography* (2012), **64**, no. 1-2, 143–151.

[6] B. Schmidt, `http://www.ntu.edu.sg/home/bernhard/CW/CW.html`