MACHINE LEARNING-BASED ROAD CONDITION ASSESSMENT USING REMOTE SENSING DATA

Deeksha Arya

Centre for Transportation Systems
Indian Institute of Technology Roorkee - IIT Roorkee
Uttarakhand 247667, INDIA

Abstract

Road infrastructure is one of the major components having direct impact on growth and development of any country. These infrastructures require regular upkeep, maintenance and identification of failure zones to ensure their proper working. However, maintaining a colossal road network of millions of kilometres is a matter of concern. Apropos, huge financial investments are pumped in every year for maintenance and repairs of roads throughout the world. For minimizing these costs, early detection of pavement defects is imperative which demands timely assessment of roads for existing and upcoming faults.

The traditional methods for road condition assessment involve manual inspection of road surfaces. These methods fail to meet the requirements at country-level owing to the large area of road networks to be inspected, the level of details expected and the limited availability of time. Hence there rises a need to analyse whether the current technologies like Machine Learning and Remote Sensing can provide requisite solutions. This talk addresses the same.

**This work is being carried out under the supervision of Professor S.K. Ghosh (Civil Engineering, IIT Roorkee) and Professor Durga Toshniwal (Computer Science and Engineering, IIT Roorkee).*

MONOMIAL GROUPS AND THEIR GROUP ALGEBRAS

Gurmeet K. Bakshi

Panjab University
Chandigarh 160014, India

Abstract

A finite group G is called a monomial group if each complex irreducible character of G is induced from a linear character of a subgroup of G. It is well known that all monomial groups are solvable and every solvable group embedds in a monomial group. Group algebras occur naturally in the study of groups and play a major role in understanding them. In this talk, we are concerned with the structure of the semi simple group algebra of a monomial group. We will show that for a large class of monomial groups, it is possible to describe the complete algebraic structure of their semi simple group algebras. By the complete algebraic structure of a semi simple group algebra, we mean its primitive central idempotents and the Wedderburn decomposition. This is a fundamental problem which is of interest in view of its applications in both pure and applied algebra.

A RANK-1 CONSTRAINED SEMIDEFINITE PROGRAMMING FORMULATION FOR FINDING D-OPTIMAL DESIGNS

Dursun Bulutoglu

Department of Mathematics and Statistics
Air Force Institute of Technology
Wright Patterson AFB, USA

Abstract

Finding a two-symbol, N row, N column and D-optimal design for estimating all main effects is a fundamental problem in statistics. Such a design $\boldsymbol{X}$ must achieve the maximum possible value of $\det(\boldsymbol{X}^T\boldsymbol{X})$, where $\boldsymbol{X}$ is an $N \times N$ matrix of ± 1s. There are upper bounds for the maximum possible value of $\det(\boldsymbol{X}^T\boldsymbol{X})$ depending on $N \pmod 4$. These bounds are not achievable for each N, and improving them requires enumeration. In cases when these bounds are achievable, for many values of N, the size of the search space for $\boldsymbol{X}$ can be decreased drastically by using circulant matrices without removing all optimum solutions. This reduction stems from decreasing the number of variables by a factor of N. In fact, there are several infinite families of optimum solutions within the decreased search space that come from finite fields and Gauss sums in number theory. The set of all optimum solutions $\boldsymbol{X}$ within the decreased search space also constitutes the feasible set of a family of rank-1 constrained semidefinite programming problems. In particular, a Legendre pair of length ℓ exists if and only if a rank-1 constrained semidefinite programming problem is feasible. I will be discussing these rank-1 constrained semidefinite programming problems as well as the augmented Lagrangian method for solving them.

ON VECTORIAL FUNCTIONS IN CHARACTERISTIC TWO

Claude Carlet

University of Bergen
LAGA, University of Paris 8

Abstract

The differential uniformity of a vectorial function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ equals

$$\delta_F = \max_{\substack{a \in \mathbb{F}_2^n, a \neq 0 \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n; F(x) + F(x+a) = b\}.$$

This notion plays a central role in symmetric cryptography. Much work has been done on the case $m = n$, which corresponds to a use of F as a substitution box in a model of block ciphers called Substitution-Permutation-Networks; the best (i.e. smallest) possible value of δ_F equals then 2.
Some work has been done also on the case n even and $m \leq \frac{n}{2}$, where the best possible value is $2^{\frac{n}{2}}$ and is achievd by bent (perfect nonlinear) functions, related to difference sets of $\mathbb{F}_2^n$.
Little theoretical work has been done on (n, m)-functions when $\frac{n}{2} < m < n$, although these functions can be used in the other important model of block ciphers called Feistel. Kaisa Nyberg has shown that the differential uniformity of such functions is bounded below by $2^{n-m} + 2$.

We shall construct $(2m - 1, m)$-functions with $m \geq 3$ achieving Nyberg's bound with equality, differentially 4-uniform $(m + 1, m)$-functions, and $(2m - 2, m)$-functions with $\delta_F \leq 2^{m-1} - 2^{m-6} + 2$ for any $m \geq 8$.

We shall state some open questions.

MORPHISMS OF COMPLEX HADAMARD MATRICES

Padraig Ó Catháin

Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, MA 01609 USA

Abstract

Let M be a matrix with complex entries of unit norm. A well-known theorem of Hadamard bounds the magnitude of the determinant of M as a function of its dimension, and M is a complex Hadamard matrix if M meets Hadamard's bound with equality.

In this talk we will survey some known results on existence of special types of complex Hadamard matrices, in particular matrices with entries in the k^{th} roots of unity. I will report on recent joint work with Ronan Egan and Eric Swartz on the existence of tensor-product-like maps which reduce the number of entries in a complex Hadamard matrix at the cost of increasing the dimension. This work generalises previous constructions of Turyn and Compton-Craigen-de Launey of real Hadamard matrices from certain complex Hadamard matrices with entries in the fourth and sixth roots of unity respectively.

THE GROUP OF TERNARY COMPLEMENTARY PAIRS RELATIVE TAKEN MODULUS 2 AND MODULUS 3

Robert Craigen

Department of Mathematics
University of Manitoba
Winnipeg, MB Canada

Abstract

While circulant Hadamard matrices do not exist in general (and may not exist at all in orders > 4) and circulant weighing matrices are rare, it is quite common to find these important orthogonal matrices constructed using the standard construction involving two circulants,

$$\begin{pmatrix} A & B \\ -B^\top & A \end{pmatrix}.$$

So common, in fact, that it is expected that, with relatively few exceptions, when Hadamard and weighing matrices of even order exist, a matrix having the same parameters exists in this form. This observation suggests the potential for some relatively uniform master construction that will solve the Hadamard matrix conjecture and many of the outstanding questions about the existence of weighing matrices.

Many classes of suitable pairs A, B are known but the search for a uniform class subsuming all cases and addressing the big questions remains elusive, because outside of some special orders it is hard to discern a sufficiently strong algebraic pattern.

One way to describe such matrices A, B is by the total periodic autocorrelation of the sequences formed by their first rows. At the level of autocorrelation it is hard to discern sufficient structural patterns to address these problems. One approach is to further restrict the class by considering nonperiodic autocorrelation, two sequences satisfying the resulting condition are called a ternary complementary pair, TCPs) TCPs lend themselves extremely well to recursive constructions, making them useful beyond this theoretical context. But those which give Hadamard matrices Golay pairs are evidently very rare and probably already completely known. TCPs themselves arise from certain primitive cases by a recursive construction, but unfortunately no systematic pattern is known for the existence of these primitive cases, forcing those seeking them to resort to computer searches, an approach with no hope of solving the general case.

We discuss a method by which slightly weaker classes of objects obtained by reducing modulo 2 or 3 are systematically characterized as the elements of a relatively tractable group, which offers a possible complete characterization of a slightly more general class containing TCPs. At minimum this characterization offers a drastic reduction on the size of search space for TCPs; it may open a path to a successful attack on the general problem of existence.

LANDER'S TABLES REVISITED: WHAT CAN WE LEARN?

James A. Davis

University of Richmond
Richmond VA 23173, USA

Abstract

Lander's book "Symmetric Designs, an algebraic approach", published in 1983, motivated work in difference sets for many years. Included in the book was a table of possible parameters, possible (abelian) groups, and the status of the existence question for a difference set. K.T. Arasu was a major player in this research area, providing nonexistence proofs for many of the open cases as well as constructions of difference sets. We revisit a few of the results from this era, and we point to recent results that indicate that there is much more to be done in the general area of difference sets. In particular, we focus on progress in groups of order a power of 2 and also on McFarland difference sets in nonabelian groups. We will describe a recent result that constructs difference sets in more than 99% of the possible groups of order 256, and we will also discuss a partitioning of several groups of order 96 into four McFarland difference sets and a subgroup of order 16.

ALL KINDS OF COMPLEMENTARY SEQUENCES

Ronan Egan

School of Mathematics, Statistics and Applied Mathematics
National University of Ireland, Galway
Ireland

Abstract

Pairs of complementary sequences such as Golay pairs have zero sum autocorrelation at all non-trivial phases. Several generalizations are known where conditions on either the autocorrelation function, or the entries of the sequences are altered. In this talk I will attempt to unify many of these ideas. I will introduce autocorrelation functions that apply to any sequences with entries in a set equipped with a ring-like structure which is closed under multiplication and contains multiplicative inverses. Depending on the elements of the chosen set, the resulting complementary pairs may be used to construct a variety of combinatorial structures such as Hadamard matrices, complex generalized weighing matrices, and signed group weighing matrices.

BINARY SEQUENCES WITH MODULAR CONSTRAINTS

Shalom Eliahou

Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral Côte d'Opale
62228 Calais, France

Abstract

Many binary sequences of particular interest – and subject of many open problems – are defined via the satisfaction of polynomial constraints with integer coefficients, such as Barker sequences, Golay pairs and Hadamard matrices, to name a few. Weakening these constraints by requiring them to hold modulo some given integer m gives rise to new interesting binary sequences, about which open problems still abound. For instance, Hadamard matrices modulo 32 have been constructed for any order n divisible by 4, but analogous constructions modulo 64 are still lacking. Similarly, exotic binary Golay pairs modulo 16 have been constructed, but what about higher moduli? In this talk, we shall review some constructions in this vein and shall highlight some related open problems.

ON QUASI-ORTHOGONAL COCYCLES

Dane Flannery

National University of Ireland
Galway, Ireland

Abstract

Orthogonal cocycles arise in the study of symmetry of pairwise combinatorial designs. In the simplest and best known case, these are cocycles $\psi \in Z^2(G, \langle -1 \rangle)$ for a group G (of order divisible by 4) whose display table $[\psi(g,h)]_{g,h \in G}$ is a Hadamard matrix. A natural analogue is *quasi-orthogonal cocycle*, defined over G of order congruent to 2 modulo 4. There is a connection to the maximal determinant problem (for example, if a cocyclic binary matrix of order $4t+2$ attains the maximal determinant bound then the cocycle is quasi-orthogonal). Quasi-orthogonal cocycles seem to be far more prevalent than the orthogonal kind.

We survey some recent results on quasi-orthogonal cocycles. These encompass new and known combinatorial objects: quasi-Hadamard groups, relative quasi-difference sets, and partially balanced incomplete block designs. In another direction, we note that generalized perfect binary arrays are known to be cocyclic; generalized optimal binary arrays are the relevant quasi-cocyclic analogue, and these lead to a new construction of negaperiodic Golay pairs. The next step is to widen the coefficient group from $\langle -1 \rangle$, obtaining (for example) quaternary sequences of odd length with optimal autocorrelation.

We also mention a few prominent open problems. Apart from the obvious (existence), one of these concerns transposability of quasi-cocyclic matrices.

This is joint work with José Andrés Armario, University of Seville.

NEW COMBINATORIAL STRUCTURES IN PROJECTIVE PLANES OF ORDER 16

Mustafa Gezek*[1] and Vladimir D. Tonchev[2]

[1]Department of Mathematics, Tekirdag Namik Kemal University
Tekirdag, Turkey 59030
[2]Department of Mathematical Sciences, Michigan Technological University
Houghton, MI USA 49931

Abstract

In this talk, the results of a number of computer searches related to maximal arcs of degree 4 in projective planes of order 16 will be discussed. Details of 2-(52,4,1) designs, partial geometries pg(12,12,9) and linear codes associated to known maximal (52,4)-arcs will be given. New connections between projective planes of order 16, and pairs of new 104-sets of type (4,8) will be shown to exist.

COHOMOLGY DESIGNS AS BUILDING BLOCKS IN CONSTRUCTIONS OF WEIGHING AND HADAMARD MATRICES

Assaf Goldberger

-

Abstract

Let G be a finite group, let X and Y be two G-sets, and R be a commutative ring equipped with a G-action. An (X,Y)-matrix is a matrix M over the ring R of size $|X| \times |Y|$, indexed by X and Y. The group G acts on the set of all (X,Y)-matrices, by an action which we denote by $(g,M) \mapsto gM$. A Cohomology Design is an (X,Y)-matrix M, such that for every $g \in G$, $gM = D_1 M D_2$ for invertible diagonal matrices $D_i = D_i(g),\ i = 1,2$.
All Cohomology Designs are generated by some cohomology classes in the group cohomology of G, of dimension≤ 2. Some well known families of Weighing matrices, such as Payley and Projective Space Matrices are Cohomology Designs. In fact, the orthogonality of these matrices follows from a clean theoretical argument, without the need for computation. In addition, we are able to construct some new families of Weighing Matrices, such as the family of Grassmannian Matrices, and also new families of Hadamard Matrices, which are built from blocks that are rectangular Cohomology Designs.
The theory of Cohomology Designs generalizes the theory of Cocyclic matrices. But more than this, it sheds light other fields in algebra, such as the theory of Brauer Groups, Hecke Algebras and Representation Theory. It can also generalize to higher tensors, giving interpretation to higher cohomology groups.

THE LA JOLLA DIFFERENCE SET REPOSITORY

Daniel M. Gordon

IDA Center for Communications Research
4320 Westerra Court, San Diego, CA 92121 USA

Abstract

The *La Jolla Difference Set Repository* is an online database created in 2006 to document existence results on cyclic difference sets from [1], and in 2015 extended to abelian difference sets with $v < 10^6$ for computations with multiplier theorems in [2].

In this talk we use this database to investigate the state of our knowledge about difference sets. We look at evidence for several of the numerous open conjectures involving difference sets, and formulate some new ones.

References

1 L. D. Baumert and D. M. Gordon, On the existence of cyclic difference sets with small parameters. In: *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams.* Fields Inst. Commun., vol. 41, pp. 61—68, 2004.

2 D. M. Gordon and B. Schmidt, A survey of the multiplier conjecture, *Des. Codes Cryptogr.* (2016) 78: 221–236.

50 YEARS OF CROSS CORRELATION OF M-SEQUENCES

Tor Helleseth

University of Bergen

Abstract

Maximum-length sequences (or m-sequences) having period $2^m - 1$ are generated by a linear feedback shift register of degree m. These sequences have many important applications in modern communication systems. The most well known property of m-sequences is their well-known two-level ideal autocorrelation. The first major result on the cross correlation is the determination of the cross correlation between the m-sequences used in constructing the famous Gold sequences that was published 50 years ago in January 1968. During the last 50 years the cross correlation between m-sequences of the same period has been intensively studied by many research groups. Many important results have been obtained but still many open problems remain in this area. This talk will give an updated survey of the status of the cross correlation of m-sequences as well as some consequences of these results.

THE DOMINATION NUMBER OF THE GRAPH DEFINED BY TWO LEVELS OF THE N-CUBE

Gyula O.H. Katona

MTA Rényi Institute
Budapest, Hungary

Abstract

Consider all k-element subsets and ℓ-element subsets ($k > \ell$) of an n-element set as vertices of a bipartite graph. Two vertices are adjacent if the corresponding ℓ-element set is a subset of the corresponding k-element set. Let $G_{k,\ell}$ denote this graph The domination number of $G_{k,1}$ is exactly determined. We also prove that $\gamma(G_{k,2})$ is asymptotically equal to

$$\frac{k+3}{2(k-1)(k+1)}n^2$$

for $k \geq 3$. The upper estimate is proved by a random construction.We also suggest a way to find a deterministic construction, but it is completed only for $k = 3$ and 4.

Joint work with Leila Badakhshian and Zsolt Tuza.

BALANCEDLY SPLITTABLE HADAMARD MATRICES AND APPLICATIONS

Hadi Kharaghani

University of Lethbridge
Lethbridge, Alberta, Canada

Abstract

A Hadamard matrix of order n is said to be balancedly splittable if by a suitable permutation of the rows it can be splitted in two parts such as

$$\begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$$

where H_1 is an $\ell \times n$ matrix, $\ell < n$, and $H_1^T H_1$ has at most two distinct off diagonal entries. Feasible parameters and construction methods will be presented. The connection to Hadamard diagonalizable strongly regular graphs, maximal equiangular lines set, and unbiased Hadamard matrices will be discussed. As an application, commutative association schemes of 4, 5, and 6 classes are constructed. This is a joint work with Sho Suda.

MY FIVE FAVOURITE PRIMES: LEGENDRE STRIKES AGAIN

Ilias Kotsireas

CARGO Lab
Wilfrid Laurier University
Waterloo, ON, Canada

Abstract

I will explain what my five favourite primes have to do with Legendre and with Hadamard matrices.

ERASURE CODING FOR DISTRIBUTED STORAGE: AN OVERVIEW

P. Vijay Kumar

Indian Institute of Science
Bengaluru, INDIA

Abstract

This talk will present an accessible overview, from the speaker's perspective, of progress made over the past decade, on the topic of erasure coding for distributed storage. In the distributed storage of large amounts of data such as takes place in a data center, data pertaining to a given file is first broken into k fragments. A total of $(n-k)$ redundant fragments are then added, to make a total of n fragments and each fragment is stored on a different storage unit. An important criterion for code selection is the efficiency with which a given code is able to handle the repair of a single failed node. This efficiency is measured in terms of factors such as the total amount of data downloaded from the remaining nodes for node repair, the number of helper nodes contacted for node repair and the amount of data read from each helper node. Different classes of codes have sprung up to meet this demand, such as regenerating codes and locally recoverable codes. This talk will draw primarily from the recent survey appearing in [1].

References

1 Balaji S B, M. Nikhil Krishnan, Myna Vajha, Vinayak Ramkumar, Birenjith Sasidharan, P. Vijay Kumar, "Erasure coding for distributed storage: an overview," *Science China Information Sciences*, vol. 61, October 2018, 45 pages.

LOVÁSZ HAMILTONICITY PROBLEM

Klavdija Kutnar

University of Primorska
Slovenia

Abstract

In 1969 László Lovász asked for a construction of a finite connected vertex-transitive graph without a simple path visiting all vertices of the graph i.e. a Hamilton path. A commonly accepted phrasing of his question, based on lack of supporting examples, reads as follows: Does every finite connected vertex-transitive graph have a Hamilton path?

Not only that no connected vertex-transitive graph without a Hamilton path is known to exist, we know of just five connected vertex-transitive graphs without a Hamilton cycle i.e. a simple cycle containing all vertices of the graph.

In this talk I will present a recent result proving that every connected vertex-transitive graph of order a product of two primes, other than the Petersen graph, contains a Hamilton cycle.

This is a joint work with Shaofei Du and Dragan Marušič.

NONEXISTENCE RESULTS ON GENERALIZED BENT FUNCTIONS

Ka Hin Leung

Department of Mathematics
National University of Singapore
Singapore

Abstract

Let q and m be positive integers and let ζ_q be a primitive complex qth root of unity. A function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called a **generalized bent function (GBF)** if

$$\left| \sum_{x \in \mathbb{Z}_q^m} \mathbb{Z}eta_q^{f(x)-v\cdot x} \right|^2 = q^m \text{ for all } v \in \mathbb{Z}_q^m. \tag{1}$$

Here $x \cdot v$ denotes the usual dot product.

Bent functions are a highly active research field due to their numerous applications in information theory, cryptography and coding theory. In fact, the defining condition ensures that bent functions are "maximally nonlinear", which is desirable property for cryptographic purposes.

In this talk, we will give a survey on recent work [1,2] on the case when $q = 2p^a$ where p is prime. Furthermore, we report some new results on another generalization in [3].

Let $m \geq 2$ and n be positive integers. and $\mathbb{Z}eta_m$ be a primitive complex qth root of unity. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_m$ is called a (m, n)-**generalized bent function (GBF)** if

$$\left| \sum_{x \in \mathbb{Z}_2^n} \zeta_m^{f(x)} (-1)^{y\cdot x} \right|^2 = 2^n \text{ for all } y \in \mathbb{Z}_2^n. \tag{2}$$

Here $x \cdot y$ denotes the usual dot product.

If both m and n are even, or $4|m$; then such f exists. In this talk, we will discuss the case when $n = 3$. It can be shown that no such (GBF) exists if $n = 3$ and $m \equiv 2 \bmod 4$.

References

1 Y. Jiang, Y. Deng: New results on nonexistence of generalized bent functions, *Des. Codes Cryptogr.* **75** (2015), 375–385.

2 K.H. Leung, B. Schmidt: Nonexistence Results on Generalized Bent Functions $\mathbb{Z}_q^m \to \mathbb{Z}_q$ with Odd m and $q \equiv 2 \pmod 4$, *Journal of Combinatorial Theory, Series A* **163** (2019) 1–33

3 H Liu K Feng R Feng: *Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$*, *Des. Codes Crytogr.* **82** (2017), 647-662.

CONSTRUCTION OF LINKING SYSTEM OF DIFFERENCE SETS IN 2-GROUPS

Shuxing Li

Otto von Guericke University Magdeburg
Germany

Abstract

Linking systems of difference sets are a collection of difference sets which satisfy the pairwise linking property. For instance, linking systems in elementary abelian 2-groups are a collection of bent functions, so that sum of any pair of bent functions is also bent. So far, there are few known constructions of linking systems. In this talk, we propose a new construction of linking systems in 2-groups, which consist of difference sets derived from McFarland's approach. The pairwise linking property of such difference sets boil down to a proper arrangement of group elements, which is guaranteed by the use of group difference matrices.

This is joint work with Jonathan Jedwab and Samuel Simon.

References

1 J. Jedwab, S. Li, and S. Simon. Linking systems of difference sets, *Journal of Combinatorial Designs*, 27(3): 161–187, 2019.

CONSTRUCTIONS OF VARIANCE BALANCED DESIGNS USING COMBINATORIAL TECHNIQUES

Nutan Mishra, Dinesh G. Sarvate

University of South Alabama, College of Charleston

Abstract

While variance balance (VB) is a statistical property of the block designs, if the block designs are proper, i.e. all blocks are of same size, then the concept of variance balance can be translated into a combinatorial property of the design namely pairwise balance. That is proper variance balanced designs are pairwise designs. We exploit this fact in constructing the VB designs and apply several combinatorial techniques in the constructions. Since replication number is allowed to vary, the designs are non binary. The combinatorial entities those we use in construction are difference set families with half blocks and quarter blocks, mandatory representations designs, balanced incomplete block designs and maximum packings.

Keywords: Block designs, pairwise balance, maximum packings, difference set families, half block.

OPTIMIZATION PROBLEMS WITH ORTHOGONAL MATRIX CONSTRAINTS

Manil T. Mohan

Department of Mathematics
Indian Institute of Technology Roorkee - IIT Roorkee
Haridwar Highway, Roorkee, Uttarakhand 247667, INDIA

Abstract

In this talk, we consider some interesting optimization problems involving orthogonal matrix constraints like Shannon and Renyi entropies of orthogonal matrices, minimum distance orthostochastic matrices to the uniform van der Waerden matrices, p-almost Hadamard matrices etc. We prove that in the cases when a Hadamard matrix of order n exists, such optimization problems achieve their global optima. For other orders in which a Hadamard matrix does not exist, we obtain some local optimum of these problems using multi variable analysis techniques. We establish that the matrices like $K_n := (1/n)J_n - I_n$, where J_n is the square matrix of order n with all entries 1 and I_n is the identity matrix, orthogonal matrices corresponding to finite projective planes, biplanes and triplanes etc, are local optimum for the aforementioned optimization problems. Remember that the existence of finite projective planes, biplanes and triplanes are inevitably connected with symmetric designs. For large values of n, for which Hadamard matrices are not existing, the existence of conference and weighing matrices help us to get local optimum. For the corresponding optimization problems with unitary matrix constraints, we show that a global optimum exists for all orders. The talk is based on the following works [1],[2],[3],[4]

References

1 K. T. Arasu, M. T. Mohan, A. Pathak, and R. J. Rama, On the Maximum of Entropy for Orthogonal Matrices, submitted.

2 K. T. Arasu and M. T. Mohan, Optimization problems with orthogonal matrix constraints, *Numerical Algebra, Control and Optimization (NACO)*, 8(4), 413–440, 2018.

3 K. T. Arasu and M. T. Mohan, Entropy of Orthogonal Matrices and Minimum Distance Orthostochastic Matrices from the Uniform van der Waerden Matrices, Discrete Optimization, 31 (1), 115–144, 2019.

4 M. T. Mohan, On some p-almost Hadamard matrices, Operators and Matrices, 13 (1), 253–281, 2019.

REGULAR GRADED SKEW CLIFFORD ALGEBRAS OF LOW GLOBAL DIMENSION

Manizheh Nafari

Department of Mathematics & Computer Science
Central State University
Ohio, United States

Abstract

M. Artin, W. Schelter, J. Tate, and M. Van den Bergh introduced the notion of non-commutative regular algebras, and classified regular algebras of global dimension 3 on degree-one generators by using geometry (i.e., point schemes) in the late 1980s. Recently, T. Cassidy and M. Vancliff generalized the notion of a graded Clifford algebra and called it a graded skew Clifford algebra. In this talk, we prove that all classes of quadratic regular algebras of global dimension 3 contain graded skew Clifford algebras or Ore extensions of graded skew Clifford algebras of global dimension 2. We also show that a certain subalgebra R of a regular graded skew Clifford algebra A is a twist of the polynomial ring if A is a twist of a regular graded Clifford algebra B. We have an example that demonstrates that this can fail when A is not a twist of B.

FORMAL DUALITY IN FINITE ABELIAN GROUPS

Alexander Pott

Otto von Guericke University Magdeburg
Universitätsplatz 2
39016 Magdeburg, Germany

Abstract

Inspired by an experimental study of energy-minimizing periodic configurations in Euclidean space, Cohn, Kumar and Schürmann proposed the concept of formal duality between a pair of periodic configurations, which indicates an unexpected symmetry possessed by the energy-minimizing periodic configurations. Later on, Cohn, Kumar, Reiher and Schürmann translated the formal duality between a pair of periodic configurations into the formal duality of a pair of subsets in a finite abelian group. This combinatorial counterpart of formal duality is called a formal dual pair. We will give an overview of formal dual pairs in finite abelian groups, which involves nonexistence results, constructions and characterizations. In cyclic groups, we derive some nonexistence results of primitive formal dual pairs, which are in favor of the main conjecture that except two small examples, no primitive formal dual pair exists in cyclic group. On the other hand, we present several constructions of primitive formal dual pairs in noncyclic groups. These constructions enlighten us to propose the concept of even set, which reveals more structural information of formal dual pairs and leads to a characterization of rank three primitive formal dual pairs.

In this talk we use this database to investigate the state of our knowledge about difference sets. We look at evidence for several of the numerous open conjectures involving difference sets, and formulate some new ones.

This is joint work with Shuxing Li (Magdeburg) and Robert Schüler (Rostock).

COUNTING BIPARTITE GRAPHS: MATCHING-EQUIVALENT TO A GIVEN BIPARTITE GRAPH

C. R. Pranesachar

Formerly of: Homi Bhabha Centre for Science Education (TIFR)
Department of Mathematics
Indian Institute of Science
Bangalore-560012, INDIA

Abstract

Let $G_1 = (U_1, V_1, E_1)$ and $G_2 = (U_2, V_2, E_2)$ be two bipartite graphs, with U_1, U_2 as 'upper' vertex sets and V_1, V_2 as 'lower' vertex sets, $|U_1| = |U_2| = n$. The graphs G_1, G_2 are said to be matching-equivalent if they have the same matching polynomial. Let $G = (U, V, E)$ be a given bipartite graph with $|U| = n$ and $U = \{u_1, u_2, \cdots, u_n\}$. Suppose N_j is the set of vertices in V adjacent to u_j, $1 \leq j \leq n$, such that $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n$. In this talk, we count the number of bipartite graphs which have the same matching polynomial as G and which satisfy a similar inclusion condition as above. We take in G,

$$\begin{array}{l} |N_1| = m,\ |N_2| = m, \cdots,\ |N_{m-k}| = m, \\ |N_{m-k+1}| = m,\ |N_{m-k+2}| = m+1, \cdots, \\ |N_{m-k+r}| = m+r-1,\ |N_{m-k+r+1}| = m+r-1, \\ |N_{m-k+r+2}| = m+r-1,\ \cdots, |N_{m+r-1}| = m+r-1, \end{array}$$

where, of course, $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n$. We make use of the Modified Matching Polynomial in stead of the usual one. The modified matching polynomial for each bipartite graph in the above equivalence class will be

$$(x+1)(x+2)(x+3)\cdots(x+k-1)(x+k)^r(x+k+1)(x+k+2)\cdots(x+m).$$

HIGH RATE LDPC CODES FROM PARTIALLY BALANCED INCOMPLETE BLOCK DESIGNS

Asha Rao

School of Science
RMIT University
Melbourne, Australia

Abstract

This talk presents a combinatorial construction of low-density parity check (LDPC) codes from partially balanced incomplete block designs. Since Gallager's construction of LDPC codes by randomly allocating bits in a sparse parity check matrix, many researchers have used a variety of more structured combinatorial approaches. Many of these constructions start with the Galois field, however this limits the choice of parameters of the constructed codes. Here we present a construction of LDPC codes of length $4n^2 - 2n$ for all n using the cyclic group of order 2n. These codes achieve high information rate (greater than 0.8) for $n \geq 8$, have girth at least 6 and have minimum distance 6 for n odd. The error correction performance of the proposed codes is also presented. The theoretical and computational results provide proof of concept and lays the groundwork for potential high performing codes.

CODES OVER LOCAL RINGS OF ORDER 16

Esengül Saltürk

The Scientific and Technological Research Council of Turkey

Abstract

This talk covers the basics of coding theory and codes over local Frobenius rings of order 16. We give the structure of local Frobenius rings of order 16 and construct codes over these rings. We define a weight preserving Gray map and study the images of these codes under this map. The existence of self-dual and formally self-dual codes is determined.
This is a joint work with Steven Dougherty.

ON RYSER DESIGNS AND THE CONJECTURE

Sharad S. Sane

Chennai Mathematical Institute
Chennai-603013, India

Abstract

Consider an arrangement where we have a point set S of order v and a collection of v distinguished proper subsets of S called the blocks such that every pair of blocks intersects in exactly λ points. A classical example of this situation is called a symmetric $(v; k; \lambda)$-design where all the blocks are of size k and each point has constant frequency (replication number) k. If we further stipulate that we have at least two distinct point frequencies, then the resulting configuration is called a Ryser design. Every known Ryser design is constructed by some kind of set theoretic (combinatorial) process and a long standing and celebrated conjecture (called the λ-design conjecture) of Ryser and Woodall states that every Ryser design is obtained precisely in that canonical manner. The conjecture has been proved for many families of Ryser designs. The talk will present some old and new results relating to the conjecture with a possible direction for proving the conjecture.

A NEW DISTANCE REGULAR GRAPH RELATED TO THE DODECACODE

Patrick Solé

CNRS/LAGA
University of Paris8
Saint-Denis, France

Abstract

The dodecacode is a nonlinear additive self-dual quaternary code of length 12, introduced in 1998 in the context of quantum codes. By puncturing it at any of the twelve coordinates, we obtain a new uniformly packed code of distance 5. Its parameters solve a problem open in 1974 by Bassalygo et al. In particular, this latter code is completely regular but not completely transitive. Its coset graph is distance-regular of diameter three on 2^{10} vertices, with intersection array $\{33, 30, 15; 1, 2, 15\}$. The existence of a DR graph with that intersection array had been an open problem since 1989 in the famous book by Brouwer Cohen and Neumaier. The automorphism groups of the code, and of the graph, are determined.

This is joint work with Minjia Shi, Anhui University, Hefei, China, and Denis Krotov, Sobolev Institute, Novosibirsk, Russia.

CONSTRUCTIONS OF OPTIMAL ORTHOGONAL ARRAYS WITH REPEATED ROWS

Douglas Stinson

Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA

Abstract

We construct orthogonal arrays $OA\lambda(k, n)$ (of strength two) having a row that is repeated m times, where m is as large as possible. In particular, we consider OAs where the ratio m/λ is as large as possible; these OAs are termed optimal. We provide constructions of optimal OAs for any $k \geq n+1$, albeit with large λ. We also study basic OAs; these are optimal OAs in which $gcd(m, \lambda) = 1$. We construct a basic OA with $n = 2$ and $k = 4t + 1$, provided that a Hadamard matrix of order $8t+4$ exists. This completely solves the problem of constructing basic OAs wth $n = 2$, modulo the Hadamard matrix conjecture.

This is joint work with Charlie Colbourn and Shannon Veitch.

HADAMARD AND WEIGHING MATRICES BUILT FROM A PRESCRIBED SET OF ATOMIC BLOCKS - AUTOMORPHISMS AND ENTROPY

Yossi Strassler

-

Abstract

In the search for Hadamard and Weighing matrices, we would like to reduce the entropy of the problem, and one way to achieve this is to tile a matrix from blocks that carry an algebraic structure.

A Hadamard matrix constructed from only two atoms is easily constructed via the Kronecker product. For example $H_2 \bigotimes H_4$, which gives a H8 with block structure:

$$\begin{bmatrix} H_4 & H_4 \\ -H_4 & H_4 \end{bmatrix},$$

In general a Hadamard H_{8m} can be built from two blocks taken from - H_{4m}, H_{4m}. So we may ask, what is the minimal set of blocks from which we can construct any Hadamard matrix, up to equivalence.

For example, if we consider the set of all 4×4 Hadamard blocks, then we can construct from it a representative Hadamard matrix of any order $4 \leq n \leq 24$. This is a relatively small set of size 728, which carries an interesting algebraic structure.

The approach we take is to apply Hadamard operations to an existing matrix in order to reveal the block structure. We employ methods from graph theory.

SUBGROUP DEVELOPMENT AND 2-ANALOG OF A FANO PLANE

Kristijan Tabak

Rochester Institute of Technology
Zagreb Campus
D.T. Gavrana 15, 10000 Zagreb, Croatia

Abstract

A 2-analog of a Fano plane is a collection $\mathcal{H}$ of 3-dimensional subspaces of $\mathbb{F}_2^7$ such that each 2-dimensional space is contained in exactly one subspace from $\mathcal{H}$. Although, Fano plane is a classical example of a symmetric design, till this point it is still unknown if 2-analog of a Fano plane exists. Using group rings and group theory, we introduce a development of a subspace $W \leq \mathbb{F}_2^7$ on a smaller spaces. Using these developments we confirm some known results also providing new facts about putative 2-analog and their underling structures. Additionally, a group ring approach is used to measure a level of symmetry of group coverings that are type of generalization of putative 2-analog of a Fano plane.

GEOMETRIC APPROACH TO GENERATING COCYCLIC HADAMARD MATRICES

Jonathan Turner

Department of Mathematics and Statistics
Air Force Institute of Technology
Wright Patterson AFB, USA

Abstract

We present an efficient decimation class generation algorithm and supplemental comparison algorithm to construct Hadamard matrices with two circulant cores. The generation algorithm extends a novel CAT bracelet generation algorithm based upon geometric properties of the Discrete Fourier Transform under affine transformations. This approach lends itself to well known restrictions on power spectral density and more expedient fathoming. The comparison algorithm exploits multiple key features of Legendre Pairs and basic ring theory, as well as a derived condition based upon the sum of squared periodic auto-correlations. This algorithm generated previously undiscovered Hadamard matrices of orders 112 and 116.