Abstracts for talks to be presented in the CCCS 98 Workshop

Instructional Lectures

Cryptography and Combinatorial Designs

Charles J. Colbourn, Dorothean Professor of Computer Science
University of Vermont

In this series of five lectures, we explore some of the many problems in cryptography where combinatorial designs have played a substantial role. To set the stage, we review some ideas from classical cryptography and cryptanalysis, and briefly outline the major advances in public key cryptography. Using this foundation, we examine problems in authentication, secret sharing and threshold schemes, key distribution schemes, and visual cryptography. Our theme is how requirements for balance and regularity lead to well-studied combinatorial designs; how the cryptographic problem leads to challenging combinatorial problems; and, in a few cases, how combinatorial existence theorems provide useful information in the application. With this in mind, the focus is on applicable mathematics.

The lectures are accessible to those without substantial background in either cryptography or combinatorial designs.

Mathematics and Computer Security

Jennifer Seberry
Director of the Centre for Computer Security Research,
School of Information Technology and Computer Science,
University of Wollongong, Wollongong, Australia

We give five talks on the mathematics associated with aspects of computer security including complexity, elliptic curves, secret sharing, authentication and bent functions.

The talks start from first principles and move to recent research in the area.

Coding Theory

Vladimir D. Tonchev
Michigan Technological University

The first three lectures provide a brief introduction to coding theory and its links to combinatorial designs in the spirit of Chapter "Codes" of the CRC Handbook of Combinatorial Designs, with mentioning some new results that have occurred after the publication of the handbook. The third lecture discusses a class of codes arising from graphs, with an application to quantum error-correcting codes. The fifth lecture describes how linear perfect codes are used to characterize the classical geometric designs by the minimum dimension of their codes. This characterization generalizes a result by Hamada and Ohmori (1975) for the binary case, and proves a conjecture of Assmus.

Research Talks

Some Observations on Quasi-3 Designs and Hadamard Matrices

Wayne Broughton
Okanagan University College, Kelowna, B.C.
Gary McGuire
National University of Ireland, Maynooth Co. Kildare, Ireland

We consider Hadamard matrices with the quasi-3 property, and their implications for the existence of certain quasi-symmetric designs, strongly regular graphs, and codes meeting the Grey-Rankin bound. These questions lead naturally to an interesting infinite family of parameters, and we pose some existence questions.

Configurations in Triple Systems: Group Testing and Optical Communications

Charles J. Colbourn
University of Vermont

In this talk, we discuss the development of group testing algorithms, erasure-correcting codes, and codes for spread-spectrum optical communications that all arise from triple systems in which certain configurations of triples are forbidden. Computational methods and recursive techniques for the construction of triple systems avoiding the specified configurations are outlined, and some existence theorems for weakly union-free systems are established.

On the Reciprocal Non-Existence of Some Generalized Hadamard Matrices Over Groups

Charlie H. Cooke and Iem Heng
Old Dominion University, Norfolk, Virginia

Non-existence of generalized Hadamard Matrices over groups is investigated by means of a necessary condition of Brock, which may be found in CRC Handbook of Combinatorial Design. Methods for establishing the lack of non-trivial solutions to quadratic diophantine equations are used to obtain sequences $\{t_n\}$ for which Butson Hadamard Matrices $BH(p, pt_n)$ do not exist, where $p > 2$ is a prime.

On the Relationship between Signed Groups, Projective Representations of Groups, and Cocyclic Hadamard Matrices.

Robert Craigen
Fresno Pacific University, CA

In the last decade the theory of signed groups, the theory of cocyclic designs, and the application of these theories to Hadamard matrices have been developing independently. In both cases, exciting new results have been established, and there is great promise for future work—it may not be unreasonable to say that

either one of these theories has the potential to completely revolutionize the way we think about Hadamard matrices.

Both theories are grounded in the same basic facts in the projective (and linear) representation theory of groups, but with different approaches, language and notation. Therefore, it is natural to ask: to what degree are the two theories equivalent or analogous to each other? To what extent are they different or complementary? In what ways can the two theories contribute to each other, or form a larger, more comprehensive picture?

I shall make what I believe to be a first effort at addressing some of these questions.

Skew $k-$arcs and Codes

Michelle Davidson
University of Manitoba, Winnipeg, Manitoba

In a projective geometry, $PG(m, 2)$, of dimension m over $GF(2)$, we define a skew $k-$arc S to be a set of k points such that there are at most two points of each line in S, and the diagonals of any 4 points of S do not meet. I will discuss the relationship between skew k-arcs and linear binary codes. Special attention is paid to the situation where the codes has minimum distance 5.

The Relative Difference Sets of the Paley Conference and Type I Hadamard Matrices

Warwick de Launey, Richard M. Stafford
Center For Communications Research, San Diego, CA

Any conference matrix or Hadamard matrix may be used in a particular way to obtain a group divisible design of twice the order. A conference matrix or Hadamard matrix D is said to be cocyclic if there is a group G, a 2-cocycle $f : G \times G \to \{0, \pm 1\}$, and a map $a : G \to \{0, \pm 1\}$ such that D may be written in the form

$$D = [f(x, y)a(xy)]_{x,y \in G}.$$

We say D is cocyclic over the group G with cocycle f. Let E be the extension group obtained from G via f.

In both cases the conference matrix or Hadamard matrix is cocyclic over G with cocycle f and extension group E if and only if the automorphism group of the corresponding group divisible design has a regular subgroup isomorphic to E and containing the involution which interchanges the points in each group. Any such regular subgroup yields a relative difference set in the extension group E.

In this paper we completely characterize all relative difference sets associated with Paley conference matrix and the Paley type I Hadamard matrix. We accomplish this by exhibiting a one to one correspondence between the regular subgroups and certain near fields. Our characterization follows from the fact that all finite near fields are known. This allows us to determine all the groups over which the Paley matrices above are cocyclic.

Our arguments apply in several exceptional near fields. We include some examples.

On Cocyclic Orthogonal Designs and the Asymptotic Existence of Cocyclic Hadamard Matrices

Warwick de Launey
Center For Communications Research, San Diego, CA

A Hadamard matrix H of order n is an $n \times n$ matrix whose entries are all equal to ± 1 and which satisfies

$$HH^T = nI_n.$$

Soon after proving the prime number theorem in 1893, Hadamard conjectured that for any odd integer t divisible by 4, there is a Hadamard matrix of order t. Despite the efforts of several mathematicians, this conjecture remains unproved even though it is widely believed to be true.

In the mid seventies, Seberry proved that for any odd integer $m > 0$, there is a Hadamard matrix of order $2^a m$ for any integer $a > 2 \log_2 m$.

More recently, researchers have formed the opinion that Hadamard matrices with additional structure exist. Any such matrix corresponds to or yields (a) a binary 2-cocycle with specific combinatorial properties, (b) a group divisible design with a regular group action, (c) a normal relative difference set with specific parameters, and (d) a Hadamard group in the sense of Ito. The discovery of these connections has spurred a new generation of researchers to re-examine the wealth of constructions and ideas developed over the past thirty years with an eye to finding and studying new classes of the related objects.

As part of this process the speaker has proved, with Michael J. Smith, that there is a cocyclic Hadamard matrix of order $2^a m$ for any odd integer $m > 0$ and any integer $a > 8 \log_2 m$. A corollary to the argument is the existence of a very large class of maximal size normal relative difference sets with forbidden subgroup generated by a central involution. In particular, any group of odd square-free order m may be embedded as a direct factor into a Hadamard group of order $2^{\lceil 8 \log_2 m \rceil} m$.

Application of the discrete Fourier transform to the search for Hadamard matrices

Roderick J. Fletcher, Jennifer Seberry and Marc Gysin

Two sequences are said to be compatible if their periodic autocorrelation functions sum to a constant. We show that a pair of sequences are compatible if and only if the squared magnitudes of corresponding terms in their discrete Fourier transforms (DFTs) also sum to a constant. It follows that the DFT of any sequence that belongs to a compatible pair is limited in magnitude. This limit may thus be employed as a test to reduce the number of sequences for consideration in the search for compatible pairs. We call this the power spectral density (PSD) test.

The effectiveness of the PSD test is demonstrated by searching for compatible pairs of $0, 1$ sequences of odd length ℓ and Hamming weight $w = (\ell + 1)/2$. Such pairs are equivalent to 2-$(\ell; w, w; w)$ supplementary difference sets and can be used to construct Hadamard matrices of order $2(\ell + 1)$ with a two block circulant core. Exhaustive searches were performed for $\ell \leq 45$. For $\ell = 45$, the PSD test reduced the number of candidate sequences by a factor of 625. Of those passing the test, only about 1 per 1000 belong to compatible pairs. The number of compatible pairs appears to be growing somewhat less than exponentially with ℓ, growing approximately as $2^{\ell/3}$ in the range $29 \leq \ell \leq 45$. Unfortunately, the probability of finding such pairs by random search appears to be decreasing exponentially. The exhaustive searches confirm that the vast majority of sequences in compatible pairs are uniquely compatible with just one other sequence, not counting cyclic shifts and reversals.

On the Orthogonal designs of Order 24

W. H. Holzmann and H. Kharaghani
University of Lethbridge, Lethbridge, Alberta

In the seventies it was shown that all possible 3-tuples are the types of orthogonal designs of order 24 except $(4, 4, 15)$, $(7, 7, 7)$ and $(7, 8, 8)$. We will present a new method to construct all these together will all remaining full 4-tuples, 18 in all.

On the Plotkin Arrays

W. H. Holzmann and H. Kharaghani
University of Lethbridge, Lethbridge, Alberta

A colorful version of Plotkin arrays of order 24, 40 and 56 is shown. Using these and some new arrays, we show the existence of an infinite family of new orthogonal designs.

Cocyclic generalised Hadamard matrices

K. J. Horadam
Royal Melbourne Institute of Technology, Australia

Many codes and sequences designed for robust or secure communications are built from Hadamard matrices or from related symmetric block designs or difference sets.

If an alphabet larger than $\{0, 1\}$ is required, the natural extension is to generalised Hadamard matrices (GHM), with entries in a group C: that is, $v \times v$ matrices H satisfying

$$HH^* = vI_v + (v/w)(\sum_{c \in C} c)(J_v - I_v)$$

where $|C| = w,\ w|v$ and H^* is the transinverse of H.

An abelian GHM which is also cocyclic, is equivalent to a semiregular central relative difference set and to a divisible design with a regular group of automorphisms, class regular with respect to the forbidden central subgroup. Therefore the code and sequence construction techniques for Hadamard matrices are applicable to the general case.

In the first talk I will introduce cocycles and their properties, give some familiar examples of this unfamiliar concept and demonstrate the equivalence of the above-mentioned objects.

In the second talk I will present recent results on the theory of cocyclic GHM and their applications to cocyclic Hadamard codes and perfect arrays.

Trades over Finite Fields and Their Codes

G. B. Khosrovshahi
Institute for Studies in Theoretical Physics and Mathematics (IPM), University of Tehran, Iran

For given integers v, k, and t such that $v > k > t$, let P^v_{tk} be $\binom{v}{t}$ by $\binom{v}{k}$ $(0, 1)$ matrices whose rows are indexed by the t-subsets of a v-set S, whose columns are indexed by the k-subsets B of S, and the entry $P^v_{tk}(A, B)$ of row A and column B is 1 if $A \subset B$ and 0 otherwise.

In this lecture, we consider the null space of P^v_{tk} over $GF(q)$, denoted by $C^v_{tk}(q)$. The elements of $C^v_{tk}(q)$ are called *trades over* $GF(q)$. We discuss the combinatorial properties of these objects and through that we study the code space formed by them. Specifically, by examining the case $C^v_{23}(3)$, we characterize the codewords of small weights and for $v \equiv 0 \pmod 3$, the spectrum of weights is obtained. A very simple algorithm for decoding is presented and the automorphism group of these codes are discussed. Also the family of $C^v_{1k}(2)$ is completely characterized and some optimal codes are found.

On Aperiodic and Periodic Complementary Binary Sequences

Peter Jau-Shyong Shiue
University of Nevada Las Vegas, USA

The present paper represents a continuation of work done by Bömer and Antweiler ("Periodic complementary binary sequences", IEEE Trans. on Information Theory, Vol. 36, pp. 1487–1494, Nov. 1990). We give direct and recursive constructions of aperiodic and periodic complementary sequences. Using these constructions, many missing entries in the table of Bömer and Antweiler can be filled.

Designs and codes in association schemes

Sung-Yell Song
Iowa State University

Let X denote the set of all k-subsets of a fixed set V with size v, and give this set some extra structure by defining two k-subsets x and y to be at *distance* i if $|x \cap y| = k - i$. A simple t-design on v points is just a subset of X satisfying a regular condition. Let Ω denote the set of all n-tuples (words of length n) of a fixed alphabet set S of size q, and define two words x and y to be at distance i if x and y differ in i coordinate positions. A perfect e-code of length n is just a subset C of Ω satisfying the condition that every word in Ω lies at distance e or smaller from exactly one codeword in C. If we do view a t-design and an e-code in this way then a number of new parameters suggest themselves. The talk will be an introduction to the Delsarte's theory on t-designs and e-codes. It will survey the works of Bannai, Biggs, Delsarte, Godsil, Ito, Munemasa and others, highlighting the use of association schemes in design theory and coding theory.

Quasisymmetric circulant weighing matrices

Yoseph Strassler
Bar-Ilan University, Ramat-Gan, Israel

Quasisymmetric circulant weighing matrices are circulant weighing matrices whose pattern of zeroes is symmetric. We address the existence question of such matrices and according to the parity of the the order and the parity of the weight give an answer.

A Family of Hadamard matrices of Dihedral Group Type

Mieko Yamada
Kanazawa University, Japan

Let D_{2n} be a dihedral group of order $2n$ and $\mathbf{Z}$ be the rational integer ring. Kimura gave the necessary and sufficient conditions such that a matrix of order $8n+4$ obtained from the elements of the group ring $\mathbf{Z}[D_{2n}]$ of a dihedral group D_{2n} becomes a Hadamard matrix, where n is an odd integer. We show that if p is an odd prime and $q = 2p-1$ is a prime power, then there exists a family of Hadamard matrices of dihedral group type. We prove this theorem by giving the elements of $\mathbf{Z}[D_{2p}]$ concretely. Gauss sum over $GF(p)$ and the relative Gauss sum over $GF(q^2)$ are important to prove the theorem.