Abstracts for the International Workshop on Finite Fields Constructions of Combinatorial Arrays April 21-27, 2013 – Florianópolis, Brazil

MONDAY

The structure of Costas arrays

Jonathan Jedwab, Simon Fraser University

Abstract. A Costas array is a permutation array in which the vectors joining pairs of 1s are all distinct. This property was identified by J. Costas in the 1960s for use in sonar. The central problem is to determine all orders for which a Costas array exists.

The classical constructions, due to Welch and Golomb, use finite fields to generate infinite families of Costas arrays. These constructions, together with exhaustive search results, show that Costas arrays exist for all orders less than 32. Numerical evidence suggests that some orders of Costas arrays might not exist, but no nonexistence result has yet been found.The smallest orders for which existence is open are 32 and 33, and this has been the case for at least 25 years.

I shall describe some new results that shed light on the structure of Costas arrays, including a proof of a recent conjecture due to Russo, Erickson and Beard.

Joint work with J. Wodlinger.

Algebraic symmetries of generic (m+1)-dimensional periodic Costas arrays

Jose Ortiz-Ubarri, Universidad de Puerto Rico

Abstract. We present two generators for the group of symmetries of the generic $(m+1)$-dimensional periodic Costas arrays over elementary abelian $(Z_p)^m$ groups: one that is defined by multiplication on dimensions and the other by shear (addition) on dimensions. Through exhaustive search, we observe that these two generators characterize the group of symmetries for the examples we were able to compute. Following the results, we conjecture that these generators characterize the group of symmetries of the generic $(m+1)$-dimensional periodic Costas arrays over elementary abelian $(Z_p)^m$ groups.

Synchronization patterns to detect one or multiple targets

Oscar Moreno, nic.pr

Abstract. I will talk on the problem of one target detection, where Costas and sonar sequence constructions are proposed as the solution since they have ideal auto-correlation. The main constructions for this case will be discussed including our new major construction coming from the discovery of a characterization of small Kasami sequences in terms of sonar sequences.

Sonar sequences families for multiple targets will also be discussed and we will present their relationship to the small Kasami family. From this we will obtain many new sonar families for multiple targets. Finally we will present the main problems in this area as well as their relationship to optical orthogonal codes, to watermarking and to classical CDMA. Joint work with Andrew Tirkel.

TUESDAY MORNING

Linked designs and MUBs
Bill Martin, Worcester Polytechnic Institute

Abstract. Linked systems of symmetric designs were introduced by Cameron and studied by Mathon and Noda and others. Only a few examples are known and these give 3-class Q-antipodal association schemes – in fact, a result of Van Dam shows that they are equivalent. Many open parameter sets remain, but it may be that stronger non-existence results are more in demand.

In this talk, we will consider several extensions of this class of designs. Linked systems of strongly regular designs were introduced by D. Higman and some beautiful examples exist, coming from groups, codes, and geometry (e.g., hemisystems in generalized quadrangles). Linked systems of Hadamard designs have been proven to be equivalent to real mutually unbiased bases (MUBs), studied by Boykin, et al. in the context of quantum information theory. The more practical question regarding measurements of finite-dimensional quantum systems is one of MUBs in a complex vector space of finite dimension n. It is known that at most $n+1$ MUBs can be constructed in C^n, and this is achieved when n is a prime power. But very little is known about MUBs in other dimensions. I will try to offer my meager ideas on this problem as well.

Matrix codes and channels over finite fields and rings
Danilo Silva, Universidade Federal de Santa Catarina

Abstract. We consider the problem of transmitting information over a channel of the form $Y = AX + Z$, where A, X, Y, Z are matrices over a finite field. Such channels are useful to model end-to-end communication over packet networks employing random linear network coding. We will describe the problem both from a coding theory perspective, where it is related to the construction of large matrix or subspace codes with a given minimum distance, as well as from an information-theory perspective, where the channel has a stochastic formulation and may be used multiple times. Nearly optimal constructions and/or bounds will presented in both cases. We will also describe our recent work in the generalization of these tools to the case of finite chain rings.

Joint work with Roberto Nobrega, Bartolomeu Uchoa, Chen Feng and Frank Kschischang.

TBA
Ariane Masuda, New York City College of Technology

Abstract. TBA

TUESDAY AFTERNOON

Differential map, ambiguity and deficiency of permutations over finite fields
Daniel Panario, Carleton University

Abstract. We introduce the concepts of weighted ambiguity and deficiency for a mapping between two finite Abelian groups of the same size. Then, we study the optimum lower bounds of these measures for permutations of an Abelian group. The ambiguity and deficiency of some permutation functions over finite fields are investigated; most of these functions are APN permutations. We show that, when they are not optimal, the Mobius function in the multiplicative group of a finite field is closer to being optimal in ambiguity than the inverse function in the additive group of the field. We note that the inverse function over the finite feld with 2^8 elements is used in AES. A twisted permutation polynomial of a finite field is again closer to being optimal in ambiguity than the APN function employed in the SAFER cryptosystem. We briefly comment on the other related measures like dispersion and the differential spectrum.

Ambiguity and deficiency for use in a design theory scheduling problem
Brett Stevens, Carleton University

Abstract. We review a scheduling problem in design theory and geometry that originally motivated my investigation into ambiguity and deficiency. We require a double orthogonally resolvable design on n^2 points with n^2 blocks of size n. If this design has an automorphism group isomorphic to $G_1 \times G_2$ then the best possible performance is governed by the bounds on the ambiguity and deficiency of maps $f : G_1 \to G_2$.

Difference maps between unequal finite groups
David Thomson, Carleton University

Abstract. In this talk, we relate difference maps with other combinatorial objects. Using a conjecture of Golomb and Moreno (1996) on a semi-multiplicative analogue of planar functions, we introduce studying difference maps of functions between finite groups of different cardinalities. The Golomb-Moreno conjecture originally comes from the study of Costas arrays/sequences, and has been resolved in the language of difference sets (with an eye towards projective geometry). We will draw some of the connections between the combinatorial interpretations and give some first steps on studying the ambiguity and deficiency of maps between different finite groups.

WEDNESDAY MORNING

Bachelors, monogamists and the Delta lemma
Bridget Webb, The Open University

Abstract. As their names suggest, a bachelor square has no orthogonal mate, and a monogamous square has a mate but is in no triple of MOLS. More generally, a set of k-maxMOLS is a set of k MOLS that is not contained in any set of $k+1$ MOLS. I will show how the Delta lemma can be used to prove existence of bachelor and monogamous squares, and hence sets of 2-maxMOLS, thus giving a glimpse of the power of this deceptively simple result on transversals.

Sets of orthogonal hypercubes
David Thomson, Carleton University

Abstract. A d-dimensional hypercube of order n and class r is a generalization of a Latin square of order n, where the alphabet size is increased to n^r. In order to define orthogonality, $d \geq 2r$. In the minimal case $d = 2r$, the maximum number of mutually orthogonal class-r hypercubes is $(n-1)^r$. We present a construction of class-r hypercubes based on multi-dimensional permutation polynomials over finite fields; in particular, if we pick linear polynomials, then we cast the problem in terms of matrices over finite fields. We give a complete set of $(n-1)^2$ mutually orthogonal hypercubes over almost all prime powers n, but we fail to find a complete set of mutually orthogonal hypercubes for any class $r > 2$.

Gröbner basis and sudokus
Jonas Szutkoski, Universidade Federal do Rio Grande do Sul

Abstract. Given an ideal in the multivariate polynomial ring, a Gröbner basis for this ideal is a special set of generators. In this small talk we show how we can use Gröbner basis to get information about the solutions of sudokus.

A Gao-Lecerf approach for factoring bivariate polynomials with coefficients in $\mathbb{F}_2$
Luiz Emilio Allem, UniversidadeFederal do Rio Grande do Sul

Abstract. We introduce an algorithm for bivariate polynomial factorization over $\mathbb{F}_2$ combining ingredients of algorithms due to Gao [Factoring Multivariate Polynomials via Partial Differential Equations, *Mathematics of Computation* **72** (2003), 801-822] and to Lecerf [New recombination algorithms for bivariate polynomial factorization based on Hensel lifting, *Applic. Alg. Eng. Comm. Comp.* **21(2)** (2010), 151–176].

WEDNESDAY AFTERNOON

LFSR constructions of difference sets, orthogonal arrays and covering arrays
Brett Stevens, Carleton University

Abstract. The set of fixed length subintervals of a linear feedback shift register form a linear code. A very nice theorem of Bose from 1961 proves that these codewords form the rows of an orthogonal array of strength t if and only if the dual linear code has minimum weight $t+1$. Munemasa observed that whenever the length of the intervals is less than a generous bound, the dual code is the Hamming code which has minimum distance 3 and this orthogonal array is guaranteed to have strength 2. In fact the only 3-coverage that is missing corresponds to the weight-3 multiples of the generating polynomial of the LFSR. We use this and results on difference sets over finite fields to construct a new family of strength 3 covering arrays which improve many best known upper bounds on covering arrays. We will discuss the higher strength analogues of this construction which will connect to open problems.

A construction of strength-3 covering arrays using LFSR sequences
Lucia Moura, University of Ottawa

Abstract. In this talk, we present a construction of covering arrays based on Linear Feedback Shift Register (LFSR) sequences constructed using primitive polynomials over finite fields. For any prime power q, this construction gives a covering array of strength 3 with q^2+q+1 columns over q symbols that has size $2q^3-1$ (number of rows). The construction can be extended to non-prime powers q by a fusion operation from a larger prime power. This results in significant reductions on known upper bounds for covering array sizes in most cases covered by this construction. In particular, for the values of $q \leq 25$ kept in Colbourn's covering array tables, this construction improved upper bounds for all $q \neq 2, 3, 6$.

This is joint work with Sebastian Raaphorst and Brett Stevens.

THURSDAY MORNING

2-factorisations of the complete graph: The Oberwolfach problem and beyond

Peter Danziger, Ryerson University

Abstract. We will discuss various types and variations of 2-factorisations of the complete graph. Factorisation into triples was introduced by Kirkman in 1848, though the so called Kirkman problem was only solved in 1971 by Ray-Chadhuri and Wilson. In the 1960's Ringel introduced the so called Oberwolfach problem, which asks for a 2-factorisation of the complete graph, K_n, or the complete graph minus a 1-factor, $K_n - I$, if n is even into a specific factor. The Oberwolfach problem remains open, though many special cases are known. Subsequently a number of variations on this problem have been suggested, including looking at different graphs and multiple factor types. We will discuss some general types of 2-factorization and give some results on these, with particular focus on the case when the 2-factors are bipartite.

Group divisible packing designs with block size 3: relationship to coverings

Nevena Francetić, Carleton University

Abstract. Group divisible packing designs (GDPDs) are a generalization of group divisible designs (GDDs) in which a pair of elements from two distinct groups is contained it at most one block. As such, GDPDs are related to packing arrays with row limit.

In this talk we discuss two counting upper bounds on the size of a GDPD. Then we construct optimal group divisible covering designs (GDCDs) with block size three which "transform" into optimal GDPDs. The "transformation" consists of performing the minimal adjustment to the set of blocks: removing only the blocks which contribute to the excess in a GDCD to get a packing design and, if necessary, addition of a number of new blocks to obtain a maximal GDPD.

Covering arrays and OR-arrays

Elizabeth Maltais, University of Ottawa

Abstract. Covering arrays on graphs are generalizations of strength 2 covering arrays, studied by Meagher and Stevens (2005). We specify required pairs of factors (all possible interactions must be tested) and encode these as the edges of a graph. Unspecified pairs of factors are optional.

We now introduce a further generalization of covering arrays on graphs. Binary relational systems are used to encode the required interactions. Rather than specifying pairs of factors for which coverage is required, we specify particular pairwise interactions to be covered. Unspecified interactions are optional. Arrays that cover the required interactions of these systems are called OR-arrays (optional & required).

This talk focusses mainly on OR-arrays for binary alphabets. We give several introductory results. We compare OR-arrays to covering arrays and covering arrays on graphs and discuss asymptotic behaviour using tournaments.

This is joint work with my supervisors Lucia Moura and Mike Newman.