Special Days on

Combinatorial Constructions

Using Finite Fields

December 05-06, 2013

as part of the
Radon Special Semester 2013 on
Applications of Algebra and Number Theory

ÖAW
Austrian Academy
of Sciences

RICAM
JOHANN · RADON · INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

Timetable
"Combinatorial Constructions Using Finite Fields"

December 5-6, 2013

	Thursday Dec. 5	**Friday Dec. 6**
09:00 - 10:00	Mullen	Thomson
10:00 - 10:30	***Coffee Break***	***Coffee Break***
10:30 - 11:00	Jungnickel	Pace
11:00 - 11:30	Moura	Pott
11:30 - 12:00	Tzanakis	Jungnickel
12:00 - 14:00	***Lunch Break***	***Lunch Break***
14:00 - 14:30	Meidl	Qureshi
14:30 - 15:30	Stevens	Wassermann
15:30 - 16:00	***Coffee Break***	***Coffee Break***

"*Perfect codes and balanced generalized weighing matrices*"

Dieter Jungnickel University of Augsburg, Germany

Abstract

Balanced generalized weighing matrices include well-known classical combinatorial objects such as Hadamard matrices and conference matrices. They have an interesting interpretation in Finite Geometries, and in this context they generalize notions like projective planes admitting a full elation or homology group. We give some general background discussing these connections.

Next, we present an elegant method for constructing such matrices: any set of representatives of the distinct 1-dimensional subspaces in the dual code of the unique linear perfect single-error-correcting code of length $\frac{q^d-1}{q-1}$ over $GF(q)$ is a balanced generalized weighing matrix over the multiplicative group of $GF(q)$. Moreover, this matrix is characterized as the unique (up to equivalence) weighing matrix for the given parameters with minimum q-rank (namely d). We will describe the relation to the classical, more involved construction for this type of BGW-matrices (using affine geometry and relative difference sets). We can also obtain a wealth of monomially inequivalent examples and determine the q-ranks of all these matrices, by exploiting a connection with linear shift register sequences.

Thus the talk discusses a topic which connects three central areas of Discrete Mathematics and uses finite fields as an essential tool.

This is joint work with V.D. Tonchev.

"*Blocking sets of the Hermitian unital*"

Dieter Jungnickel University of Augsburg, Germany

Abstract

In any point-line geometry, a *blocking set* is a subset B of the point set that has nonempty intersection with each line. The case where B does not contain any line is of particular interest; such blocking sets are called *proper*.

In this talk, we consider (proper) blocking sets in the Hermitian unital $\mathcal{U}$ embedded in the classical projective plane $\Pi = PG(2, q^2)$. The points of $\mathcal{U}$ are given by the Hermitian curve $\mathcal{H}(2, q^2)$ of Π, say with equation $xz^q + y^{q+1} + zx^q = 0$, and the lines of the unital are the intersections of the non-absolute lines with $\mathcal{H}(2, q^2)$. It is well-known that $\mathcal{U}$ is a resolvable $(q^3 + 1, q + 1, 1)$-design.

Our principal result shows that $\mathcal{U}$ has a proper blocking set if and only if $q \geq 4$. We present general constructions and also prove a lower bound on the size of blocking sets in the classical unital. It is not surprising that all this relies heavily on finite fields; the main tools are Singer groups, the polynomial method and some (elementary) algebraic geometry.

This is joint work with A. E. Brouwer, V. Krčadinac, S. Rottey, L. Storme, T. Szőnyi and P. Vandendriessche.

"*Bent functions, difference sets and strongly regular graphs*"

Wilfried Meidl Sabancı University, Istanbul, Turkey

Abstract

A function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called bent if its *Walsh transform* $\widehat{f}(b) = \sum_{x \in \mathbb{F}_p^n} \varepsilon_p^{f(x) - b \cdot x}$, $\varepsilon_p = e^{2\pi i/p}$, has always absolute value $p^{n/2}$. If $p = 2$ then $\widehat{f}(b) = \pm 2^{n/2}$. If p is odd, then for a bent function we always have $\widehat{f}(b) = \pm \epsilon_p^{f^*(b)} p^{n/2}$ if n is even or n is odd and $p \equiv 1 \bmod 4$, and $\widehat{f}(b) = \pm i \epsilon_p^{f^*(b)} p^{n/2}$ if n is odd and $p \equiv 3 \bmod 4$, for a function $f^* : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$. If the sign is independent from b, then f is called a weakly regular bent function, if it changes with b then f is called not weakly regular.

Bent functions have many interesting relations to combinatorial objects. Boolean Bent functions are in one to one correspondence with Hadamard difference sets, for arbitrary primes p bent functions relate to relative difference sets with certain parameters. Weakly regular bent functions with some additional properties yield strongly regular graphs.

After recalling some basic properties of bent functions, I present a secondary construction of bent functions (i.e. a construction of new bent function from bent functions), and analyse this constructions with respect to constructing the related combinatorial objects.

"*A construction for strength-*3 *covering arrays from linear feedback shift register sequences*"
Lucia Moura University of Ottawa, Canada

Abstract

A covering array with k columns, v symbols, strength t and size N, denoted by $CA(N;t,k,v)$, is an N by k array on v symbols such that for any of the possible t-subsets of columns, its corresponding N by t subarray contains each of the t-tuples on v symbols appearing at least once as one of its rows. The main problem of interest is: given t, k, v, construct a $CA(N;t,k,v)$ with the minimum possible N. 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 $t=3$ with $k=q^2+q+1$ columns over $v=q$ symbols that has size $N=2q^3-1$ (number of rows). The construction can be extended to non-prime powers v by a fusion operation from a larger prime power. This yields significant reductions on known upper bounds for covering array sizes in most cases covered by the construction. In particular, for the values of $v \leq 25$ kept in Colbourn's covering array tables, this construction improved upper bounds for all v except $2,3,6$.

Joint work with Sebastian Raaphorst and Brett Stevens, which recently appeared in Designs, Codes and Cryptography, published online September 8, 2013.

"*Sets of orthogonal hypercubes*"
Gary Mullen Pennsylvania State University, USA

Abstract

As motivation for discussing sets of orthogonal hypercubes, we will first discuss several results concerning sets of orthogonal latin squares. These latin square ideas have been extended to hypercubes of dimension $d \geq 2$. In most of the older work on these topics, orthogonality of cubes and hypercubes was always defined pairwise, as with latin squares.

In this talk we will discuss a number of different notions of orthogonality for hypercubes of dimension $d \geq 2$. These new notions of orthogonality not only provide interesting combinatorial objects worthy of study in their own rights, but some of these notions lead to connections to error-correcting codes; for example to MDS codes. We will also discuss a new class of orthogonal hypercubes, namely hypercubes of class r, in which the number of symbols is larger than the order of the hypercube.

"*k–nets in a projective plane over a field*"
Nicola Pace ICMC–University of São Paulo, Brazil

Abstract

This talk deals with *k–nets* embedded in the projective plane $PG(2,\mathbb{K})$ defined over a field $\mathbb{K}$. They are line configurations in $PG(2,\mathbb{K})$ consisting of $k \geq 3$ pairwise disjoint line–sets, called *components*, such that any two lines from distinct families are concurrent with exactly one line from each component.

The case $k=3$ is particularly interesting because, in some instances, it is possible to realize finite groups. A 3-net is said to *realizing a group* $(G,.)$ when the following condition holds. If A, B, C are the components, then there exists a triple of bijective maps from G to (A,B,C), say $\alpha : G \to A, \beta : G, \to B, \gamma : G \to C$ such that $a \cdot b = c$ if and only if $\alpha(a), \beta(b), \gamma(c)$ are three collinear points, for any $a,b,c \in G$. If $\mathbb{K}$ has zero characteristic, 3-nets realizing a finite group are classified. If the characteristic of the field $p > |G|$, then the same classification holds true apart from three possible exceptions: A_4, S_4 and A_5.

The case $k \geq 4$ is also considered. If $\mathbb{K}$ has zero characteristic, no embedded 5–net exists, see [3, 4]. A different proof is provided in [2] and it can be extended to the case of positive characteristic p, as long as p is sufficiently large compared with the order of the k-net.

Key results and short proofs from [1, 2] are presented.

This is joint work with G. Korchmaros and G. Nagy.

References

[1] G. Korchmaros, G. Nagy, N. Pace, 3-nets realizing a group in a projective plane, to appear in J. Alg. Combinatorics, 2013.

[2] G. Korchmaros, G. Nagy, N. Pace, k–nets embedded in a projective plane over a field, preprint arXiv:1306.5779.

[3] J. Stipins, Old and new examples of k–nets in P^2, math.AG/0701046.

[4] S. Yuzvinsky, A new bound on the number of special fibers in a pencil of curves, Proc. Amer. Math. Soc. 137 (2009), 1641–1648.

"*Construction of skew Hadamard difference sets*"

Alexander Pott Otto-von-Guericke-University Magdeburg, Germany

Abstract

A skew Hadamard difference set is simply a difference set D in a group G such that the difference set, the identity element, and the set of inverse elements D form a partition of the group G. The classical examples are the squares in the additive group of a finite field of order 3 modulo 4. Following a seminal paper by Cunsheng Ding and Jin Yuan, who constructed more and new of such difference sets, several authors provided new constructions. In my talk, I want to review some of these, and I will present a new construction using Dickson polynomials. Connections to planar functions will be explained.

This is joined work with Qi Wang.

"*Some combinatorial aspects of perfect Lee codes*"

Claudio Qureshi Universidade Estadual de Campinas - Unicamp, Brazil

Abstract

In the first part of the talk we will review some classical combinatorial results on perfect codes in the Hamming metric. Then, we will focus on perfect codes in the Lee metric. We will discuss the bi-dimensional case in detail and show the latest results in the general case, presenting some open problems concerning the existence of perfect and dense codes in this metric.

"*Highly non linear sequences and combinatorial applications*"

Brett Stevens Carleton University, Ottawa, Canada

Abstract

Sequences can be viewed more generally as maps from one group to another. We survey some common uses of highly non-linear sequences for constructing covering arrays, combinatorial designs, APN permutations and Costas arrays. We will define two natural definitions that quantify non-linearity: weighted ambiguity and deficiency. We study the lower bounds of these measures for bijections between two groups of the same size and show that optimal ambiguity implies the APN property. We then discuss known connections between these measures and existing measures of non-linearity. We give several constructions of mappings which are optimal with respect to these lower bounds and give results on the ambiguity and deficiency of families of permutation polynomials.

“*Costas arrays from projective planes of prime-power order.*”

David Thomson Carleton University, Ottawa, Canada

Abstract

A Costas array is an $n \times n$ array of dots and blanks with exactly one dot in every row and column such that the line segments joining any two dots are distinct. There are few known constructions of Costas arrays, all of which are based on finite fields. In fact, it is not known if Costas arrays of size 32 exist!

In this talk, we will investigate properties of periodic Costas arrays. It can be shown that doubly-periodic Costas arrays cannot exist; however the Welch construction of Costas arrays generates the smallest variant of a Costas array which is doubly-periodic. A conjecture of Golomb and Moreno (1996) states that all doubly-periodic arrays are Welch. An equivalent conjecture, also due to Golomb and Moreno, characterizes a semi-multiplicative analogue of planar functions over prime fields. We call these functions Costas polynomials. We prove of the Golomb-Moreno conjecture which is based on direct-product difference sets. We give a family of Costas polynomials over all finite fields, and conjecture that we have found all Costas polynomials. Our conjecture is equivalent to the conjectured non-existence of non-Desarguesian planes of a certain type having prime-power order.

“*Construction of covering arrays from m-sequences*”

Georgios Tzanakis Carleton University, Ottawa, Canada

Abstract

Let q be a prime power and $\mathbb{F}_q$ the finite field of q elements. A *q-ary m-sequence* is a periodic sequence of elements from $\mathbb{F}_q$, which is generated by a linear recurrence relation of order n, and has period $q^n - 1$. These sequences play a crucial role in a wide variety of engineering and cryptographic applications.

A *covering array* $CA(N;t,k,v)$ is a $N \times k$ array with entries from an alphabet of size v, with the property that any $N \times t$ sub-array has at least one row equal to every possible t-tuple. Covering arrays are used in applications such as software and hardware testing. It is crucial for such applications, and probably the main focus of this research area, to find covering arrays $CA(N;t,k,v)$ with the smallest N possible, for given t, k, v.

There are various algebraic and combinatorial constructions, as well as computer generation methods for covering arrays. Although constructions using m-sequences exist in the literature, these are a few and, until recently, only focused on similar combinatorial objects (that are covering arrays with more restrictions orthogonal arrays); in 2013, Moura, Raaphorst and Stevens gave a construction for covering arrays of strength 3 using m-sequences, which are the best known for certain parameters.

We are working on extending this construction to strengths larger than 3; we have currently developed a backtracking algorithm that yields covering arrays of strength 4. For certain parameters, these are either the best, or close to being the best known. Furthermore, our findings suggest connections with finite geometry that we want to explore further, with the ultimate goal being a concrete mathematical construction of covering arrays of general strengths. In this talk we present the current state of our research in that direction.

“*On designs and Steiner systems over finite fields*”

Alfred Wassermann University of Bayreuth, Germany

Abstract

Let $\mathcal{V}$ be a v-set (i.e. a set with v elements) whose elements are called *points*. A t-(v,k,λ) *design* is a collection of k-subsets (called *blocks*) of $\mathcal{V}$ with the property that any t-subset of $\mathcal{V}$ is contained in exactly λ blocks. A t-$(v,k,1)$ design is called *Steiner system.*

The notion of t-designs and Steiner systems has been extended to vector spaces over finite fields by Cameron and Delsarte in the 1970s: Now, $\mathcal{V}$ is a v-dimensional vector space over a finite field $\mathbb{F}_q$. A t-$(v,k,\lambda;q)$ design is a collection of k-dimensional subspaces of $\mathcal{V}$ (called blocks) with the property that any t-dimensional subspace of $\mathcal{V}$ is contained in exactly λ blocks.

Since 2008, due to the work of Kötter and Kschischang on random network codes [3], the interest in these *designs over finite fields* has much increased. In the setting of network coding, Steiner systems over finite fields are constant dimension subspace codes with the maximum number of codewords – so called *perfect diameter codes*.

In 1999, Metsch conjectured that Steiner systems over finite fields do not exist for $t \geq 2$. However, in [2] the first Steiner systems over finite fields with $t = 2$, and in [1] the first *large sets of designs* over finite fields with $t = 2$ have been constructed.

In my talk I will give an introduction to network coding, give a survey on recent results on designs over finite fields and explain the construction of 2-$(13, 3, 1; 2)$ Steiner systems over finite fields.

This is joint work with M. Braun, T. Etzion, A. Kohnert, P. R. J. Östergård, and A. Vardy.

References

[1] M. Braun, A. Kohnert, P. R. J. Östergård, and A. Wassermann, *Large Sets of t-Designs over Finite Fields*, ArXiv e-prints, May 2013.

[2] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann, *Existence of q-Analogs of Steiner Systems*, ArXiv e-prints, April 2013.

[3] R. Kötter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory **54** (2008), 3579–3591.