
Algebraic and Combinatorial Approaches to Designs and Codes - Part III

(Org: **Thaís Bardini Idalino** (Universidade Federal de Santa Catarina, Brazil), **Jonathan Jedwab** (Simon Fraser University) and/et **Shuxing Li** (Simon Fraser University))

MARCO BURATTI, University of Perugia, Italy

Old and new results on elementary abelian 2-designs

A 2-design is *elementary abelian* if it admits an elementary abelian group of automorphisms acting sharply transitively on its points.

In this talk I will briefly survey the main results on this topic and I will present some new infinite families of elementary abelian 2 - (q^n, kq, λ) designs in which every block is a union of k parallel lines of $AG(n, q)$, the n -dimensional affine geometry over the field of order q .

EIMEAR BYRNE, University College Dublin, Ireland

New subspace designs from q -matroids

A perfect matroid design (PMD) is a matroid whose flats of the same rank all have the same size. In this talk we introduce the q -analogue of a PMD. A subspace design is a collection B of k -dimensional spaces such that every t -dimensional subspace is contained in the same number λ of members of B . For $\lambda = 1$, the design is called a q -Steiner system. Currently, the only known q -Steiner system parameters that have been realised is $S(2, 3, 13; 2)$. We show that q -Steiner systems are examples of q -PMD's and we use this q -matroid structure to construct subspace designs from q -Steiner systems.

NIKOLAY KALEYSKI, University of Bergen, Norway

Bounding the Hamming distance between APN functions

Almost perfect nonlinear (APN) functions are defined as those functions that provide the best possible resistance to differential cryptanalysis. Their significance reaches far beyond the practical needs of cryptography: APN functions have a natural combinatorial definition, and thus correspond to optimal objects in many diverse areas of study (design theory, coding theory, sequence design, algebra, affine geometry, etc.) APN functions have very little structure by design and are difficult to study. We show how a lower bound on the distance between APN functions can be derived, and explore some of its practical and theoretical applications.

GOHAR KYUREGHYAN, University of Rostock, Germany

Image sets of APN maps

Almost perfect nonlinear (APN) maps of finite fields yield constructions for optimal objects in cryptology, coding theory, combinatorics. In this talk we study the size of the image set and the preimage distribution of an APN map. The talk is based on a joint work with Björn Kriepke and Lukas Kölsch.

ALEX POTT, Otto-von-Guericke University, Germany

Designs and bent functions

The connection between bent functions and difference sets (which give rise to designs) is well known. It is not so well known that the classical Boolean as well as vectorial bent functions can be also used to construct incidence structures using the concept of vanishing flats, as it has been introduced recently by S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera and P. Stănică.

The results in this talk are based on W. Meidl, A. Polujan, A. Pott, *Linear codes and incidence structures of bent functions and their generalizations*, arXiv:2012.06866v1.