Bilateral workshop

Designs, codes, graphs and cryptography - an interdisciplinary approach in analysis of certain discrete structures

Department of Mathematics, University of Rijeka

Friday, May 10, 2019

Room O–355 (3rd floor of the Department building, R. Matejčić 2, Rijeka)

11:00 – 11:30

Nina Mavrović (Department of Mathematics, University of Rijeka)

Self-dual codes from orbit and quotient matrices of certain combinatorial designs

In this talk we will give some constructions of self-orthogonal and self-dual codes, with respect to certain scalar products, obtained with the help of orbit matrices and quotient matrices related to certain combinatorial designs. Specifically, we will describe constructions from symmetric and non-symmetric block designs and their extended orbit matrices, induced by the action of an automorphism group of the design. Then we will give some constructions of self-dual codes from symmetric (group) divisible designs (SGDDs) with the dual property and their quotient matrices.

11:30 – 12:00

Samir Hodžić (FAMNIT, University of Primorska)

Generalized Boolean functions and their connection to MC-CDMA sequences

Generalized Boolean functions are mappings from the vector space F_2^n to the ring Z_q where q is a positive integer. Such mappings can be represented as a collection of $\log_2 q$ many Boolean functions when q is a power of two. We recall some main results related to the properties of these functions, in particular in terms of their representative Boolean functions. These functions have a natural connection to linear codes over Z_q and can be used to construct a set of MC-CDMA sequences. Some open problems related to the maximum cardinality and an efficient implementation of MC-CDMA sequences will be given.

12:30 – 13:00

Nastja Cepak (FAMNIT, University of Primorska)

Boolean functions, their generalization, and derived linear codes

Boolean functions have important applications in cryptography, though they are related to other compbinatorial objects such as Cayley graphs, 2-design, association schemes to name a few. Recently, a connection of Boolean functions and linear codes was established both for standard Boolean functions

and as well as their generalizations. Associating certain classes of Boolean functions to so-called 2-design several classes of interesting family of linear codes (someof which are optimal) were derived by Chunseng Ding in 2015. In this talk, we will recall most important concepts related to this particular design of linear codes and mention certain research directions towards their extension.

13:00 – 13:30

Marina Šimac (Department of Mathematics, University of Rijeka)

On some results about LDPC codes based on cubic symmetric graphs and μ-geodetic graphs

LDPC codes were first presented by Gallager in 1962. and since then they have been the subject of much interest and study. In this talk we shall define LDPC codes and present some of their important properties. We focus on the construction of LDPC codes without 4-cycles using adjacency matrices of cubic symmetric graphs and μ-geodetic graphs obtained from block designs. We will discuss some of the properties of the constructed codes, and moreover, present information on the constructed codes.

Lunch break

15:30 – 17:30

Group discussion

Organizers:

Enes Pašalić, FAMNIT, University of Primorska

Sanja Rukavina, Department of Mathematics, University of Rijeka