
Group 3 :

On non-monomial APcN permutations over finite fields of even characteristic

- Speaker : Jaeseong Jeong (AORC)

- Abstract : Recently, a new concept called the c -differential uniformity was proposed by Ellingsen et al. (2020), which allows to simplify some types of differential cryptanalysis. After the notion of c -differential uniformity was proposed, finding functions with low c -differential uniformity has attracted the attention of many researchers. For example, many classes of PcN and APcN functions were proposed by using the cyclotomic technique, switching method, AGW criterion and generalized Dillon's switching method. In this talk, I will present new classes of (almost) perfect c -nonlinear non-monomial permutations over a binary field.

AORC Monthly Seminar

Aug. 26 (Fri), 2022 @ AORC (Online)

AORC Monthly Seminar

- Object : Active collaboration within and between groups, fitting the aim of SRC
- Plan : Newly-joined researchers take pivotal roles.
- Operations Committee :
 - Nhan Phu Chung (Committee Chair)
 - Bumtlee Kang (Group 1), Juyoung Jeong (Group 2), Bomi Shin (Group 3)

Program

- 2:00 - 2:50 pm : Hayan Nam (Group 1) & discussion
- 3:00 - 3:50 pm : Juyoung Jeong (Group 2) & discussion
- 4:00 - 4:50 pm : Jaeseong Jeong (Group 3) & discussion

Abstracts

Group 1 :

Counting the number of certain partitions by using numerical semigroups

- Speaker : Hayan Nam (Duksung Women's University)
- Abstract : A partition of n is an expression of n as the sum of positive integers. By assigning non-negative numbers to the boundary of a partition's Ferrers diagram, we get the numerical set corresponding to the partition. Considering several invariants of numerical semigroups, we classify partitions under those invariants and count the number of partitions corresponding to numerical semigroups with fixed invariants.

Group 2 :

Transfer principles and a subdifferential formula in Fan-Theobald-von Neumann systems

- Speaker : Juyoung Jeong (AORC)
- Abstract : A Fan-Theobald-von Neumann system is a triple $(\mathcal{V}, \mathcal{W}, \lambda)$, where \mathcal{V} and \mathcal{W} are real inner product spaces and $\lambda : \mathcal{V} \rightarrow \mathcal{W}$ is a norm-preserving map satisfying a Fan-Theobald-von Neumann type inequality together with a condition for equality. Examples include Euclidean Jordan algebras, systems induced by certain hyperbolic polynomials, and normal decomposition systems (Eaton triples). The present talk is a continuation of an AORC monthly seminar talk held last year, where the concepts of commutativity, automorphisms, majorization, and reduction were introduced and elaborated. In the present talk, we describe transfer principles and formulate a subdifferential formula.