INSTITUTUL DE MATEMATICĂ "SIMION STOILOW" AL ACADEMIEI ROMÂNE

Conferinţă Lunară cu sprijinul **Bitdefender**

Cyclotomic Cosets and an Affine Equivalences Count in Prime Dimensions

Pante Stănică

IMAR and Naval Postgraduate School, Monterey, U.S.A.

Wednesday, April 20, 13:00

IMAR, amfiteatrul Miron Nicolescu, ground floor

Abstract: A Boolean function is a map from the n-dimensional vector space $\mathbb{F}_2^n$ with values in the two-element field $\mathbb{F}_2$. They are extensively used as combiners in stream ciphers, as well as some other cryptographic and coding theory settings. A Boolean function is called rotation symmetric if its algebraic normal form (polynomial representation) is invariant under a cyclic permutations of indices. A monomial rotation symmetric function (MRS) of degree d is a rotation symmetric function generated by a single monomial $x_1x_{j_2}x_{j_3}\ldots x_{j_d}$, that is, $f(x_1,\ldots,x_n) = x_1x_{j_2}x_{j_3}\ldots x_{j_d} + x_2x_{j_2+1}x_{j_3+1}\ldots x_{j_d+1} + \cdots$ where indices are taken Mod n. For more than 40 years, many papers were written dealing with the following (related) questions:

(A) *Given two multivariable functions f, g, does there exist a permutation σ on the variables such that $f \circ \sigma = g$?*

(B) *How many classes of (such) equivalent functions are there?*

These questions are relevant for cryptography, since if all "things" are equal, then one might want to use in a stream cipher an easier representable function from the same equivalence class. Using a new method previously developed by the author, D. Canright and J.H. Chung, we are able to completely count the number of equivalence classes for MRS of small degrees in prime power dimension, as well as give tight asymptotics for arbitrary degrees.

Most of the lecture will be accessible to a general mathematical audience.