University of Puerto Rico Mayaguez Campus
Faculty of Arts and Sciences
Department of Mathematical Sciences
call box 9000, Mayagüez, P.R. 00681

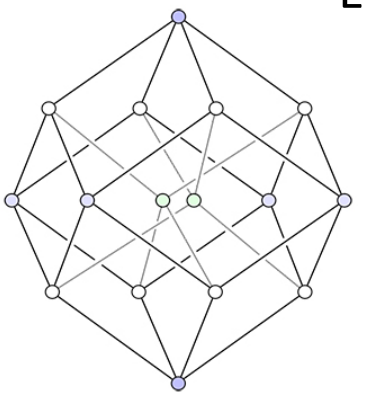
THE DEPARTMENT OF MATHEMATICAL SCIENCES PROUDLY PRESENTS

COLLOQUIUM

August-December 2025

Recursive Exponential Sums for *k*-Rotation Symmetric Boolean Functions

Eiver Rodríguez Pérez



UPR-Mayaguez

Sept 16 - 2025
10:45 am
Monzón 201

Abstract

Let $\mathfrak{B}_n$ be the set of all n-variables Boolean functions. A function $f \in \mathfrak{B}_n$ is said to be rotation symmetric (or *Rot* for short) if it is fixed under the action of the cyclic group C_n of n elements. This family of functions is known to contain highly non-linear elements, which is important in some applications in cryptography. Cusick proved that, under certain conditions, exponential sums of rotation symmetric Boolean functions are linear recursive (see [1]). Recently, in [2], Castro et al. obtained explicit recurrences for exponential sums of some Rots over $\mathbb{F}_q$.

A function $f \in \mathfrak{B}_n$ is said to be k-rotation symmetric if it is fixed under the action of the subgroup $\langle k \rangle$ of $C_n \simeq \mathbb{Z}_n$. These functions are generalizations of rotation symmetric Boolean functions (see [3]) and, as in the case of *Rots*, they contain highly non-linear elements. In this talk we show that, under certain conditions, exponential sums of k-rotation symmetric Boolean functions also satisfy linear recursions (we provide their characteristic polynomials). We also show that, under certain conditions, this result can be extended to $\mathbb{F}_q$.

Ph.D. in CISE
University of Puerto Rico