Recursive Exponential Sums for k-Rotation Symmetric Boolean Functions

Eiver Julio Rodríguez Pérez,
eiver.rodriguez@upr.edu
Department of Mathematics, UPR-RP.

DISSERTATION
DEPARTMENT OF
MATHEMATICS

July 21, 2025

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 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 [12]). Recently, in [5], Castro et al. obtained explicit recurrences for exponential sums for 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 [24]) and, as in the case of *Rots*, they contain highly non-linear elements. In this work we show that, under certain conditions, exponential sums of k-rotation symmetric Boolean functions also satisfy linear recursions. We also show that, under certain conditions, this result can be extended to $\mathbb{F}_q$. Additionally, inspired by [9], we study the associated the graph of k-rotation symmetric Boolean functions.