Exponential Sums and Nonlinearity of Cubic k-Rotation Symmetric Boolean Functions

DISSERTATION
DEPARTMENT OF
MATHEMATICS

Rodrigo A. León Prato,
rodrigo.leon@upr.edu
Department of Mathematics, UPR-RP.

July 23, 2026

Abstract

Boolean functions are fundamental objects in cryptography, where properties such as balancedness and nonlinearity are critical for ensuring resilience against attacks. In this thesis, we study k-rotation symmetric Boolean functions (k-RSBFs), a class of functions invariant under the action of the cyclic group $\langle \sigma_n^k \rangle$, where $\sigma_n = (1,2,\ldots,n)$ is the standard cycle permutation. While these functions are highly regarded for their efficiency, their spectral evaluation traditionally relies on exhaustive computational methods. Since direct evaluation requires iterating over all 2^n possible inputs, this approach quickly becomes computationally intractable as the number of variables n increases.

We develop a unified theoretical framework for the structural decomposition of mixed cubic k-cycles. By establishing that these functions can be decomposed into independent blocks via affine equivalence, we derive exact closed-form expressions for their exponential sums, which are governed by second-order linear recurrences linked to Lucas sequences. We successfully extend these results to arbitrary Galois fields $\mathbb{F}_q$.

Furthermore, we demonstrate that the nonlinearity (nl) and Hamming weight (wt) of simple, short, and non-equidistant mixed cubic k-cycles are equal. That is, the identity $nl(f) = wt(f)$ holds for this class of Boolean functions. These findings replace exhaustive computational searches with direct algebraic evaluations that execute in fractions of a second, drastically reducing the complexity required for cryptographic assessment.

Keywords: Boolean functions, k-rotation symmetric, structural decomposition, direct sums, exponential sums, nonlinearity, Lucas sequences, Galois fields.