Characterization and affine equivalence of k-rotation symmetric Boolean functions

José E. Calderón Gómez,
joseemilio.calderon@upr.edu
Department of Mathematics, UPR-RP.

DISSERTATION
DEPARTMENT OF
MATHEMATICS

May 13, 2024

Abstract

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in 1999. They proved that these functions have efficient and secured cryptographic implementations. Later, in 2007, Kavut and Yücel provided a generalization of these functions. These generalized functions are known as k-rotation symmetric Boolean functions. Kavut and Yücel found a function that exceed the Bent concatenation bound in this new class of functions. In later years, many research has been developed for this type of functions for small degree. Concepts such as affine equivalence, Hamming weight, and nonlinearity have been extensively studied.

In this work we give an explicit characterization of generators of k-rotation monomial Boolean functions. These generators can be used to determined when a k-rotation monomail is a short cycle or a long one. We also use such generators to count the number of cycles for a given value of the degree and a given value of length. We also present a study on the affine equivalence of such monomials to determine whenever two k-rotation monomials are affine equivalent.

Keywords: Boolean functions, k-rotation, affine equivalence.