Generators of Monomial Rotation Symmetric Boolean Functions and a Characterization of Monomial Dihedral Symmetric Boolean Functions

DISSERTATION
DEPARTMENT OF
MATHEMATICS

Carlos A. Molina Salazar,
carlos.molina2@upr.edu
Department of Mathematics, UPR-RP.

June 28, 2023

Abstract

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in 1999. They proved that these functions have efficient and secured cryptographic implementations. In recent years, a subclass of rotation symmetric Boolean functions have been found in examples of Boolean functions that exceed the bent concatenation bound for odd number of variables. This has sparked the interest of researchers. Members of this subclass of rotation symmetric Boolean functions are known as dihedral symmetric Boolean functions. They are useful, among other things, in the design of fast hashing algorithms with strong cryptographic properties.

In this work we give an explicit representation of generators of short cycles of monomial rotation symmetric Boolean functions, and we use such representation to count the number of short cycles. We present a study of exponential sums of Boolean functions that are fixed under the action of the Dihedral group and a method to show that sequences of exponential sums of some families of Dihedral invariant Boolean functions are C-finite sequences.