Involutions of Finite Fields Obtained From Binomials of the Form $x^m(x^{\frac{q-1}{2}}+a)$

Lillian González-Albino,
lillian.gonzalez2@upr.edu
Department of Mathematics, UPR-RP.

THESIS
DEPARTMENT OF
MATHEMATICS

December 3, 2021

Abstract

Permutations of finite fields $\mathbb{F}_q$ have many applications ranging from cryptography and combinatorics to the theory of computation. In many of these applications, a permutation and its inverse are stored in memory. A good option to reduce the memory footprint is to generate the permutation with a polynomial at the time of implementation. A better option is to use a permutation polynomial that is its own inverse, called an involution. In applications to cryptography, the number of fixed points is correlated with its cryptographic properties.

In 2018, Zheng et al. characterized involutions of the form $x^m h(x^s)$ over $\mathbb{F}_q$, however they did not provide results on their fixed points. In 2017, Castro et al. gave explicit formulas for monomial involutions of $\mathbb{F}_q$ and their fixed points. The next simplest polynomials to implement would be the binomials.

The goal of this work is to characterize involutions of the form $x^m(x^{\frac{q-2}{2}}+a)$ of $\mathbb{F}_q$. We present explicit formulas for obtaining these involutions with a prescribed number of fixed points.