On a Class of Permutation Polynomials over Finite Feilds

Francis Castro
Jose Ortiz
Christian A. Rodríguez
Ivelisse Rubio
Alex D. Santos
University of Puerto Rico, Rio Piedras
Department of Computer Science

Abstract

A polynomial $f(x)$ defined over a set A is called a **permutation polynomial** if $f(x)$ acts as a permutation over the elements of A. We study the coefficients a and b that make polynomials of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ be permutation polynomials over the finite field $\mathbb{F}_p$, $a, b \in \mathbb{F}_p^{\times}$. We show that this family of polynomials is rich in permutations, and that the amount of permutation polynomials for any q is divisible by 6. Our approach in studying $F_{a,b}(x)$ is to use the division algorithm to consider $x = \alpha^n$ where $n = 6k+r, r = 0, ..., 5$. If $F_{a,b}(x)$ is a permutation, this partitions $\mathbb{F}_q^{\times}$ into 6 classes: $F_{a,b}(\alpha^{6k+r})$ for $r = 0, ..., 5$ each with $\frac{(q-1)}{6}$ elements. We also conjecture that, given a finite field F_q, the number of permutation polynomials of the form $G_{a,b}(x) = x^{\frac{q+1}{2}} + ax^{\frac{q+d-1}{d}} + x$ is divisible by d if d is even.