Ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields

Daniel Panario
School of Mathematics and Statistics, Carleton University
e-mail: daniel@math.carleton.ca

May 11, 2019

Abstract

Let $\mathbb{F}_q$ be the finite field of q elements, q a prime power. If $f : \mathbb{F}_q \to \mathbb{F}_q$ induces a bijection, f is a *permutation polynomial*; if f is monic, $f(0) = 0$, and, when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero, f is in *normalized* form. Normalized permutation polynomials are known exhaustively up to degree six.

For $a \in \mathbb{F}_q^*$, the *difference map* of f is defined as $\Delta_{f,a}(x) = f(x+a) - f(x)$. This map plays a central role in differential cryptanalisis. To resist linear and differential cryptanalysis, we want permutations functions f such that $|\Delta_{f,a}^{-1}(b)|$ is low for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We define $n_k(f)$ as the number of pairs (a, b) such that $f(x+a) - f(x) = b$ has exactly k solutions. The vector $[n_0(f), \ldots, n_q(f)]$ is the *spectrum* vector of the difference map of f. The *deficiency* of f is $D(f) = n_0(f)$; it measures how close the $\Delta_{f,a}$'s are to be surjective. The *(weighted) ambiguity* of f is $A(f) = \sum_{0 \le k \le n} n_k(f) \binom{k}{2}$; it measures how close the $\Delta_{f,a}$'s are to be injective.

After introducing these concepts and related topics, we give exact formulas for the differential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

Joint work with Daniel Santana (Federal University of Santa Catarina, Brazil) and Qiang Wang (Carleton University, Canada)