

Permutation polynomials over finite fields

Daniele Bartoli

UNIVERSITÀ DEGLI STUDI DI PERUGIA - DIPARTIMENTO DI MATEMATICA E INFORMATICA

Abstract

Let $q = p^h$ be a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial (PP) if it is a bijection of the finite field \mathbb{F}_q into itself. On the one hand, each permutation of \mathbb{F}_q can be expressed as a polynomial over \mathbb{F}_q . On the other hand, particular, simple structures or additional extraordinary properties are usually required by applications of PPs in other areas of mathematics and engineering, such as cryptography, coding theory, or combinatorial designs. Permutation polynomials meeting these criteria are usually difficult to find.

A standard approach to the problem of deciding whether a polynomial $f(x)$ is a PP is the investigation of the plane algebraic curve

$$\mathcal{C}_f : \frac{f(x) - f(y)}{x - y} = 0;$$

in fact, f is a PP over \mathbb{F}_q if and only if \mathcal{C}_f has no \mathbb{F}_q -rational point (a, b) with $a \neq b$.

In this talk, we will see applications of the above criterion to classes of permutation polynomials, complete permutation polynomials, exceptional polynomials, Carlitz rank problems, the Carlitz conjecture.

Keywords: Permutation polynomials; algebraic curves