Permutation Polynomials over Finite Fields

Omar Kihel
Department of Mathematics
Brock University
Ontario, Canada L2S 3A1
okihel@brocku.ca

January 24, 2014

Abstract

Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if the induced map $f : \mathbb{F}_q \to \mathbb{F}_q$ is one to one. The study of permutation polynomials goes back to Hermite for $\mathbb{F}_p$ and Dickson for $\mathbb{F}_q$. The interest in permutation polynomials increased in part because of their applications in cryptography and coding theory. Despite the interest of numerous people in the subject, characterizing permutation polynomials and finding new families of permutation polynomials remain open questions. We will introduce the permutation polynomials over finite fields and talk about some cryptographical applications. We will outline what is known about the permutation polynomials and show some known families of permutation polynomials. This first part of the talk is accessible to undergraduate students.

In the second part of this talk, we give some new results that I obtained with my collaborator Prof. M. Ayad. Permutation monomials are completely understood, however permutation binomials are not well understood. we will prove in particular that if $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in {\mathbb{F}_p}^*$, then $p - 1 \leq (d-1)d$, where $d = \gcd(n - m, p - 1)$, and that this bound of p in term of d only, is sharp, which improve certain results of Masuda and Zieve, Wan, and Turnwald. We show as well, that binomials of certain types

over $\mathbb{F}_q$ do not exist, and how to obtain in certain cases a new permutation binomial over a subfield of $\mathbb{F}_q$ from a permutation binomial over $\mathbb{F}_q$.