Low-degree planar polynomials over finite fields of characteristic two

Daniele Bartoli

Università degli Studi di Perugia - Dipartimento di Matematica e Informatica

(Joint work with Kai-Uwe Schmidt)

Abstract

Planar functions are mappings from a finite field $\mathbb{F}_q$ to itself with an extremal differential property. Such functions give rise to finite projective planes and other combinatorial objects. There is a subtle difference between the definitions of these functions depending on the parity of q and we consider the case that q is even. We classify polynomials of degree at most $q^{1/4}$ that induce planar functions on $\mathbb{F}_q$, by showing that such polynomials are precisely those in which the degree of every monomial is a power of two. As a corollary we obtain a complete classification of exceptional planar polynomials, namely polynomials over $\mathbb{F}_q$ that induce planar functions on infinitely many extensions of $\mathbb{F}_q$. The proof strategy is to study the number of $\mathbb{F}_q$-rational points of an algebraic curve attached to a putative planar function. Our methods also give a simple proof of a new partial result for the classification of almost perfect nonlinear functions.