On the Cycle Structure of Permutation Polynomials of Shape $x^t + \gamma\,\mathrm{Tr}_{q^n/q}(x^k)$

Daniel Gerike

Otto-von-Guericke University of Magdeburg

(Joint work with Gohar M. Kyureghyan — University of Rostock)

Abstract

The cycle decomposition of a permutation contains information about its algebraic and combinatorial properties, e. g. its order and parity. Much of that information is retained in its cycle structure. A central challenge in the study of permutations over finite fields is finding connections between its polynomial representation and its combinatorial properties. Determining the cycle structure of a permutation polynomial gives insight into this problem.

A class of permutation polynomials, whose properties need to be better understood is the class of permutation polynomials of shape $X^t + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$ over F_{q^n}, where $\gamma \in \mathbb{F}_{q^n}^*$ and $1 \le t, k \le q^n - 1$. These permutation polynomials are interesting, because they have a simple algebraic structure and because they depend on both the additive and the multiplicative structure of the finite field $\mathbb{F}_{q^n}$. Further, these permutation polynomials also belong to a larger class, where instead of $\mathrm{Tr}_{q^n/q}(X^k)$ any map $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ can be used.

In this talk we take a look at the known infinite families of permutation polynomials of shape $X^t + \gamma\,\mathrm{Tr}_{q^n/q}(X^k)$. Among others we determine the cycle structure of permutations $x + \gamma\,\mathrm{Tr}_{q^2/q}(x^{2q-1})$ over $\mathbb{F}_{q^2}$, where $q \equiv -1 \pmod 3$, $\gamma \in \mathbb{F}_{q^2}$ and $\gamma^3 = -\frac{1}{27}$.

Keywords: permutation polynomial, cycle structure, compositional inverse, switching construction, sparse polynomials over finite fields, subspaces