On the complete characterization of a class of permutation trinomials in characteristic five

Burcu Gülmez Temür
Atılım University, Turkey

30th Applications of Computer Algebra - ACA 2025

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. A polynomial $g(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_q$ if $g(x)$ is a bijection of $\mathbb{F}_q$.

Due to their simple algebraic structure and extraordinary properties, there has been a great interest in permutation polynomials with a few terms, such as binomials or trinomials. Permutation polynomials are also very important in terms of their applications in areas such as cryptography, coding theory and combinatorial designs. As far as we know, the studies on permutation polynomials go back to the work done by Dickson and Hermite (see, [2] and [4]). In this paper, we address an open problem posed by Bai and Xia in [1]. We study polynomials of the form $f(x) = x^{4q+1} + \lambda_1 x^{5q} + \lambda_2 x^{q+4}$ over the finite field $\mathbb{F}_{5^k}$, which are not quasi-multiplicative equivalent to any of the known permutation polynomials in the literature. We find necessary and sufficient conditions on $\lambda_1, \lambda_2 \in \mathbb{F}_{5^k}$ so that $f(x)$ is a permutation monomial, binomial, or trinomial of $\mathbb{F}_{5^{2k}}$. This is a collaborated work done by Markus Grassl, Ferruh Özbudak, Buket Özkaya and B.G.T.

References

[1] Bai T., Xia Y., A new class of permutation trinomials constructed from Niho exponents, Cryptogr. Commun. 10, 1023–1036 (2018).
[2] Dickson, L.E., The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. Math. 11, 65–120 (1896).
[3] Grassl, M., Özbudak, F., Özkaya, B., Gülmez Temür, B., Complete characterization of a class of permutation trinomials in characteristic five. Cryptogr. Commun. 16, 825–841 (2024).
[4] Hermite, Ch., Sur les fonctions de sept lettres, C.R. Acad. Sci. Paris 57, 750–757 (1863).