A Carlitz type result for linearized polynomials

Giuseppe Marino

Università degli Studi della Campania “Luigi Vanvitelli”

(Joint work with B. Csajbók and O. Polverino)

Let $F_{q^n}$ denote the finite field of $q^n$ elements where $q = p^h$ for some prime $p$. Every function $f : F_{q^n} \to F_{q^n}$ can be given uniquely as a polynomial with coefficients in $F_{q^n}$ and of degree at most $q^n - 1$. The function $f$ is $F_{q^n}$-linear if and only if it is represented by a $q$-polynomial, that is, $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, with coefficients in $F_{q^n}$. Such polynomials are also called linearized. In the set of $q$-polynomials over $F_{q^n}$ it is possible to define an equivalence relation. Two $F_{q^n}$-linear polynomials $f(x)$ and $h(x)$ of $F_{q^n}[x]$ are equivalent if the two graphs $G_f := \{(x, f(x)) : x \in F_{q^n}\} \subset AG(2, q^n)$ and $G_h$ are equivalent under the action of the group $\Gamma L(2, q^n)$, i.e. if there exists an element $\varphi \in \Gamma L(2, q^n)$ such that $G_{\varphi f} = G_h$.

In this talk we will consider the following question: what can be said about two $q$-polynomials $f$ and $g$ over $F_{q^n}$ if they satisfy

$$\text{Im} \left( \frac{f(x)}{x} \right) = \text{Im} \left( \frac{g(x)}{x} \right),$$

where $\text{Im} (f(x)/x) := \{f(x)/x : x \in F_{q^n}^*\}$. This problem can be investigated up to equivalence. Also, it is related to the study of the directions determined by an additive function and to the $\Gamma L(2, q^n)$-equivalence of $F_{q^n}$-linear sets of rank $n$ of $\text{PG}(1, q^n)$.

For a given $q$-polynomial $f = \sum_{i=0}^{n-1} a_i x^{q^i}$, the equality (1) clearly holds with $g(x) = f(\lambda x)/\lambda$ for each $\lambda \in F_{q^n}^*$. A less obvious choice when (1) holds is when $g(x) = \hat{f}(\lambda x)/\lambda$, where $\hat{f}(x) := \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}$ is the adjoint of $f$ w.r.t. the symmetric non-degenerate bilinear form defined by $\langle x, y \rangle = \text{Tr}(xy)$ ([1], [2]).

For $n = 2$, there is a unique equivalence class of $q$-polynomials, with maximum field of linearity $F_q$, corresponding to $x^q$. For $n = 3$ there are two non-equivalent classes and they correspond to the classical examples: $\text{Tr}(x)$ and $x^q$ ([3]). By [2], for $n \leq 4$, the only solutions for $g$ in Problem (1) are the trivial ones, i.e. either $g(x) = f(\lambda x)/x$ or $g(x) = \hat{f}(\lambda x)/x$ ([2]).

For the case $n = 5$, we have the following result.
Theorem 1. Let $f(x)$ and $g(x)$ be two $q$-polynomials over $\mathbb{F}_q^5$, with maximum field of linearity $\mathbb{F}_q$, such that $\text{Im}(f(x)/x) = \text{Im}(g(x)/x)$. Then either there exists $\varphi \in \Gamma L(2, q^5)$ such that $f_{\varphi}(x) = \alpha x^{q^i}$ and $g_{\varphi}(x) = \beta x^{q^j}$ with $\frac{q^i}{q-1} = \frac{q^j}{q-1}$ for some $i, j \in \{1, 2, 3, 4\}$, or there exists $\lambda \in \mathbb{F}_q^*$, such that $g(x) = f(\lambda x)/\lambda$ or $g(x) = \hat{f}(\lambda x)/\lambda$.

References

