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 $\mathbb{F}_{q^n}$ denote the finite field of q^n elements where $q = p^h$ for some prime p. Every function $f \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ can be given uniquely as a polynomial with coefficients in $\mathbb{F}_{q^n}$ and of degree at most $q^n - 1$. The function f is $\mathbb{F}_q$-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 $\mathbb{F}_{q^n}$. Such polynomials are also called *linearized*. In the set of q-polynomials over $\mathbb{F}_{q^n}$ it is possible to define an equivalence relation. Two $\mathbb{F}_q$-linear polynomials $f(x)$ and $h(x)$ of $\mathbb{F}_{q^n}[x]$ are *equivalent* if the two graphs $\mathcal{G}_f := \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\} \subset \mathrm{AG}(2, q^n)$ and $\mathcal{G}_h$ are equivalent under the action of the group $\Gamma\mathrm{L}(2, q^n)$, i.e. if there exists an element $\varphi \in \Gamma\mathrm{L}(2, q^n)$ such that $\mathcal{G}_f^{\varphi} = \mathcal{G}_h$.

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

$$Im\left(\frac{f(x)}{x}\right) = Im\left(\frac{g(x)}{x}\right), \tag{1}$$

where $Im\,(f(x)/x) := \{f(x)/x \colon x \in \mathbb{F}_{q^n}^*\}$. 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 $\mathrm{P}\Gamma\mathrm{L}(2, q^n)$-equivalence of $\mathbb{F}_q$-linear sets of rank n of $\mathrm{PG}(1, q^n)$.

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 $\lambda \in \mathbb{F}_{q^n}^*$. 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 $\langle x, y\rangle = \mathrm{Tr}(xy)$ ([1], [2]).

For $n = 2$, there is a unique equivalence class of q-polynomials, with maximum field of linearity $\mathbb{F}_q$, corresponding to x^q. For $n = 3$ there are two non-equivalent classes and they correspond to the classical examples: $\mathrm{Tr}(x)$ 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 $Im\,(f(x)/x) = Im\,(g(x)/x)$. Then either there exists $\varphi \in \Gamma\mathrm{L}(2, q^5)$ such that $f_\varphi(x) = \alpha x^{q^i}$ and $g_\varphi(x) = \beta x^{q^j}$ with $\alpha^{\frac{q^5-1}{q-1}} = \beta^{\frac{q^5-1}{q-1}}$ for some $i, j \in \{1, 2, 3, 4\}$, or there exists $\lambda \in \mathbb{F}^*_{q^5}$ such that $g(x) = f(\lambda x)/\lambda$ or $g(x) = \hat{f}(\lambda x)/\lambda$.*

References

[1] D. Bartoli, M. Giulietti, G. Marino and O. Polverino: Maximum scattered linear sets and complete caps in Galois spaces, Combinatorica **38** (2018), to appear. DOI: 10.1007/s00493-016-3531-6.

[2] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$, J. Combin. Theory Ser. A **157** (2018), 402–426.

[3] M. Lavrauw and G. Van de Voorde: On linear sets on a projective line, Des. Codes Cryptogr. **56** (2010), 89–104.