Linearized Polynomials and Their Adjoints, and Some Connections to Linear Sets and Semifields

Gary McGuire and John Sheekey(✉)

UCD School of Mathematics and Statistics, University College Dublin, Dublin, Ireland
{gary.mcguire,john.sheekey}@ucd.ie

For a q-linearized polynomial function L on a finite field, we give a new short proof of a known result, that $L(x)/x$ and $L^*(x)/x$ have the same image, where $L^*(x)$ denotes the adjoint of L. We give some consequences for semifields, recovering results first proved by Lavrauw and Sheekey. We also give a characterization of planar functions.

1 Introduction

Throughout this paper we let p be a prime number, let $q = p^r$ and let $\mathbb{F}_{q^n}$ denote a finite field with q^n elements, where n is a positive integer.

Any function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ can be expressed uniquely as a polynomial function (with coefficients in $\mathbb{F}_{q^n}$) of degree less than q^n. This is because there are $(q^n)^{q^n}$ such polynomials, they are distinct as functions, and this is also the total number of functions. We call this polynomial the reduced form of the function.

A polynomial in $\mathbb{F}_{q^n}[x]$ is called a permutation polynomial (PP) if it its reduced form induces a bijective function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$.

Thinking of $\mathbb{F}_{q^n}$ as an n-dimensional vector space over $\mathbb{F}_q$, a polynomial of the form

$$a_0 x + a_1 x^q + a_2 x^{q^2} + \cdots + a_{n-1} x^{q^{n-1}} \tag{1}$$

with $a_i \in \mathbb{F}_{q^n}$ induces an $\mathbb{F}_q$-linear function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$. Conversely, any $\mathbb{F}_q$-linear function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ can be written in this form, because there are $(q^n)^n$ such polynomials, they are distinct as functions, and this is also the total number of $\mathbb{F}_q$-linear functions. A polynomial of the form (1) is called a q-linearized polynomial. This is already in reduced form. In this paper, when we use the term q-linearized polynomial, we mean the function $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ that is induced by the polynomial.

Let Tr denote the absolute trace map $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_p$ defined by

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{rn-1}}.$$

Let tr denote the relative trace map $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ defined by

$$tr(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

J. C. Bajard and A. Topuzoğlu (Eds.): WAIFI 2020, LNCS 12542, pp. 37–41, 2021.
https://doi.org/10.1007/978-3-030-68869-1_2

The *adjoint* of $L(x) = a_0x + a_1x^q + a_2x^{q^2} + \cdots + a_{n-1}x^{q^{n-1}}$ is defined to be

$$L^*(x) = a_0x + a_1^{q^{n-1}}x^{q^{n-1}} + a_2^{q^{n-2}}x^{q^{n-2}} + \cdots + a_{n-1}^q x^q.$$

The adjoint has the property that $tr(L(u)v) = tr(uL^*(v))$ for all $u, v \in \mathbb{F}_{q^n}$. This property implies that $\mathrm{Tr}(L(u)v) = \mathrm{Tr}(uL^*(v))$ for all $u, v \in \mathbb{F}_{q^n}$.

We introduce some notation. Let

$$V(L) = \left\{-a \in \mathbb{F}_{q^n} : L(x) + ax \text{ is a PP } \right\}$$

and let

$$I(L) = \left\{\frac{L(z)}{z} : z \in \mathbb{F}_{q^n}, z \neq 0\right\}.$$

The following theorem was first proved in Lemma 2.6 of [2].

Theorem 1. *Let $L(x)$ be a q-linearized polynomial. Then $I(L) = I(L^*)$ and $V(L) = V(L^*)$.*

In this paper we will provide a new proof of this fact. In addition to giving an alternative viewpoint on this result, this approach may be of use towards studying the following problem.

Open Question. Let $L(x)$ be a q-linearized polynomial. For what other q-linearized polynomials $M(x)$ does it hold that $I(L) = I(M)$ and $V(L) = V(M)$?

This question has been addressed in [3]; in particular it has been shown that for $n \leq 5$, and $L(x)$ *not* a monomial, then $I(L) = I(M)$ if and only if $L(x) = M(\lambda x)/\lambda$ or $L^*(x) = M(\lambda x)/\lambda$ for some $\lambda \in \mathbb{F}_{q^n}^\times$. If $L(x) = x^{q^i}$ and $M(x) = x^{q^j}$ then $I(L) = I(M)$ if and only if $(i, n) = (j, n)$. The general case remains an open problem.

Motivation for this question stems from the study of *linear sets*, which are sets of points on a projective line $\mathrm{PG}(1, q^n)$. The set $U_L = \{(x, L(x)) : x \in \mathbb{F}_{q^n}^\times\}$ defines a set $\mathcal{L}_L$ of points on the projective line $\mathrm{PG}(1, q^n)$ in a natural way. Then it is straightforward to see that $\mathcal{L}_L = \mathcal{L}_M$ if and only if $I(L) = I(M)$. This problem, which has been studied in [4,5], has applications in the study of MRD codes, as well as for semifields, which we will see in Sect. 3.

2 Alternative Proof of Main Theorem

Let ζ be a primitive complex p-th root of unity. The additive characters of $\mathbb{F}_{q^n}$ may be written

$$\chi_\alpha(x) = \zeta^{\mathrm{Tr}(\alpha x)},$$

one character for each $\alpha \in \mathbb{F}_{q^n}$.

The following is a well known characterization of PPs based on additive characters (Theorem 7.7 in [8]).

Theorem 2. *A polynomial $P(x) \in \mathbb{F}_{q^n}[x]$ is a permutation polynomial if and only if*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi(P(x)) = 0$$

for every nontrivial additive character χ of $\mathbb{F}_{q^n}$.

We will use the following well known fact (Theorem 7.9 in [8]).

Lemma 1. *If $L(x) \in \mathbb{F}_{q^n}[x]$ is a q-linearized polynomial, then $L(x)$ is a PP on $\mathbb{F}_{q^n}$ if and only if the only solution in $\mathbb{F}_{q^n}$ of $L(x) = 0$ is $x = 0$.*

We use this characterisation in order to provide a new proof of the Main Theorem.

Theorem 3. *Let $L(x)$ be a q-linearized polynomial. Then $I(L) = I(L^*)$ and $V(L) = V(L^*)$.*

Proof. We will show that both $I(L)$ and $I(L^*)$ are equal to the complement of $V(L)$. In part (i) we show that $-a \in I(L)$ if and only if $L(x) + ax$ is not a PP, and in part (ii) we will show that $-a \in I(L^*)$ if and only if $L(x) + ax$ is not a PP.

(i) Note that $L(x) + ax$ maps 0 to 0, and so $L(x) + ax$ is a PP if and only if $-a \notin Im(L(x)/x)$ by Lemma 1. This proves that

$$I(L) = \left\{ -a \in \mathbb{F}_{q^n} : L(x) + ax \text{ is not a PP } \right\}$$

which shows that $I(L)$ is equal to the complement of $V(L)$.

(ii) By Theorem 2, $L(x) + ax$ is a PP if and only if

$$\sum_{x \in \mathbb{F}_{q^n}} \chi(L(x) + ax) = 0$$

for all nontrivial additive characters χ, or equivalently, if and only if

$$\sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(\alpha(L(x)+ax))} = 0$$

for all nonzero $\alpha \in \mathbb{F}_q$. But

$$\sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(\alpha(L(x)+ax))} = \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(L^*(\alpha)x+\alpha ax)} = \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}((L^*(\alpha)+\alpha a)x)}$$

which is 0 if and only if $L^*(\alpha) + \alpha a \neq 0$. In other words, $L(x) + ax$ is a PP if and only if $L^*(\alpha) + \alpha a \neq 0$ for all nonzero $\alpha \in \mathbb{F}_{q^n}$. Thus $L(x) + ax$ is a PP if and only if $-a \notin Im(L^*(x)/x)$. This proves that $I(L^*)$ is equal to the complement of $V(L)$.

We have shown that both $I(L)$ and $I(L^*)$ are equal to the complement of $V(L)$, and it follows that $I(L) = I(L^*)$. Applying this to L^* instead of L shows that both $I(L)$ and $I(L^*)$ are equal to the complement of $V(L^*)$. Therefore $V(L) = V(L^*)$, and $L(x) + ax$ is a PP if and only if $L^*(x) + ax$ is a PP.

3 Application to Semifields

We now present an alternative proof of a result of Lavrauw and Sheekey [6].

A finite *semifield* is a nonassociative division algebra of finite dimension over $\mathbb{F}_q$. There are many constructions for semifields, many of which use q-linearized polynomials. In [6] a particular class of semifields were studied, namely those of *BEL-rank two*. These are those semifields whose multiplication can be written in the form

$$x \circ y = xL(y) - M(x)y$$

for some q-linearized polynomials $L(x)$ and $M(x)$. As noted and studied in [7,9], the condition for the pair (L, M) to defines a semifield is equivalent to the condition $I(L) \cap I(M) = \emptyset$, and equivalent to the condition that the sets of points $\mathcal{L}_L$ and $\mathcal{L}_M$ in $\mathrm{PG}(1, q^n)$ are disjoint. In [6] it was shown that if the pair (L, M) define a semifield, then so do the pairs (L^*, M), (L, M^*), and (L^*, M^*) (as well as the obvious fact that (M, L) also defines a semifield, the dual or opposite semifield). The proof of this was an application of the *switching* operation defined in [1]. In fact we can now see that this is an immediate consequence of the main theorem.

Corollary 1. *Let $L(x)$ and $M(x)$ be q-linearized polynomials. Suppose $I(L)$ and $I(M)$ are disjoint, so that $xL(y) - M(x)y$ defines a semifield multiplication law. Then*

1. *$xL^*(y) - M(x)y$ defines a semifield,*
2. *$xL^*(y) - M^*(x)y$ defines a semifield,*
3. *$xL(y) - M^*(x)y$ defines a semifield.*

Proof. If $I(L) \cap I(M) = \emptyset$ then $x * y = xL(y) - M(x)y$ defines a semifield multiplication law. By Theorem 3 we have $I(L) = I(L^*)$ and $I(M) = I(M^*)$. Since $I(L) \cap I(M) = \emptyset$ we also get $I(L^*) \cap I(M) = \emptyset$ and $I(L^*) \cap I(M^*) = \emptyset$ and $I(L) \cap I(M^*) = \emptyset$. The result follows.

Note that the main theorem is in fact stronger than the result of [6], in which it was shown that if $I(L)$ and $I(M)$ are disjoint, then (for example) $I(L^*)$ and $I(M)$ are disjoint, which does not necessarily imply that $I(L) = I(L^*)$.

4 A Criterion for Planarity

Assume q is odd. A function $f : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ is said to be *planar* if the functions $x \mapsto f(x + a) - f(x)$ are bijective for all nonzero $a \in \mathbb{F}_{q^n}$. The term PN (perfect nonlinear) is also used instead of the word 'planar'.

Sometimes a polynomial $xL(x)$ will be planar, where $L(x)$ is a q-linearized polynomial. For example, x^2 is planar. We present a criterion for the planarity of $xL(x)$.

Theorem 4. *Let $L(x)$ be a q-linearized polynomial. The polynomial $xL(x)$ is planar if and only if $L^*(bx) + bL(x)$ is a PP for all nonzero $b \in \mathbb{F}_{q^n}$.*

Proof. First,

$$\begin{aligned} xL(x) \text{ is PN} &\iff (x+u)L(x+u) - xL(x) \text{ is a PP for all nonzero } u \\ &\iff uL(x) + xL(u) + uL(u) \text{ is a PP for all nonzero } u \\ &\iff uL(x) + xL(u) \text{ is a PP for all nonzero } u. \end{aligned}$$

By Theorem 2, $uL(x) + xL(u)$ is a PP if and only if

$$\sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(b(uL(x)+xL(u)))} = 0$$

for all nonzero $b \in \mathbb{F}_{q^n}$. However

$$\sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(buL(x)+bxL(u))} = \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{Tr}(L^*(bu)x+bxL(u))}$$

so $uL(x) + xL(u)$ is a PP if and only if $L^*(bu) + bL(u) \neq 0$ for all nonzero b. By Lemma 1 we are done.

References

1. Ball, S., Ebert, G., Lavrauw, M.: A geometric construction of finite semifields. J. Algebra **311**, 117–129 (2007)
2. Bartoli, D., Giulietti, M., Marino, G., Polverino, O.: Maximum scattered linear sets and complete caps in Galois spaces. Combinatorica **38**, 255–278 (2018)
3. Csajbók, B., Marino, G., Polverino, O.: A Carlitz type result for linearized polynomials. Ars Math. Contemp. **16**(2), 585–608 (2019)
4. Csajbók, B., Marino, G., Polverino, O.: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$. J. Comb. Theory Ser. A **157**, 402–426 (2018)
5. Csajbók, B., Zanella, C.: On the equivalence of linear sets. Des. Codes Cryptogr. **81**, 269–281 (2016)
6. Lavrauw, M., Sheekey, J.: The BEL-rank of finite semifields. Des. Codes Cryptogr. **84**, 345–358 (2017)
7. Sheekey, J., Van de Voorde, G.: Rank-metric codes, linear sets, and their duality. Des. Codes Cryptogr. **88**, 655–675 (2020)
8. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley (1983)
9. Zini, G., Zullo, F.: On the intersection problem for linear sets in the projective line. arXiv:2004.09441