SWITCHINGS OF SEMIFIELD MULTIPLICATIONS

XIANG-DONG HOU, FERRUH ÖZBUDAK AND YUE ZHOU

Abstract. Let $B(X, Y)$ be a polynomial over $\mathbb{F}_{q^n}$ which defines an $\mathbb{F}_q$-bilinear form on the vector space $\mathbb{F}_{q^n}$, and let ξ be a nonzero element in $\mathbb{F}_{q^n}$. In this paper, we consider for which $B(X, Y)$, the binary operation $xy + B(x, y)\xi$ defines a (pre)semifield multiplication on $\mathbb{F}_{q^n}$. We prove that this question is equivalent to finding q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ such that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$. For $n \leq 4$, we present several families of $L(X)$ and we investigate the derived (pre)semifields. When q equals a prime p, we show that if $n > \frac{1}{2}(p-1)(p^2-p+4)$, $L(X)$ must be a_0X for some $a_0 \in \mathbb{F}_{p^n}$ satisfying $\mathrm{Tr}_{q^n/q}(a_0) \neq 0$. Finally, we include a natural connection with certain cyclic codes over finite fields, and we apply the Hasse-Weil-Serre bound for algebraic curves to prove several necessary conditions for such kind of $L(X)$.

1. Introduction

A *semifield* $\mathbb{S}$ is an algebraic structure satisfying all the axioms of a skewfield except (possibly) the associativity. In other words, it satisfies the following axioms:

(S1) $(\mathbb{S}, +)$ is a group, with identity element 0;

(S2) $(\mathbb{S} \setminus \{0\}, *)$ is a quasigroup;

(S3) $0 * a = a * 0 = 0$ for all a;

(S4) The left and right distributive laws hold, namely for any $a, b, c \in \mathbb{S}$,

$$(a + b) * c = a * c + b * c,$$
$$a * (b + c) = a * b + a * c;$$

(S5) There is an element $e \in \mathbb{S}$ such that $e * x = x * e = x$ for all $x \in \mathbb{S}$.

A finite field is a trivial example of a semifield. Furthermore, if $\mathbb{S}$ does not necessarily have a multiplicative identity, then it is called a *presemifield*. For a presemifield $\mathbb{S}$, $(\mathbb{S}, +)$ is necessarily abelian [17]. A semifield is not necessarily commutative

Date: October 22, 2018.

2000 *Mathematics Subject Classification.* 11T55, 12E20, 12K10, 14H05, 94B15.

Key words and phrases. cyclic code, finite field, linearized polynomial, semifield, the Hasse-Weil-Serre bound.

Xiang-dong Hou is with the Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, USA; e-mail: xhou@usf.edu; research partially supported by NSA grant H98230-12-1-0245.

Ferruh Özbudak is with the Department of Mathematics and the Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Bulvarı No. 1, 06800, Ankara, Turkey; e-mail: ozbudak@metu.edu.tr; research partially supported by TUBİTAK under Grant no. TBAG-112T011.

Yue Zhou is with the College of Science, National University of Defense Technology, Yanwachi Street No. 137, 410073, Changsha, China; e-mail: yue.zhou.ovgu@gmail.com. This work is partially supported by the National Natural Science Foundation of China (No. 61272484) and the National Basic Research Program of China (No. 2013CB338002).

or associative. However, by Wedderburn's Theorem [27], in the finite case, associativity implies commutativity. Therefore, a non-associative finite commutative semifield is the closest algebraic structure to a finite field. We refer to [18] for a recent and comprehensive survey.

The first family of non-trivial semifields was constructed by Dickson [7] more than a century ago. In [17], Knuth showed that the additive group of a finite semifield $\mathbb{S}$ is an elementary abelian group, and the additive order of the nonzero elements in $\mathbb{S}$ is called the *characteristic* of $\mathbb{S}$. Hence, any finite semifield can be represented by $(\mathbb{F}_q, +, *)$, where q is a power of a prime p. Here $(\mathbb{F}_q, +)$ is the additive group of the finite field $\mathbb{F}_q$ and $x * y$ can be written as $x * y = \sum_{i,j} a_{ij} x^{p^i} y^{p^j}$, which forms a mapping from $\mathbb{F}_q \times \mathbb{F}_q$ to $\mathbb{F}_q$.

Geometrically speaking, there is a well-known correspondence, via coordinatisation, between (pre)semifields and projective planes of Lenz-Barlotti type V.1, see [5, 13]. In [1], Albert showed that two (pre)semifields coordinatise isomorphic planes if and only if they are isotopic.

Definition 1.1. *Let $\mathbb{S}_1 = (\mathbb{F}_p^n, +, *)$ and $\mathbb{S}_2 = (\mathbb{F}_p^n, +, \star)$ be two presemifields. If there exist three bijective linear mappings $L, M, N : \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that*

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_p^n$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are called isotopic*, and the triple (M, N, L) is called an* isotopism *between $\mathbb{S}_1$ and $\mathbb{S}_2$.*

Let $\mathbb{P} = (\mathbb{F}_{p^n}, +, *)$ be a presemifield. We can obtain a semifield from it via isotopisms in several ways, such as the well known Kaplansky's trick (see [18, page 2]). The following method was recently given by Bierbrauer [2]. Define a new multiplication $\star$ by the rule

$$x \star y := B^{-1}(B_1(x) * y), \tag{1.1}$$

where $B(x) := 1 * x$ and $B_1(x) * 1 = 1 * x$. We have $x \star 1 = B^{-1}(B_1(x) * 1) = B^{-1}(1 * x) = x$ and $1 \star x = B^{-1}(B_1(1) * x) = B^{-1}(1 * x) = x$, thus $(\mathbb{F}_{p^n}, +, \star)$ is a semifield with identity 1. In particular, when $\mathbb{P}$ is commutative, B_1 is the identity mapping.

Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ be a semifield. The subsets

$$N_l(\mathbb{S}) = \{a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S}\},$$
$$N_m(\mathbb{S}) = \{a \in \mathbb{S} : (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathbb{S}\},$$
$$N_r(\mathbb{S}) = \{a \in \mathbb{S} : (x * y) * a = x * (y * a) \text{ for all } x, y \in \mathbb{S}\},$$

are called the *left, middle* and *right nucleus* of $\mathbb{S}$, respectively. It is easy to check that these sets are finite fields. The subset $N(\mathbb{S}) = N_l(\mathbb{S}) \cap N_m(\mathbb{S}) \cap N_r(\mathbb{S})$ is called the *nucleus* of $\mathbb{S}$. It is easy to see, if $\mathbb{S}$ is commutative, then $N_l(\mathbb{S}) = N_r(\mathbb{S})$ and $N_l(\mathbb{S}) \subseteq N_m(\mathbb{S})$, therefore $N_l(\mathbb{S}) = N_r(\mathbb{S}) = N(\mathbb{S})$. In [13], a geometric interpretation of these nuclei is discussed. The subset $\{a \in \mathbb{S} : a * x = x * a \text{ for all } x \in \mathbb{S}\}$ is called the *commutative center* of $\mathbb{S}$ and its intersection with $N(\mathbb{S})$ is called the *center* of $\mathbb{S}$.

Let G be a group and N a subgroup. A subset D of G is called a *relative difference set* with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$. We call N the *forbidden subgroup.*

Jungnickel [15] showed that every semifield $\mathbb{S}$ of order q leads to a $(q, q, q, 1)$-relative difference set D in a group G which is not necessarily abelian. Assume that $\mathbb{S}$ is commutative. If $q = p^n$ and p is odd, then G is isomorphic to the elementary abelian group C_p^{2n}; if $q = 2^n$, then $G \cong C_4^n$. (C_m is the cyclic group of order m.)

Let p be an odd prime. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called *planar*, if the mapping

$$x \mapsto f(x + a) - f(x)$$

is a permutation of $\mathbb{F}_{p^n}$ for every $a \in \mathbb{F}_{p^n}^*$. Planar functions were first defined by Dembowski and Ostrom in [6]. It is not difficult to verify that planar functions over $\mathbb{F}_{p^n}$ are equivalent to $(p^n, p^n, p^n, 1)$-relative difference sets in C_p^{2n}. Planar functions over $\mathbb{F}_{2^n}$, introduced recently in [25, 29], has a slightly different definition: A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *planar*, if the mapping

$$x \mapsto f(x + a) + f(x) + ax$$

is a permutation of $\mathbb{F}_{2^n}$ for every $a \in \mathbb{F}_{2^n}^*$. They are equivalent to $(2^n, 2^n, 2^n, 1)$-relative difference sets in C_4^n; see [29, Theorem 2.1].

Let f be a planar function over $\mathbb{F}_{q^n}$, where q is a power of prime. A *switching* of f is a planar function of the form $f + g\xi$ where g is a mapping from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and $\xi \in \mathbb{F}_{q^n}^*$. Switchings of planar functions over $\mathbb{F}_{p^n}$, where p is an odd prime, were investigated by Pott and the third author in [24]. In [29], it is proved that switchings of the planar function $f(x) = 0$ defined over $\mathbb{F}_{2^n}$ can be written as affine polynomials $\sum a_i x^{2^i} + b$, which are equivalent to $f(x)$ itself.

In the present paper, we will investigate the switchings of (pre)semifield multiplications. To be precise, we will consider when the binary operation

$$x * y = x \star y + B(x, y)\xi$$

on $\mathbb{F}_{q^n}$ defines a (pre)semifield multiplication, where $\star$ is a given (pre)semifield multiplication, $\xi \in \mathbb{F}_{q^n}^*$ and $B(x, y)$ is an $\mathbb{F}_q$-bilinear form from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ to $\mathbb{F}_q$. (One may identify $\mathbb{F}_{q^n}$ with $\mathbb{F}_q^n$, although it is not necessary.) We call $x * y$ a *switching neighbour* of $x \star y$. In particular, we will concentrate on the case in which $\star$ is the multiplication of a finite field.

In Section 2, we show that finding B such that $x * y := xy + B(x, y)\xi$ defines a (pre)semifield multiplication is equivalent to finding q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ such that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$. For $n \leq 4$, we give in Section 3 several q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ satisfying this condition and we discuss the presemifields of the corresponding switchings. In Section 4, we prove that when $q = p$ is a prime and $n > (p - 1)(p^2 - p + 4)/2$, the only $L(X)$ satisfying the above condition are those of the form βX where $\mathrm{Tr}_{p^n/p}(\beta) \neq 0$. In Section 5, we explore a connection of the q-linearized polynomials $L(X)$ satisfying the above condition with certain cyclic codes over $\mathbb{F}_q$. Finally, in Section 6 we derive several necessary conditions for the existence of the q-linearized polynomials $L(X)$ from the Hasse-Weil-Serre bound for algebraic curves over finite fields.

2. Preliminary discussion

Let $\mathrm{Tr}_{q^n/q}$ be the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. We define

$$B(x, y) := \mathrm{Tr}_{q^n/q}\Big(\sum_{i=0}^{n-1} b_i x y^{q^i}\Big), \qquad x, y \in \mathbb{F}_{q^n},$$

where $b_i \in \mathbb{F}_{q^n}$. It is easy to see that $B(x,y)$ defines an $\mathbb{F}_q$-bilinear form from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ to $\mathbb{F}_q$, and every such bilinear form can be written in this way.

In the next theorem, we consider the switchings of a finite field multiplication.

Theorem 2.1. *Let $x * y := xy + B(x,y)\xi$, where $B(x,y) := \mathrm{Tr}_{q^n/q}(\sum_{i=0}^{n-1} b_i x y^{q^i})$, $b_i \in \mathbb{F}_{q^n}$, and $\xi \in \mathbb{F}_{q^n}^*$. Then $*$ defines a presemifield multiplication on $\mathbb{F}_{q^n}$ if and only if for any $a \in \mathbb{F}_{q^n}^*$, $\mathrm{Tr}_{q^n/q}(M(a)/a) \neq -1$, where $M(X) := \xi \sum_{i=0}^{n-1} b_i X^{q^i} \in \mathbb{F}_{p^n}[X]$.*

Proof. ($\Rightarrow$) Let $x * y$ be a presemifield multiplication. Assume to the contrary that there is $a \in \mathbb{F}_{q^n}^*$ such that

$$\mathrm{Tr}_{q^n/q}(M(a)/a) = -1.$$

We consider the equation $x * a = 0$. It has a solution x if and only if there exists $u \in \mathbb{F}_q$ such that

$$xa = \xi u \quad \text{and} \tag{2.1}$$

$$B(x,a) = -u. \tag{2.2}$$

Plugging (2.1) into (2.2), we have $B(\xi u/a, a) = -u$, which means that

$$u\mathrm{Tr}_{q^n/q}\left(\xi \sum_{i=0}^{n-1} b_i a^{q^i - 1}\right) = -u,$$

i.e.

$$u\mathrm{Tr}_{q^n/q}(M(a)/a) = -u,$$

which holds for any $u \in \mathbb{F}_q$ according to our assumption. Therefore, $x * a = 0$ has a nonzero solution. It contradicts our assumption that $*$ defines a presemifield multiplication.

($\Leftarrow$) It is easy to see that the left and right distributivity of the multiplication $*$ hold. We only need to show that for any $a \neq 0$, $x * a = 0$ if and only if $x = 0$. This is achieved by reversing the first part of the proof. □

Let $x*y$ be the multiplication defined in Theorem 2.1. Then it is straightforward to verify that the presemifield $(\mathbb{F}_{q^n}, +, *)$ is isotopic to $(\mathbb{F}_{q^n}, +, \star)$, where

$$x \star y := xy + B'(x,y)$$

and $B'(x,y) = \mathrm{Tr}_{q^n/q}(\xi \sum_{i=0}^{n-1} b_i x y^{q^i})$. Therefore, we can restrict ourselves to the switchings of finite field multiplications with $\xi = 1$.

For the switchings

$$x \star y + B(x,y)\xi$$

of a (pre)semifield multiplication $\star$, it is difficulty to obtain explicit conditions on $B(x,y)$. The reason is that generally we can not explicitly write down the solution of $x \star a = \xi u$ as we did for (2.1).

Let α be an element in $\mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{q^n/q}(\alpha) = 1$. To find $M(X)$ satisfying the condition in Theorem 2.1, we only need to consider the q-linearized polynomial $L(X) := M(X) + \alpha X \in \mathbb{F}_{q^n}[X]$ such that

$$\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0 \quad \text{for all } x \in \mathbb{F}_{q^n}^*. \tag{2.3}$$

Obviously, when $L(X) = \beta X$, where $\mathrm{Tr}_{q^n/q}(\beta) \neq 0$, we have $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for every nonzero x. The question is whether there are other L's. We will give several results concerning this question throughout Sections 3 – 6.

The proof of next proposition is also straightforward.

Proposition 2.2. *Let $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$. If $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$, then the mapping $x \mapsto L(x)$ is a permutation of $\mathbb{F}_{q^n}$.*

We include several lemmas which will be used later to investigate the commutativity of presemifield multiplications.

Lemma 2.3. *Let $x*y := xy + B(x,y)$, where $B(x,y) := \mathrm{Tr}_{q^n/q}(\sum_{i=0}^{n-1} b_i x y^{q^i})$, $b_i \in \mathbb{F}_{q^n}$. Then $*$ is commutative if and only if $b_i \in \mathbb{F}_{q^{\gcd(i,n)}}$ for every $i = 0, 1, \ldots, n-1$.*

Proof. Clearly, $x*y = y*x$ if and only if $B(x,y) = B(y,x)$, i.e.

$$\mathrm{Tr}_{q^n/q}\left(\sum_{i=0}^{n-1} b_i x y^{q^i}\right) = \mathrm{Tr}_{q^n/q}\left(\sum_{i=0}^{n-1} b_i y x^{q^i}\right),$$

which means that

$$\mathrm{Tr}_{q^n/q}\left(x \sum_{i=0}^{n-1} (b_i - b_i^{q^i}) y^{q^i}\right) = 0$$

for every $x, y \in \mathbb{F}_{q^n}$. Therefore $*$ is commutative if and only if $b_i = b_i^{q^i}$ for every i. □

It is possible that a non-commutative presemifield $\mathbb{P}$ is isotopic to a commutative presemifield. We can use the next criterion given by Bierbrauer [2], as a generalization of Ganley's criterion [8], to test whether this happens.

Lemma 2.4. *A presemifield $(\mathbb{P}, +, *)$ is isotopic to a commutative semifield if and only if there is some nonzero v such that $A(v*x)*y = A(v*y)*x$, where $A : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is defined by $A(x)*1 = x$.*

Given an arbitrary presemifield multiplication, it is not easy to get the explicit expression for $A(x)$. However, we can do it for the switchings of multiplications of finite fields.

Lemma 2.5. *Let $x*y := xy + B(x,y)$ be a switching of $\mathbb{F}_{q^n}$, where $B(x,y) := \mathrm{Tr}_{q^n/q}(\sum_{i=0}^{n-1} b_i x y^{q^i})$, $b_i \in \mathbb{F}_{q^n}$. Let $A : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be such that $A(x)*1 = x$ for every $x \in \mathbb{F}_{q^n}$. Then*

$$A(x) = x + \mathrm{Tr}_{q^n/q}\left(\frac{-tx}{1 + \mathrm{Tr}_{q^n/q}(t)}\right), \tag{2.4}$$

where $t = \sum_{i=0}^{n-1} b_i$.

Proof. First, we have

$$\begin{aligned} u*1 &= u + B(u,1) \\ &= u + \mathrm{Tr}_{q^n/q}\left(\sum_{i=0}^{n-1} b_i u\right) \\ &= u + \mathrm{Tr}_{q^n/q}(tu). \end{aligned}$$

It is worth noting that $1 * 1 = 1 + \mathrm{Tr}_{q^n/q}(t) \neq 0$. Let $s := -t/(1 + \mathrm{Tr}_{q^n/q}(t))$. Replacing u by the expression in (2.4), we have

$$\begin{aligned} A(x) * 1 &= x + \mathrm{Tr}_{q^n/q}(sx) + \mathrm{Tr}_{q^n/q}\big[tx + t\mathrm{Tr}_{q^n/q}(sx)\big] \\ &= x + \mathrm{Tr}_{q^n/q}\big[s(1 + \mathrm{Tr}_{q^n/q}(t))x + tx\big] \\ &= x. \end{aligned}$$

□

3. Switchings of $\mathbb{F}_{q^n}$ for small n

In this section, we investigate the switchings of finite fields $(\mathbb{F}_{q^n}, +, \cdot)$ where $n \leq 4$.

Lemma 3.1. *Let $L(X) = a_1X^q + a_0X \in \mathbb{F}_{q^2}[X]$. Then the polynomial*

$$f(X) = \mathrm{Tr}_{q^2/q}(L(X)/X)$$

has no root in $\mathbb{F}_{q^2}^*$ if and only if the equation $x^{q-1} = y$ has no solution $x \in \mathbb{F}_{q^2}^*$ for every $y \in \mathbb{F}_{q^2}$ satisfying

$$a_1y^2 + \mathrm{Tr}_{q^2/q}(a_0)y + a_1^q = 0. \tag{3.1}$$

Proof. Let $y := x^{q-1}$, where $x \in \mathbb{F}_{q^2}^*$. Then

$$\begin{aligned} \mathrm{Tr}_{q^2/q}(L(x)/x) &= \mathrm{Tr}_{q^2/q}(a_1x^{q-1} + a_0) \\ &= \mathrm{Tr}_{q^2/q}(a_1y + a_0) \\ &= a_1^qy^q + a_1y + \mathrm{Tr}_{q^2/q}(a_0) \\ &= y^q(a_1y^2 + \mathrm{Tr}_{q^2/q}(a_0)y + a_1^q) \end{aligned}$$

since $y^{q+1} = 1$. Therefore, f has a nonzero root if and only if there exists a $(q-1)$-th power in $\mathbb{F}_{q^2}^*$ satisfying (3.1). □

Theorem 3.2. *Let $L(X) = a_1X^q + a_0X \in \mathbb{F}_{q^2}[X]$. Then*

$$f(X) = \mathrm{Tr}_{q^2/q}(L(X)/X) \tag{3.2}$$

has no root in $\mathbb{F}_{q^2}^*$ if and only if $g(X) = X^2 + \mathrm{Tr}_{q^2/q}(a_0)X + a_1^{q+1} \in \mathbb{F}_q[X]$ has two distinct roots in $\mathbb{F}_q$.

Proof. If $a_1 = 0$, then $f(X) = \mathrm{Tr}_{q^2/q}(a_0)$ and $g(X) = X^2 + \mathrm{Tr}_{q^2/q}(a_0)X$. It is clear that f has no nonzero roots if and only if g has two distinct roots.

In the rest of the proof, we assume that $a_1 \neq 0$.

($\Leftarrow$) Let $a_1y \in \mathbb{F}_q$ ($y \in \mathbb{F}_{q^2}$) be a root of g. By Lemma 3.1, it suffices to show that $y^{q+1} \neq 1$.

Case 1. Assume that q is even. Since g has two distinct roots, we have $\mathrm{Tr}_{q^2/q}(a_0) \neq 0$. Since

$$(a_1y)^{q+1} = (a_1y)^2 = \mathrm{Tr}_{q^2/q}(a_0)a_1y + a_1^{q+1},$$

we have

$$y^{q+1} = 1 + \frac{\mathrm{Tr}_{q^2/q}(a_0)y}{a_1^q} \neq 1.$$

Case 2. Assume that q is odd. We have $y = \frac{1}{2a_1}(-\mathrm{Tr}_{q^2/q}(a_0) + d)$, where $d \in \mathbb{F}_q^*$ and $d^2 = \mathrm{Tr}_{q^2/q}(a_0)^2 - 4a_1^{q+1}$. Suppose to the contrary that $y^{q+1} = 1$. It follows that

$$(-\mathrm{Tr}_{q^2/q}(a_0) + d)^{q+1} = 4a_1^{q+1},$$

which means
$$\mathrm{Tr}_{q^2/q}(a_0)^2 + d^2 - 2d\mathrm{Tr}_{q^2/q}(a_0) = 4a_1^{q+1}.$$
Hence
$$2d^2 - 2d\mathrm{Tr}_{q^2/q}(a_0) = 0.$$
Therefore $d = \mathrm{Tr}_{q^2/q}(a_0)$. But then $d^2 = \mathrm{Tr}_{q^2/q}(a_0)^2 \neq \mathrm{Tr}_{q^2/q}(a_0)^2 - 4a_1^{q+1}$, which is a contradiction.

($\Rightarrow$) We first show that g is reducible in $\mathbb{F}_q[x]$. Otherwise, let $a_1 y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be a root of g. Then $(a_1 y)^{q+1} = a_1^{q+1}$, thus $y^{q+1} = 1$. By Lemma 3.1, f has nonzero roots.

It remains to show that $\mathrm{Tr}_{q^2/q}(a_0)^2 - 4a_1^{q+1} \neq 0$. Assume to the contrary that $\mathrm{Tr}_{q^2/q}(a_0)^2 - 4a_1^{q+1} = 0$.

Case 1. Assume that q is even. It follows that $\mathrm{Tr}_{q^2/q}(a_0) = 0$. Write $a_1 = x^2$, where $x \in \mathbb{F}_{q^2}$, and let $y = x^{q-1}$. Then $a_1 y$ is a root of g, which leads to a contradiction.

Case 2. Assume that q is odd. Then $a_1 y = -\mathrm{Tr}_{q^2/q}(a_0)/2$ is a root of g, and
$$y^{q+1} = \frac{\mathrm{Tr}_{q^2/q}(a_0)^2}{4a_1^{q+1}} = 1,$$
which is impossible by Lemma 3.1. $\square$

Remark. When $n = 2$, if there is some $L(X)$ such that (3.2) has no root in $\mathbb{F}_{q^2}^*$, then we can define a presemifield multiplication $*$ over $\mathbb{F}_{q^2}$ via Theorem 2.1. Let $\mathbb{S} = (\mathbb{F}_{q^2}, +, \star)$ be a semifield which is isotopic to $(\mathbb{F}_{q^2}, +, *)$. We may assume that $\star$ is defined by (1.1) and hence $\mathbb{S}$ has identity 1. There are $a_{ij} \in \mathbb{F}_{q^2}$ such that $x * y = \sum_{i,j} a_{ij} x^{q^i} y^{q^j}$ for all $x, y \in \mathbb{F}_{q^2}$. Thus there are $b_{ij} \in \mathbb{F}_{q^2}$ such that $x \star y = \sum_{i,j} b_{ij} x^{q^i} y^{q^j}$ for all $x, y \in \mathbb{F}_{q^2}$. It follows that the center of $\mathbb{S}$ contains $\mathbb{F}_q$. (For $x \in \mathbb{F}_q$ and $y \in \mathbb{F}_{q^2}$, we have $x \star y = x(1 \star y) = xy$ and $y \star x = x(y \star 1) = xy$. This implies that $\mathbb{F}_q$ is contained in both the commutative center and the nucleus of $\mathbb{S}$.) Due to the classification of two-dimensional finite semifields by Dickson [7], $\mathbb{S}$ is isotopic to a finite field.

Theorem 3.3. *Let q be a power of odd prime and let $L(X) = a_1 X^{q^2} + a_0 X \in \mathbb{F}_{q^4}[X]$ with $a_1 \neq 0$. Then $\mathrm{Tr}_{q^4/q}(L(X)/X)$ has no root in $\mathbb{F}_{q^4}^*$ if and only if $a_1^{q^2+1}$ is a square in $\mathbb{F}_q^*$ and $\mathrm{Tr}_{q^4/q}(a_0) = 0$.*

Proof. Let $b = \mathrm{Tr}_{q^4/q}(a_0)$. Let $x \in \mathbb{F}_{q^4}^*$ and set $y := x^{q^2-1}$ and $z := a_1 y + a_1^{q^2}/y$. Then
$$\begin{aligned}\mathrm{Tr}_{q^4/q}(L(x)/x) &= \mathrm{Tr}_{q^4/q}(a_1 x^{q^2-1} + a_0)\\ &= a_1 y + a_1^q y^q + a_1^{q^2}/y + a_1^{q^3}/y^q + \mathrm{Tr}_{q^4/q}(a_0)\\ &= z + z^q + b.\\ &= \left(z + \frac{b}{2}\right)^q + \left(z + \frac{b}{2}\right). \end{aligned} \tag{3.3}$$

Thus $\mathrm{Tr}_{q^4/q}(L(x)/x) = 0$ if and only if $(z + \frac{b}{2})^{q-1} = -1$ or 0, i.e., $z = t - \frac{b}{2}$ for some $t \in T := \{t \in \mathbb{F}_{q^4} : t^q = -t\} \subset \mathbb{F}_{q^2}$. Since $z = a_1 y + a_1^{q^2}/y$, we see that $z = t - \frac{b}{2}$ if and only if

$$a_1 y^2 + \left(\frac{b}{2} - t\right) y + a_1^{q^2} = 0. \tag{3.4}$$

By the proof of Theorem 3.2, we see that $\{x \in \mathbb{F}_{q^4}^* : y = x^{q^2-1}$ satisfies (3.4)$\} \neq \emptyset$ if and only if

$$g(X) := X^2 + \left(\frac{b}{2} - t\right) X + a_1^{q^2+1}$$

has two distinct roots in $\mathbb{F}_{q^2}$. Therefore, to sum up, $\mathrm{Tr}_{q^4/q}(L(x)/x)$ has no root in $\mathbb{F}_{q^4}^*$ if and only if $g(X)$ has two distinct roots in $\mathbb{F}_{q^2}$ for every $t \in T$. We now proceed to prove the "if" and the "only if" portions of the theorem separately.

($\Leftarrow$) Assume $b = 0$ and $a_1^{q^2+1}$ is a square in $\mathbb{F}_q^*$. Then $a_1^{q^2+1} \neq t^2$ for all $t \in T$. Hence

$$\Delta := \left(\frac{b}{2} - t\right)^2 - 4a_1^{q^2+1} = t^2 - 4a_1^{q^2+1} \in \mathbb{F}_q^*.$$

It follows that g has two distinct roots in $\mathbb{F}_{q^2}$.

($\Rightarrow$) Assume that $\mathrm{Tr}_{q^4/q}(L(X)/X)$ has no root in $\mathbb{F}_{q^4}^*$. We want to show

R1. $b = 0$, and

R2. $a_1^{q^2+1}$ is a square in $\mathbb{F}_q^*$. Equivalently, $a_1^{q^2+1}$ is in $\mathbb{F}_q$ and there is no $t \in T$ such that $t^2 = 4a_1^{q^2+1}$.

Now we assume that $\Delta = \left(\frac{b}{2} - t\right)^2 - 4a_1^{q^2+1} \neq 0$ always has a square root in $\mathbb{F}_{q^2}$, for every $t \in T$. Choose an element ξ of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, such that $\xi^{q-1} = -1$. Then every element of $\mathbb{F}_{q^2}$ can be written as $z + w\xi$, where z, $w \in \mathbb{F}_q$, and $T = \{x\xi : x \in \mathbb{F}_q\}$. We write $a_1^{q^2+1} = A_1 + A_2\xi$. As Δ is always a square in $\mathbb{F}_{q^2}^*$, the equation

$$(z + w\xi)^2 = (x\xi - b/2)^2 - (A_1 + A_2\xi) \tag{3.5}$$

in (z, w) has solutions for every $x \in \mathbb{F}_q$. Expanding (3.5), we have

$$z^2 + w^2\alpha = x^2\alpha + b^2/4 - A_1, \tag{3.6}$$

$$2wz = -xb - A_2, \tag{3.7}$$

where $\alpha = \xi^2 \in \mathbb{F}_q$.

If we can show that $b = 0$ and $A_2 = 0$, then the proof is complete (**R2** can be easily derived from the condition that $\Delta \neq 0$). Suppose to the contrary that at least one of b and A_2 is not 0. Then there exists at most one $x = x_0 \in \mathbb{F}_q$ such that $w = 0$ by (3.7). Now assume that $w \neq 0$. From (3.7) we have

$$z = -\frac{xb + A_2}{2w}.$$

Plugging it into (3.6), we get

$$\frac{(xb + A_2)^2}{4w^2} + w^2\alpha = x^2\alpha + \frac{b^2}{4} - A_1,$$

i.e.,

$$\alpha(w^2)^2 - (x^2\alpha + \frac{b^2}{4} - A_1)w^2 + \frac{(xb + A_2)^2}{4} = 0.$$

For every given $x \in \mathbb{F}_q \setminus \{x_0\}$, this equation always has a solution w in $\mathbb{F}_q$. It follows that

$$f(x) = (x^2\alpha + \frac{b^2}{4} - A_1)^2 - \alpha(xb + A_2)^2$$

is always a square in $\mathbb{F}_q$. Let ψ be the multiplicative character of $\mathbb{F}_q$ of order 2, and for convenience we set $\psi(0) = 0$. Then we have

$$\sum_{c \in \mathbb{F}_q} \psi(f(c)) \geq q - 6. \tag{3.8}$$

On the other hand, by Theorem 5.41 in [19] (it is routine to verify all the conditions for $f(x)$, because $(b, A_2) \neq (0, 0)$ and $(A_1, A_2) \neq (0, 0)$), we have

$$\sum_{c \in \mathbb{F}_q} \psi(f(c)) \leq 3\sqrt{q}.$$

Therefore $q - 6 \leq 3\sqrt{q}$, which means that $q = 3, 5, 7, 9, 11, 13, 17, 19$. We can use MAGMA [3] to show that $f(x)$ is not always a square for $x \in \mathbb{F}_q \setminus \{x_0\}$ when $q \leq 19$. Hence $b = A_2 = 0$, which completes the proof. □

Theorem 3.4. *Let q be a power of an odd prime. Let $a_1 \in \mathbb{F}_{q^4}^*$ such that $a_1^{q^2+1}$ is a square in $\mathbb{F}_q^*$ and let $\tilde{a}_0$ be an element in $\mathbb{F}_{q^4}$ such that $\mathrm{Tr}_{q^4/q}(\tilde{a}_0) = -1$. Define*

$$x * y = xy + \mathrm{Tr}_{q^4/q}(a_1 x y^{q^2} + \tilde{a}_0 xy).$$

According to Theorem 2.1 and Theorem 3.3, $(\mathbb{F}_{q^4}, +, *)$ forms a presemifield. Furthermore, it is isotopic to a commutative semifield.

Proof. According to Lemma 2.4, we only have to show that there exists some v such that

$$A(v * x) * y = A(v * y) * x$$

for every x, $y \in \mathbb{F}_{q^4}$, where A is given by (2.4).

Using the same notation as in Lemma 2.5, we set $t = a_1 + \tilde{a}_0$ and $s = -t/(1 + \mathrm{Tr}_{q^4/q}(t))$. Now,

$$\begin{aligned}
A(v * x) &= A(vx + \mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} + \tilde{a}_0 vx)) \\
&= vx + \mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} + \tilde{a}_0 vx) + \mathrm{Tr}_{q^4/q}\left[s(vx + \mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} + \tilde{a}_0 vx))\right] \\
&= vx + (1 + \mathrm{Tr}_{q^4/q}(s))\mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} + \tilde{a}_0 vx) + \mathrm{Tr}_{q^4/q}(svx) \\
&= vx + \frac{\mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} + \tilde{a}_0 vx)}{1 + \mathrm{Tr}_{q^4/q}(a_1 + \tilde{a}_0)} - \frac{\mathrm{Tr}_{q^4/q}((a_1 + \tilde{a}_0)vx)}{1 + \mathrm{Tr}_{q^4/q}(a_1 + \tilde{a}_0)} \\
&= vx + \frac{\mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} - a_1 vx)}{1 + \mathrm{Tr}_{q^4/q}(a_1 + \tilde{a}_0)}.
\end{aligned}$$

For convenience, let $r(x)$ denote $A(v * x) - vx$. Then

$$\begin{aligned}
A(v * x) * y &= vxy + r(x)y + \mathrm{Tr}_{q^4/q}(a_1 vxy^{q^2} + \tilde{a}_0 vxy) + r(x)\mathrm{Tr}_{q^4/q}(a_1 y^{q^2} + \tilde{a}_0 y) \\
&= vxy + \frac{\mathrm{Tr}_{q^4/q}(a_1 v x^{q^2} - a_1 vx)}{1 + \mathrm{Tr}_{q^4/q}(a_1 + \tilde{a}_0)}(y + \mathrm{Tr}_{q^4/q}(a_1 y^{q^2} + \tilde{a}_0 y)) \\
&\quad + \mathrm{Tr}_{q^4/q}(a_1 vxy^{q^2} + \tilde{a}_0 vxy).
\end{aligned}$$

It is not difficult to see that if v is an element in $\mathbb{F}_{q^4}$ such that $a_1 v \in \mathbb{F}_{q^2}$, then $A(v * x) * y = A(v * y) * x$, from which it follows that $(\mathbb{F}_{q^4}, +, *)$ is isotopic to a commutative semifield. □

Theorem 3.5. *Let q be a power of an odd prime. Let $a_1 \in \mathbb{F}_{q^4}^*$ such that $a_1^{q^2+1}$ is a square in $\mathbb{F}_q^*$ and let $\tilde{a}_0$ be an element in $\mathbb{F}_{q^4}$ such that $\mathrm{Tr}_{q^4/q}(\tilde{a}_0) = -1$. Let $x * y$ be defined as in Theorem 3.4, i.e.,*

$$x * y = xy + \mathrm{Tr}_{q^4/q}(a_1 x y^{q^2} + \tilde{a}_0 xy).$$

Then the presemifield $(\mathbb{F}_{q^4}, +, *)$ is isotopic to Dickson's semifield.

Proof. We have already shown in Theorem 3.4 that $(\mathbb{F}_{q^4}, +, *)$ is isotopic to a commutative semifield, which is denoted by $\mathbb{S}$. Next we are going to prove that its middle nucleus $N_m(\mathbb{S})$ is of size q^2 and its left nucleus $N_l(\mathbb{S})$ is of size q. Furthermore, as $\mathbb{S}$ is commutative, we have $N_r(\mathbb{S}) = N_l(\mathbb{S})$. Due to the classification of semifields planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ by Cardinali, Polverino and Trombetti in [4], $(\mathbb{F}_{q^4}, +, *)$ is isotopic to Dickson's semifield.

To determine the middle and left nuclei of $\mathbb{S}$, we need to introduce another presemifield multiplication $x \circ y$, which corresponds to the *dual spread* of the spread defined by $x * y$. (For more details on the dual spread, see [16].) Actually, $x \circ y$ is defined as

$$x \circ y := xy + (a_1 y^{q^2} + \tilde{a}_0 y)\mathrm{Tr}_{q^4/q}(x). \tag{3.9}$$

It is straightforward to verify that $\mathrm{Tr}_{q^4/q}(x(z \circ y) - z(x * y)) = 0$. Let $\mathbb{S}'$ denote a semifield which is isotopic to the presemifield defined by $x \circ y$. According to the interchanging of nuclei of semifields in the so called *Knuth orbit* ([16] and [18, Section 1.4]), we have $N_l(\mathbb{S}') \cong N_m(\mathbb{S})$ and $N_m(\mathbb{S}') \cong N_l(\mathbb{S})$.

To determine $N_l(\mathbb{S}')$ and $N_m(\mathbb{S}')$, we use the connection between certain homology groups as described in [13, Theorem 8.2] and [14, Result 12.4]. To be precise, we want to find every q-linearized polynomial $A(X)$ over $\mathbb{F}_{q^4}$ such that for every $y \in \mathbb{F}_{q^4}$, there is a $y' \in \mathbb{F}_{q^4}$ satisfying $A(x) \circ y = x \circ y'$ for every $x \in \mathbb{F}_{q^4}$. The set $\mathcal{M}(\mathbb{S}')$ of all such $A(X)$ is equivalent to the middle nucleus $N_m(\mathbb{S}')$.

First, it is routine to verify that $A(X) = uX$ with $u \in \mathbb{F}_q$ is in $\mathcal{M}(\mathbb{S}')$. Next we show that there are no other $A(X)$ in $\mathcal{M}(\mathbb{S}')$.

Assume that

$$A(x)y + \mathrm{Tr}_{q^4/q}(A(x))(a_1 y^{q^2} + \tilde{a}_0 y) = xy' + \mathrm{Tr}_{q^4/q}(x)(a_1 y'^{q^2} + \tilde{a}_0 y') \tag{3.10}$$

holds for every $x \in \mathbb{F}_{q^4}$.

Let $x_0 \in \mathbb{F}_{q^4}^*$ be such that $\mathrm{Tr}_{q^4/q}(x_0) = \mathrm{Tr}_{q^4/q}(A(x_0)) = 0$. Then

$$A(x_0)y = x_0 y'.$$

It means that $y' = uy$ holds for each $y \in \mathbb{F}_{q^4}$, where $u = A(x_0)/x_0$. Plugging it into (3.10), we have

$$A(x)y + \mathrm{Tr}_{q^4/q}(A(x))(a_1 y^{q^2} + \tilde{a}_0 y) = uxy + \mathrm{Tr}_{q^4/q}(x)(a_1 (uy)^{q^2} + \tilde{a}_0 uy).$$

From this equation we can deduce that

$$A(x) - ux + (\mathrm{Tr}_{q^4/q}(A(x)) - \mathrm{Tr}_{q^4/q}(x)u)\tilde{a}_0 = 0, \tag{3.11}$$

$$(\mathrm{Tr}_{q^4/q}(A(x)) - \mathrm{Tr}_{q^4/q}(x)u^{q^2})a_1 = 0. \tag{3.12}$$

Since $a_1 \neq 0$, from (3.12) we see that

$$\mathrm{Tr}_{q^4/q}(A(x)) = u^{q^2}\mathrm{Tr}_{q^4/q}(x) \tag{3.13}$$

for every $x \in \mathbb{F}_{q^4}$. From (3.13) it follows that $u \in \mathbb{F}_q$. Therefore, by (3.11), we have $A(x) = ux$ where $u \in \mathbb{F}_q$. Hence $|N_l(\mathbb{S})| = |N_m(\mathbb{S}')| = q$.

Next we determine every q-linearized polynomial $A(X)$ over $\mathbb{F}_{q^4}$ such that for every $y \in \mathbb{F}_{q^4}$, there is a $y' \in \mathbb{F}_{q^4}$ satisfying $A(x \circ y) = x \circ y'$ for every $x \in \mathbb{F}_{q^4}$. The set of all such $A(X)$ is equivalent to the left nucleus $N_l(\mathbb{S}')$.

Assume that

$$A(xy + \mathrm{Tr}_{q^4/q}(x)(a_1 y^{q^2} + \tilde{a}_0 y)) = xy' + \mathrm{Tr}_{q^4/q}(x)(a_1 y'^{q^2} + \tilde{a}_0 y'). \tag{3.14}$$

It is readily verified that when $A(X) = cX$ for some $c \in \mathbb{F}_{q^2}$, (3.14) holds for all x and y in $\mathbb{F}_{q^4}$ with $y' = cy$. Hence $\mathbb{F}_{q^2}$ is a subfield contained in $N_l(\mathbb{S}')$. On the other hand, $N_l(\mathbb{S}')$ has to be a proper subfield of $\mathbb{F}_{q^4}$, for otherwise $\mathbb{S}'$ would be a finite field, which would lead to a contradiction. Therefore, we have $|N_m(\mathbb{S})| = |N_l(\mathbb{S}')| = q^2$, which completes the proof. □

Theorem 3.6. *Let q be a power of prime and let u, v be elements in $\mathbb{F}_{q^3}^*$ such that $\mathrm{N}_{q^3/q}(-v/u) \neq 1$. For every $\beta \in \mathcal{B}$, where*

$$\mathcal{B} := \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{q^3/q}(u^{q^2} v^q x) = u^{q^2+q+1} + v^{q^2+q+1}\},$$

the equation

$$u x^{q^2-1} + v x^{q-1} + \beta = 0 \tag{3.15}$$

has no solution in $\mathbb{F}_{q^3}^*$. Let $L(X) := u^{q^2} v^q (u a^{q^2-1} X^{q^2} + v a^{q-1} X^q + \theta X)$, where $\theta \in \mathcal{B}$ and $a \in \mathbb{F}_{q^3}^*$. Then the polynomial $\mathrm{Tr}_{q^3/q}(L(X)/X)$ has no root in $\mathbb{F}_{q^3}^*$.

Proof. When $\beta = 0$, (3.15) becomes $x^{q-1}(u x^{q(q-1)} + v) = 0$. If there exists $x \in \mathbb{F}_{q^3}^*$ such that $u x^{q(q-1)} + v = 0$, then $\mathrm{N}_{q^3/q}(-v/u) = \mathrm{N}_{q^3/q}(x^{q(q-1)}) = 1$, which leads to a contradiction.

Now suppose $\beta \neq 0$. Assume to the contrary that (3.15) has a solution $x \in \mathbb{F}_{q^3}^*$. Let $y := x^{q-1}$. Then we have $u y^{q+1} + v y + \beta = 0$. It follows that

$$y^q = \frac{-vy - \beta}{uy}, \tag{3.16}$$

and

$$y^{q^2} = \frac{v^q(vy + \beta) - \beta^q u y}{-u^q(vy + \beta)}.$$

Hence

$$y^{q^2} y^q y = \frac{v^q(vy + \beta) - \beta^q u y}{u^{q+1}},$$

which is equal to 1 since $y = x^{q-1}$. Therefore,

$$(v^{q+1} - \beta^q u)y + v^q \beta = u^{q+1}. \tag{3.17}$$

Suppose that $u\beta^q = v^{q+1}$. Then $u^{q^2} v^q \beta = v^{q^2+1} v^q$, and $\mathrm{Tr}_{q^3/q}(u^{q^2} v^q \beta) = 3v^{q^2+q+1}$. On the other hand, we also have $u^{q+1} = v^q \beta$ from (3.17). It follows that $\mathrm{Tr}_{q^3/q}(u^{q^2} v^q \beta) = 3u^{q^2+q+1}$. All together with $\beta \in \mathcal{B}$, we have that

$$u^{q^2+q+1} + v^{q^2+q+1} = 3v^{q^2+q+1} = 3u^{q^2+q+1},$$

which can not holds for $3 \nmid q$. Moreover, if $3 \mid q$, then $u^{q^2+q+1} = -v^{q^2+q+1}$ which contradicts the assumption that $\mathrm{N}_{q^3/q}(-v/u) \neq 1$. Hence $u\beta^q \neq v^{q+1}$.

Since $u\beta^q \neq v^{q+1}$, from (3.17) we obtain

$$y = \frac{u^{q+1} - v^q\beta}{v^{q+1} - \beta^q u} \tag{3.18}$$

Plugging (3.18) into (3.16), we have

$$\frac{u^{q^2+q} - v^{q^2}\beta^q}{v^{q^2+q} - \beta^{q^2}u^q} = \frac{vu^q - \beta^{q+1}}{v^q\beta - u^{q+1}}.$$

Hence

$$\begin{aligned} &u^{q^2+q}v^q\beta - u^{q^2+2q+1} + u^{q+1}v^{q^2}\beta^q - v^{q^2+q}\beta^{q+1} \\ =& v^{q^2+q+1}u^q - \beta^{q^2}vu^{2q} - v^{q^2+q}\beta^{q+1} + \beta^{q^2+q+1}u^q. \end{aligned}$$

Dividing it by u^q, we have

$$\beta^{q^2+q+1} - (u^q v\beta^{q^2} + uv^{q^2}\beta^q + u^{q^2}v^q\beta) + u^{q^2+q+1} + v^{q^2+q+1} = 0.$$

It follows from $\mathrm{Tr}_{q^3/q}(u^{q^2}v^q\beta) = u^{q^2+q+1} + v^{q^2+q+1}$ that

$$\beta^{q^2+q+1} = 0.$$

Hence $\beta = 0$, which is a contradiction. Therefore, (3.15) has no solution in $\mathbb{F}_{q^3}^*$.

Furthermore, if $\mathrm{Tr}_{q^3/q}(L(X)/X)$ has a root $x_0 \in \mathbb{F}_{q^3}^*$, then $u^{q^2}v^q(u(ax_0)^{q^2-1} + v(ax_0)^{q-1} + \theta) = \gamma$ for some $\gamma \in \mathbb{F}_{q^3}$ satisfying $\mathrm{Tr}_{q^3/q}(\gamma) = 0$. We write γ as $\gamma = u^{q^2}v^q\tau$ for some $\tau \in \mathbb{F}_{q^3}$. Then $\theta - \tau \in \mathcal{B}$ and

$$u(ax_0)^{q^2-1} + v(ax_0)^{q-1} + \theta - \tau = 0,$$

which contradicts the fact that (3.15) has no solution in $\mathbb{F}_{q^3}^*$. □

For given u and v, it is not difficult to see that for different a, we obtain isotopic semifields via Theorem 3.6: Let the multiplication corresponding to $a = 1$ be $xy + B(x, y)$. Then for other $a \in \mathbb{F}_{q^3}^*$, the semifield multiplication is $\frac{axy+B(x,ay)}{a}$. Furthermore, when $u, v \in \mathbb{F}_q$ and $a = 1$, it follows from Lemma 2.3 that the presemifield $\mathbb{P}$ derived from $L(x)$ in Theorem 3.6 is commutative. It is worth noting that, up to isotopism, we can obtain non-commutative semifields via Theorem 3.6. For instance, let $q = 4$ and let ξ be a primitive element of $\mathbb{F}_{q^3}$ which is a root of $X^6 + X^4 + X^3 + X + 1$. Setting $u = \xi^5$, $v = \xi$ and $\beta = \xi^{62}$, we can use computer to show that the presemifield $\mathbb{P}$ derived from Theorem 3.6 is not isotopic to a commutative one.

According to the classification of semifields of order q^3 with center containing $\mathbb{F}_q$ in [21], the presemifield obtained via Theorem 3.6 is either finite field or generalized twisted field.

Besides all the L's described in this section, we did not find any other examples. Thus we propose the following question:

Question 3.7. *For $n > 4$, is there a q-linearized polynomial $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ with $(a_1, \dots, a_{n-1}) \neq (0, \dots, 0)$ satisfying (2.3)?*

4. Switchings of $\mathbb{F}_{p^n}$ for large n

The main result of this section is a negative answer to Question 3.7 when $q = p$ (prime) and n is large.

Theorem 4.1. *Let $q = p$, where p is a prime, and assume $n \ge \frac{1}{2}(p-1)(p^2-p+4)$. If $L(X) = \sum_{i=0}^{n-1} a_i X^{p^i} \in \mathbb{F}_{p^n}[X]$ satisfies (2.3), i.e.,*

$$\mathrm{Tr}_{p^n/p}\big(L(x)/x\big) \ne 0 \quad \text{for all } x \in \mathbb{F}_{p^n}^*,$$

then $a_1 = \cdots = a_{n-1} = 0$.

In 1971, Payne [22] considered a similar problem which calls for the determination of all 2-linearized polynomials $L = \sum_{i=0}^{n-1} a_i X^{2^i} \in \mathbb{F}_{2^n}[X]$ such that both $L(X)$ and $L(X)/X$ are permutation polynomials of $\mathbb{F}_{2^n}$. Such linearized polynomials give rise to translation ovoids in the projective plane $\mathrm{PG}(2, \mathbb{F}_{2^n})$ [23]. Payne later solved the problem by showing that such linearized polynomials can have only one term [23]. For a different proof of Payne's theorem, see [11, §8.5]. For the q-ary version of Payne's theorem, see [12].

4.1. **Preliminaries.** Let $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$. For $x \in \mathbb{F}_{q^n}^*$, we have

$$\mathrm{Tr}_{q^n/q}\Big(\frac{L(x)}{x}\Big) = \mathrm{Tr}_{q^n/q}\Big(\sum_{i=0}^{n-1} a_i x^{q^i-1}\Big) = \sum_{0\le i,j\le n-1} a_i^{q^j} x^{q^j(q^i-1)}.$$

Therefore (2.3) is equivalent to

$$\Big[\sum_{0\le i,j\le n-1} a_i^{q^j} X^{q^j(q^i-1)}\Big]^{q-1} \equiv \mathrm{Tr}_{q^n/q}(a_0)^{q-1} + \Big[1 - \mathrm{Tr}_{q^n/q}(a_0)^{q-1}\Big] X^{q^n-1} \pmod{X^{q^n} - X}. \tag{4.1}$$

Let $\Omega = \{0, 1, \dots, q^n - 1\}$ and $\Omega_0 = \{0, 1, \dots, \frac{q^n-1}{q-1}\}$. For $\alpha, \beta \in \Omega_0$, define $\alpha \oplus \beta \in \Omega_0$ such that $\alpha \oplus \beta \equiv \alpha + \beta \pmod{\frac{q^n-1}{q-1}}$ and

$$\alpha \oplus \beta = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ \frac{q^n-1}{q-1} & \text{if } \alpha + \beta \equiv 0 \pmod{\frac{q^n-1}{q-1}} \text{ and } (\alpha, \beta) \ne (0, 0). \end{cases}$$

For $d_0, \dots, d_{n-1} \in \mathbb{Z}$, we write

$$(d_0, \dots, d_{n-1})_q = \sum_{i=0}^{n-1} d_i q^i.$$

When q is clear from the context, we write $(d_0, \dots, d_{n-1})_q = (d_0, \dots, d_{n-1})$. For $j, i \in \mathbb{Z}$, $i \ge 0$, let

$$s(j, i) = (\overset{0}{0}\ \cdots\ 0\ \underbrace{\overset{j}{1}\ \cdots\ 1}_{i}\ 0\ \cdots\ \overset{n-1}{0})_q,$$

where the positions of the digits are labeled modulo n and the string of 1's may wrap around. For example, with $n = 4$,

$$s(1, 3) = (0\ 1\ 1\ 1), \qquad s(3, 2) = (1\ 0\ 0\ 1).$$

Note that

$$s(j, i) \equiv q^j \frac{q^i - 1}{q - 1} \pmod{q^n - 1}.$$

For each $\alpha \in \Omega_0$, let $C(\alpha)$ denote the coefficient of $X^{\alpha(q-1)}$ in the left side of (4.1) after reduction modulo $X^{q^n} - X$. Then we have

$$C(\alpha) = \sum_{\substack{0\le j_1,i_1,\dots,j_{q-1},i_{q-1}\le n-1 \\ s(j_1,i_1)\oplus\cdots\oplus s((j_{q-1},i_{q-1})=\alpha}} a_{i_1}^{q^{j_1}} \cdots a_{i_{q-1}}^{q^{j_{q-1}}}. \tag{4.2}$$

Let

$$S = \{s(j,i) : 0 \le j \le n-1,\ 1 \le i \le n-1\}.$$

If $C(\alpha) = 0$, we can derive from (4.2) useful information about a_i's if we know the possible ways to express α as an $\oplus$ sum of $q-1$ elements (not necessarily distinct) of $S \cup \{0\}$.

Let $\alpha = (d_0, \dots, d_{n-1})_q \in \Omega$, where $0 \le d_i \le q-1$. If $d_i > d_{i-1}$ ($d_i < d_{i-1}$), where the subscripts are taken modulo n, we say that i is an *ascending* (*descending*) position of α with multiplicity $|d_i - d_{i-1}|$. The multiset of ascending (descending) positions of α is denoted by $\mathrm{Asc}(\alpha)$ ($\mathrm{Des}(\alpha)$). The multiset cardinality $|\mathrm{Asc}(\alpha)|$ ($= |\mathrm{Des}(\alpha)|$) is denoted by $\mathrm{asc}(\alpha)$. For example, if $\alpha = (2\ 0\ 1\ 1\ 3\ 0)$, then

$$\mathrm{Asc}(\alpha) = \{0,0,2,4,4\}, \quad \mathrm{Des}(\alpha) = \{1,1,5,5,5\}, \quad \mathrm{asc}(\alpha) = 5.$$

Assume that $\alpha \in \Omega$ has $\mathrm{asc}(\alpha) = q-1$. Then α cannot be a sum of less than $q-1$ elements (not necessarily distinct) of S. Moreover, if

$$\alpha = s(j_1, i_1) + \cdots + s(j_{q-1}, i_{q-1}),$$

where $0 \le j_1, \dots, j_{q-1} \le n-1$ and $1 \le i_1, \dots, i_{q-1} \le n-1$, we must have $\{j_1, \dots, j_{q-1}\} = \mathrm{Asc}(\alpha)$ and $\{j_1 + i_1, \dots, j_{q-1} + i_{q-1}\} = \mathrm{Des}(\alpha)$, where $j_k + i_k$ is taken modulo n.

4.2. **Proof of Theorem 4.1.**

Lemma 4.2. *Let $q = p$, where p is a prime, and assume $L = \sum_{i=0}^{n-1} a_i X^{p^i} \in \mathbb{F}_{p^n}[X]$ satisfies* (2.3). *Then for all $1 \le i_1 < \cdots < i_{p-1}$ and $0 \le t_{p-2} \le \cdots \le t_1$ with $i_{p-1} + t_1 \le n-2$, we have*

$$\sum_\tau a_{i_{p-1}+\tau(p-1)} a_{i_{p-2}+\tau(p-2)}^{p^{i_{p-1}-i_{p-2}}} \cdots a_{i_1+\tau(1)}^{p^{i_{p-1}-i_1}} = 0, \tag{4.3}$$

where $(\tau(1), \dots, \tau(p-1))$ runs through all permutations of $(t_1, \dots, t_{p-2}, 0)$.

Proof. Let

$$\begin{aligned} \alpha = (\ & \overbrace{1\ \cdots\ 1}^{i_{p-1}-i_{p-2}}\ \cdots\ \overbrace{p-2\ \cdots\ p-2}^{i_2-i_1}\ \overbrace{p-1\ \cdots\ p-1}^{i_1} \\ & \underbrace{p-2\ \cdots\ p-2}_{t_{p-2}}\ \underbrace{p-3\ \cdots\ p-3}_{t_{p-3}-t_{p-2}}\ \cdots\ \underbrace{1\ \cdots\ 1}_{t_1-t_2}\ \underbrace{0\ \cdots\ 0}_{\substack{n-i_{p-1}-t_1 \\ \ge 2}}\ ) \in \Omega_0. \end{aligned}$$

For $1 \le k \le p-2$, we have

$$\begin{aligned} & \alpha + (k\ \cdots\ k) \\ = (\ & \overbrace{k+1\ \cdots\ k+1\ \cdots\ p-1\ \cdots\ p-1\ 0\ 1\ \cdots\ 1\ \cdots}^{i_{p-1}}\ \overbrace{\cdots\ d}^{t_1}\ \overbrace{e\ \underbrace{k\ \cdots\ k}_{\ge 1}}^{n-i_{p-1}-t_1}), \end{aligned}$$

where $e = k+1$ or k, depending on whether it receives a carry from the preceding digit. If $e = k+1$, then $\mathrm{asc}(\alpha + (k\ \cdots\ k)) \ge p-1-k+k+1 = p$. If $e = k$, then

$t_1 > 0$ and $d \ge k+1$, which also implies that $\mathrm{asc}(\alpha + (k\ \cdots\ k)) \ge p$. Therefore $\alpha + (k\ \cdots\ k)$ is not a sum of $\le p-1$ elements (not necessarily distinct) of S, i.e., not a sum of $p-1$ elements (not necessarily distinct) of $S \cup \{0\}$.

On the other hand, we have $\mathrm{asc}(\alpha) = p-1$ and

$$\begin{aligned}\mathrm{Asc}(\alpha) &= \{0, i_{p-1} - i_{p-2}, \dots, i_{p-1} - i_1\},\\ \mathrm{Des}(\alpha) &= \{i_{p-1}, i_{p-1} + t_{p-2}, \dots, i_{p-1} + t_1\}.\end{aligned}$$

Therefore, the only possible ways to express α as a sum of $p-1$ elements (not necessarily distinct) of $S \cup \{0\}$ are

$$\alpha = s(0, i_{p-1} + \tau(p-1)) + s(i_{p-1} - i_{p-2}, i_{p-2} + \tau(p-2)) + \cdots + s(i_{p-1} - i_1, i_1 + \tau(1)),$$

where $(\tau(1), \dots, \tau(p-1))$ is a permutation of $(t_1, \dots, t_{p-2}, 0)$. Together with the fact that for $1 \le k \le p-2$, $\alpha + (k\ \cdots\ k)$ is not a sum of $p-1$ elements (not necessarily distinct) of $S \cup \{0\}$, we have proved that

$$\alpha = \alpha_1 \oplus \cdots \oplus \alpha_{p-1}, \quad \alpha_i \in S \cup \{0\},$$

if and only if

$$\begin{aligned}&\{\alpha_1, \dots, \alpha_{p-1}\}\\ &= \big\{s(0, i_{p-1} + \tau(p-1)), s(i_{p-1} - i_{p-2}, i_{p-2} + \tau(p-2)), \dots, s(i_{p-1} - i_1, i_1 + \tau(1))\big\},\end{aligned}$$

where $(\tau(1), \dots, \tau(p-1))$ is a permutation of $(t_1, \dots, t_{p-2}, 0)$.

Now we have

$$\begin{aligned} 0 &= C(\alpha) && \text{(by (4.1))}\\ &= (p-1)! \sum_{\tau} a_{i_{p-1}+\tau(p-1)} a_{i_{p-2}+\tau(p-2)}^{p^{i_{p-1}-i_{p-2}}} \cdots a_{i_1+\tau(1)}^{p^{i_{p-1}-i_1}} && \text{(by (4.2))},\end{aligned} \tag{4.4}$$

which gives (4.3). ☐

Proof of Theorem 4.1. 1° We first show that for all $1 \le k \le p-1$ and

$$1 + \sum_{j=0}^{k-1} j \le i_k < \cdots < i_{p-1} \le n-k-1,$$

we have

$$a_{i_k} \cdots a_{i_{p-1}} = 0.$$

We use induction on k. When $k = 1$, the conclusion follows from Lemma 4.2 with $t_{p-2} = \cdots = t_1 = 0$. Assume $2 \le k \le p-1$. In Lemma 4.2, let $t_1 = k-1$, $t_2 = k-2$, …, $t_{k-1} = 1$, $t_k = \cdots = t_{p-2} = 0$, $i_{k-1} = i_k - 1$, $i_{k-2} = i_k - 2$, …, $i_1 = i_k - (k-1)$, and note that $i_{p-1} + t_1 = i_{p-1} + k - 1 \le n-2$. We have

$$\sum_{\tau} a^*_{i_{p-1}+\tau(p-1)} \cdots a^*_{i_1+\tau(1)} = 0, \tag{4.5}$$

where $(\tau(1), \dots, \tau(p-1))$ runs through all permutations of $(k-1, k-2, \dots, 1, 0, \dots, 0)$ and the $*$'s are suitable powers of p. (In general, we use a $*$ to denote a positive integer exponent whose exact value is not important.) Multiplying (4.5) by $a_{i_k} \cdots a_{i_{p-1}}$ gives

$$a^*_{i_k} \cdots a^*_{i_{p-1}} + \sum_{\substack{\tau \\ (\tau(1),\dots,\tau(k-1)) \ne (k-1,\dots,1)}} a_{i_k} \cdots a_{i_{p-1}} a^*_{i_{p-1}+\tau(p-1)} \cdots a^*_{i_1+\tau(1)} = 0. \tag{4.6}$$

When $(\tau(1),\dots,\tau(k-1))\neq(k-1,\dots,1)$, at least one of $i_1+\tau(1),\dots,i_{p-1}+\tau(p-1)$, say i'_{k-1}, is less than i_k. Also note that $i'_{k-1}\geq i_1=i_k-(k-1)\geq 1+1+2+\cdots+(k-2)$. Therefore by the induction hypothesis, $a_{i'_{k-1}}a_{i_k}\cdots a_{i_{p-1}}=0$. Thus the $\sum$ in (4.6) equals 0, which gives $a_{i_k}\cdots a_{i_{p-1}}=0$.

2° Let $k=p-1$ in 1°. We have

$$a_i=0 \quad \text{for all } 1+\frac{1}{2}(p-2)(p-1)\leq i\leq n-p.$$

3° We claim that

$$a_i=0 \quad \text{for all } 1\leq i\leq \frac{1}{2}(p-2)(p-1).$$

Assume to the contrary that this is not true. Let $1\leq l\leq \frac{1}{2}(p-2)(p-1)$ be the largest integer such that $a_l\neq 0$. Let

$$\alpha=(\underbrace{\underbrace{1\ \cdots\ 1}_{l}\ \underbrace{0\ \cdots\ 0}_{p+1}\ \underbrace{1\ \cdots\ 1}_{l}\ \underbrace{0\ \cdots\ 0}_{p+1}\ \cdots\ \underbrace{1\ \cdots\ 1}_{l}\ \underbrace{0\ \cdots\ 0}_{p+1}}_{p-1\text{ copies}}\ 0\ \cdots\ 0)\in\Omega_0.$$

(Here we used the assumption that $n\geq(p-1)\bigl[\frac{1}{2}(p-2)(p-1)+p+1\bigr]$.) For $0\leq k\leq p-2$, we have $\mathrm{asc}(\alpha+(k\ \cdots\ k))=p-1$ and

$$\begin{aligned}&\mathrm{Asc}\bigl(\alpha+(k\ \cdots\ k)\bigr)=\bigl\{0,\,l+p+1,\,2(l+p+1),\,\dots,\,(p-2)(l+p+1)\bigr\},\\&\mathrm{Des}\bigl(\alpha+(k\ \cdots\ k)\bigr)=\bigl\{l,\,l+p+1+l,\,2(l+p+1)+l,\,\dots,\,(p-2)(l+p+1)+l\bigr\}.\end{aligned}$$

If $\alpha+(k\ \cdots\ k)$ is expressed as a sum of $p-1$ elements (not necessarily distinct) of S, the expression must be of the form

$$\alpha+(k\ \cdots\ k)=s(0,i_1)+s(l+p+1,i_2)+\cdots+s((p-2)(l+p+1),i_{p-1}), \tag{4.7}$$

where $i_1,\dots,i_{p-1}\in\{1,\dots,n-1\}$, and in modulus n

$$\begin{aligned}&\bigl\{i_1,\,l+p+1+i_2,\,\dots,\,(p-2)(l+p+1)+i_{p-1}\bigr\}\\=&\bigl\{l,\,l+p+1+l,\,2(l+p+1)+l,\,\dots,\,(p-2)(l+p+1)+l\bigr\}.\end{aligned}\tag{4.8}$$

We further require $a_{i_1}\cdots a_{i_{p-1}}\neq 0$, which implies that $i_1,\dots,i_{p-1}\in\{1,\dots,l\}\cup\{n-p+1,\dots,n-1\}$. It follows from (4.8) that $i_1=\cdots=i_{p-1}=l$. Thus we have

$$\begin{aligned}0&=C(\alpha) && \text{(by (4.1))}\\&=(p-1)!\,a_l^{p^0}a_l^{p^{l+p+1}}\cdots a_l^{p^{(p-2)(l+p+1)}} && \text{(by (4.2) and (4.7))},\end{aligned}\tag{4.9}$$

which is a contradiction.

4° Finally, we show that

$$a_i=0 \quad \text{for all } n-p+1\leq i\leq n-1.$$

Assume to the contrary that this is not true. Let $n-l\in\{n-p+1,\dots,n-1\}$ be the smallest integer such that $a_{n-l}\neq 0$. Let

$$\alpha=(1\ \cdots\ 1\ \underbrace{\underbrace{0\ \cdots\ 0}_{l}\ 1\ \cdots\ \underbrace{0\ \cdots\ 0}_{l}\ 1\ \underbrace{0\ \cdots\ 0}_{l}\ 1}_{p-1\text{ copies}})\in\Omega_0.$$

For $0 \le k \le p-2$, we have $\mathrm{asc}(\alpha + (k\ \cdots\ k)) = p-1$ and

$$\mathrm{Asc}\big(\alpha + (k\ \cdots\ k)\big) = \big\{n-1,\, n-1-(l+1),\, \dots,\, n-1-(p-2)(l+1)\big\},$$
$$\mathrm{Des}\big(\alpha + (k\ \cdots\ k)\big) = \big\{n-1-l,\, n-1-l-(l+1),\, \dots,\, n-1-l-(p-2)(l+1)\big\}.$$

If $\alpha + (k\ \cdots\ k)$ is expressed as a sum of $p-1$ elements (not necessarily distinct) of S, the expression must be of the form

$$\begin{aligned} &\alpha + (k\ \cdots\ k) \\ &= s(n-1, i_1) + s(n-1-(l+1), i_2) + \cdots + s(n-1-(p-2)(l+1), i_{p-1}), \end{aligned} \tag{4.10}$$

where $i_1, \dots, i_{p-1} \in \{1, \dots, n-1\}$, and in modulus n

$$\begin{aligned} &\big\{n-1+i_1,\, n-1-(l+1)+i_2,\, \dots,\, n-1-(p-2)(l+1)+i_{p-1}\big\} \\ &= \big\{n-1-l,\, n-1-l-(l+1),\, \dots,\, n-1-l-(p-2)(l+1)\big\}. \end{aligned} \tag{4.11}$$

We further require $a_{i_1} \cdots a_{i_{p-1}} \ne 0$, which implies that $i_1, \dots, i_{p-1} \in \{n-l, \dots, n-1\}$. Under this restriction, it is easy to see that (4.11) forces $i_1 = \cdots i_{p-1} = n-l$. Thus we have

$$\begin{aligned} 0 &= C(\alpha) && \text{(by (4.1))} \\ &= (p-1)!\, a_{n-l}^{p^{n-1}}\, a_{n-l}^{p^{n-1-(l+1)}} \cdots a_{n-l}^{p^{n-1-(p-2)(l+1)}} && \text{(by (4.2) and (4.10))}, \end{aligned} \tag{4.12}$$

which is a contradiction. □

It appears that the assumption that $n \ge \frac{1}{2}(p-1)(p^2-p+4)$ in Theorem 4.1 may be weakened. On the other hand, when q is not a prime, the proofs of Lemma 4.2 and Theorem 4.1 fail for the following reason: In (4.4), (4.9) and (4.12), $(p-1)!$ is replaced by $(q-1)!$, which is 0 in $\mathbb{F}_q$. When $q = p^e$, (4.1) becomes

$$\Bigg[\prod_{k=0}^{e-1} \sum_{0 \le i,j \le n-1} a_1^{p^k q^j} X^{p^k q^j (q^i - 1)}\Bigg]^{p-1} \equiv \mathrm{Tr}_{q^n/q}(a_0)^{q-1} + \Big[1 - \mathrm{Tr}_{q^n/q}(a_0)^{q-1}\Big] X^{q^n-1} \pmod{X^{q^n} - X}.$$

The question is how to decipher this equation.

5. A connection to some cyclic codes for general $\mathbb{F}_q$

In this section we prove certain necessary conditions for a q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ to satisfy $\mathrm{Tr}_{q^n/q}(L(x)/x) \ne 0$ for all $x \in \mathbb{F}_{q^n}^*$, where q is a prime power. In particular, we give a natural connection to some cyclic codes. There is also a connection of such cyclic codes to some algebraic curves. In the next section, we will use this connection to algebraic curves to get some necessary conditions for such q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$.

If $L(X) = a_0 X \in \mathbb{F}_{q^n}[X]$, then $\mathrm{Tr}_{q^n/q}(L(x)/x) \ne 0$ for all $x \in \mathbb{F}_{q^n}^*$ if and only if $\mathrm{Tr}_{q^n/q}(a_0) \ne 0$. Hence we assume that $L(X) = a_0 X + a_1 X^q + \cdots + a_{n-1} X^{q^{n-1}} \in \mathbb{F}_{q^n}[X]$ with $(a_1, a_2, \dots, a_{n-1}) \ne (0, 0, \dots, 0)$.

First we recall some notation and basic facts from coding theory (see, for example, [20]). Let $N = q^n - 1$. A code of length N over $\mathbb{F}_q$ is just a nonempty subset of $\mathbb{F}_q^N$. It is called a *linear* code if it is a vector space over $\mathbb{F}_q$. The set $C^\perp$ of all N-tuples in $\mathbb{F}_q^N$ orthogonal to all codewords of a linear code C with respect to the usual inner product on $\mathbb{F}_q^N$ is called the *dual code* of C. The Hamming weight of an arbitrary N-tuple $\mathbf{u} = (u_0, u_1, \dots, u_{N-1}) \in \mathbb{F}_q^N$ is

$$||\mathbf{u}|| = |\{0 \le i \le N-1 : u_i \ne 0\}|.$$

A *cyclic* code of length N over $\mathbb{F}_q$ is an ideal C of the quotient ring $R = \mathbb{F}_q[X]/\langle X^N - 1\rangle$. Here a codeword $(c_0, c_1, \dots, c_{N-1}) \in \mathbb{F}_q^N$ of C corresponds to an element $c_0 + c_1X + \cdots + c_{N-1}X^{N-1} + \langle X^N - 1\rangle \in C$. All ideals of R are principal. The monic polynomial $g(X)$ of the least degree such that $C = \langle g(X)\rangle/\langle X^N - 1\rangle$ is called the *generator* polynomial of C. The dual $C^\perp$ is cyclic with generator polynomial $X^{\deg h}h(X^{-1})/h(0)$, where $h(X) = (X^N - 1)/g(X)$.

If $\theta \in \mathbb{F}_{q^n}$ is a root of $g(X)$, then so is θ^q. A set $B \subset \mathbb{F}_{q^n}$ is called a *basic zero set* of C if both of the following conditions are satisfied:

- $\{\theta^{q^i} : \theta \in B, 0 \le i \le n-1\}$ is the set of the roots of $g(X)$.
- If $\theta_1, \theta_2 \in B$ with $\theta_1^{q^i} = \theta_2$ for some integer i, then $\theta_1 = \theta_2$.

The following proposition gives a natural connection to some cyclic codes. Some arguments in its proof will also be used in the next section.

Proposition 5.1. *Let γ be a primitive element of $\mathbb{F}_{q^n}^*$. Let C be the cyclic code of length $N = q^n - 1$ over $\mathbb{F}_q$ whose dual code $C^\perp$ has*

$$\{1, \gamma^{q-1}, \gamma^{q^2-1}, \dots, \gamma^{q^{n-1}-1}\}$$

as a basic zero set. We have the following: There exists a q-linearized polynomial $L(X) = a_0X + a_1X^q + \cdots + a_{n-1}X^{q^{n-1}} \in \mathbb{F}_{q^n}[X]$ with $(a_1, a_2, \dots, a_{n-1}) \ne (0, 0, \dots, 0)$ such that $\mathrm{Tr}_{q^n/q}(L(x)/x) \ne 0$ for all $x \in \mathbb{F}_{q^n}^*$ if and only if the cyclic code C has a codeword $(c_0, c_1, \dots, c_{N-1})$ of Hamming weight N such that $(c_0, c_1, \dots, c_{N-1}) \ne u(1, 1, \dots, 1)$ for any $u \in \mathbb{F}_q^*$. Moreover the dimension of C over $\mathbb{F}_q$ is $n^2 - n + 1$.

Proof. We first show that $\{1, \gamma^{q-1}, \gamma^{q^2-1}, \dots, \gamma^{q^{n-1}-1}\}$ is a basic zero set. This means that the exponents $0, q-1, q^2-1, \dots, q^{n-1}-1$ are in distinct q-cyclotomic cosets modulo $q^n - 1$. For $0 \le d < q^n - 1$, let $\psi(d)$ be the base q digits of d, i.e., $\psi(d) = (d_0, d_1, \dots, d_{n-1})$, where $0 \le d_i \le q-1$ are integers such that $d = \sum_{i=0}^{n-1} d_iq^i$. Let $\overline{0}, \overline{q-1}, \overline{q^2-1}, \dots, \overline{q^{n-1}-1}$ denote the q-cyclotomic cosets of $0, q-1, q^2-1, \dots, q^{n-1}-1$ modulo $q^n - 1$. Their images under ψ are

$$\begin{aligned}
&\psi(\overline{0}) = \{(0, 0, \dots, 0)\},\\
&\psi(\overline{q-1}) = \{(q-1, 0, 0, \dots, 0), (0, q-1, 0, \dots, 0), \dots, (0, 0, , \dots, 0, q-1)\},\\
&\psi(\overline{q^2-1}) = \{(q-1, q-1, 0, \dots, 0), (0, q-1, q-1, \dots, 0), \dots, (q-1, 0, \dots, 0, q-1)\},\\
&\qquad\vdots\\
&\psi(\overline{q^{n-1}-1}) = \{(q-1, \dots, q-1, 0), (0, q-1, \dots, q-1), \dots, (q-1, \dots, q-1.0)\}.
\end{aligned}$$

Note that the elements in each row are obtained via cyclic shifts of the first element of the row. This proves that $0, q-1, q^2-1, \dots, q^{n-1}-1$ are in distinct q-cyclotomic cosets modulo $q^n - 1$. Moreover the cardinality of the union of their q-cyclotomic cosets modulo $q^n - 1$ is

$$1 + (n-1)n = n^2 - n + 1.$$

Therefore the dimensions of C is $n^2 - n + 1$. Finally using Delsarte's Theorem [26, Theorem 9.1.2] we obtain that the codewords of C in $\mathbb{F}_q^N$ are

$$C = \left\{ \left(\mathrm{Tr}_{q^n/q}(a_0 + a_1 x^{q-1} + \cdots + a_{n-1} x^{q^{n-1}-1}) \right)_{x \in \mathbb{F}_{q^n}^*} : a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_{q^n} \right\}.$$

Note that $\mathrm{Tr}_{q^n/q}(L(x)/x) = u$ for all $x \in \mathbb{F}_{q^n}^*$ if and only if $\mathrm{Tr}_{q^n/q}(L(X)/X) \equiv u \pmod{X^{q^n} - X}$, from which it follows that $(a_1, a_2, \ldots, a_{n-1}) = (0, 0, \ldots, 0)$. This completes the proof. □

6. Some conditions via the Hasse-Weil-Serre bound for general $\mathbb{F}_q$

In this section we obtain some necessary conditions for the q-linearized polynomials $L(X) \in \mathbb{F}_{q^n}[X]$ such that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$.

The Hasse-Weil-Serre bound for algebraic curves over finite fields implies upper and lower bounds on the Hamming weights of codewords of cyclic codes (see [10, 28]). Using this method we obtain Theorem 6.1.

First we introduce further notations. Let $\mathrm{Res} : \mathbb{Z} \to \{0, 1, \ldots, q^n - 2\}$ be the map such that $\mathrm{Res}\,(j) \equiv j \pmod{q^n - 1}$. Put $q = p^m$ with $m \geq 1$, where p is the characteristic of $\mathbb{F}_q$. Let $\mathrm{Lead} : \{0, 1, \ldots, p^{mn} - 2\} \to \{0, 1, \ldots, p^{mn} - 2\}$ be the map sending j to the smallest integer k in $\{0, 1, \ldots, p^{mn-2}\}$ such that $k \equiv jp^u \pmod{p^{mn} - 1}$ for some integer $u \geq 0$. In other words, $\mathrm{Lead}(j)$ is the smallest nonnegative integer in the p-cyclotomic coset of j modulo $p^{mn} - 1$. It is important to note that if $0 < j < p^{mn} - 1$, then $\mathrm{Lead}(j)$ is a nonnegative integer which is coprime to p.

Theorem 6.1. *Let* $L(X) = a_0 X + a_1 X^q + \cdots + a_{n-1} X^{q^{n-1}} \in \mathbb{F}_{q^n}[X]$ *be a q-linearized polynomial with* $(a_1, \ldots, a_{n-1}) \neq (0, \ldots, 0)$*. For each* $1 \leq j \leq q^n - 2$ *with* $\gcd(j, q^n - 1) = 1$*, let*

$$\ell(j) = \max\{\mathrm{Lead}(\mathrm{Res}\,(j(q^i - 1))) : 1 \leq i \leq n-1 \text{ and } a_i \neq 0\}.$$

Moreover, let

$$\ell = \min_j \ell(j), \tag{6.1}$$

where the minimum is over all integers $1 \leq j \leq q^n - 2$ *with* $\gcd(j, q^n - 1) = 1$*. Then we have the following:*

- *Case* $\mathrm{Tr}_{q^n/q}(a_0) \neq 0$*: If*
$$q^n + 1 - \frac{(q-1)(\ell-1)}{2} \lfloor 2q^{n/2} \rfloor > 1, \tag{6.2}$$
then it is impossible that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ *for all* $x \in \mathbb{F}_{q^n}^*$*.*
- *Case* $\mathrm{Tr}_{q^n/q}(a_0) = 0$*: If*
$$q^n + 1 - \frac{(q-1)(\ell-1)}{2} \lfloor 2q^{n/2} \rfloor > q + 1, \tag{6.3}$$
then it is impossible that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ *for all* $x \in \mathbb{F}_{q^n}^*$*.*

Proof. If γ is a primite element of $\mathbb{F}_{q^n}^*$, then γ^j is also a primitive element of $\mathbb{F}_{q^n}^*$ for all $1 \leq j \leq q^n - 2$ with $\gcd(j, q^n - 1) = 1$. Note that

$$\mathrm{Tr}_{q^n/q}(L(x)/x) = \mathrm{Tr}_{q^n/q}(a_0 + a_1 x^{q-1} + \cdots + a_{n-1} x^{q^{n-1}-1}) \neq 0 \text{ for all } x \in \mathbb{F}_{q^n}^*,$$

if and only if

$$\mathrm{Tr}_{q^n/q}(L(x^j)/x^j) = \mathrm{Tr}_{q^n/q}(a_0+a_1x^{j(q-1)}+\cdots+a_{n-1}x^{j(q^{n-1}-1)}) \neq 0 \text{ for all } x \in \mathbb{F}_{q^n}^*.$$

Moreover, $x^{j(q^i-1)} = x^{\mathrm{Res}\,(j(q^i-1))}$ for $x \in \mathbb{F}_{q^n}^*$, $1 \le i \le n-1$ and $1 \le j \le q^n-2$.

Recall that ℓ is defined in (6.1). We choose and fix an integer $1 \le j \le q^n-2$ with $\gcd(j, q^n-1) = 1$ such that $\ell = \ell(j)$.

Let $a_{t_1}, \dots, a_{t_s}$ be the nonzero coefficients among $a_1, \dots, a_{n-1}$. (Note that $s \ge 1$ since $(a_1, \dots, a_{n-1}) \neq (0, \dots, 0)$.) Since $0, q^{t_1}-1, \dots, q^{t_s}-1$ belong to different p-cyclotomic cosets modulo q^n-1 and $\gcd(j, q^n-1) = 1$, we have that $0, j(q^{t_1}-1), \dots, j(q^{t_s}-1)$ belong to different p-cyclotomic cosets modulo q^n-1. Thus $\mathrm{Res}\,(j(q^{t_i}-1)) = j_ip^{u_i}$, where $u_i \ge 0$, $p \nmid j_i$, $1 \le i \le s$, and $j_1, \dots, j_s$ are distinct. We may assume $0 < j_1 < j_2 < \cdots < j_s = \ell$. We have

$$a_0 + a_1X^{\mathrm{Res}\,(j(q-1))} + \cdots + a_{n-1}X^{\mathrm{Res}\,(j(q^{n-1}-1))} = a_0 + b_1X^{j_1p^{u_1}} + \cdots + b_sX^{j_sp^{u_s}},$$

where $b_i = a_{t_i}$, $1 \le i \le s$.

Let χ be the Artin-Shreier type algebraic curve over $\mathbb{F}_{q^n}$ given by

$$\chi : Y^q - Y = a_0 + b_1X^{j_1p^{u_1}} + \cdots + b_sX^{j_sp^{u_s}}.$$

Let $S \subset \mathbb{F}_{p^{mn}}^*$ be a complete set of coset representatives of $\mathbb{F}_p^*$ in $\mathbb{F}_{p^{mn}}^*$. For $\mu \in S$, let χ_μ be the Artin-Shreier type algebraic curve over $\mathbb{F}_{q^n}$ given by

$$\chi_\mu : Y^p - Y = \mu(a_0 + b_1X^{j_1p^{u_1}} + \cdots + b_sX^{j_sp^{u_s}}).$$

Note that χ_μ is a degree p covering of the projective line. Using [9, Theorem 2.1] the genus $g(\chi)$ of χ is computed in terms of the genera of χ_μ as

$$g(\chi) = \sum_{\mu \in S} g(\chi_\mu). \tag{6.4}$$

Now we determine the genus $g(\chi_\mu)$ of χ_μ. We choose and fix $\mu \in S$. Let $c_1, c_2, \dots, c_s \in \mathbb{F}_{p^{mn}}^*$ be such that

$$c_1^{p^{u_1}} = \mu b_1,\ c_2^{p^{u_2}} = \mu b_2,\ \dots,\ c_s^{p^{u_s}} = \mu b_s.$$

Let χ'_μ be the Artin-Schreier type algebraic curve over $\mathbb{F}_{q^n}$ given by

$$\chi'_\mu : Y^p - Y = \mu a_0 + c_1X^{j_1} + \cdots + c_sX^{j_s}.$$

We observe that χ_μ and χ'_μ are birationally isomorphic and hence the genera $g(\chi_\mu)$ and $g(\chi'_\mu)$ are the same. Indeed, if $u_1 \ge 1$, then

$$\begin{aligned} Y^p - Y &= \mu a_0 + c_1^{p^{u_1}}X^{j_1p^{u_1}} + c_2^{p^{u_2}}X^{j_2p^{u_2}} + \cdots + c_s^{p^{u_s}}X^{j_sp^{u_s}} \\ &= \mu a_0 + \left(c_1^{p^{u_1-1}}X^{j_1p^{u_1-1}}\right)^p + c_2^{p^{u_2}}X^{j_2p^{u_2}} + \cdots + c_s^{p^{u_s}}X^{j_sp^{u_s}} \end{aligned}$$

and hence

$$\begin{aligned} &\left[Y - \left(c_1^{p^{u_1-1}}X^{j_1p^{u_1-1}}\right)\right]^p - \left[Y - \left(c_1^{p^{u_1-1}}X^{j_1p^{u_1-1}}\right)\right] \\ &= \mu a_0 + c_1^{p^{u_1-1}}X^{j_1p^{u_1-1}} + c_2^{p^{u_2}}X^{j_2p^{u_2}} + \cdots + c_s^{p^{u_s}}X^{j_sp^{u_s}}. \end{aligned}$$

This gives a birational isomorphism between χ_μ and the curve given by

$$Y^p - Y = \mu a_0 + c_1^{p^{u_1-1}}X^{j_1p^{u_1-1}} + c_2^{p^{u_2}}X^{j_2p^{u_2}} + \cdots + c_s^{p^{u_s}}X^{j_sp^{u_s}}.$$

By induction on u_1 we obtain a birational isomorphism between χ_μ and the curve given by

$$Y^p - Y = \mu a_0 + c_1 X^{j_1} + c_2^{p^{u_2}} X^{j_2 p^{u_2}} + \cdots + c_s^{p^{u_s}} X^{j_s p^{u_s}}.$$

Applying the same method to the monomials $c_2^{p^{u_2}} X^{j_2 p^{u_2}}, \ldots, c_s^{p^{u_s}} X^{j_s p^{u_s}}$ we conclude that the curves χ_μ and χ'_μ are birationally isomorphic.

Recall that the integers $0, j_1, \ldots, j_s$ are in distinct p-cyclotomic cosets modulo $q^n - 1$. As $c_s \neq 0$ and $\gcd(j_s, p) = 1$ we obtain that χ'_μ is absolutely irreducible over $\mathbb{F}_{q^n}$. Moreover $s \geq 1$ and $j_s = \ell$. Hence by [26, Proposition 3.7.8] we have

$$g(\chi_\mu) = g(\chi'_\mu) = (p-1)(\ell-1)/2,$$

which is independent from the choice of $\mu \in S$. Using (6.4) for the genus $g(\chi)$ of χ we obtain that

$$g(\chi) = \sum_{\mu \in S} g(\chi_\mu) = |S|(p-1)(\ell-1)/2 = (q-1)(\ell-1)/2.$$

Assume that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$. The number $N(\chi)$ of $\mathbb{F}_{q^n}$-rational points of χ is

(6.5)
$$N(\chi) = 1 + q|\{x \in \mathbb{F}_{q^n} : \mathrm{Tr}(L(x)/x) = 0\}| = \begin{cases} 1 & \text{if } \mathrm{Tr}_{q^n/q}(a_0) \neq 0, \\ q+1 & \text{if } \mathrm{Tr}_{q^n/q}(a_0) = 0. \end{cases}$$

The Hasse-Weil-Serre lower bound on $N(\chi)$ (see, for example, [26, Theorem 5.3.1]) implies that

$$N(\chi) \geq q^n + 1 - \frac{(q-1)(\ell-1)}{2} \lfloor 2q^{n/2} \rfloor. \tag{6.6}$$

Combining (6.2), (6.3), (6.5) and (6.6), we complete the proof. □

The following corollary, which is a restatement of Theorem 6.1, shows that the distribution of the nonzero coefficients of a q-linearized polynomial L satisfying $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$ is subject to certain restrictions.

Corollary 6.2. *Let $L(X) = a_0 X + a_1 X^q + \cdots + a_{n-1} X^{q^{n-1}} \in \mathbb{F}_{q^n}[X]$ be a q-linearized polynomial with $(a_1, \ldots, a_{n-1}) \neq (0, \ldots, 0)$. Assume that $\mathrm{Tr}_{q^n/q}(L(x)/x) \neq 0$ for all $x \in \mathbb{F}_{q^n}^*$. Then for each integer $1 \leq j \leq q^n - 2$ with $\gcd(j, q^n - 1) = 1$ we have the following:*

(i) *If $\mathrm{Tr}_{q^n/q}(a_0) \neq 0$, there exits $1 \leq i \leq n-1$ such that $a_i \neq 0$ and*

$$\mathrm{Lead}(\mathrm{Res}\,(j(q^i - 1))) \geq 1 + \left\lceil \frac{2q^n}{(q-1)\lfloor 2q^{n/2} \rfloor} \right\rceil.$$

(ii) *If $\mathrm{Tr}_{q^n/q}(a_0) = 0$, there exits $1 \leq i \leq n-1$ such that $a_i \neq 0$ and*

$$\mathrm{Lead}(\mathrm{Res}\,(j(q^i - 1))) \geq 1 + \left\lceil \frac{2(q^n - q)}{(q-1)\lfloor 2q^{n/2} \rfloor} \right\rceil.$$

References

[1] A. A. Albert. Finite division algebras and finite planes. In *Proc. Sympos. Appl. Math., Vol. 10*, pages 53–70. American Mathematical Society, Providence, R.I., 1960.

[2] J. Bierbrauer. Semifields, theory and elementary constructions. invited talk presented in Combinatorics 2012, Perugia, September 2012.

[3] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: the user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.

[4] I. Cardinali, O. Polverino, and R. Trombetti. Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$. *European Journal of Combinatorics*, 27(6):940–961, 2006.

[5] P. Dembowski. *Finite Geometries*. Springer, New York, 1997.

[6] P. Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103:239–258, 1968.

[7] L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(4):514–522, 1906.

[8] M. J. Ganley. Polarities in translation planes. *Geometriae Dedicata*, 1(1):103–116, 1972.

[9] A. Garcia and H. Stichtenoth. Elementary abelian p-extensions of algebraic function fields. *Manuscripta Math.*, 72(1):67–79, 1991.

[10] C. Guneri and F. Özbudak. Weil-Serre type bounds for cyclic codes. *IEEE Transactions on Information Theory*, 54(12):5381–5395, 2008.

[11] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998.

[12] X. Hou. Solution to a problem of S. Payne. *Proceedings of the American Mathematical Society*, 132(1):1–6, 2004.

[13] D. R. Hughes and F. C. Piper. *Projective Planes*. Springer-Verlag, New York, 1973.

[14] N. L. Johnson, V. Jha, and M. Biliotti. *Handbook of Finite Translation Planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[15] D. Jungnickel. On automorphism groups of divisible designs. *Canadian Journal of Mathematics*, 34(2):257–297, 1982.

[16] W. M. Kantor. Commutative semifields and symplectic spreads. *Journal of Algebra*, 270(1):96–114, 2003.

[17] D. E. Knuth. Finite semifields and projective planes. *Journal of Algebra*, 2:182–217, 1965.

[18] M. Lavrauw and O. Polverino. Finite semifields. In L. Storme and J. De Beule, editors, *Current Research Topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, Hauppauge, NY, 2011.

[19] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[20] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Co., Amsterdam, 1977.

[21] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *Journal of Algebra*, 47(2):400–410, 1977.

[22] S. E. Payne. Linear transformations of a finite field. *American Mathematical Monthly*, 78:659–660, 1971.

[23] S. E. Payne. A complete determination of translation ovoids in finite Desarguesian planes. *Lincei - Rend. Sc. fis. mat. nat. LI*, pages 328–331, 1971.

[24] A. Pott and Y. Zhou. Switching construction of planar functions on finite fields. In *Proceedings of the Third International Conference on Arithmetic of Finite Fields*, WAIFI'10, pages 135–150, Springer-Verlag, Berlin, Heidelberg, 2010.

[25] K-U. Schmidt and Y. Zhou. Planar functions over fields of characteristic two. `arXiv:1301.6999`, to appear in *Journal of Algebraic Combinatorics*.

[26] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin, 2nd edition, 2008.

[27] J. H. M. Wedderburn. A theorem on finite algebras. *Transaction of the American Mathematical Society*, 6(3):349–352, 1905.

[28] J. Wolfmann. New bounds on cyclic codes from algebraic curves. In G. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 in Lecture Notes in Computer Science, pages 47–62. Springer Berlin Heidelberg, 1989.

[29] Y. Zhou. $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations. *Journal of Combinatorial Designs*, 21(12):563–584, 2013.