SOLUTION TO A PROBLEM OF S. PAYNE

XIANG-DONG HOU

(Communicated by David E. Rohrlich)

Abstract. A problem posed by S. Payne calls for determination of all linearized polynomials $f(x) \in \mathbb{F}_{2^n}[x]$ such that $f(x)$ and $f(x)/x$ are permutations of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n}$ respectively. We show that such polynomials are exactly of the form $f(x) = ax^{2^k}$ with $a \in \mathbb{F}_{2^n}^*$ and $(k, n) = 1$. In fact, we solve a $q$-ary version of Payne’s problem.

1. Introduction

Let $\mathbb{F}_{2^n}$ be the finite field with $2^n$ elements. In 1971, S. Payne posed the following problem [6]:

Problem 1.1. Determine all linearized polynomials

$$f(x) = a_0x + a_1x^2 + \cdots + a_{n-1}x^{2^{n-1}} \in \mathbb{F}_{2^n}[x]$$

such that $f(x)$ is a permutation polynomial of $\mathbb{F}_{2^n}$ and

$$f(x)/x = a_0 + a_1x^{2-1} + \cdots + a_{n-1}x^{2^{n-1}-1}$$

is a permutation of $\mathbb{F}_{2^n}^*$.

Problem 1.1 originated from projective geometry. In fact, the polynomials in Problem 1.1 give rise to ovoids in the projective plane $\text{PG}(2, 2^n)$. (Cf. [2], p. 50 and [3]). Obviously, if $a \in \mathbb{F}_{2^n}^*$ and $k$ is a positive integer such that $(k, n) = 1$, then $f(x) = ax^{2^k}$ satisfies the requirements in Problem 1.1. However, as noted in [6], no other linearized polynomials with the same properties are known. In this paper, we will show that $f(x) = ax^{2^k}$ $(a \in \mathbb{F}_{2^n}^*, \ (k, n) = 1)$ are the only polynomials in Problem 1.1. In general, for any $\mathbb{F}_q$-linear map $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$, we say that $f(x)/x$ is a permutation of $\mathbb{F}_q^n/\mathbb{F}_q$ if given any $\alpha \in \mathbb{F}_q^n$, there exists $\beta \in \mathbb{F}_q^n$ such that $f(\beta)/\beta = \alpha \alpha$ for some $\alpha \in \mathbb{F}_q^n$. In fact, we will solve the following $q$-ary version of Problem 1.1:

Problem 1.2. Determine all linearized polynomials $f(x) = \sum_{i=0}^{n-1} a_ix^{q^i} \in \mathbb{F}_{q^n}[x]$ such that $f(x)$ is a permutation of $\mathbb{F}_{q^n}$ and $f(x)/x$ is a permutation of $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Received by the editors July 29, 2002.

2000 Mathematics Subject Classification. Primary 11T06; Secondary 51E20.

Key words and phrases. Finite field, linearized polynomial, permutation polynomial.

This research was supported by NSA grant MDA 904-02-1-0080.
We briefly review linearized polynomials over finite fields in Section 2. In particular, we prove a proposition that slightly generalizes Dickson’s criterion for a linearized polynomial to be nonsingular. The proof of our solution to Problem 1.2 is in Section 3. In Section 4, we solve another problem about linearized polynomials over $\mathbb{F}_{2^n}$ which is similar and related to Problem 1.1.

2. Linearized Polynomials

Let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ be finite fields with $q$ and $q^n$ elements respectively. The $\mathbb{F}_q$-linear maps from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ are precisely linearized polynomials

$$f(x) = a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}} \in \mathbb{F}_{q^n}[x].$$

Define

$$A(f) = \begin{bmatrix}
a_0 & a_1 & \cdots & a_{n-1} \\
a_0^q & a_0 & \cdots & a_{n-2}^q \\
\vdots & \vdots & \ddots & \vdots \\
a_0^{q^{n-1}} & a_0^{q^{n-2}} & \cdots & a_0^{q^{n-2}}
\end{bmatrix}.$$ 

It is well known that $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a permutation polynomial if and only if $\det A(f) \neq 0$ ([3], p. 66 or [4], p. 361). The following proposition slightly generalizes this criterion.

**Proposition 2.1.** In the above notation, we have

$$\text{rank } A(f) = \dim_{\mathbb{F}_q} f(\mathbb{F}_{q^n}).$$

**Proof.** Let

$$V = \left\{ \begin{bmatrix} z \\ z^q \\ \vdots \\ z^{q^{n-1}} \end{bmatrix} : z \in \mathbb{F}_{q^n} \right\} \subset \mathbb{F}_{q^n}^n$$

and define an $\mathbb{F}_q$-isomorphism

$$\iota : \mathbb{F}_{q^n} \longrightarrow V$$

$$z \longrightarrow \begin{bmatrix} z \\ z^q \\ \vdots \\ z^{q^{n-1}} \end{bmatrix}.$$ 

Note that the $\mathbb{F}_{q^n}$-linear map $A(f) : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ satisfies $A(f)(V) \subset V$. Furthermore, we have the following commutative diagram:
Therefore,
\[
\text{rank } (A(f)) = \text{dim}_{F_q^n} (A(f)(F_q^n)) = \text{dim}_{F_q^n} \left[ (t \otimes 1) \circ (f \otimes 1)(F_q^n \otimes_{F_q} F_q^n) \right] = \text{dim}_{F_q^n} \left[ f(F_q^n) \otimes_{F_q} F_q^n \right] = \text{dim}_{F_q} \left[ f(F_q^n) \right].
\]

\[
\square
\]

3. Solution to Problem 1.2

Let \( q \) be a prime power and \( n \) a positive integer.

**Lemma 3.1.** Let \( f(x) = \sum_{i=0}^{n-1} a_i x^i \in F_q^n[x] \) be a polynomial in Problem 1.2. Then the determinants of the principal submatrices of
\[
A(f) = \begin{bmatrix}
    a_0 & a_1 & \cdots & a_{n-1} \\
    a_{n-1} & a_0 & \cdots & a_{n-2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_1^{n-1} & a_2^{n-1} & \cdots & a_0^{n-1}
\end{bmatrix}
\]
of size \( m \times m \) (\( 1 \leq m \leq n - 1 \)) are all 0.

**Proof.** Let
\[
D(x) = \begin{bmatrix}
    a_0 + x & a_1 & \cdots & a_{n-1} \\
    a_1^{n-1} & (a_0 + x)^q & \cdots & a_{n-2}^{q} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_1^{q(n-1)} & a_2^{q(n-1)} & \cdots & (a_0 + x)^{q(n-1)}
\end{bmatrix} \in F_q^n[x].
\]

For each \( b \in F_q^n \), since \( f(x)/x \) is a permutation of \( F_q^n/F_q \), there exist \( z \in F_q^n \) and \( \epsilon \in F_q \) such that \( \frac{D(z)}{a_0 + \epsilon x} = -eb \). Thus \( z \) is a root of
\[
(a_0 + \epsilon b)x + a_1 x^q + \cdots + a_{n-1} x^{q(n-1)};
\]
hence the polynomial in (3.1) is not a permutation polynomial of \( F_q^n \). It follows from Proposition 2.1 that \( D(\epsilon b) = 0 \). Therefore, for every \( b \in F_q^n \), \( \prod_{e \in F_q^n} D(\epsilon b) = 0 \), which implies that
\[
\prod_{e \in F_q^n} D(\epsilon x) = \delta(x^{q(n-1)} - 1)
\]
for some \( \delta \in F_q^n \). (In fact, \( \delta = -1 \), although this fact is not needed in the proof. This is because \( D(0) \) is invariant under the Frobenius map of \( F_q^n/F_q \) and \( -\delta = (D(0))^{q-1} = 1 \).

Let \( 0 \leq i_1 < i_2 < \cdots < i_m \leq n - 1 \) with \( 1 \leq m \leq n - 1 \). Write \( \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_m\} = \{j_1, \ldots, j_k\} \) with \( 0 \leq j_1 < \cdots < j_k \leq n - 1 \). Consider the coefficient of \( x^{(q-1)j_1+\cdots+(q-1)j_k} \) in
\[
\prod_{e \in F_q^n} D(\epsilon x) = \prod_{e \in F_q^n} \begin{bmatrix}
    a_0 + \epsilon x & a_1 & \cdots & a_{n-1} \\
    a_1^{q(n-1)} & a_0^{q} + \epsilon x^q & \cdots & a_{n-2}^{q} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_1^{q(n-1)} & a_2^{q(n-1)} & \cdots & a_0^{q(n-1)} + \epsilon x^{q(n-1)}
\end{bmatrix}.
\]
By the uniqueness of the $q$-adic expansion of $(q-1)q^i + \cdots + (q-1)q^s$, we see that this coefficient equals

$$[\det(A(f)(i_1, \cdots, i_m))]^{q-1} \prod_{\epsilon \in \mathbb{F}_q} \epsilon^s = [\det(A(f)(i_1, \cdots, i_m))]^{q-1}(-1)^s,$$

where $A(f)(i_1, \cdots, i_m)$ is the principal submatrix of $A(f)$ with row and column indices $i_1, \cdots, i_m$, namely, the submatrix of $A(f)$ obtained by deleting rows and columns with indices other than $i_1, \cdots, i_m$. Comparing the coefficients of $x^{(q-1)q^i+\cdots+(q-1)q^s}$ in the two sides of (3.2), we have $\det(A(f)(i_1, \cdots, i_m)) = 0$. \hfill $\square$

**Theorem 3.2.** The polynomials in Problem 1.2 are exactly the ones of the form $f(x) = ax^k$ where $a \in \mathbb{F}_q^n$, and $k$ is a positive integer such that $(k, n) = 1$.

**Proof.** Let $f(x) = a_0x + a_1x^q + \cdots + a_{n-1}x^{q^{n-1}} \in \mathbb{F}_q^n[x]$ be a polynomial in Problem 1.2. It suffices to show that $f(x)$ has exactly one nonzero coefficient. By Lemma 3.1 the determinants of principal submatrices of

$$A(f) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_n^{q-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{bmatrix}$$

of sizes $1 \times 1$, $2 \times 2$, $\cdots$, $(n-1) \times (n-1)$ are all 0. Observe that

$$A(f) = [b_{ij}]_{0 \leq i, j \leq n-1}$$

where

$$b_{ij} = 0 \text{ if and only if } a_{j-i} = 0,$$

where the subscript is taken modulo $n$.

We claim that if $i_1 + \cdots + i_m \equiv 0 \pmod{n}$ $(1 \leq m \leq n-1)$, then

$$a_{i_1} \cdots a_{i_m} = 0.$$

To prove (3.3), we use induction on $m$. The case $m = 1$ is obvious. Assume to the contrary that $i_1 + \cdots + i_m \equiv 0 \pmod{n}$ but $a_{i_1} \cdots a_{i_m} \neq 0$. We may assume that $0, i_1, i_1+i_2, \cdots, i_1+\cdots+i_{m-1}$ are all distinct modulo $n$. (Otherwise, $i_1+\cdots+i_t \equiv 0 \pmod{n}$ for some $1 \leq s < t \leq m-1$. By the induction hypothesis, $a_{i_1} \cdots a_{i_t} = 0$, which is a contradiction.) Consider the principal submatrix of $A(f)$ with row and column indices $j_0 = 0, j_1 = i_1, j_2 = i_1+i_2, \cdots, j_{m-1} = i_1+\cdots+i_{m-1}$:

$$B = \begin{bmatrix} b_{j_0} & b_{j_1} & \cdots & b_{j_{m-1}} \\ b_{j_1} & b_{j_2} & \cdots & b_{j_{m-1}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{j_{m-1}} & b_{j_{m-1}} & \cdots & b_{j_{m-1}} \end{bmatrix}.$$
Thus the range of $F$ has dimension $1$ over $\mathbb{Z}/2\mathbb{Z}$. Then for any $c \in \mathbb{F}_{2^n}$, the range of $f(x) + cx$ has dimension $\geq n - 1$ over $\mathbb{F}_2$.

We consider another problem similar to Problem 1.1.

**Problem 4.1.** Determine all linearized polynomials $f(x) = \sum_{i=0}^{n-1} a_i x^{2i} \in \mathbb{F}_{2^n}[x]$ such that for any $c \in \mathbb{F}_{2^n}$, the range of $f(x) + cx$ has dimension $\geq n - 1$ over $\mathbb{F}_2$.

We mention that Problem 4.1 is related to a construction of partial difference sets in $\mathbb{Z}_4^k \times \mathbb{Z}_2^n$ (11). The solution of Problem 4.1 is similar to that of Problem 1.1.

**Theorem 4.2.** The polynomials in Problem 4.1 are exactly the ones of the form $f(x) = ax^{2^k} + bx$ where $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$ and $(k, n) = 1$.

**Proof.** First assume that $f(x) = ax^{2^k} + bx$ with $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$ and $(k, n) = 1$. Then for any $c \in \mathbb{F}_{2^n}$, $f(x) + cx = ax(x^{2^{k-1}} + \frac{b}{a^2})$ has at most two roots in $\mathbb{F}_{2^n}$. Thus the range of $f(x) + cx$ has dimension $\geq n - 1$ over $\mathbb{F}_2$.

Now assume that $f(x) = \sum_{i=0}^{n-1} a_i x^{2i} \in \mathbb{F}_{2^n}[x]$ is a polynomial in Problem 4.1. For each $c \in \mathbb{F}_{2^n}$, $f(x) + cx$ has at most one zero in $\mathbb{F}_{2^n}^*$, i.e., $\frac{f(x)}{x} = c$ has at most one solution in $\mathbb{F}_{2^n}^*$. Thus the map

$$
\psi : \begin{array}{c}
\mathbb{F}_{2^n}^* \\
x
\end{array} \longrightarrow \begin{array}{c}
\mathbb{F}_{2^n} \\
\frac{f(x)}{x}
\end{array}
$$
is one-to-one. Let $\mathbb{F}_{2^n} \setminus \psi(\mathbb{F}_{2^n}^*) = \{ b \}$. Then $f(x) + bx$ has no root in $\mathbb{F}_{2^n}^*$, hence is a permutation polynomial of $\mathbb{F}_{2^n}$. Furthermore, $\frac{f(x) + bx}{x} = \frac{f(x)}{x} + b$ is a permutation of $\mathbb{F}_{2^n}^*$. By Theorem 3.2, $f(x) + bx = ax^{2^k}$ where $a \in \mathbb{F}_{2^n}^*$ and $(k, n) = 1$. 

Finally, we remark that we have not found a $q$-ary version of Theorem 4.2.

References


Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435
E-mail address: xhou@euler.math.wright.edu
Current address: Department of Mathematics, University of South Florida, Tampa, Florida 33620