PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 1, Pages 1–6
S 0002-9939(03)07240-X
Article electronically published on August 13, 2003

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

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

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 $\mathrm{PG}(2, 2^n)$. (Cf. [2], p. 50 and [5].) 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 $f(\beta)/\beta = a\alpha$ for some $a \in \mathbb{F}_q^*$. In fact, we will solve the following q-ary version of Problem 1.1:

Problem 1.2. Determine all linearized polynomials $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ 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

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

Define

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

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*

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

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

$$\begin{array}{cccc} \iota: & \mathbb{F}_{q^n} & \longrightarrow & V \\ & z & \longmapsto & \begin{bmatrix} z \\ z^q \\ \vdots \\ z^{q^{n-1}} \end{bmatrix}. \end{array}$$

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:

$$\begin{array}{ccc} \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} & \xrightarrow{f\otimes 1} & \mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \\ \downarrow{\scriptstyle \iota\otimes 1} & & \downarrow{\scriptstyle \iota\otimes 1} \\ V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} & \xrightarrow{[A(f)|_V]\otimes 1} & V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} \\ \approx\downarrow & & \downarrow\approx \\ \mathbb{F}_{q^n}^n & \xrightarrow{A(f)} & \mathbb{F}_{q^n}^n \end{array}$$

Therefore,

$$\begin{aligned}\operatorname{rank}\big(A(f)\big) &= \dim_{\mathbb{F}_{q^n}}\big(A(f)(\mathbb{F}_{q^n}^n)\big)\\ &= \dim_{\mathbb{F}_{q^n}}\big[(\iota\otimes 1)\circ(f\otimes 1)(\mathbb{F}_{q^n}\otimes_{\mathbb{F}_q}\mathbb{F}_{q^n})\big]\\ &= \dim_{\mathbb{F}_{q^n}}\big[f(\mathbb{F}_{q^n})\otimes_{\mathbb{F}_q}\mathbb{F}_{q^n})\big]\\ &= \dim_{\mathbb{F}_q} f(\mathbb{F}_{q^n}).\end{aligned}$$

□

3. Solution to Problem 1.2

Let q be a prime power and n a positive integer.

Lemma 3.1. *Let $f(x)=\sum_{i=0}^{n-1}a_ix^{q^i}\in\mathbb{F}_{q^n}[x]$ be a polynomial in Problem 1.2. Then the determinants of the principal submatrices of*

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

of size $m\times m$ $(1\le m\le n-1)$ are all 0.

Proof. Let

$$D(x)=\begin{vmatrix} a_0+x & a_1 & \cdots & a_{n-1}\\ a_{n-1}^q & (a_0+x)^q & \cdots & a_{n-2}^q\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & (a_0+x)^{q^{n-1}}\end{vmatrix}\in\mathbb{F}_{q^n}[x].$$

For each $b\in\mathbb{F}_{q^n}^*$, since $f(x)/x$ is a permutation of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$, there exist $z\in\mathbb{F}_{q^n}^*$ and $\epsilon\in\mathbb{F}_q^*$ such that $\frac{f(z)}{z}=-\epsilon b$. Thus z is a root of

$$(a_0+\epsilon b)x+a_1x^q+\cdots+a_{n-1}x^{q^{n-1}}; \tag{3.1}$$

hence the polynomial in (3.1) is not a permutation polynomial of $\mathbb{F}_{q^n}$. It follows from Proposition 2.1 that $D(\epsilon b)=0$. Therefore, for every $b\in\mathbb{F}_{q^n}^*$, $\prod_{\epsilon\in\mathbb{F}_q^*}D(\epsilon b)=0$, which implies that

$$\prod_{\epsilon\in\mathbb{F}_q^*}D(\epsilon x)=\delta(x^{q^n-1}-1) \tag{3.2}$$

for some $\delta\in\mathbb{F}_{q^n}^*$. (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 $\mathbb{F}_{q^n}/\mathbb{F}_q$ and $-\delta=(D(0))^{q-1}=1$).

Let $0\le i_1<i_2<\cdots<i_m\le n-1$ with $1\le m\le n-1$. Write $\{0,\cdots,n-1\}\setminus\{i_1,\cdots,i_m\}=\{j_1,\cdots,j_s\}$ with $0\le j_1<\cdots<j_s\le n-1$. Consider the coefficient of $x^{(q-1)q^{j_1}+\cdots+(q-1)q^{j_s}}$ in

$$\prod_{\epsilon\in\mathbb{F}_q^*}D(\epsilon x)=\prod_{\epsilon\in\mathbb{F}_q^*}\begin{vmatrix} a_0+\epsilon x & a_1 & \cdots & a_{n-1}\\ a_{n-1}^q & a_0^q+\epsilon x^q & \cdots & a_{n-2}^q\\ \vdots & \vdots & \ddots & \vdots\\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}}+\epsilon x^{q^{n-1}}\end{vmatrix}. \tag{3.3}$$

By the uniqueness of the q-adic expansion of $(q-1)q^{j_1}+\cdots+(q-1)q^{j_s}$, we see that this coefficient equals

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

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 $x^{(q-1)q^{j_1}+\cdots+(q-1)q^{j_s}}$ in the two sides of (3.2), we have $\det\big(A(f)(i_1,\cdots,i_m)\big) = 0$. □

Theorem 3.2. *The polynomials in Problem 1.2 are exactly the ones of the form $f(x)=ax^{q^k}$ 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

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

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

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

where

$$b_{ij}=0 \text{ if and only if } a_{j-i}=0, \tag{3.4}$$

where the subscript is taken modulo n.

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

$$a_{i_1}\cdots a_{i_m}=0. \tag{3.5}$$

To prove (3.5), 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 $a_{i_1}\cdots a_{i_m}\ne 0$. We may assume that $0, i_1, i_1+i_2,\cdots, i_1+\cdots+i_{m-1}$ are all distinct modulo n. (Otherwise, $i_s+\cdots+i_t\equiv 0 \pmod n$ for some $1\le s<t\le m-1$. By the induction hypothesis, $a_{i_s}\cdots a_{i_t}=0$, which is a contradiction.) Consider the principal submatrix of $A(f)$ with row and column indices $j_0=0, j_1=i_1, j_2=i_1+i_2,\cdots, j_{m-1}=i_1+\cdots+i_{m-1}$:

$$B=\begin{bmatrix} 0 & b_{0j_1} & b_{0j_2} & \cdots & b_{0j_{m-1}}\\ b_{j_10} & 0 & b_{j_1j_2} & \cdots & b_{j_1j_{m-1}}\\ b_{j_20} & b_{j_2j_1} & 0 & \cdots & b_{j_2j_{m-1}}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ b_{j_{m-1}0} & b_{j_{m-1}j_1} & b_{j_{m-1}j_2} & \cdots & 0\end{bmatrix}.$$

Since $a_{i_1},\cdots,a_{i_m}$ are all nonzero, by (3.4), b_{0j_1}, $b_{j_1j_2},\cdots,b_{j_{m-2}j_{m-1}}$, $b_{j_{m-1}0}$ are all nonzero. Since all 2×2 principal submatrices of B have determinant 0, $b_{j_10} =$

$b_{j_2j_1} = \cdots = b_{j_{m-1}j_{m-2}} = 0$. Since all 3×3 principal submatrices of B have determinant 0, it follows that $b_{j_2 0} = b_{j_3 j_1} = \cdots = b_{j_{m-1}j_{m-3}} = 0$. (For example,

$$0 = \begin{vmatrix} 0 & b_{0j_1} & b_{0j_2} \\ 0 & 0 & b_{j_1j_2} \\ b_{j_2 0} & 0 & 0 \end{vmatrix} = b_{0j_1}b_{j_1j_2}b_{j_2 0}$$

implies that $b_{j_2 0} = 0$.) In the same way, by considering principal submatrices of B up to size $(m-1) \times (m-1)$, we conclude that

$$B = \begin{bmatrix} 0 & b_{0j_1} & * & \cdots & * & * \\ 0 & 0 & b_{j_1j_2} & \cdots & * & * \\ 0 & 0 & 0 & \cdots & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_{j_{m-2}j_{m-1}} \\ b_{j_{m-1}0} & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

It follows that $b_{0j_1}b_{j_1j_2}\cdots b_{j_{m-2}j_{m-1}}b_{j_{m-1}0} = \det B = 0$, which is a contradiction. Thus (3.5) is proved.

Assume that $a_k \neq 0$ for some $1 \leq k \leq n-1$. We claim that $(k,n) = 1$. Otherwise, there is an integer $1 \leq l \leq n-1$ such that $lk \equiv 0 \pmod{n}$. By (3.5), we have

$$\underbrace{a_k \cdots a_k}_{l} = 0,$$

which is a contradiction. For any $1 \leq i \leq n-1$ with $i \neq k$, we can write $i \equiv -jk \pmod{n}$ with $1 \leq j \leq n-2$. By (3.5) again, we have

$$a_i \underbrace{a_k \cdots a_k}_{j} = 0,$$

which implies that $a_i = 0$. Thus a_k is the only nonzero coefficient of f and the proof of the theorem is complete. □

4. A related problem

We consider another problem similar to Problem 1.1:

Problem 4.1. Determine all linearized polynomials $f(x) = \sum_{i=0}^{n-1} a_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ 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 $\mathbb{Z}_4^n \times \mathbb{Z}_2^n$ ([1]). 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 $c \in \mathbb{F}_{2^n}$, $f(x) + cx = ax(x^{2^k-1} + \frac{b+c}{a})$ 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 $f(x) = \sum_{i=0}^{n-1} a_i x^{2^i} \in \mathbb{F}_{2^n}[x]$ 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

$$\begin{array}{cccc} \psi: & \mathbb{F}_{2^n}^* & \longrightarrow & \mathbb{F}_{2^n} \\ & x & \longmapsto & \frac{f(x)}{x} \end{array}$$

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

[1] J. Davis and Q. Xiang, *A family of partial difference sets with Denniston parameters in nonelementary abelian 2-groups*, European J. Combin. **21** (2000), 981 – 988. MR **2002a:**05043

[2] P. Dembowski, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, New York, 1968. MR **38:**1597

[3] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, Dover, New York, 1958. MR **21:**3488

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983. MR **86c:**11106

[5] S. E. Payne, *Affine representations of generalized quadrangles*, J. Algebra **16** (1970), 473 – 485. MR **42:**8381

[6] S. E. Payne, *Linear transformations of a finite field*, Amer. Math. Monthly **78** (1971), 659 – 660.

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