A Remark on Linearized Permutation Polynomials

Kai Zhou
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS
Chinese Academy of Sciences

Abstract. We give an explicit representation of the class of linearized permutation polynomials. By the representation, the number of them can be computed easily.

Keywords: linear recurring sequences, linear permutation polynomials.

1. Introduction

An interesting class of permutation polynomials is the following. Let \( \mathbb{F}_{q^n} \) be an extension of the finite field \( \mathbb{F}_q \) and consider linearized polynomials \( L(x) \) of the form

\[
L(x) = \sum_{s=0}^{n-1} \alpha_s x^{q^s} \in \mathbb{F}_{q^n}[x].
\]

At page 362 of [1], Rudolf Lidl and Harald Niederreiter tell us that (1) is a permutation polynomial if and only if the determinant of following matrix

\[
A = \begin{pmatrix}
\alpha_0 & \alpha_{n-1} & \alpha_{n-2}^q & \cdots & \alpha_1^{q^{n-1}} \\
\alpha_1 & \alpha_0^q & \alpha_{n-1}^q & \cdots & \alpha_2^{q^{n-1}} \\
\alpha_2 & \alpha_1^q & \alpha_0^q & \cdots & \alpha_3^{q^{n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{n-1} & \alpha_{n-2}^q & \alpha_{n-3}^q & \cdots & \alpha_0^{q^{n-1}} 
\end{pmatrix}
\]

is not zero.

In this paper we represent the linearized permutation polynomials explicitly, and in this way we obtain the number of them.

Because we will use the theory of linear recurring sequences to prove our result, we first give some details of the basic terminology. A sequence \( \mathbf{a} = (a_0, a_1, a_2, \ldots) \) of elements of a finite field \( \mathbb{F}_q \) is called a linear recurring sequence in \( \mathbb{F}_q \) with characteristic polynomial \( f(x) = x^n - (c_{n-1}x^{n-1} + \cdots + c_0) \in \mathbb{F}_q[x] \) if \( a_{n+k} = \sum_{i=0}^{n-1} c_i a_{k+i} \) for \( k = 0, 1, \ldots \). Here \( n \) is any nonnegative integer. The set of all linear recurring sequences in \( \mathbb{F}_q \), with fixed characteristic polynomial \( f \in \mathbb{F}_q[x] \) is denoted by \( G(f) \). For a linear recurring sequence \( \mathbf{a} \) in \( \mathbb{F}_q \), its minimal polynomial \( m(x) \in \mathbb{F}_q[x] \) is defined to be the (uniquely determined) characteristic polynomial of \( \mathbf{a} \) of least degree. A \( q \)-ary sequence generated by an \( n \)-stage
linear feedback shift register is called a maximal length sequence (an m-sequence for short) if it has period $q^n - 1$.

Further background on linear recurring sequences can be found in [2]. In particular we list following four lemmas needed.

**Lemma 1.1** Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $n$, and let $\alpha$ be a root of $f(x)$ in $\mathbb{F}_{q^n}$. Let $a = \{a_i\}$ whose elements are given by $a_i = \text{Tr}(\beta^i\alpha)$, $i \geq 0$, $\beta \in \mathbb{F}_{q^n}$. Then $a \in G(f)$.

**Lemma 1.2** With the notation of the above lemma, for any sequence $a = \{a_i\} \in G(f)$, there exists some $\beta \in \mathbb{F}_{q^n}$ such that $a_i = \text{Tr}(\beta^i\alpha)$, $i \geq 0$.

**Lemma 1.3** Let $a$ be a sequence over $\mathbb{F}_q$. Then $a$ is an m-sequence with period $q^n - 1$ if and only if the elements of $a$ can be represented by $a_i = \text{Tr}(\beta^i\alpha)$, $i \geq 0$, $\beta \in \mathbb{F}_{q^n}$ where $\alpha$ is a primitive element in $\mathbb{F}_{q^n}$.

**Lemma 1.4** Let $a$ be an m-sequence, then in every period of $a$, each nonzero $n$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_{q^n}$ occurs exactly once.

2. Main Theorem

**Theorem 2.1** Let

$$f(x) = \sum_{s=0}^{n-1} \beta^s(\alpha_0 + \alpha q^s \alpha_1 + \alpha 2q^s \alpha_2 + \cdots + \alpha (n-1)q^s \alpha_{n-1})x^s \in \mathbb{F}_{q^n}[x],$$

where $\alpha$ is any primitive element in $\mathbb{F}_{q^n}$, $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\beta$ is any nonzero element of $\mathbb{F}_{q^n}$. Then $f(x)$ is a permutation polynomial. And there are exactly $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ different linearized permutation polynomials, in fact they must be the form of (2).

In order to obtain the result, we need the following Lemma first:

**Lemma 2.2** If $L_1(x) = \sum_{s=0}^{n-1} \alpha_s x^s$ and $L_2(x) = \sum_{s=0}^{n-1} \alpha'_s x^s$ are two linearized polynomials in $\mathbb{F}_{q^n}[x]$, then they define the same function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ if and only if $\alpha_i = \alpha'_i$, $0 \leq i \leq n - 1$.

**Proof.** If $\alpha_i = \alpha'_i$, $0 \leq i \leq n - 1$, it is clear that $L_1(x)$ and $L_2(x)$ define the same functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$.

Conversely, for any $\gamma \in \mathbb{F}_{q^n}$ we have $L_1(\gamma) = L_2(\gamma)$. If we take a basis $\{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, combining with $L_1(\gamma_s) = L_2(\gamma_s)$, $0 \leq s \leq n - 1$, we obtain

\[
\begin{pmatrix}
\gamma_0 & \gamma_0^q & \gamma_0^{q^2} & \cdots & \gamma_0^{q^{n-1}} \\
\gamma_1 & \gamma_1^q & \gamma_1^{q^2} & \cdots & \gamma_1^{q^{n-1}} \\
\gamma_2 & \gamma_2^q & \gamma_2^{q^2} & \cdots & \gamma_2^{q^{n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\gamma_{n-1} & \gamma_{n-1}^q & \gamma_{n-1}^{q^2} & \cdots & \gamma_{n-1}^{q^{n-1}}
\end{pmatrix}
\begin{pmatrix}
\alpha_0 - \alpha'_0 \\
\alpha_1 - \alpha'_1 \\
\alpha_2 - \alpha'_2 \\
\vdots \\
\alpha_{n-1} - \alpha'_{n-1}
\end{pmatrix} = \begin{pmatrix}
0 \\
0 \\
0 \\
\vdots \\
0
\end{pmatrix}.
\]
Since \( \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \) is a basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \), by Lemma 3.51 in [1], the determinant of the matrix in the above equation is nonzero. It follows that \( (\alpha_0 - \alpha'_0, \alpha_1 - \alpha'_1, \ldots, \alpha_{n-1} - \alpha'_{n-1}) = (0, 0, \ldots, 0) \), hence \( \alpha_i = \alpha'_i, 0 \leq i \leq n - 1 \).

Now we give the proof of the main Theorem:

**Proof.** By Lemma 1.3, we can take an \( m \)-sequence \( \mathbf{a} = (a_i), a_i \in \mathbb{F}_n, \) given by \( a_i = \text{Tr}(\beta \alpha^i), i \geq 0, \) where \( \alpha \) is any primitive element in \( \mathbb{F}_{q^n} \), and \( \beta \) is any nonzero element of \( \mathbb{F}_{q^n} \). Suppose \( \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \) is any basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_n \). Let

\[
B_i = \sum_{s=0}^{n-1} a_{s+i} x^s = \sum_{s=0}^{n-1} \alpha_s (\beta \alpha^{s+i} + \beta^q \alpha^{(s+i)q} + \cdots + \beta^{q^{n-1}} \alpha^{(s+i)q^{n-1}})
\]

\[
= \left( \sum_{s=0}^{n-1} \alpha_s \beta^s \alpha^s \right) x^i + \left( \sum_{s=0}^{n-1} \alpha_s \beta^q \alpha^{sq} \right) (\alpha^i)^q + \cdots + \left( \sum_{s=0}^{n-1} \alpha_s \beta^{q^{n-1}} \alpha^{sq^{n-1}} \right) (\alpha^i)^{q^{n-1}},
\]

\[0 \leq i \leq q^n - 2, \text{ by Lemma 1.4 we know } \{B_i\} \mid 0 \leq i \leq q^n - 2 \} \cup \{0\} = \mathbb{F}_{q^n}.
\]

Hence if we let

\[
f(x) = \left( \sum_{s=0}^{n-1} \alpha_s \beta^s \alpha^s \right) x + \left( \sum_{s=0}^{n-1} \alpha_s \beta^q \alpha^{sq} \right) x^q + \cdots + \left( \sum_{s=0}^{n-1} \alpha_s \beta^{q^{n-1}} \alpha^{sq^{n-1}} \right) x^{q^{n-1}},
\]

which is the same as (2), then \( B_i = f(\alpha^i), 0 \leq i \leq q^n - 2, \) and \( f(0) = 0, \) so \( f(x) \) is a permutation polynomial in \( \mathbb{F}_{q^n}[x] \). Now if we take another basis \( \{\alpha'_0, \alpha'_1, \ldots, \alpha'_{n-1}\} \) of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_n \), combining with the same given pair \( (\beta, \alpha) \) above, we obtain another permutation polynomial \( g(x) \), we will prove that \( f(x) = g(x) \) if and only if \( \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} = \{\alpha'_0, \alpha'_1, \ldots, \alpha'_{n-1}\} \).

By Lemma 1.4, there is an \( n \)-tuple \( (a_i, a_{i+1}, \ldots, a_{i+n-1}) = (1, 0, 0, \ldots, 0) \) for some \( i \in \{0, 1, 2, \ldots, q^n - 2\} \). Then \( a_0 = B_i = f(\alpha^i) = g(\alpha^i) = B'_i = a'_0 \). As the same way, there are \( n \)-tuples \( (0, 1, 0, \ldots, 0), (0, 0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 0, 1) \) in every period of the sequence \( \mathbf{a} \), we can also obtain \( \alpha_x = \alpha'_x, 1 \leq s \leq n - 1 \).

So if we fix a nonzero element \( \beta \) and a primitive element \( \alpha \) in \( \mathbb{F}_{q^n} \), we can get \( (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \) different linearized permutation polynomials, which is the same as the number of different bases of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_n \).

Now if we take another pair \( (\beta', \alpha') \) of one nonzero and one primitive element in \( \mathbb{F}_{q^n} \), and any basis \( \{\alpha'_0, \alpha'_1, \ldots, \alpha'_{n-1}\} \) of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_n \), then doing the same as above they determine a permutation polynomial

\[
h(x) = \sum_{s=0}^{n-1} (\beta'^q (\alpha'_0 + (\alpha')^q \alpha'_1 + (\alpha')^{2q} \alpha'_2 + \cdots + (\alpha')^{(n-1)q} \alpha'_{n-1}) x^{q^s}.
\]

We will show that there is a basis \( \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \) of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_n \), with the former \( (\beta, \alpha) \) can construct the same permutation polynomial \( h(x) \).

By Lemma 2.2, we consider the linear equations

\[
\beta'^q (x_0 + \alpha'^q x_1 + \alpha'^{2q} x_2 + \cdots + \alpha'^{(n-1)q} x_{n-1})
\]

\[
= (\beta'^q (\alpha'_0 + (\alpha')^q \alpha'_1 + (\alpha')^{2q} \alpha'_2 + \cdots + (\alpha')^{(n-1)q} \alpha'_{n-1}).
\]
Let Rudolf Lidl, Harald Niederreiter, Solomon W. Golomb, Guang Gong, \( i \leq \)

Then the coefficient matrix \( M = \begin{pmatrix}
\beta & \beta^q & \beta^{q^2} & \ldots & \beta^{q^{n-1}} \\
\beta \alpha & (\beta \alpha)^q & (\beta \alpha)^{q^2} & \ldots & (\beta \alpha)^{q^{n-1}} \\
\beta \alpha^2 & (\beta \alpha^2)^q & (\beta \alpha^2)^{q^2} & \ldots & (\beta \alpha^2)^{q^{n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\beta \alpha^{n-1} & (\beta \alpha^{n-1})^q & (\beta \alpha^{n-1})^{q^2} & \ldots & (\beta \alpha^{n-1})^{q^{n-1}}
\end{pmatrix}
\)
of linear equations (3) is invertible. So we can suppose \( (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \) is the solution of (3) in \( \mathbb{F}_q^n \). By (3), we know \( \beta, \alpha \) and \( (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \) construct the permutation polynomial \( h(x) \). Let \( a = \{a_i\} = \{\text{Tr}(\beta \alpha^i)\}, i \geq 0 \), then it is an \( m \)-sequence. Since \( \{\sum_{s=0}^{n-1} a_{s+i} \alpha_s, 0 \leq i \leq q^n - 2\} = \{h(\alpha^i), 0 \leq i \leq q^n - 2\} = \mathbb{F}_q^n \), by Lemma 1.4, \( (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \) must be a basis.

So by the construction in the proof of the above we have obtained \( (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \) different permutation polynomials of the form (1).

Now we will show that there are exactly \( (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \) different permutation polynomials of the form (1). Suppose

\[
L(x) = \sum_{s=0}^{n-1} a_s' x^{q^s} \in \mathbb{F}_{q^n}[x].
\]
is any permutation polynomials of the form (1). We solve the following linear equations

\[
\beta^{q^s} (x_0 + \alpha^{q^s} x_1 + \alpha^{2q^s} x_2 + \cdots + \alpha^{(n-1)q^s} x_{n-1}) = a_s', 0 \leq s \leq n - 1,
\]
where \( (\beta, \alpha) \) is a pair fixed elements as above in \( \mathbb{F}_q^n \). Then the coefficient matrix \( M \) of linear equations (5) is invertible. So we can suppose \( (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \) is the solution of (5) in \( \mathbb{F}_q^n \).

Because \( L(x) \) is permutation polynomial, the same as above, we know \( (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \) is a basis. Hence all of the linearized permutation polynomials must be of the form (2). \( \square \)

In the proof of the Theorem 2.1, we actually obtain the following Corollary 2.3.

**Corollary 2.3** Let \( \alpha \) be a fixed primitive element in \( \mathbb{F}_q^n \), then the set

\[
\{f(x) = \sum_{s=0}^{n-1} (\alpha_0 + \alpha^{q^s} \alpha_1 + \alpha^{2q^s} \alpha_2 + \cdots + \alpha^{(n-1)q^s} \alpha_{n-1}) x^{q^s} \in \mathbb{F}_q^n[x] \mid \text{where} \}
\]
\[\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \text{ is any basis of } \mathbb{F}_q^n \text{ over } \mathbb{F}_q \]
is contains and only contains all of the different linearized permutation polynomials of the form (1).

**References**
