On Some Classes of Permutation Polynomials

Amir Akbary, Sean Alaric, and Qiang Wang*

Abstract

Let p be a prime and $q = p^m$. We investigate permutation properties of polynomials $P(x) = x^r + x^{r+s} + \cdots + x^{r+ks}$ ($0 < r < q-1$, $0 < s < q-1$, and $k \geq 0$) over a finite field $\mathbb{F}_q$. More specifically, we construct several classes of permutation polynomials of this form over $\mathbb{F}_q$. We also count the number of permutation polynomials in each class.

Keywords: Lacunary sums of multinomial coefficients, permutation polynomials, Dickson polynomials, Lucas sequences.

2000 *Mathematics Subject Classification.* Primary 11T06.

1 Introduction

Let p be prime and $q = p^m$. A polynomial is a permutation polynomial (PP) over $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ to itself. The study of permutation polynomials of a finite field goes back to 19-th century when Hermite and later Dickson pioneered this area of research. In recent years interest in permutation polynomials has increased due to their applications in cryptography. For more background material on permutation polynomials we refer to Chapter 7 of [4]. For a detailed survey of open questions and recent results see [2], [3] and [6].

In general, finding classes of permutation polynomials of $\mathbb{F}_q$ is a challenging problem. Here we are interested in permutation properties of polynomials $P(x) = x^r(1 + x^s + \cdots + x^{ks})$. These polynomials have been first considered by Matthews [5]. For $r = 0$ and $s = 1$, these polynomials reduce to the polynomials $1 + x + \cdots + x^k$ whose permutation behavior, for odd q, has been described by Matthews in the same paper. The following general result has also been proved in [5] (Theorem 5.1).

Theorem (Matthews) Let $(r, s) = 1$ and $l = \frac{q-1}{(s,q-1)}$. Then $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a permutation polynomial of $\mathbb{F}_q$ if

$$k + 1 \equiv 1 \pmod{l}, \ (k+1)^s \equiv 1 \pmod{p}, \text{ and } (r, q-1) = 1,$$

*Research of all authors is partially supported by NSERC.

or

$$k+1 \equiv -1 \pmod{l},\ (k+1)^s \equiv (-1)^s \pmod{p},\ \text{and } (r-s, q-1) = 1.$$

We observe that in studying the permutation properties of the polynomial $P(x) = x^r(1 + x^s + \cdots + x^{ks})$, without loss of generality, we can assume that $s \mid (q-1)$. To explain this, let $(s, q-1) = u$ and choose an integer t relatively prime to $q-1$ such that $st \equiv u \pmod{q-1}$. Since x^t is a permutation polynomial of $\mathbb{F}_q$, $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a PP if and only if $P(x^t)$ is a PP. However, $P(x^t) = x^{rt}(1 + x^u + \cdots + x^{ku})$ in $\mathbb{F}_q[x]$, where $u \mid (q-1)$. So from now on we assume that $q - 1 = ls$ for some integer l. We also note that if $l = 1$, then $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a PP if and only if $(r, q-1) = 1$ and $(k+1, p) = 1$. So in the rest of this paper we assume that $q - 1 = ls$ where $l \neq 1$.

Our first result states that for $l \neq 2$ if $k + 1 \equiv \pm 1 \pmod{l}$ then conditions given in Matthews' theorem completely describe all permutation polynomials of the form $P(x) = x^r(1 + x^s + \cdots + x^{ks})$.

Proposition 1.1 *Let $q = p^m$, $q - 1 = ls$, and $P(x) = x^r(1 + x^s + \cdots + x^{ks})$.*
(i) *If $l \neq 2$ and $k + 1 \equiv 1 \pmod{l}$ then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(k+1)^s \equiv 1 \pmod{p}$, and $(r, q-1) = 1$.*
(ii) *If $l \neq 2$ and $k + 1 \equiv -1 \pmod{l}$ then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(k+1)^s \equiv (-1)^s \pmod{p}$, and $(r - s, q-1) = 1$.*
(iii) *If $l = 2$ and $k + 1 \equiv \pm 1 \pmod{l}$ (i.e. k is even) then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(k+1)^s \equiv (-1)^{r-1} \pmod{p}$, and $(r, q-1) = 1$ or $(r - s, q-1) = 1$.*

In [8], the authors speculated that if $P(x) = x^r(1+x^s+\cdots+x^{ks})$ is a PP then $k+1 \equiv \pm 1 \pmod{l}$. In other words permutation polynomials described by Matthews' theorem are the only possible such permutation polynomials. In the case $s = 1$ and $q = p$ or p^2, Park and Lee [8] proved that in fact this statement is true.

In this paper we show that this assertion is not true in general. More precisely we construct two new classes of permutation polynomials $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ different from Matthews' class. More generally, for odd q and odd l, we obtain necessary and sufficient conditions under which the polynomial $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ becomes a permutation polynomial of $\mathbb{F}_q$ (Theorem 4.1 and Corollary 4.2). We employ these conditions to construct two new classes of permutation polynomials of the form $P(x) = x^r(1 + x^s + \cdots + x^{ks})$. More precisely, we prove the following theorems.

Theorem 5.2 *Let p be an odd prime and $q = p^m$. Let l be an odd positive integer such that $q - 1 = ls$. Let 1) $p \equiv -1 \pmod{l}$ or 2) $p \equiv 1 \pmod{l}$ and $l \mid m$. Then the polynomial $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(lp, k+1) = 1$ and $(2r + ks, l) = 1$.*

Corollary 5.3 *Under the conditions of Theorem 5.2 on q and l, there are exactly $\phi(q-1)\phi(l)(p-1)$ permutation polynomials $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ $(k \geq 0,\ 0 < r < q-1)$ of $\mathbb{F}_q$. Here, ϕ is the Euler totient function.*

Theorem 5.2 can be considered as a generalization of the main theorem of [1]. In the next theorem, $\{L_n\}$ is the Lucas sequence determined by the recurrence $L_n = L_{n-1} + L_{n-2}$ and the initial conditions $L_0 = 2$ and $L_1 = 1$.

Theorem 5.4 *Let $q = p^m$ with odd prime p, $q - 1 = 5s$, and $P(x) = x^r(1 + x^s + ... + x^{ks})$. Then $P(x)$ is a PP if and only if one of the following holds.*
(i) $k + 1 \equiv \pm 1 \pmod 5$, $(r, s) = 1$, $(k + 1)^s \equiv 1 \pmod p$ *and* $(2r + ks, 5) = 1$.
(ii) $k + 1 \equiv \pm 2 \pmod 5$, $(r, s) = 1$, $(k + 1)^s \equiv 1 \pmod p$, $(2r + ks, 5) = 1$ *and* $L_s = 2$ *in* $\mathbb{F}_p$.

This theorem gives a generalization of a theorem of L. Wang (Theorem 2, [10]).

The method of the proof of the above theorems is based on Hermite's Criterion for permutation polynomials of $\mathbb{F}_q$ (see Section 4) and an application of an explicit representation of the lacunary sum of the multinomial coefficients in terms of a primitive root of unity in the algebraic closure of a finite field $\mathbb{F}_q$ (Lemma 3.2).

The structure of the paper is as follows. Section 2 gives the proof of Proposition 1.1. In Section 3, we prove a Lemma which plays an important role in the rest of the paper. In Section 4, we prove a general theorem regarding the permutation polynomials of the form $P(x) = x^r(1 + x^s + \cdots + x^{ks})$. In Section 5, we employ this theorem to prove the above theorems.

Acknowledgment The third author would like to thank Daniel Panario for several helpful discussions related to this work.

2 Proof of Proposition 1.1

Proof. (i) We assume that $k+1 \equiv 1 \pmod l$ and $l \neq 2$. By Matthews' theorem it is clear that $P(x)$ is a PP if $(r, s) = 1$, $(k + 1)^s \equiv 1 \pmod p$ and $(r, q - 1) = 1$. Now suppose that $P(x)$ is a PP. Then by Theorem 1.2 of [9], we have $(r, s) = 1$. Next we note that for $a \in \mathbb{F}_q$, if $a^s \neq 1$ then $P(a) = a^r$ and if $a^s = 1$ then $P(a) = (k + 1)a^r$. Let $S = \{a \in \mathbb{F}_q \mid \ a^s = 1\}$, so the permutation polynomial $P(x)$ induces a bijection $(k+1)x^r$ from S to $(k+1)S$ and a bijection x^r from $\mathbb{F}_q \setminus S$ to $\mathbb{F}_q \setminus (k+1)S$.

From Theorem 4.7 of [8] we have $(k+1)^s \equiv (-1)^{r-1} \pmod p$. We show that $(k+1)^s \equiv 1 \pmod p$. This is obvious when q is even or r is odd. We prove that if q is odd and $P(x)$ is a PP then in fact r is odd. To prove this, note that $|S| = s = \frac{q-1}{l} < \frac{q-1}{2}$, so we can choose $\alpha \in \mathbb{F}_q \setminus S$ such that $-\alpha \in \mathbb{F}_q \setminus S$. Now since x^r is a bijection from $\mathbb{F}_q \setminus S$ to $\mathbb{F}_q \setminus (k+1)S$, r cannot be even, otherwise $\alpha^r = (-\alpha)^r$. Therefore r is odd and so $(k + 1)^s \equiv 1 \pmod p$. This shows that $(k+1)x^r$ permutes S and x^r permutes $\mathbb{F}_q \setminus S$. Hence the polynomial x^r is a PP of $\mathbb{F}_q$ and so $(r, q - 1) = 1$. This completes the proof of the necessity of conditions given in (i).

Proofs of (ii) and (iii) are similar to the above proof. □

For odd l, we can combine parts (i) and (ii) of Proposition 1.1 to write the proposition as the following single statement.

Corollary 2.1 *Let l be an odd positive integer such that $q-1=ls$. Let $k+1\equiv\pm1 \pmod{l}$. Then $P(x)=x^r(1+x^s+\cdots+x^{ks})$ is a PP over $\mathbb{F}_q$ if and only if $(r,s)=1$, $(k+1)^s\equiv 1 \pmod{p}$ and $(2r+ks,l)=1$.*

Corollary 2.2 *Under the assumptions of Corollary 2.1 on q and l, there are exactly $\phi(q-1)(p-1,s)$ permutation polynomials $P(x)=x^r(1+x^s+\cdots+x^{ks})$ ($k\geq 0$, $k+1\equiv$ either 1 or $-1 \pmod{l}$, $0<r<q-1$) of $\mathbb{F}_q$. Here $(p-1,s)$ is the greatest common divisor of $p-1$ and s.*

Proof. First of all note that we only need to consider k such that $0\leq k\leq lp-1$. This is true since if $k\equiv k' \pmod{lp}$ then $a^r(1+a^s+\cdots+a^{ks})=a^r(1+a^s+\cdots+a^{k's})$ for any $a\in\mathbb{F}_q$. Also we assume that $k+1\equiv 1 \pmod{l}$, the proof in the case $k+1\equiv -1 \pmod{l}$ is similar.

Next for fixed k with $0\leq k\leq lp-1$ and $(k+1,l)=1$, we count the number of r's between 0 and $q-1$ such that $(r,s)=1$ and $(2r+ks,l)=1$. We denote this number by $N(k)$. One can show that $N(k)=\phi(q-1)$ (see [1], page 20 for a proof), where ϕ is Euler's phi function. Now let $\mathbb{F}_p^{l,q}$ be the set of non-zero elements of $\mathbb{F}_p$ that are l-th powers in $\mathbb{F}_q$. We have $|\mathbb{F}_p^{l,q}|=(p-1,s)$. From here, since $\{1,l+1,\cdots,(p-1)l+1\}$ forms a complete set of residues modulo p, the number of k ($0\leq k\leq lp-1$) that is a multiple of l and $k+1$ is an l-th power in $\mathbb{F}_q$ is $(p-1,s)$.

Finally let $M(q,l)$ be the number of permutation polynomials determined by conditions given in Corollary 2.1. We have

$$M(q,l)=\sum_{\substack{0\leq k\leq lp-1,k+1\in\mathbb{F}_p^{l,q}\\ k+1\equiv 1 \pmod{l}}} N(k)=\phi(q-1)(p-1,s).$$

□

Example: From the above corollary, one can deduce that the total number of permutation polynomials of the form $P(x)=x^r(1+x^s+\cdots+x^{ks})$ over any $\mathbb{F}_q$ such that $3\mid(q-1)$ is $2\phi(q-1)(p-1,s)$. For example, there are 64 such permutation polynomials over $\mathbb{F}_{25}$, 1296 such permutation polynomials over $\mathbb{F}_{343}$, and 1536 such permutation polynomials over $\mathbb{F}_{625}$.

3 Lemma

Definition 3.1 *The lacunary sum for the coefficient $C(n,i,k)$ of x^i in the polynomial expansion of $g(x)=(1+x+x^2+...+x^k)^n$ is defined as*

$$S(n,l,a,k+1)=\sum_{\substack{i=0\\ i\equiv a \pmod{l}}}^{nk} C(n,i,k),$$

where

$$C(n,i,k) = \sum_{\substack{n_0+n_1+\cdots+n_k=n \\ n_1+2n_2+\cdots+kn_k=i}} \frac{n!}{n_0!\ n_1!\cdots n_k!}.$$

We next derive a formula for the lacunary sum of the multinomial coefficients over a finite field. We use this formula in the proof of Theorem 4.1.

Lemma 3.2 *Let $(p,2l)=1$, $q=p^m$ and η be a primitive $2l$-th root of unity in the algebraic closure of $\mathbb{F}_q$. Let*

$$E_k(x+x^{-1}) = \frac{x^{k+1}-x^{-(k+1)}}{x-x^{-1}}$$

be the Dickson polynomial of the second kind of degree k over $\mathbb{F}_q$. Let n, l, a, and k be integers. We have

$$S(n,l,a,k+1) = \frac{(k+1)^n+\delta_{l,a}}{l} + \frac{1}{l}\sum_{t=1}^{\lfloor\frac{l-1}{2}\rfloor}\left(\eta^{t(2a-kn)}+\eta^{-t(2a-kn)}\right)\left(E_k\left(\eta^t+\eta^{-t}\right)\right)^n,$$

where

$$\delta_{l,a} = \begin{cases} (-1)^a & \text{if } l \text{ is even and } k \text{ is even} \\ 0 & \text{otherwise} \end{cases}.$$

Proof. Let $g(x) = (1+x+\cdots+x^k)^n = \sum_{i=0}^{nk} C(n,i,k)x^i$. Then we have

$$\sum_{\substack{i=0 \\ i\equiv a \pmod{l}}}^{nk} C(n,i,k)x^i = \frac{1}{l}\sum_{t=0}^{l-1}\eta^{2at}\sum_{i=0}^{nk}C(n,i,k)\eta^{-2it}x^i = \frac{1}{l}\sum_{t=0}^{l-1}\eta^{2at}g(\eta^{-2t}x).$$

From here we have

$$\begin{aligned} S(n,l,a,k+1) &= \frac{(k+1)^n}{l} + \frac{1}{l}\sum_{t=1}^{l-1}\eta^{2at}g(\eta^{-2t}) \\ &= \frac{(k+1)^n}{l} + \frac{1}{l}\sum_{t=1}^{l-1}\eta^{2at}\left(\frac{\eta^{-2(k+1)t}-1}{\eta^{-2t}-1}\right)^n \\ &= \frac{(k+1)^n}{l} + \frac{1}{l}\sum_{t=1}^{l-1}\eta^{2at-tn(k+1)+tn}\left(\frac{\eta^{-t(k+1)}-\eta^{t(k+1)}}{\eta^{-t}-\eta^t}\right)^n \\ &= \frac{(k+1)^n}{l} + \frac{1}{l}\sum_{t=1}^{l-1}\eta^{t(2a-kn)}\left(E_k(\eta^t+\eta^{-t})\right)^n. \end{aligned}$$

Furthermore,

$$\begin{aligned} \eta^{(l-i)(2a-kn)}(E_k(\eta^{l-i}+\eta^{-(l-i)}))^n &= (-1)^{2a-kn}\eta^{-i(2a-kn)}(-1)^{kn}(E_k(\eta^i+\eta^{-i}))^n \\ &= \eta^{-i(2a-kn)}(E_k(\eta^i+\eta^{-i}))^n \end{aligned}$$

for any $1 \le i \le \lfloor (l-1)/2 \rfloor$. Finally we let

$$\delta_{l,a} = \begin{cases} \eta^{\frac{l}{2}(2a-kn)}(E_k(\eta^{\frac{l}{2}} + \eta^{-\frac{l}{2}}))^n = (-1)^a & \text{if } l \text{ is even and } k \text{ is even} \\ 0 & \text{otherwise} \end{cases}.$$

Therefore we have

$$S(n,l,a,k+1) = \frac{(k+1)^n + \delta_{l,a}}{l} + \frac{1}{l}\sum_{t=1}^{\lfloor \frac{l-1}{2} \rfloor} \left(\eta^{t(2a-kn)} + \eta^{-t(2a-kn)}\right)\left(E_k(\eta^t + \eta^{-t})\right)^n.$$

□

4 The Main Theorem

In this section, we deduce some necessary and sufficient conditions regarding a permutation polynomial in the form $P(x) = x^r(1 + x + \cdots + x^{ks})$, where $0 < r < q-1$, $k \ge 0$, $q-1 = ls$, and l is odd. A classical result which describes the permutation polynomials of a finite field is the following theorem of Hermite (Theorem 7.2, [4]).

Hermite's Criterion: *$P(x)$ is a PP over $\mathbb{F}_q$ if and only if*
(a) *$P(x)$ has exactly one root in $\mathbb{F}_q$.*
(b) *For each integer n with $1 \le n \le q-2$ and $n \not\equiv 0 \pmod p$, the reduction of $[P(x)]^n \bmod (x^q - x)$ has degree less than or equal to $q-2$.*

Next we consider the following conditions:
(i) $(r,s) = 1$
(ii) $(l, k+1) = 1$
(iii) $(2r + ks, l) = 1$
(iv) $(k+1)^s \equiv 1 \pmod p$
(v) $\sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{2tj} + \eta^{-2tj}\right)\left(E_k(\eta^t + \eta^{-t})\right)^{jc_0 s} = -1$ in $\mathbb{F}_q$, for $j = 1, \cdots, l-1$, where η is a primitive $2l$-root of unity in $\mathbb{F}_q$, $E_k(x)$ is the Dickson polynomial of the second kind of degree k over $\mathbb{F}_q$, and c_0 is the multiplicative inverse of $r + k(s/2)$ modulo l.

Using Hermite's Criterion and the lemma in the previous section, we obtain the following.

Theorem 4.1 *Let l be an odd positive integer, p be an odd prime, $q = p^m$ and $q - 1 = ls$. Let $P(x) = x^r f(x^s) = x^r(1 + x^s + ... + x^{ks})$. Then*
(A) *The conditions* (i), (ii), (iii), (iv), *and* (v) *imply that $P(x)$ is a PP.*
(B) *If $P(x)$ is a PP then* (i), (ii) and (iv) *hold.*
(C) *If $P(x)$ is a PP and $l < 2p+1$ then $2r + ks \not\equiv 0 \pmod l$.*

Proof. (A) We assume that conditions (i) to (v) are satisfied. It is sufficient to verify that Hermite's Criterion holds under these assumptions. Note that if $x^s = 1$, then $f(x^s) = k+1 \neq 0$ in $\mathbb{F}_q$ by (iv). Also if $x^s \neq 1$, again (ii) implies that $f(x^s) = \frac{x^{(k+1)s}-1}{x^s-1}$ has no zeroes in $\mathbb{F}_q$. Hence $P(x)$ has only one zero in $\mathbb{F}_q$ and so the first condition of Hermite's Criterion is satisfied.

Next we observe that since $(r, s) = 1$ and

$$[P(x)]^n = x^{rn}(1 + x^s + \cdots x^{ks})^n = \sum_{i=0}^{nk} C(n, i, k)x^{is+rn},$$

then the possible nonzero coefficient of x^{q-1} happens only if $s|n$. Let $n = cs$ for some c $(1 \leq c \leq l-1)$. Then we have

$$[P(x)]^{cs} \pmod{x^q - x} = S(cs, l, -cr, k+1)x^{q-1} + \cdots,$$

for $c = 1, \cdots, l-1$. So to show that the second condition of Hermite's criterion holds, it is enough to show that $S(cs, l, -cr, k+1) = 0$ in $\mathbb{F}_q$ for $c = 1, \cdots, l-1$. Let c_0 be the multiplicative inverse of $r + k(s/2)$ modulo l, then for each $c = 1, \cdots, l-1$ there exists a unique j $(1 \leq j \leq l-1)$ such that $c = jc_0 \bmod l$. Thus by Lemma 3.2, (iv) and (v), for $c = 1, \cdots, l-1$, we have

$$\begin{aligned} lS(cs, l, -cr, k+1) &= lS(jc_0 s, l, -jc_0 r, k+1) \\ &= (k+1)^{jc_0 s} + \sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{2tj} + \eta^{-2tj}\right) \left(E_k(\eta^t + \eta^{-t})\right)^{jc_0 s} \\ &= 0 \end{aligned}$$

in $\mathbb{F}_q$. This shows that $[P(x)]^{cs} \pmod{x^q - x}$ has degree less than $q-1$ and so by Hermite's criterion $P(x)$ is a PP over $\mathbb{F}_q$.

(B) We assume that $P(x) = x^r(1 + x^s + ... + x^{ks})$ is a PP. Then by Theorem 1.2 of [9], we have $(r, s) = 1$ and thus (i) holds. Next by Theorem 4.7 of [8], $(k+1)^s \equiv (-1)^{r-1} \equiv 1 \pmod{p}$ and therefore (iv) holds. To prove (ii) note that if $(l, k+1) = e \neq 1$ then $1 + x^s + ... + x^{ks} = \frac{x^{(k+1)s}-1}{x^s-1}$ has $(e-1)s$ zeros in $\mathbb{F}_q$. Hence $P(x)$ has more than one root in $\mathbb{F}_q$ which is a contradiction. So $(l, k+1) = 1$.

(C) Let us assume that $2r + ks \equiv 0 \pmod{l}$. Since $P(x)$ is a PP, by Hermite's criterion, for $c = 1, \cdots, l-1$ we have $S(cs, l, -cr, k+1) = 0$ in $\mathbb{F}_q$. So from Lemma 3.2 and (iv), we obtain that

$$\begin{aligned} 0 &= S(cs, l, -cr, k+1) \\ &= \frac{(k+1)^{cs}}{l} + \frac{1}{l} \sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{t(-2cr-kcs)} + \eta^{-t(-2cr-kcs)}\right) \left(E_k(\eta^t + \eta^{-t})\right)^{cs} \\ &= \frac{1}{l} + \frac{2}{l} \sum_{t=1}^{\frac{l-1}{2}} \left(E_k(\eta^t + \eta^{-t})\right)^{cs} \end{aligned} \tag{1}$$

for $c = 1, \cdots, l-1$. Let $\alpha_t = (E_k(\eta^t + \eta^{-t}))^s$. Then from (1) we have

$$\alpha_1^i + \alpha_2^i + \cdots + \alpha_{\frac{l-1}{2}}^i = \alpha_1^{i+1} + \alpha_2^{i+1} + \cdots + \alpha_{\frac{l-1}{2}}^{i+1} = -\frac{1}{2}$$

for $i = 1, \cdots, \frac{l+1}{2}$. Next by renaming the variables α_j's we can assume that there are m distinct α_j's with n_j copies of each α_j for $j = 1, \cdots, m$. So we have

$$n_1\alpha_1^i + n_2\alpha_2^i + \cdots + n_m\alpha_m^i = n_1\alpha_1^{i+1} + n_2\alpha_2^{i+1} + \cdots + n_m\alpha_m^{i+1} = -\frac{1}{2} \tag{2}$$

for $i = 1, \cdots, m+1$. We consider the following system of linear equations

$$\begin{cases} n_1x_1 + n_2x_2 + \cdots + n_mx_m & = & -\frac{1}{2} \\ n_1\alpha_1x_1 + n_2\alpha_2x_2 + \cdots + n_m\alpha_mx_m & = & -\frac{1}{2} \\ & \vdots & \\ n_1{\alpha_1}^{m-1}x_1 + n_2{\alpha_2}^{m-1}x_2 + \cdots + n_m{\alpha_m}^{m-1}x_m & = & -\frac{1}{2} \end{cases}.$$

Since for any j, $n_j < p$ (this is true since $l < 2p+1$) and α_j's are distinct, $x_j = \alpha_j$ for $j = 1, \cdots, m$ is the unique solution of this system. However, by (2) $x_j = \alpha_j^2$ is also a solution. So $\alpha_j = \alpha_j^2$ for $j = 1, \cdots, m$. This implies that for $1 \le t \le \frac{l-1}{2}$, $\alpha_t = (E_k(\eta^t + \eta^{-t}))^s = 0$ or 1 in $\mathbb{F}_q$. Now note that if η_{k+1} is a primitive $2(k+1)$-root of unity in the algebraic closure of $\mathbb{F}_q$, then

$$E_k(x) = \prod_{t=1}^{k} \left(x - (\eta_{k+1}^t + \eta_{k+1}^{-t})\right).$$

From here since $(k+1, l) = 1$, we have $(E_k(\eta^t + \eta^{-t}))^s \neq 0$ and thus it is true that $(E_k(\eta^t + \eta^{-t}))^s = 1$. Hence

$$\sum_{t=1}^{\frac{l-1}{2}} \left(E_k(\eta^t + \eta^{-t})\right)^s = \frac{l-1}{2}$$

in $\mathbb{F}_q$. However, from (1) we have

$$\sum_{t=1}^{\frac{l-1}{2}} \left(E_k(\eta^t + \eta^{-t})\right)^s = -\frac{1}{2}$$

in $\mathbb{F}_q$. Hence $\frac{l-1}{2} = -\frac{1}{2}$ and so $l \equiv 0 \pmod{p}$, this is a contradiction since $l \mid p^m - 1$. Therefore we have $2r + ks \not\equiv 0 \pmod{l}$ and so (C) holds. □

Corollary 4.2 *In Theorem* 4.1*, let l be an odd prime such that $l < 2p+1$, then $P(x)$ is a PP if an only if conditions* (i), (ii), (iii), (iv), *and* (v) *hold.*

Proof. It is enough to show that if $P(x)$ is a PP then (v) holds. If $P(x)$ is a PP, by part (C) of Theorem 4.1, $(2r + ks, l) = 1$. Let c_0 be the multiplicative inverse of $r + k(s/2)$ modulo l, then (v) follows immediately from $S(c_0js, l, -c_0jr, k+1) = 0$ for $j = 1, \cdots, l-1$, Lemma 3.2, and (iv). □

5 Some Classes of Permutation Polynomials

In this section we employ Theorem 4.1 and Corollary 4.2 to construct two new classes of permutation polynomials of $\mathbb{F}_q$. We start with a lemma which describes certain finite fields $\mathbb{F}_q$ in which every non-zero element in $\mathbb{F}_p$ can be written as an l-th power in $\mathbb{F}_q$.

Lemma 5.1 *Let l be an odd integer. Let p be an odd prime, $q = p^m$, $s = \frac{q-1}{l}$ and α be any nonzero element of $\mathbb{F}_p$. Then*

(i) *If $p \equiv -1 \pmod{l}$, we have $\alpha^s = 1$ in $\mathbb{F}_p$.*

(ii) *If $p \equiv 1 \pmod{l}$ and $l \mid m$, we have $\alpha^s = 1$ in $\mathbb{F}_p$.*

Proof. See [1] Lemma 4.1. □

For polynomials $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ over finite fields described in Lemma 5.1, we can obtain the following simple conditions under which they are PP. The next result is a generalization of the main theorem of [1].

Theorem 5.2 *Let p be an odd prime and $q = p^m$. Let l be an odd positive integer such that $q - 1 = ls$. Let 1) $p \equiv -1 \pmod{l}$ or 2) $p \equiv 1 \pmod{l}$ and $l \mid m$. Then the polynomial $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(lp, k + 1) = 1$ and $(2r + ks, l) = 1$.*

Proof. First we assume that $P(x)$ is a PP. Then from Theorem 4.1 we know that $(r, s) = 1$ and $(lp, k + 1) = 1$. Now suppose that $(2r + ks, l) = d$ with $d > 1$. Let $u = \frac{l}{d}$. Then $u < l$ and $2ur + kus \equiv 0 \pmod{l}$. Since $P(x)$ is a PP, we have $S(us, l, -ur, k+1) = 0$ in $\mathbb{F}_q$. From Lemma 3.2 we obtain

$$0 = S(us, l, -ur, k + 1) = \frac{1}{l} + \frac{2}{l} \sum_{t=1}^{\frac{l-1}{2}} (E_k(\eta^t + \eta^{-t}))^{us}. \tag{3}$$

Now note that $\eta^t + \eta^{-t}$ for $1 \le t \le \frac{l-1}{2}$ are roots of the Dickson polynomial $E_{l-1}(x)$. Under given conditions for p, by Theorem 7 of [7] we know that $E_{l-1}(x)$ splits in $\mathbb{F}_p[x]$. So $\eta^t + \eta^{-t} \in \mathbb{F}_p$ and thus by Lemma 5.1 we have $(E_k(\eta^t + \eta^{-t}))^s = 1$. This together with (3) imply that $l = 0$ in $\mathbb{F}_q$, which is a contradiction, so $(2r + ks, l) = 1$.

To prove the sufficiency, we first note that from Lemma 5.1 $(k+1)^s \equiv 1 \pmod{p}$ as long as $(p, k + 1) = 1$. By applying Theorem 4.1, we only need to show that for $j = 1, \cdots, l - 1$,

$$\sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{2tj} + \eta^{-2tj}\right) \left(E_k(\eta^t + \eta^{-t})\right)^{jc_0 s} = -1.$$

Again we have $(E_k(\eta^t + \eta^{-t}))^s = 1$ for $1 \le t \le \frac{l-1}{2}$. Thus

$$\sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{2tj} + \eta^{-2tj}\right) \left(E_k(\eta^t + \eta^{-t})\right)^{jc_0 s} = \sum_{t=1}^{\frac{l-1}{2}} \left(\eta^{2tj} + \eta^{-2tj}\right) = \sum_{t=1}^{l-1} \eta^{2tj} = -1,$$

for $j = 1, \cdots, l - 1$. This completes the proof. □

Corollary 5.3 *Under the conditions of Theorem* 5.2 *on* q *and* l*, there are exactly* $\phi(q-1)\phi(l)(p-1)$ *permutation polynomials* $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ $(k \geq 0,\ 0 < r < q-1)$ *of* $\mathbb{F}_q$*. Here,* ϕ *is the Euler totient function.*

Proof. Let $N(k)$ be as defined in the proof of Corollary 2.2. Let $N(q,l)$ be the number of permutation polynomials determined by conditions given in Theorem 5.2 and $\mu(d)$ denote the Möbius function. Then we have

$$\begin{aligned}
N(q,l) &= \sum_{\substack{0\leq k\leq lp-1 \\ (k+1,l)=1,\ k+1\not\equiv 0 \pmod p}} N(k) \\
&= \phi(q-1) \sum_{\substack{0\leq k\leq lp-1 \\ k+1\not\equiv 0 \pmod p}} \sum_{d\mid (k+1,l)} \mu(d) \\
&= \phi(q-1) \sum_{d\mid l} \mu(d) \sum_{\substack{1\leq t\leq \frac{lp}{d} \\ t\not\equiv 0 \pmod p}} 1 \\
&= \phi(q-1)(p-1)l \sum_{d\mid l} \frac{\mu(d)}{d} \\
&= \phi(q-1)\phi(l)(p-1).
\end{aligned}$$

□

To describe our next result we need the following definition. We define the n-th Lucas number L_n over $\mathbb{F}_p$ $(p \neq 2)$ by the recurrence relation

$$L_n = L_{n-1} + L_{n-2} \tag{4}$$

and the initial conditions $L_0 = 2$ and $L_1 = 1$. Let $q = p^m$ and $q - 1 = 5s$. Let η be a primitive 10th-root of unity in $\mathbb{F}_q$. Then one can show that L_n has representation

$$L_n = (\eta + \eta^{-1})^n + (-(\eta^2 + \eta^{-2}))^n \tag{5}$$

over $\mathbb{F}_q$.

We say that the sequence $\{L_n\}$ is *s-periodic* over $\mathbb{F}_p$ if $a_{n+ks} = a_n$ in $\mathbb{F}_p$ for integers k and n. Some useful properties regarding the sequence $\{L_n\}$ are the following.

(P1) If $p \neq 2$ and 5, $\{L_n\}$ is $5s$-periodic over $\mathbb{F}_p$.
(P2) $\{L_n\}$ is s-periodic over $\mathbb{F}_p$ if and only if $L_s = 2$ in $\mathbb{F}_p$ (see [10], Lemmas 6 and 7).
(P3) $L_n^2 = L_{2n} + (-1)^n 2$.

Now we are set to state and prove the final result of this paper.

Theorem 5.4 *Let* $q = p^m$ *with odd prime* p*,* $q - 1 = 5s$*, and* $P(x) = x^r f(x^s) = x^r(1 + x^s + \ldots + x^{ks})$*. Then* $P(x)$ *is a PP if and only if one of the following holds.*
(i) $k + 1 \equiv \pm 1 \pmod 5$*,* $(r,s) = 1$*,* $(k+1)^s \equiv 1 \pmod p$ *and* $(2r + ks, 5) = 1$.
(ii) $k + 1 \equiv \pm 2 \pmod 5$*,* $(r,s) = 1$*,* $(k+1)^s \equiv 1 \pmod p$*,* $(2r + ks, 5) = 1$ *and* $L_s = 2$ *in* $\mathbb{F}_p$.

Proof. First of all we note that (i) follows from Corollary 2.1.

We now consider the case for $k+1 \equiv 2 \pmod 5$. First we assume that $P(x)$ is a PP of $\mathbb{F}_q$. Then from Corollary 4.2, we have $(r,s)=1$, $(k+1)^s \equiv 1 \pmod p$ and $(2r+ks,5)=1$. It remains to show that in this case $L_s = 2$ in $\mathbb{F}_p$. To do this we note that condition (v) in Corollary 4.2 can be re-written as

$$\sum_{t=1}^{2}(-1)^{tj}(\eta^{tj}+\eta^{-tj})(E_k(\eta^t+\eta^{-t}))^{jc_1s} = -1, \tag{6}$$

for $j = 1,\ 2,\ 3$ and 4, where c_1 is the multiplicative inverse of $ks+2r$ modulo 5. Here η is a primitive 10-th root of unity in $\mathbb{F}_q$. Also note that since $k+1 \equiv 2 \pmod 5$, we have

$$(E_k(\eta^t+\eta^{-t}))^s = \left(\frac{\eta^{t(k+1)}-\eta^{-t(k+1)}}{\eta^t-\eta^{-t}}\right)^s = (\eta^t+\eta^{-t})^s. \tag{7}$$

Now considering (6) for $j=1$ and 2 together with (7) and (5) yield

$$-L_{c_1s+1} = -1, \quad \text{and} \quad L_{2c_1s+2} - 2L_{2c_1s} = -1.$$

By applying (4) in the latter identity, we have

$$L_{c_1s+1} = 1, \quad \text{and} \quad L_{2c_1s-1} = -1.$$

Next by employing (P3) we have

$$L_{2c_1s+2} - 2 = L_{c_1s+1}^2 = 1 = -L_{2c_1s-1},$$

and thus

$$2 = L_{2c_1s+2} + L_{2c_1s-1} = L_{2c_1s+1} + L_{2c_1s} + L_{2c_1s-1} = 2L_{2c_1s+1}.$$

This follows that

$$L_{2c_1s} = L_{2c_1s+1} - L_{2c_1s-1} = 2,$$

and thus by applying (P3) and (P1) we have $L_{2c_1s} = L_{4c_1s} = L_{8c_1s} = L_{16c_1s} = L_{c_1s} = 2$. Since c_1 is a nonzero element of $\mathbb{F}_5$, these equalities imply that $L_s = 2$. This completes the proof of necessity of conditions given in (ii).

To prove the sufficiency of these conditions, by Corollary 4.2, we only need to show that for $j = 1, 2, 3$ and 4, we have

$$\sum_{t=1}^{2}(-1)^{tj}(\eta^{tj}+\eta^{-tj})(E_k(\eta^t+\eta^{-t}))^{jc_1s} = -1.$$

To establish these identities, we first note that

$$\eta^{tj}+\eta^{-tj} = D_j(\eta^t+\eta^{-t}),$$

where $D_j(x)$ denotes the Dickson polynomial of the first kind of degree j. We have $D_j(-x) = (-1)^j D_j(x)$. Let

$$D_j(x) = d_j^{(j)} x^j + d_{j-1}^{(j)} x^{j-1} + \cdots + d_0^{(j)}.$$

So

$$\begin{aligned}
& \sum_{t=1}^{2} (-1)^{tj} (\eta^{tj} + \eta^{-tj}) \left(\eta^t + \eta^{-t}\right)^{jc_1 s} \\
= & \sum_{t=1}^{2} (-1)^{tj} D_j(\eta^t + \eta^{-t}) \left(\eta^t + \eta^{-t}\right)^{jc_1 s} \\
= & (-1)^j \sum_{m=0}^{j} d_m^{(j)} \left(\left(\eta + \eta^{-1}\right)^{jc_1 s+m} + \left(-(\eta^2 + \eta^{-2})\right)^{jc_1 s+m} \right) \\
= & (-1)^j \sum_{m=0}^{j} d_m^{(j)} L_{jc_1 s+m}.
\end{aligned}$$

Since $L_s = 2$, from (P2) we know that $L_{jc_1 s+m} = L_m$. Applying this and (5) in the previous identity yield

$$\begin{aligned}
1 + \sum_{t=1}^{2} (-1)^{tj} (\eta^{tj} + \eta^{-tj}) \left(\eta^t + \eta^{-t}\right)^{jc_1 s} &= 1 + (-1)^j \sum_{m=0}^{j} d_m^{(j)} L_m \\
&= 1 + \sum_{t=1}^{2} (-1)^{tj} (\eta^{tj} + \eta^{-tj}) \\
&= 0.
\end{aligned}$$

So condition (v) of Corollary 4.2 is satisfied and thus $P(x)$ is a PP.

The proof of necessity and sufficiency of conditions given in (ii) for $k + 1 \equiv -2 \pmod 5$ is similar. The proof is now complete. □

Note: One can show that if $q - 1 = p^m - 1 = 5s$ for an odd prime p such that $p \not\equiv 1 \pmod 5$ or $5 \mid m$, then $(k+1)^s \equiv 1 \pmod p$ as long as $k+1 \not\equiv 0 \pmod p$ and also $L_s = 2$ always hold in $\mathbb{F}_p$. Therefore in this case $P(x) = x^r(1 + x^s + \cdots + x^{ks})$ is a PP if and only if $(r, s) = 1$, $(5p, k + 1) = 1$ and $2r + ks \not\equiv 0 \pmod 5$.

References

[1] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.*, **134** (1) (2006), 15–22.

[2] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* **95** (1988), 243-246.

[3] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* **100** (1993), 71-74.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1997.

[5] R. Matthews, Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field, *Proc. Amer. Math. Soc.* **120** (1994), 47–51.

[6] G. L. Mullen, Permutation polynomials over finite fields, *Finite Fields, Coding Theory, and Advances in Communications and Computing,* pp. 131-151, Marcel Dekker, New York, 1993.

[7] M. O. Rayes, V. Trevisan and P. Wang, Factorization of Chebyshev polynomials, *http://icm.mcs.kent.edu/reports/index1998.html.*

[8] Y. H. Park and J. B. Lee, Permutation polynomials with exponents in an arithmetic progression, *Bull. Austral. Math. Soc.* **57** (1998), 243–252.

[9] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* **112** (1991), 149–163.

[10] L. Wang, On permutation polynomials, *Finite Fields and Their Applications* **8** (2002), 311–322.

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, Alberta, T1K 3M4, CANADA
E–mail address: amir.akbary@uleth.ca

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, Alberta, T1K 3M4, CANADA

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6, CANADA
E–mail address: wang@math.carleton.ca