Cyclotomic Mapping Permutation Polynomials over Finite Fields

Qiang Wang*

School of Mathematics and Statistics, Carleton University,
1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada,
wang@math.carleton.ca,
http://math.carleton.ca/~wang.html

Abstract. We explore a connection between permutation polynomials of the form $x^r f(x^{(q-1)/l})$ and cyclotomic mapping permutation polynomials over finite fields. As an application, we characterize a class of permutation binomials in terms of generalized Lucas sequences.

Key words: permutation polynomials, cyclotomic mappings, generalized Lucas sequences, finite fields

1 Introduction

Let p be prime and $q = p^m$. A polynomial is a permutation polynomial (PP) of a finite field $\mathbb{F}_q$ 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, interests in permutation polynomials have significantly increased because of their potential applications in public key cryptosystems ([12],[13],[14]), RC6 block ciphers ([21], [22]), combinatorial designs like de Bruijn sequences ([6]), Tuscan-k arrays ([8]), and Costas arrays ([5], [11]), among many others. Permutation polynomials are also used in coding theory, for instance, permutation codes in power communications ([7]), and interleavers in Turbo codes ([26]) etc. In some of these applications, the study of permutation polynomials over finite fields has also been extended to the study of permutation polynomials over finite rings and other algebraic structures. For more background material on permutation polynomials we refer to Chap. 7 of [18]. For a detailed survey of open questions and recent results see [9], [15], [16], and [19].

Every polynomial $P(x)$ over $\mathbb{F}_q$ such that $P(0) = 0$ has the form $x^r f(x^s)$ with $r > 0$ and some positive integer $s \mid q-1$. Here we are interested in permutation behavior of polynomials $P(x) = x^r f(x^s)$ over finite field $\mathbb{F}_q$, where $f(x)$ is an arbitrary polynomial of degree $e > 0$, $0 < r < q-1$, and $q - 1 = ls$ for some positive integers l and s. In Sect. 2, we introduce the notion of r-th order cyclotomic mappings $f^r_{A_0,A_1,\cdots,A_{l-1}}$ of index l and reveal a simple and very useful connection between polynomials of the form $x^r f(x^s)$ and so-called r-th order

* The research is partially supported by NSERC of Canada.

cyclotomic mapping polynomials. That is, $P(x) = x^r f(x^s) = f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ where $A_i = f(\zeta^i)$ for $0 \le i \le l-1$ and ζ is a primitive l-th root of unity. This provides us an easier way to study polynomials of the form $x^r f(x^s)$. Indeed, many different criteria of when these polynomials are permutation polynomials are summarized in Theorem 1. Some new classes of permutation polynomials are given to demonstrate the potential applications of these criteria. In particular, in Sect. 3, we characterize permutation binomials of the form $P(x) = x^r(x^{es}+1)$ over $\mathbb{F}_q$ in terms of the generalized Lucas sequences of order $\frac{l-1}{2}$ over $\mathbb{F}_p$ as a concrete application (Theorem 3). Earlier study in this direction can be found in [1], [2] and [3].

2 Cyclotomic Mapping Permutation Polynomials

Let γ be a primitive element of $\mathbb{F}_q$, $q-1 = ls$ for some positive integers l and s, and the set of all nonzero l-th powers of $\mathbb{F}_q$ be $C_0 = \{\gamma^{lj} : j = 0, 1, \cdots, s-1\}$. Then C_0 is a subgroup of $\mathbb{F}_q^*$ of index l. The elements of the factor group $\mathbb{F}_q^*/C_0$ are the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i = 0, 1, \cdots, l-1.$$

For any integer $r > 0$ and any $A_0, A_1, \cdots, A_{l-1} \in \mathbb{F}_q$, we define an *$r$-th order cyclotomic mapping $f^r_{A_0,A_1,\cdots,A_{l-1}}$ of index l* from $\mathbb{F}_q$ to itself by $f^r_{A_0,A_1,\cdots,A_{l-1}}(0) = 0$ and

$$f^r_{A_0,A_1,\cdots,A_{l-1}}(x) = A_i x^r \quad \text{if } x \in C_i, \quad i = 0, 1, \cdots, l-1.$$

Moreover, $f^r_{A_0,A_1,\cdots,A_{l-1}}$ is called an *r-th order cyclotomic mapping of the least index l* if the mapping can not be written as a cyclotomic mapping of any smaller index. The polynomial $f^r_{A_0,A_1,\cdots,A_{l-1}}(x) \in \mathbb{F}_q[x]$ of degree at most $q-1$ representing the cyclotomic mapping $f^r_{A_0,A_1,\cdots,A_{l-1}}$ is called an *r-th order cyclotomic mapping polynomial*. In particular, when $r = 1$, it is known as a *cyclotomic mapping polynomial* (see [10] or [20]).

Let $\zeta = \gamma^s$ be a primitive l-th root of unity. Next we show that polynomials of the form $x^r f(x^s)$ and the r-th order cyclotomic mapping polynomials $f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ where $A_i = f(\zeta^i)$ for $0 \le i \le l-1$ are the same.

Lemma 1. *For any $r > 0$, $x^r f(x^s) = f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ where $A_i = f(\zeta^i)$ for $0 \le i \le l-1$.*

Proof. For any $x \in C_i$, $x = \gamma^{lj+i}$ for some $0 \le j \le s-1$. Hence $f(x^s) = f((\gamma^{lj}\gamma^i)^s) = f(\gamma^{is}) = f(\zeta^i) = A_i$. Therefore $P(x) = x^r f(x^s) = f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$. □

This simple connection provides us some useful criteria of when polynomials $P(x) = x^r f(x^s)$ are permutation polynomials of $\mathbb{F}_q$. It is well known that if $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ then $(r, s) = 1$, where (r, s) denotes the greatest common divisor of r and s. Otherwise, let $(r, s) = d \ne 1$, then two distinct d-th roots of unity are mapped to the same element by $P(x)$,

a contradiction. Moreover, we note that $A_j \neq 0$ for all $j = 0, \cdots l-1$ in any permutation polynomial $f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ since, otherwise, $f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ has more than 1 zeros. Hence we assume that $(r,s) = 1$ and $A_i \neq 0$ for $0 \leq i \leq l-1$ without loss of generality.

We first recall the following Lemma from [4].

Lemma 2. *Let $l \mid q-1$ and $\xi_0, \xi_1, \cdots, \xi_{l-1}$ be some l-th roots of unity in $\mathbb{F}_q$. Then $\xi_0, \xi_1, \cdots, \xi_{l-1}$ are all distinct if and only if*

$$\sum_{i=0}^{l-1} \xi_i^c = 0, \quad \text{for all } c = 1, \cdots, l-1.$$

Proof. For the sake of completeness, we include the proof from [4]. First note that for an l-th root of unity ξ, we have

$$1 + \xi + \cdots + \xi^{l-1} = \begin{cases} 0 \text{ if } \xi \neq 1, \\ l \text{ if } \xi = 1. \end{cases}$$

Now for $t = 0, \ \cdots, \ l-1$, let

$$h_t(x) = \sum_{j=0}^{l-1} \xi_t^{l-j} x^j.$$

We have

$$h_t(\xi_j) = \begin{cases} 0 \text{ if } t \neq j, \\ l \text{ if } t = j. \end{cases}$$

Let

$$h(x) = \sum_{t=0}^{l-1} h_t(x) = l + \sum_{j=1}^{l-1} \left(\sum_{t=0}^{l-1} \xi_t^{l-j} \right) x^j.$$

We consider h as a function from μ_l to $\mathbb{F}_q$. Since the degree of $h(x)$ is less than or equal to $l-1$, it is clear that $\xi_0, \xi_1, \cdots, \xi_{l-1}$ are all distinct if and only if $h(x) = l$. This implies the result. □

Theorem 1. *Let p be prime and $q = p^m$, $q - 1 = ls$ for some positive integers l and s, γ be a given primitive element of $\mathbb{F}_q$ and $\zeta = \gamma^s$ be a primitive l-th root of unity. Assume $P(x) = x^r f(x^s) = f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ with $(r,s) = 1$ and $A_i = f(\zeta^i) \neq 0$ for $0 \leq i \leq l-1$. Then the following are equivalent:*

(a) $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$.
(b) $f^r_{A_0,A_1,\cdots,A_{l-1}}(x)$ is a permutation polynomial of $\mathbb{F}_q$.
(c) $A_i C_{ir} \neq A_{i'} C_{i'r}$ for any $0 \leq i < i' \leq l-1$.
(d) $Ind_\gamma(\frac{A_i}{A_{i'}}) \not\equiv r(i'-i) \pmod{l}$ for any $0 \leq i < i' \leq l-1$, where $ind_\gamma(a)$ is residue class $b \bmod q-1$ such that $a = \gamma^b$.
(e) $\{A_0, A_1\gamma^r, \cdots, A_{l-1}\gamma^{(l-1)r}\}$ is a system of distinct representatives of $\mathbb{F}_q^*/C_0$.

(f) $\{A_0^s, A_1^s\zeta^r, \cdots, A_{l-1}^s\zeta^{(l-1)r}\} = \mu_l$, *where* μ_l *is the set of all distinct* l*-th roots of unity.*

(g) $\sum_{i=0}^{l-1} \zeta^{cri} A_i^{cs} = 0$ *for all* $c = 1, \cdots, l-1$.

Proof. By Lemma 1, (a) and (b) are equivalent. Since $C_i = \{\gamma^{lj+i} : j = 0, 1, \cdots, s-1\}$, for any two elements $x \neq y \in C_i$, we have $x = \gamma^{lj+i}$ and $y = \gamma^{lj'+i}$ for some $0 \leq j \neq j' \leq s-1$. Since $(r, s) = 1$, we obtain $A_i x^r = A_i \gamma^{lrj+ir} \neq A_i y^r = A_i \gamma^{lrj'+ir}$. Moreover, it is easy to prove that $C_0^r = C_0$ and more generally $C_i^r = C_{ir}$ for any $0 \leq i \leq l-1$. Hence (b) and (c) are equivalent.

Because $A_i\gamma^{ir}$ is a coset representative of $A_i C_{ir}$, it is easy to see that (c), (d), (e), and (f) are equivalent. Finally, since all of $A_0^s, A_1^s\zeta^r, \cdots, A_{l-1}^s\zeta^{(l-1)r}$ are l-th roots of unity, (f) means that A_0^s, $A_1^s\zeta^r$, $\cdots$, $A_{l-1}^s\zeta^{(l-1)r}$ are all distinct. By Lemma 2, (f) is equivalent to (g). □

We note that the equivalence of (a) and (d) was first found in [24] and the equivalence of (a) and (g) was first proved in [4]. In fact, $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $A_i = f(\zeta^i) \neq 0$ for all $0 \leq i \leq l-1$, and any one of the conditions in Theorem 1 holds. From now on, permutation polynomials $P(x) = x^r f(x^s) = f^r_{A_0, A_1, \cdots, A_{l-1}}(x)$ where $A_i = f(\zeta^i)$ for $0 \leq i \leq l-1$ are called *r-th order cyclotomic mapping permutation polynomials of index l*. In the following, we use Theorem 1 (e) to obtain the number of r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of index l as in Theorem 2 [20]. The second part is obtained by using Möbius inversion formula of $\sum_{d|l} Q_d = P_l$.

Corollary 1. *Let p be prime, $q = p^m$, and $l \mid q-1$ for some positive integer l. For each positive integer r such that $(r, s) = 1$, there are $P_l = l!(\frac{q-1}{l})^l$ distinct r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of index l. Moreover, the number Q_l of r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of least index l is*

$$Q_l = \sum_{\substack{d|l \\ (r,(q-1)/d))=1}} \mu\left(\frac{l}{d}\right)\left(\frac{q-1}{d}\right)^d d!.$$

Therefore there are $l!(\frac{q-1}{l})^l\phi(\frac{q-1}{l})$ distinct permutation polynomials of the form $x^r f(x^s)$ of $\mathbb{F}_q$ in total, which was also obtained in [24] through a study of the group structure of these permutation polynomials.

In the rest of this section, we will see some examples of permutation polynomials of this form. It is well known that $P(x) = x^{r+es}$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r + es, q-1) = 1$, which is equivalent to conditions $(r + es, s) = 1$ and $(r + es, l) = 1$. Obviously, $(r + es, s) = 1$ is the same as $(r, s) = 1$. And the condition $(r + es, l) = 1$ is equivalent to the conditions stated in Theorem 1 for $f(x) = x^e$.

For $l = 3 \mid q-1$ and an integer $s = \frac{q-1}{3}$, by Theorem 1, $x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$ and $\{A_0^s, A_1^s\theta^r, A_2^s\theta^{2r}\} =$

$\mu_3 = \{1, \theta, \theta^2\}$ where $\theta^3 = 1$ and $A_i = f(\theta^i)$ for $i = 0, 1, 2$. The condition $\{A_0^s, A_1^s\theta^r, A_2^s\theta^{2r}\} = \{1, \theta, \theta^2\}$ is equivalent to $A_0^s \neq A_1^s\theta^r, A_0^s \neq A_2^s\theta^{2r}, A_1^s\theta^r \neq A_2^s\theta^{2r}$. However, in some cases, we always have $A_0^s = 1$. Next we construct some new classes of permutation polynomials of this type.

Theorem 2. *Let p be prime, $q = p^m$, and $q-1 = 3s$ for some positive integer s. Assume $f(x) \equiv ax^2+bx+c \pmod{x^3-1}$ such that $a^2+b^2+c^2-ab-ac-bc = 1$. Then $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $A_0^s = 1$ and $A_1^s\theta^r \neq A_2^s\theta^{2r}$ where $\theta^3 = 1$ and $A_i = f(\theta^i)$ for $i = 0, 1, 2$.*

Proof. If $a^2 + b^2 + c^2 - ab - ac - bc = 1$, then $A_1A_2 = f(\theta)f(\theta^2) = 1$. If $P(x)$ is a PP, then $\prod_{x\in\mathbb{F}_q^*} P(x) = -1$ implies that $A_0^s = 1$. Hence $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $A_0^s = 1$ and $\{A_1^s\theta^r, A_2^s\theta^{2r}\} = \{\theta, \theta^2\}$. Since $A_0^s = 1$, we note that $\{A_1^s\theta^r, A_2^s\theta^{2r}\} = \{\theta, \theta^2\}$ is also equivalent to $A_1^s\theta^r \neq A_2^s\theta^{2r}$. Indeed, $A_0^s = (A_1^s\theta^r)(A_2^s\theta^{2r}) = 1$ implies that either $A_1^s\theta^r = A_2^s\theta^{2r} = 1$ or $\{A_1^s\theta^r, A_2^s\theta^{2r}\} = \{\theta, \theta^2\}$. □

Corollary 2. *Let p be prime, $q = p^m$, and $q - 1 = 3s$ for some positive integer s. Assume that $f(x) \equiv ax^2 + bx + a \pmod{x^3 - 1}$ such that $(a - b)^2 = 1$. Then $x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(2a+b)^s = 1$ and $(r + s, 3) = 1$.*

Proof. Since $f(x) \equiv ax^2 + bx + a \pmod{x^3 - 1}$ and $\theta^3 = 1$, $A_2 = f(\theta^2) = \theta f(\theta) = \theta A_1$. Hence $A_1^s\theta^r \neq A_2^s\theta^{2r}$ reduces to $\theta^{r+s} \neq 1$, which is equivalent to $(r + s, 3) = 1$. The rest follows from Theorem 2 and $A_0 = f(1) = 2a + b$. □

3 Permutation Binomials and Generalized Lucas Sequences

In this section, we explain how permutation binomials and generalzied Lucas sequences are closely related as a result of Theorem 1. Again, we let p be prime, $q = p^m$, $q - 1 = ls$ for some positive integers l and s, and ζ be a primitive l-th root of unity. Here we consider permutation polynomials over $\mathbb{F}_q$ of the form $P(x) = x^r(x^{es} + 1)$ with $(e, l) = 1$. That is, $P(x) = x^r f(x^s)$ where $f(x) = x^e + 1$ and $(e, l) = 1$. We note that the case of $f(x) = x^e + b$ with an l-th root of unity b is similar. In this case, p is odd. Otherwise, $P(0) = P(1) = 0$. Moreover, we must have $\zeta^{ei} \neq -1$ for $i = 0, \cdots, l - 1$. Hence l must be odd. Then s must be even. In fact, without loss of generality, we can assume $l \geq 3$ from now on. Moreover, since $l \mid q - 1$ and both p and l are odd, there exists $\eta \in \mathbb{F}_q$ such that $\eta^2 = \zeta$. Hence η is a primitive $2l$-th root of unity in $\mathbb{F}_q$.

We define the sequence $\{a_n\}_{n=0}^{\infty}$ by

$$a_n = \sum_{t=1}^{\frac{l-1}{2}} \left((-1)^{t+1}(\eta^t + \eta^{-t})\right)^n = \sum_{\substack{t=1 \\ t \ odd}}^{l-1} \left(\eta^t + \eta^{-t}\right)^n.$$

The sequence $\{a_n\}_{n=0}^{\infty}$ is then called *generalized Lucas sequence of order* $\frac{l-1}{2}$ because $\{a_n\}_{n=0}^{\infty} = \{L_n\}_{n=0}^{\infty}$ when $l = 5$, where the Lucas sequence $\{L_n\}_{n=0}^{\infty}$ is an integer sequence satisfying the recurrence relation $L_{n+2} - L_{n+1} - L_n = 0$ and $L_0 = 2$ and $L_1 = 1$.

For any integer $n \geq 1$ and $a \in \mathbb{F}_q$, the Dickson polynomial of the first kind $D_n(x, a) \in \mathbb{F}_q[x]$ of degree n with parameter a is defined by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

Similarly, the Dickson polynomial of the second kind $E_n(x, a) \in \mathbb{F}_q[x]$ of degree n with parameter a is defined by

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

For $a \neq 0$, we write $x = y + a/y$ with y an indeterminate. Then the Dickson polynomials can often be rewritten as

$$D_n(x,a) = D_n\left(y + \frac{a}{y}, a\right) = y^n + \frac{a^n}{y^n},$$

and

$$E_n(x,a) = E_n\left(y + \frac{a}{y}, a\right) = \frac{y^{n+1} - a^{n+1}/y^{n+1}}{y - a/y}.$$

In the case $a = 1$, we denote Dickson polynomials of degree n by $D_n(x)$ and $E_n(x)$ respectively. It is well known that Dickson polynomials are closely related to the Chebyshev polynomials by the connections $D_n(2x) = 2T_n(x)$ and $E_n(2x) = U_n(x)$, where $T_n(x)$ and $U_n(x)$ are Chebyshev polynomials of degree n, of the first kind and the second kind respectively. More information on Dickson polynomials can be found in [17].

We consider the Dickson polynomial $E_{l-1}(x)$ of the second kind of degree $l-1$ with parameter $a = 1$. It is well known that $\eta^t + \eta^{-t}$ with $1 \leq t \leq l-1$ are all the roots of $E_{l-1}(x)$ where η is a primitive $2l$-th root of unity. Let

$$E_{l-1}^{odd}(x) = \prod_{\substack{t=1 \\ odd\ t}}^{l-1} (x - (\eta^t + \eta^{-t})).$$

Then the characteristic polynomial of the sequence $\{a_n\}_{n=0}^{\infty}$ is $E_{l-1}^{odd}(x)$. Using the factorization of $U_{l-1}(x)$ over $\mathbb{Z}$ (Theorem 2 in [23]) and the fact $E_{l-1}(2x) = U_{l-1}(x)$, it is obvious to conclude that $E_{l-1}^{odd}(x)$ is also a polynomial with integer coefficients (thus over $\mathbb{F}_p$). It then follows from Waring's formula (Theorem 1.76 in [18]) that $\{a_n\}_{n=0}^{\infty}$ is an integer sequence and thus a sequence over $\mathbb{F}_p$. For more information on the sequence $\{a_n\}_{n=0}^{\infty}$, one can also refer [1], [2], and [3].

Theorem 3. *Let p be odd prime and $q = p^m$. Assume that l, s, r, e are positive integers such that l is odd, $q - 1 = ls$, and $(e, l) = 1$. Then $P(x) = x^r(x^{es} + 1)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

(i) $(r, s) = 1$;
(ii) $2^s \equiv 1 \pmod{p}$;
(iii) $2r + es \not\equiv 0 \pmod{l}$;
(iv) $\sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k a_{cs+cj-2k} = -1$ *in* $\mathbb{F}_p$ *for all* $c = 1, \cdots, l-1$, *where* $\{a_n\}_{n=0}^{\infty}$ *is the generalized Lucas sequence of order* $\frac{l-1}{2}$ *and* $2e^{\phi(l)-1}r + s \equiv j \pmod{2l}$.

Proof. Let $P(x)$ be a PP of $\mathbb{F}_q$. It is well-known that $(r, s) = 1$. Moreover, $\prod_{x \in \mathbb{F}_q^*} P(x) = -1$ implies that $\prod_{x \in \mathbb{F}_q^*} (x^{es} + 1) = 1$. Then $\left(\prod_{i=0}^{l-1}(\zeta^i + 1)\right)^s = 1$. Since l is odd, $\prod_{i=0}^{l-1}(\zeta^i + 1) = \prod_{i=0}^{l-1}(1 - (-\zeta^i)) = 1 - (-1) = 2$. Hence $2^s \equiv 1 \pmod{p}$ and (ii) holds.

Assume that $2r + es \equiv 0 \pmod{l}$. Since s is even, $2r + es \equiv 0 \pmod{2l}$. By Theorem 1 (g), we have $\sum_{i=0}^{l-1} \zeta^{cri} A_i^{cs} = 0$ for all $c = 1, \cdots, l-1$, where $A_i = \zeta^{ei} + 1$. Since $l \mid q - 1$ and l is odd, we can find $\eta \in \mathbb{F}_q$ such that $\eta^2 = \zeta$. Thus we obtain

$$\sum_{i=0}^{l-1} \eta^{(2r+es)ci}(\eta^{ei} + \eta^{-ei})^{cs} = 0, \ \textit{for all } c = 1, \cdots, l-1. \tag{1}$$

It follows from $2r + es \equiv 0 \pmod{2l}$ that

$$\sum_{i=0}^{l-1}(\eta^{ei} + \eta^{-ei})^{cs} = 0, \ \textit{for all } c = 1, \cdots, l-1.$$

Since each $(\eta^{ei} + \eta^{-ei})^s$ is an l-th root of unity, by Lemma 2, $(\eta^{ei} + \eta^{-ei})^s$, $i = 0, \cdots, l-1$, are all distinct. However, since s is even, we have $(\eta^{ei} + \eta^{-ei})^s = (\eta^{e(l-i)} + \eta^{-e(l-i)})^s$, a contradiction. Hence $2r + es \not\equiv 0 \pmod{l}$ and (iii) holds.

Using $(e, l) = 1$, we have $e^{\phi(l)} \equiv 1 \pmod{l}$ where ϕ is the Euler's totient function. Then we can rewrite (1) as

$$2^{cs} + \sum_{t=1}^{(l-1)/2} (\eta^{c(2e^{\phi(l)-1}r+s)t} + \eta^{-c(2e^{\phi(l)-1}r+s)t})(\eta^t + \eta^{-t})^{cs} = 0, \ \textit{for all } c = 1, \cdots, l-1. \tag{2}$$

Let $2e^{\phi(l)-1}r + s \equiv j \pmod{2l}$. Then it yields that $\eta^{cjt} + \eta^{-cjt} = D_{cj}(\eta^t + \eta^{-t})$ where $D_{cj}(\eta^t + \eta^{-t})$ is the Dickson polynomial of the first kind of degree

cj. That is, $D_{cj}(\eta^t+\eta^{-t}) = \sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k(\eta^t+\eta^{-t})^{cj-2k}$. Because both s and j are even, we obtain

$$\begin{aligned}
&2^{cs} + \sum_{t=1}^{(l-1)/2} (\eta^{c(2e^{\phi(l)-1}r+s)t} + \eta^{-c(2e^{\phi(l)-1}r+s)t})(\eta^t+\eta^{-t})^{cs} \\
&= 1 + \sum_{t=1}^{(l-1)/2}\sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k(\eta^t+\eta^{-t})^{cj-2k}(\eta^t+\eta^{-t})^{cs} \\
&= 1 + \sum_{t=1}^{(l-1)/2}\sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k(\eta^t+\eta^{-t})^{cj-2k}(\eta^t+\eta^{-t})^{cs} \\
&= 1 + \sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k a_{cs+cj-2k} \\
&= 0.
\end{aligned}$$

Hence (iv) follows. Conversely, assume that (i)-(iv) are satisfied, then it is straightforward to show that $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$ by Theorem 1. □

We can also rewrite the above theorem in the following way.

Corollary 3. *Let $q = p^m$, p is an odd prime, and $q-1 = ls$ for positive integers l and s. Assume that p, l, r, s satisfies*

$$l \text{ is odd}, (e,l) = 1, (r,s) = 1, 2^s \equiv 1 \pmod{p}, 2r+es \not\equiv 0 \pmod{l}.$$

Then $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if

$$\sum_{n=0}^{j_c} t_n^{(j_c)} a_{cs+n} = -1 \text{ in } \mathbb{F}_p, \text{ for all } c = 1, \cdots, l-1,$$

where $\{a_n\}_{n=0}^{\infty}$ is the generalized Lucas sequence of order $\frac{l-1}{2}$, $2e^{\phi(l)-1}r + s \equiv j \pmod{2l}$, $j_c = cj \bmod 2l$ and $t_n^{(j_c)}$ is the coefficient of x^n in the Dickson polynomial of the first kind of degree j_c.

Furthermore, if $(2r+es, l) = 1$, then we let j' be the inverse of $2e^{\phi(l)-1}r + s$ mod l. Then (2) can be rewritten as

$$2^{c'j's} + \sum_{t=1}^{(l-1)/2} (-1)^{c't}(\eta^{c't}+\eta^{-c't})(\eta^t+\eta^{-t})^{c'j's} = 0, \text{ for all } c' = 1, \cdots, l-1. \quad (3)$$

Using (3) and similar arguments as before, we can improve the previous result by using Dickson polynomials of the first kind of smaller degrees. We note that

if c' is even, then the coefficient $t_n^{(c')}$ of x^n in the Dickson polynomial of the first kind of degree c' is always 0 for all odd n. Similarly, if c' is odd, then $t_n^{(c')} = 0$ for all even n.

Corollary 4. *Let $q = p^m$, p is odd prime, and $q - 1 = ls$ for positive integers l and s. Assume that p, l, r, s satisfies*

$$l \text{ is odd}, \ (e,l) = 1, (r,s) = 1, 2^s \equiv 1 \pmod{p}, (2r + es, l) = 1.$$

Then $P(x) = x^r(x^{es} + 1)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if

$$\sum_{n=0}^{c'} t_n^{(c')} a_{c'j's+n} = (-1)^{c'+1} \text{ in } \mathbb{F}_p, \ \text{for all } c' = 1, \cdots, l-1,$$

where $\{a_n\}_{n=0}^{\infty}$ is the generalized Lucas sequence of order $\frac{l-1}{2}$, $j'(2e^{\phi(l)-1}r + s) \equiv 1 \pmod{l}$, $t_n^{(c')}$ is the coefficient of x^n in the Dickson polynomial of the first kind of degree c'.

In particular, when l is a small prime (e.g. $l = 3, 5, 7$), the sequences $\{a_n\}$ that correspond to permutation binomials can be further described explicitly by using the above conditions (see [2], [25]).

References

1. A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory*, to appear.
2. A. Akbary and Q. Wang, On some permutation polynomials, *Int. J. Math. Math. Sci.*, **16** (2005), 2631–2640.
3. A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.*, **134** (2006), no 1, 15-22.
4. A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, preprint.
5. J. Bell and Q. Wang, A note on Costas arrays and cyclotomic permutations, *Ars Combin.*, to appear.
6. S. R. Blackburn, T. Etzion, and K. G. Paterson, permutation polynomials, de Bruijn sequences, and linear complexity. *J. Combin. Theory Ser. A* **76** (1996), no. 1, 55–82.
7. W. Chu, C. J. Colbourn, P. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.* **32** (2004), no. 1-3, 51–64.
8. W. Chu and S. W. Golomb, Circular Tuscan-k arrays from permutation binomials, *J. Combin. Theory Ser. A* **97** (2002), no. 1, 195–202.
9. S. D. Cohen, Permutation group theory and permutation polynomials. Algebras and combinatorics (Hong Kong, 1997), 133–146, Springer, Singapore, 1999
10. A. B. Evans, Cyclotomy and orthomorphisms: A survey, *Congr. Numer.* **101** (1994), 97-107.
11. S. W. Golomb and O. Moreno, On periodicity properties of Costas arrays and a conjecture on permutation polynomials, *IEEE Trans. Inform. Theory* **42** (1996), no. 6, part 2, 2252–2253.

12. J. Levine and J. V. Brawley, Some cryptographic applications of permutation polynomials, *Cryptologia.* **1** (1977), 76-92.
13. J. Levine and R. Chandler, Some further cryptographic applications of permutation polynomials, *Cryptologia.* **11** (1987), 211-218.
14. R. Lidl and W. B. Müller, Permutation polynomials in RSA-cryptosystems, Adv. in Cryptology, Plenum, New York, 1984, 293-301.
15. 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.
16. 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.
17. R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London/Harlow/Essex, 1993.
18. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, 1997.
19. G. L. Mullen, Permutation polynomials over finite fields, "Finite Fields, Coding Theory, and Advances in Communications and Computing", 131-151, Marcel Dekker, New York, 1993.
20. H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, *Discrete Math.* **295** (2005), 161-171.
21. R. L. Rivest, Permutation polynomials modulo 2^w, *Finite fields Appl.*, **7** (2001), 287 -292.
22. R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, *The RC6 block cipher*, Published electoronically at http://theory.lcs.mit.edu/ rivest/rc6.pdf
23. M. O. Rayes, V. Trevisan and P. Wang, Factorization of Chebyshev polynomials, *http://icm.mcs.kent.edu/reports/index1998.html.*
24. 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.
25. L. Wang, On permutation polynomials, *Finite Fields Appl.* **8** (2002), 311–322.
26. J. Sun and O. Y. Takeshita, Interleavers for Turbo codes using permutation polynomials over integer rings, *IEEE Trans. Inform. Theory*, **51** (2005), no. 1, 101-119.