On Polynomials of the Form $x^r f(x^{(q-1)/l})$

Amir Akbary and Qiang Wang[*]

Abstract

We give a general criterion for permutation polynomials of the form $x^r f(x^{(q-1)/l})$, where $r \geq 1$, $l \geq 1$ and $l \mid (q-1)$. We employ this criterion to characterize several classes of permutation polynomials.

Keywords: finite fields , permutation polynomials
2000 *Mathematics Subject Classification.* 11T06

1 Introduction

Let p be prime and $q = p^m$. A polynomial is a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ to $\mathbb{F}_q$. In recent years, there has been a lot of interests in studying permutation polynomials, partly due to their applications in coding theory, combinatorics and cryptography. For more background material on permutation polynomials we refer to Chapter 7 of [7]. For a detailed survey of open questions and recent results see [5], [6] and [8].

In general, it is a challenging task to characterize permutation polynomials. In fact there are only a few classes of permutation polynomials are known. Many examples of permutation polynomials can be constructed as sub-classes of polynomials of the form $x^r f(x^{(q-1)/l})$, where $r \geq 1$, $l \geq 1$ and $l \mid (q-1)$. More precisely, we observe that any polynomial $h(x) \in \mathbb{F}_q[x]$ can be written as $a(x^r f(x^{(q-1)/l})) + b$, for some $r \geq 1$ and $l \mid (q-1)$. To see this, without loss of generality, we can write

$$h(x) = a(x^n + a_{n-i_1}x^{n-i_1} + \cdots + a_{n-i_k}x^{n-i_k}) + b,$$

where $a,\ a_{n-i_j} \neq 0$, $j = 1, \cdots, k$. Here we suppose that $j \geq 1$ and $n - i_k = r$. Then $h(x) = a\left(x^r f(x^{(q-1)/l})\right) + b$, where $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + \cdots + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$l = \frac{q-1}{\gcd(n-r, n-r-i_1, \cdots, n-r-i_{k-1}, q-1)},$$

[*]Research of both authors is partially supported by NSERC.

and $\gcd(e_0, e_1, \cdots, e_{k-1}, l) = 1$.

Due to the importance of the polynomials of the form $x^r f(x^{(q-1)/l})$, it is interesting to give criteria for PPs of this type. One such criterion was given by Wan and Lidl (Theorem 1.2, [10]).

Theorem (Wan-Lidl) *Let g be a primitive element of $\mathbb{F}_q$ and $\zeta = g^{(q-1)/l}$ be a primitive l-th root of unity in $\mathbb{F}_q$. Then the polynomial $P(x) = x^r f(x^{(q-1)/l})$ is a PP of $\mathbb{F}_q$ if and only if*

(i) $(r, (q-1)/l) = 1$.

(ii) $f(\zeta^t) \neq 0$, *for each* $t = 0, \cdots, l-1$.

(iii) *For all* $0 \leq i < j < l$,

$$Ind_g(\frac{f(\zeta^i)}{f(\zeta^j)}) \not\equiv r(j-i) \pmod{l},$$

where $Ind_g(\frac{f(\zeta^i)}{f(\zeta^j)})$ is the residue class b modulo $q-1$ such that $\frac{f(\zeta^i)}{f(\zeta^j)} = g^b$.

In this paper we give another general criterion (Theorem 2.2) for PPs of the form $P(x) = x^r f(x^{(q-1)/l})$. It turns out that by employing our criterion we can give a unified treatment of several classes of permutation polynomials. Along the way, by applying our theorem, we construct some new classes of permutation polynomials, and give simplified proofs for some known classes of permutation polynomials. They include the class of polynomials of the form $P(x) = x^r f(x^{(q-1)/2})$ (Corollary 2.4), the class of polynomials of the form $P(x) = x^r f(x^{(q-1)/l})$ such that $f(\zeta)^{(q-1)/l} = 1$ for all l-th roots of unity ζ (Theorem 3.1), and the class of polynomials of the form $P(x) = x^r f(x^{(q-1)/l})$ with $f(x) = 1 + x + \cdots + x^k$, where $r \geq 1$ and $k \geq 0$ (Theorem 4.4).

The structure of the paper is as follows. In Section 2, we prove our new criterion. Then we describe some applications of this criterion in Sections 3 and 4.

2 A General Criterion

Lemma 2.1 *Let $l \mid q-1$ and μ_l be the set of all distinct l-th roots of unity in $\mathbb{F}_q$. Let $\xi_0, \xi_1, \cdots, \xi_{l-1}$ be some l-th roots of unity. Then*

$$\{\xi_0, \xi_1, \cdots, \xi_{l-1}\} = \mu_l \iff \sum_{t=0}^{l-1} \xi_t^c = 0, \text{ for } c = 1, \cdots, l-1.$$

Proof. 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

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

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. □

Using Lemma 2.1 we obtain the following general criterion.

Theorem 2.2 *Let $q-1 = ls$ for some positive integers l and s. Let ζ be a primitive l-th root of unity in $\mathbb{F}_q$ and $f(x)$ be a polynomial over $\mathbb{F}_q$. Then the polynomial $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if*

(i) $(r, s) = 1$.

(ii) $f(\zeta^t) \neq 0$, *for each* $t = 0, \cdots, l-1$.

(iii) $\sum_{t=0}^{l-1} \zeta^{crt} f(\zeta^t)^{cs} = 0$ *for each* $c = 1, \cdots, l-1$.

Proof. If $P(x) = x^r f(x^s)$ is a PP, then for a primitive l-th root of unity ζ, $f(\zeta^i) \neq 0$ for $i = 0, \ \cdots, \ l-1$. Moreover, $(r, s) = 1$. This is true, since otherwise $(r, s) = e > 1$. Let ω be a primitive e-th root of unity. Then $P(1) = P(\omega)$, and $P(x)$ is not a PP.

So suppose that conditions (i) and (ii) are satisfied. Let g be a primitive element of $\mathbb{F}_q$. We know that $P(x)$ is a PP if and only if $P(g^k)$ for $k = 1, \ \cdots, \ q-1$ are all distinct. Let $k = ld + t$ where $0 \leq t < l$. Then

$$P(g^k) = g^{l(dr)} g^{tr} f(g^{ts}) = g^{l(dr)} g^{a_t},$$

where $g^{a_t} = g^{tr} f(g^{ts})$. Here a_t is well defined mod $q-1$. Now since $(r, s) = 1$, then dr for $0 \leq d < s$ form a complete set of residues mod s. So $P(g^k)$'s are distinct if and only if a_t's form a complete set of residues mod l. However $\{a_0, \cdots, a_{l-1}\}$ forms a complete set of residues mod l if and only if the mapping $\phi : a \to a^s$ from $\{g^{a_0}, \cdots, g^{a_{l-1}}\}$ to μ_l is surjective. By Lemma 2.1 this is true if and only if

$$\sum_{t=0}^{l-1} g^{csa_t} = 0,$$

for $c = 1, \cdots, l-1$. Hence we are done. □

Combining Wan-Lidl Theorem (see the Introduction) with our Theorem 2.2, we obtain the following equivalent conditions.

Corollary 2.3 *Let $q-1=ls$, $(r,s)=1$, ζ be a primitive l-th root of unity in $\mathbb{F}_q$, and $f(x)$ be a polynomial over $\mathbb{F}_q$ such that none of ζ^t, $t=0,\cdots,l-1$, is a zero of $f(x)$. Then the following are equivalent.*

(i) $\sum_{t=0}^{l-1} \zeta^{crt} f(\zeta^t)^{cs} = 0$ *for each* $c = 1,\cdots,l-1$.

(ii) *For all* $0 \le i < j < l$, $Ind_g(\frac{f(\zeta^i)}{f(\zeta^j)}) \not\equiv r(j-i) \pmod{l}$, *where* $Ind_g(\frac{f(\zeta^i)}{f(\zeta^j)})$ *is the residue class b modulo $q-1$ such that* $\frac{f(\zeta^i)}{f(\zeta^j)} = g^b$, *where g is a fixed primitive element of* $\mathbb{F}_q$.

In [9], Niederreiter and Robinson proved that for odd q, the binomial $x^{(q+1)/2}+ax$ is a PP if and only if $\eta(a^2-1)=1$. Here η is the quadratic character of $\mathbb{F}_q$ with the standard convention $\eta(0)=0$. Next corollary gives a generalization of this theorem.

Corollary 2.4 *For odd q, the polynomial $P(x)=x^r f(x^{(q-1)/2})$ is a PP of $\mathbb{F}_q$ if and only if $(r,(q-1)/2)=1$ and $\eta(f(-1)f(1))=(-1)^{r+1}$.*

Proof. In Theorem 2.2, let $l=2$. Then the result is evident since

$$f(1)^{\frac{q-1}{2}} + (-1)^r f(-1)^{\frac{q-1}{2}} = 0 \iff \eta(f(1)(f(-1)) = (-1)^{r+1}.$$

□

3 First Application

The following is a consequence of our general criterion.

Theorem 3.1 *Let $q-1=ls$. Assume that $f(\zeta^t)^s=1$ for any $t=0,\cdots,l-1$. Then $P(x)=x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r,q-1)=1$.*

Proof. We have

$$\sum_{t=0}^{l-1} \zeta^{crt} f(\zeta^t)^{cs} = \sum_{t=0}^{l-1} \zeta^{crt}.$$

This is zero if and only if $(l,r)=1$. □

Next we show that how the above theorem can result in a unified and simplified treatment of some known classes of PPs. As a special case of Theorem 3.1, we have the following result of Wan and Lidl (see Corollary 1.4 in [10]). The sufficiency part is a classical result of Rogers and Dickson ([4], Theorem 85).

Corollary 3.2 *Let $l \mid q-1$ and $g(x)$ be any polynomial over $\mathbb{F}_q$. Then $P(x) = x^r g(x^s)^l$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, q-1) = 1$ and $g(\zeta^t) \neq 0$ for all $0 \leq t \leq l-1$.*

Proof. This is true since if we set $f(x) = g(x)^l$, then we have $f(\zeta^t)^s = g(\zeta^t)^{ls} = g(\zeta^t)^{q-1} = 1$. The result follows from Theorem 3.1. □

We next consider a class of PPs with coefficients in some appropriate subfield which has been studied in [3]. Special cases of next Corollary has also been considered in [1] and [2].

Corollary 3.3 (Laigle-Chapuy) *Let p be a prime, l be a positive integer and v be the order of p in $\mathbb{Z}/l\mathbb{Z}$. For any positive integer n, take $q = p^m = p^{lvn}$ and $ls = q-1$. Assume $f(x)$ is a polynomial in $\mathbb{F}_{p^{vn}}[x]$. Then the polynomial $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, q-1) = 1$ and $f(\zeta^t) \neq 0$ for all $0 \leq t \leq l-1$.*

Proof. This is clear from Theorem 3.1, since we have

$$\begin{aligned} f(\zeta^t)^{\frac{q-1}{l}} &= f(\zeta^t)^{\frac{p^{vln}-1}{l}} \\ &= f(\zeta^t)^{\frac{p^{vn}-1}{l}\left((p^{vn})^{l-1}+(p^{vn})^{l-2}+\cdots+1\right)} \\ &= \left(\prod_{i=0}^{l-1} f(\zeta^t)^{p^{vni}}\right)^{\frac{p^{vn}-1}{l}} \\ &= \left(f(\zeta^t)^l\right)^{\frac{p^{vn}-1}{l}} \\ &= 1. \end{aligned}$$

□

Note: Laigle-Chapuy has proved the previous corollary under the stronger assumption that $(r, q-1) = 1$ (Theorem 3.1 in [3]). Our proof shows that under the conditions of Corollary 3.3 if $P(x)$ is a PP then $(r, q-1) = 1$.

4 Second Application

In this section, we give another application of our main criterion and construct some new classes of PPs.

Theorem 4.1 *Let $q-1 = ls$, and suppose that $\overline{\mathbb{F}_q}$ (algebraic closure of $\mathbb{F}_q$) contains a primitive jl-th root of unity η. Assume that $\left(\eta^{-ut} f(\eta^{jt})\right)^s = 1$ for any $t = 0, \cdots, l-1$ and a fixed u. Moreover assume that $j \mid us$. Then $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

(i) $(r, s) = 1$,

(ii) $(r+\frac{us}{j},l)=1$.

Proof. From the Theorem 2.2, we need to show that condition (ii) is equivalent to $\sum_{t=0}^{l-1}\zeta^{crt}f(\zeta^t)^{cs}=0$ for $c=1,\cdots,l-1$. We have

$$\begin{aligned}\sum_{t=0}^{l-1}\zeta^{crt}f(\zeta^t)^{cs} &= \sum_{t=0}^{l-1}\eta^{jcrt}f(\eta^{jt})^{cs}\\ &= \sum_{t=0}^{l-1}\eta^{jcrt}(\eta^{ut})^{cs}\\ &= \sum_{t=0}^{l-1}\zeta^{c(r+\frac{us}{j})t},\end{aligned}$$

which is zero if and only if $l\nmid c(r+\frac{us}{j})$ for each c with $1\le c\le l-1$. This is equivalent to $(r+\frac{us}{j},l)=1$. □

From now on, we consider $P(x)=x^rf(x^s)$ such that $f(x)=1+x+\cdots+x^k$, where $r\ge 1$, $k\ge 0$ and $q-1=ls$ for some positive integer l. We first prove two lemmas.

Lemma 4.2 *Let p be an odd prime, $q-1=ls$. Let $f(x)=1+x+\cdots+x^k$. Then $f(\zeta^t)\ne 0$ for any $t=0,\cdots,l-1$ if and only if $(lp,k+1)=1$.*

Proof. $f(\zeta^0)=k+1\ne 0$ is equivalent to $(p,k+1)=1$. Moreover, $f(\zeta^t)\ne 0$ for all $1\le t\le l-1$ is equivalent to $(l,k+1)=1$. □

Lemma 4.3 *Let p be an odd prime, $q-1=ls$, and α be any non-zero element of $\mathbb{F}_p$. Then*
(i) *If $p\equiv -1 \pmod{l}$, and $l>1$ is odd, we have $\alpha^s=1$ in $\mathbb{F}_p$.*
(ii) *If $p\equiv -1 \pmod{l}$, $l=2l_1$, where $l_1>1$ is odd, we have $\alpha^s=1$ in $\mathbb{F}_p$.*

Proof. (i) See [1] Lemma 4.1.
(ii) Since $d=(p-1,l_1)=1$ and $\alpha^{\frac{p-1}{d}}=\alpha^{p-1}=1$ in $\mathbb{F}_p$, α is the l_1-th power of an element β of $\mathbb{F}_p$ ([7], Exercise 2.14), i.e. $\alpha=\beta^{l_1}$. Since $p\equiv -1 \pmod{l}$ and $l\mid q-1$, we have $2\mid m$ and thus $p-1\mid \frac{q-1}{2}$. Therefore $\alpha^s=(\beta^{l_1})^s=\beta^{\frac{q-1}{2}}=1$ in $\mathbb{F}_p$. □

Using Theorem 4.1 we can also obtain the following result which extends Theorem 5.2 in [2].

Theorem 4.4 *Let p be an odd prime, $q-1=ls$. Assume that either (1) $l>1$ is odd or (2) $l=2l_1$, where $l_1>1$ is odd. If $p\equiv -1 \pmod{2l}$, 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 $(r+\frac{ks}{2},l)=1$.*

Proof. For $u = k$ and $j = 2$, let

$$A = \eta^{-ut} f(\eta^{jt}) = \frac{\eta^{(k+1)t} - \eta^{-(k+1)t}}{\eta^t - \eta^{-t}}.$$

Since $2l \mid p+1$, we have

$$\begin{aligned} A^p &= \left((\eta^t)^k + (\eta^t)^{k-1}(\eta^{-t}) + \cdots + (\eta^t)(\eta^{-t})^{k-1} + (\eta^{-t})^k\right)^p \\ &= (\eta^{pt})^k + (\eta^{pt})^{k-1}(\eta^{-pt}) + \cdots + (\eta^{pt})(\eta^{-pt})^{k-1} + (\eta^{-pt})^k \\ &= (\eta^{-t})^k + (\eta^{-t})^{k-1}(\eta^{t}) + \cdots + (\eta^{-t})(\eta^{t})^{k-1} + (\eta^{t})^k \\ &= A. \end{aligned}$$

Therefore $A \in \mathbb{F}_p$. Then we have $A^s = 1$ by Lemma 4.3. Using Theorem 4.1, we conclude our result. □

Note: Note that in the case that both p and l are odd, $p \equiv -1 \pmod{2l}$ is equivalent to $p \equiv -1 \pmod{l}$.

Acknowledgments

The main result of this paper was presented by Qiang Wang in BIRS Workshop on Polynomials over Finite Fields and Applications in November 2006. He wants to thank BIRS for the hospitality.

References

[1] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.*, **134** (2006), no 1, 15-22.

[2] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory*, to appear.

[3] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.*, **13** (2007), 58-70.

[4] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, 1958.

[5] 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.

[6] 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.

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

[8] 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.

[9] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33** (1982) 197–212.

[10] 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.

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

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, CANADA
E–mail address: wang@math.carleton.ca