BULL. AUSTRAL. MATH. SOC. 11T06
VOL. 63 (2001) [67–74]

# PERMUTATION POLYNOMIALS AND GROUP PERMUTATION POLYNOMIALS

YOUNG HO PARK AND JUNE BOK LEE

Permutation polynomials of the form $x^r f(x^s)$ over a finite field give rise to group permutation polynomials. We give a group theoretic criterion and some other criteria in terms of symmetric functions and power functions.

## 1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field of $q = p^e$ elements of characteristic $p$. A polynomial in $\mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if it is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. General study of permutation polynomials started with Hermite, followed by Dickson [**3**]. See [**6**] for general material about permutation polynomials, and [**4, 5**] for open problems concerning permutation polynomials, and [**8**] for recent results.

One of the families of permutation polynomials consists of polynomials of the form $x^r f(x^s)$, where $s \mid q-1$. This class originated from the work of Rogers and Dickson [**3**] who considered the case $f(x) = g(x)^d$, and then several other special cases have been studied by Carlitz and Wells [**2**], Niederreiter and Robinson [**9**]. Wan and Lidl [**12**] gave a simple unified treatment (criterion) for this class in terms of the primitive roots and determined its group structure. The purpose of this article is to give a group theoretic criterion for this family, and explain how this naturally leads to the notion of group permutation polynomials of a subgroup of the multiplicative group $G = \mathbb{F}_q^*$. Brison [**1**] also considered group permutation polynomials and generalised the Hermite criterion. In Section 3, we discuss a conjecture of Brison [**1**]. Turnwald [**11**] gave new criteria for permutation polynomials in terms of symmetric functions and power functions of their values. In the final section, we generalise these to group permutation polynomials.

## 2. GROUP PERMUTATION POLYNOMIALS

Let $N$ be a subgroup of the multiplicative group $G = \mathbb{F}_q^*$. A polynomial in $\mathbb{F}_q[x]$ is called a *group permutation polynomial over* $N$ or simply a *permutation polynomial over*

Received 27th March, 2000
This work is supported by BSRI-97-1423

$N$ if it induces a bijection on $N$. For example, if $(r, |N|) = 1$ and $\alpha \in N$, $\alpha x^r$ is a group permutation polynomial over $N$. These are called *monomials*.

The permutation polynomials of the form $h(x) = x^r f(x^s)$ over $\mathbb{F}_q$ are closely related to the group permutation polynomials over some subgroup of $\mathbb{F}_q^*$. As in [10], we may restrict our attention to polynomials $h(x)$ such that $(r, s) = 1$ and $s \mid q-1$. Let $d = (q-1)/s$. Suppose that $h(x) = x^r f(x^s)$ is a permutation polynomial over $\mathbb{F}_q$. Since $f(x)$ has no nonzero roots, the group $G = \mathbb{F}_q^*$ is $f(x)$-stable. Let

$$H = \{g \in G \mid g^s = 1\} = \{g^d \mid g \in G\}$$

and

$$N = \{g^s \mid g \in G\} = \{g \in G \mid g^d = 1\}.$$

Note that $|H| = s$, and $|N| = d$.

**PROPOSITION 2.1.** *A polynomial $\phi(x)$ maps $N$ into $N$ if and only if $\phi(x) \equiv x^r f(x)^s \pmod{x^d - 1}$ for some $f \in \mathbb{F}_q[x]$.*

PROOF: Suppose $\phi(N) \subset N$. Let $\phi(x) = x^r \phi_1(x)$, where $\phi_1(0) \neq 0$. For each $a \in N$, $\phi_1(a) \in N$, and thus $\phi_1(a) = b_a^s$ for some $b_a \in G$. Choose a polynomial $f(x) \in \mathbb{F}_q[x]$ such that $f(a) = b_a$. Then $\phi(a) = a^r f(a)^s$ for all $a \in N$, and hence $\phi(x) \equiv x^r f(x)^s \pmod{x^d - 1}$. The converse is clear. ∎

**PROPOSITION 2.2.** *For each $g \in G$, the restriction of $h(x)$ to the coset $gH$ is a bijection onto the coset $h(g)H$.*

PROOF: For $\alpha \in H$, we have $h(g\alpha) = (g\alpha)^r f\big((g\alpha)^s\big) = \alpha^r h(g) \in h(g)H$. Thus $h(x)$ maps $gH$ into $h(g)H$. To prove that it is 1-1, suppose $\alpha, \beta \in H$ and $h(g\alpha) = h(g\beta)$. As above, we then have $\alpha^r h(g) = \beta^r h(g)$, or $(\alpha\beta^{-1})^r = 1$. Since $(\alpha\beta^{-1})^s = 1$ and $(r, s) = 1$, this implies that $\alpha = \beta$. Hence the restriction of $h(x)$ to $gH$ is an injection, and hence a bijection onto $h(g)H$. ∎

By Proposition 2.2, $h(x)$ induces a well-defined map on $G/H$ given by

$$\overline{h} : G/H \to G/H, \quad gH \mapsto h(g)H.$$

We use the group isomorphism

$$G/H \simeq N, \qquad gH \mapsto g^s$$

to transform $\overline{h}$ to a function $\phi_h$ on $N$; $\phi_h(g^s) = h(g)^s = g^{rs} f(g^s)^s$. Hence $\phi_h$ is determined as

$$\phi_h(x) = x^r f(x)^s.$$

We can reverse our construction above. Suppose we are given a polynomial $\phi(x) = x^r f(x)^s$ and a $\phi(x)$-stable subgroup $N$ of order $d$, where $ds = q - 1$. Consider the polynomial $h(x) = x^r f(x^s)$. Then $G$ is $h(x)$-stable. Now it is clear, from the construction above, $h(x)$ is the unique polynomial of the given type such that $\phi_h = \phi$. We therefore have the following theorem.

**THEOREM 2.3.** *$x^r f(x^s)$ is a group permutation polynomial over $G = \mathbb{F}_q^*$ if and only if $x^r f(x)^s$ is a group permutation polynomial over $N = \{g^s \mid g \in G\}$.*

It is an easy matter to prove the following two well-known results [6] using Theorem 2.3.

**COROLLARY 2.4.** *Let $(r, q-1) = 1$. Then $h(x) = x^r\left(f(x^s)\right)^{(q-1)/s}$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $f(x^s)$ has no root in $\mathbb{F}_q^*$.*

PROOF: $h(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if

$$\phi(x) = x^r\left(f(x)^{(q-1)/s}\right)^s = x^r f(x)^{q-1}$$

is a permutation polynomial over $N = \{g^s \mid g \in \mathbb{F}_q^*\}$ if and only if $f(x)$ has no root in $N$ if and only if $f(x^s)$ has no root in $\mathbb{F}_q^*$. ∎

**COROLLARY 2.5.** *$h(x) = x(x^{(q-1)/2} + a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(a^2-1)^{(q-1)/2} = 1$.*

PROOF: $h(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $\phi(x) = x(x+a)^{(q-1)/2}$ is a permutation polynomial over $\{\pm 1\}$ if and only if $\phi(1)\phi(-1) = -(a^2-1)^{(q-1)/2} = -1$. ∎

In [10], the authors examined permutation properties of the polynomials

$$h_{k,r,s}(x) = x^r(1 + x^s + \cdots + x^{sk})$$

over $\mathbb{F}_q$, where $k, r, s$ are positive integers. The study of these polynomials originated in [7]. Under suitable assumptions (see [10, Theorem 4.7]) it is proved, using the notion of circulant matrices, that if $h_{k,r,s}(x)$ is a permutation polynomial over $\mathbb{F}_q$, then $(k+1)^s \equiv (-1)^{r-1} \pmod p$. Here we present a quick proof of this using Theorem 2.3. Suppose $h_{k,r,s}(x)$ is a permutation polynomial over $G = \mathbb{F}_q^*$. By Theorem 2.3 $\phi(x) = x^r(1 + x + \cdots + x^k)^s$ is a permutation polynomial over $N = G^s$. Let $d = (q-1)/s$. As proved in [10] $(k+1, d) = 1$ so that $x^{k+1}$ permutes $N$ and $N - \{1\}$. We thus have, in $\mathbb{F}_q^*$,

$$\begin{aligned}
(-1)^{d-1} = \prod_{a\in N} a = \prod_{a\in N} \phi(a) &= (k+1)^s \prod_{1\neq a\in N} a^r\left(\frac{1-a^{k+1}}{1-a}\right)^s \\
&= (k+1)^s(-1)^{(d-1)r}\left(\frac{\prod_{a\neq 1}(1-a^{k+1})}{\prod_{a\neq 1}(1-a)}\right)^s \\
&= (k+1)^s(-1)^{(d-1)r}\left(\frac{\prod_{a\neq 1}(1-a)}{\prod_{a\neq 1}(1-a)}\right)^s \\
&= (k+1)^s(-1)^{(d-1)r}.
\end{aligned}$$

Therefore, we have $(k+1)^s \equiv (-1)^{(d-1)(r-1)} \equiv (-1)^{r-1} \pmod p$.

## 3. $H$-UNIFORMITY

Let $\omega$ be the primitive element of the multiplicative group $G = \mathbb{F}_q^*$ so that $G = \langle\omega\rangle$, and let $H$ be a subgroup of order $s$ of $G$. Let $d = (q-1)/s$. Then $H = \langle\omega^d\rangle$ and

$$G = H \cup H\omega \cup \cdots \cup H\omega^{d-1}.$$

Let $P(G)$ be the group of permutation polynomials over $G = \mathbb{F}_q^*$ and let $P(G/H)$ be the subgroup of $P(G)$ consisting of permutation polynomials of $G$ which induces a permutation of $G/H$.

Observe that $f \in P(G/H)$ if and only if there is a permutation $\pi$ in $S_d$, the symmetric group on $\{0, 1, \ldots, d-1\}$, and permutation polynomials $f_0, \ldots, f_{d-1}$ of $H$ such that

$$f : h\omega^i \mapsto f_i(h)\omega^{\pi(i)}$$

for all $h \in H$ and $0 \leqslant i \leqslant d-1$. If all $f_i(x) \in P(H)$ are monomials of degree $r$ with $(r, s) = 1$, then $f$ is called an *$H$-uniform permutation* of $G$ of index $r$ [**1**]. An $f \in P(G)$ is called an *$H$-uniform polynomial* of index $r$ if $f(x)$ is of the form

$$f(x) = x^r\left(a_0 + a_1x^s + \cdots + a_{d-1}x^{(d-1)s}\right)$$

with $a_i \in \mathbb{F}_q$ [**1**].

The following two results are proved in [**1**].

**Theorem 3.1.** *Let $\pi \in S_d$, $f_i \in P(H)$, $0 \leqslant i \leqslant d-1$ where*

$$f_i(x) = a_{i,1}x + \cdots + a_{i,s-1}x^{s-1}.$$

*Then there exists a unique permutation polynomial $f \in P(G/H)$ of degree $\leqslant q-2$ such that*

1. *the coefficients of $x^s, x^{2s}, \ldots, x^{(d-1)s}$ are all zero;*
2. *$f(h\omega^i) = f_i(h)\omega^{\pi(i)}$ for all $h \in H$ and $0 \leqslant i \leqslant d-1$;*
3. *if there exists $j$ such that $a_{i,j} = 0$ for all $i$, then the coefficients in $f$ of $x^j, x^{s+j}, \ldots, x^{(d-1)s+j}$ are all zero.*

**Corollary 3.2.** *If $(r, s) = 1$, and $\alpha_0, \ldots, \alpha_{d-1} \in H$, then there exists a polynomial of the form $f(x) = x^r\left(a_0 + a_1x^s + \cdots + a_{d-1}x^{(d-1)s}\right)$ in $P(G)$ such that $f(h\omega^i) = \alpha_i h^r\omega^{\pi(i)}$ for all $i$. That is, every $H$-uniform permutation is induced by a suitable $H$-uniform polynomial.*

Brison [**1**] considered a pair of finite subgroups $H \leqslant G \leqslant K^*$ inside any field $K$ and has conjectured that every $H$-uniform polynomial is a $H$-uniform permutation and proved it in several cases. Even in this general setting, the following argument shows that his conjecture is true. Let $H$ be a subgroup of a finite subgroup $G = \langle\omega\rangle$ of $K^*$ and suppose that

$$f(x) = x^r\left(a_0 + a_1x^s + \cdots + a_{d-1}x^{(d-1)s}\right)$$

is a $H$-uniform polynomial, where $s = |H|$. For any $a, b \in G$ with $a^s = b^s$, we have

$$\begin{aligned} f(a)^s &= a^{rs}\left(a_0 + a_1 a^s + \cdots + a_{d-1} a^{(d-1)s}\right)^s \\ &= b^{rs}\left(a_0 + a_1 b^s + \cdots + a_{d-1} b^{(d-1)s}\right)^s \\ &= f(b)^s. \end{aligned}$$

Thus $f$ induces a permutation on $G/H$, that is, $f \in P(G/H)$. As before, we have

$$f(h\omega^i) = f_i(h)\omega^{\pi(i)}$$

for some $f_0, \dots, f_{d-1} \in P(H)$ and $\pi \in S_d$, where $d = |G/H|$. In particular,

$$\omega^{ir}\left(a_0 + a_1\omega^{is} + \cdots + a_{d-1}\omega^{i(d-1)s}\right) = f(\omega^i) = f_i(1)\omega^{\pi(i)}.$$

Thus we have

$$f(h\omega^i) = h^r\omega^{ir}\left(a_0 + a_1\omega^{is} + \cdots + a_{d-1}\omega^{i(d-1)s}\right) = h^r f_i(1)\omega^{\pi(i)}.$$

Therefore, we have:

**Theorem 3.3.** *$f \in P(G)$ is an $H$-uniform permutation if and only if it is an $H$-uniform polynomial.*

## 4. New Criteria for group permutation polynomials

Let $H$ be a subgroup of order $s$ of $\mathbb{F}_q^*$. The following generalised version of the Hermite criterion for group permutation polynomials is proved in [**1**].

**Theorem 4.1.** *For $f(x) \in \mathbb{F}_q[x]$, let*

$$f(x)^t = q_t(x)(x^s - 1) + f_t(x), \quad \deg(f_t) < s,$$

*and let $f_t(0)$ be the constant term of $f_t(x)$. Then $f(x)$ induces a permutation on $H$ if and only if*

1. $f_s(x) = 1$,
2. $f_t(0) = 0$ *for each* $1 \leqslant t \leqslant s - 1$.

For $f \in \mathbb{F}_q[x]$ of degree $\leqslant s$, we shall define, following Turnwald [**11**], three quantities $u, w, v$ and investigate their properties. First define the symmetric polynomials $S_k(f)$ on the values of $f$ by the equation

$$\prod_{a \in H}(x - f(a)) = \sum_{k=0}^{s}(-1)^k S_k(f) x^{s-k}.$$

https://doi.org/10.1017/S0004972700019110 Published online by Cambridge University Press

Let $u = u(f)$ be the smallest positive integer $k$ such that $S_k(f) \neq 0$ if such $k$ exists and otherwise set $u = \infty$. It is easy to see that $u = s - \deg\Bigl(x^s - \prod_{a\in H}(x - f(a))\Bigr)$. Next let

$$P_k(f) = \sum_{a\in H} f(a)^k$$

and define $w = w(f)$ to be the smallest positive integer $k$ such that $P_k(f) \neq 0$ if such $k$ exists, otherwise set $w = \infty$. Replacing $f(x)$ by $f(x)^k \pmod{x^s - 1}$, we see that $w$ is the smallest positive integer such that $f(x)^k \pmod{x^s - 1}$ has a nonzero constant term. Finally let

$$v = v(f) = \bigl|f(H) \cap H\bigr|.$$

**THEOREM 4.2.** *If $f$ is a group permutation polynomial over $H$, then $u = w = v = s$.*

**PROOF:** Since a permutation polynomial $g(x)$ of $H$ permutes the elements of $H$, we have $u(f) = u(f \circ g)$, $w(f) = w(f \circ g)$, and $v(f) = (f \circ g)$. Thus it suffices to prove the statement for $f(x) = x$. Suppose $f(x) = x$. Since $H$ is the set of roots of $x^s - 1$, we have

$$\prod_{a\in H}(x - f(a)) = \prod_{a\in H}(x - a) = x^s - 1,$$

and hence $u(f) = s$. Also $P_k(f) = \sum_{a\in H} f(a)^k = \sum_{a\in H} a^k \neq 0$ if and only if $k \equiv 0 \pmod{s}$. Thus $w(f) = s$. Finally it is clear that $v(f) = s$. ∎

**THEOREM 4.3.** *If $w < \infty$, then $w \leqslant v$.*

**PROOF:** Let $g(x) = d\sum_{a\in H}(x - f(a))^{q-1} + x^{q-1}$. Since

$$\begin{aligned}(x - f(a))^{q-1} &= \frac{(x - f(a))^q}{x - f(a)} = \frac{x^q - f(a)^q}{x - f(a)} \\ &= x^{q-1} + x^{q-2}f(a) + \cdots + xf(a)^{q-2} + f(a)^{q-1}\end{aligned}$$

we have

$$\begin{aligned}g(x) &= d\bigl(sx^{q-1} + P_1(f)x^{q-2} + \cdots + P_{q-2}(f)x + P_{q-1}(f)\bigr) + x^{q-1} \\ &= d\bigl(P_1(f)x^{q-2} + \cdots + P_{q-2}(f)x + P_{q-1}(f)\bigr).\end{aligned}$$

Therefore $\deg g = q - 1 - w$. For each $b \in \mathbb{F}_q^*$, let $n_b = \Bigl|\{a \in H \mid f(a) = b\}\Bigr|$. Then $g(b) = d\sum_{a\in H}(b - f(a))^{q-1} + 1 = d(s - n_b) + 1 = -dn_b$. In particular, if $0 \neq b \notin f(H)$, then $g(b) = 0$. Thus $\deg g \geqslant q - 1 - v$. Since $\deg g = q - 1 - w$, we conclude that $w \leqslant v$. ∎

**THEOREM 4.4.** *If $f(H) \subsetneq H$, then $v + u \leqslant s$.*

PROOF: Consider the polynomial $g(x) = x^s - 1 - \prod_{a\in H}\bigl(x - f(a)\bigr)$. Note $f(x)$ is a permutation polynomial of $H$ if and only if $g(x) = 0$. Since $g\bigl(f(b)\bigr) = 0$ for all $b \in H$, we have $v \leqslant \deg g$. But $g(x) = S_1(f)x^{s-1} - S_2(f)x^{s-2} + \cdots + (-1)^{s+1}S_s(f) - 1$. Thus $\deg g = s - u$. Hence $v \leqslant s - u$. □

**THEOREM 4.5.** *If $f \neq 0$ and $w < \infty$, then $u \leqslant w$.*

PROOF: By Newton's formula, for any $k \geqslant 1$ we have

$$P_k = S_1P_{k-1} - S_2P_{k-2} + \cdots + (-1)^{k-2}S_{k-1}P_1 + (-1)^{k-1}kS_k.$$

In particular, $P_w = (-1)^{w-1}wS_w$. Thus it suffices to show that $p$ does not divide $w$. But if $w = pj$, then

$$0 \neq P_w = \sum_{a\in H} f(a)^{pj} = \Bigl(\sum_{a\in H} f(a)^j\Bigr)^p$$

and hence $P_j \neq 0$, a contradiction. □

**THEOREM 4.6.** *If $f(0) = 0$, then $u \geqslant s/(\deg f)$.*

PROOF: Let $n = \deg f$ and suppose $1 < k < s/n$. Then

$$\deg S_k\bigl(f(x_1), \ldots, f(x_s)\bigr) \leqslant nk < s.$$

By the fundamental theorem of symmetric polynomials, we have

$$S_k\bigl(f(x_1), \ldots, f(x_s)\bigr) = P\bigl(S_1(x_1, \ldots, x_s), \cdots, S_{s-1}(x_1, \ldots, x_s)\bigr)$$

for some polynomial $P$ and the constant term of $P$ is obtained when $x_1 = \cdots = x_s = 0$. Since $f(0) = 0$, this constant term is 0. Now let $H = \{a_1, \ldots, a_s\}$, so that

$$S_k\bigl(f(a_1), \ldots, f(a_s)\bigr) = P\bigl(S_1(a_1, \ldots, a_s), \ldots, S_{s-1}(a_1, \ldots, a_{s-1})\bigr).$$

But $x^s - 1 = \prod_{i=1}^{s}(x - a_i) = x^s - S_1x^{s-1} + S_2x^{s-2} - \cdots + (-1)^{s-1}S_{s-1}x - 1$. Thus $S_i(a_1, \ldots, a_s) = 0$ for all $i = 1, \ldots, s-1$. Therefore

$$S_i\bigl(f(a_1), \ldots, f(a_s)\bigr) = P(0, \ldots, 0) = 0.$$

Consequently, if $1 < k < s/n$, then $S_k(f) = 0$. Hence $u \geqslant s/n$. □

**COROLLARY 4.7.** *If $f(0) = 0$ and $f(H) \subsetneq H$, then $v \leqslant s - s/(\deg f)$.*

**THEOREM 4.8.** *Let $f(H) \subset H$, $f(0) = 0$ and $\deg f = n$. Then the following statements are equivalent:*

1. *$f$ is a group permutation polynomial over $H$;*
2. *$u = s$;*

https://doi.org/10.1017/S0004972700019110 Published online by Cambridge University Press

3. $w = s$;
4. $v = s$;
5. $v > s - (s/n)$;
6. $u > s - v$;
7. $u > (s/2)$;
8. $s - u < w$.

PROOF: Clearly (1) implies all. Note that $w < \infty$ since $f(H) \subset H$. By Theorem 4.5, (2) implies (3). By Theorem 4.3, (3) implies (4). Clearly (4) implies (1). By Corollary 4.7, (5) implies (1). Finally (6) implies (1) by Theorem 4.4. $\square$

## References

[1] O.J. Brison, 'On group-permutation polynomials', *Portugal Math.* **59** (1993), 335–383.

[2] L. Carlitz and C. Wells, 'The number of solutions of a special system of equations in a finite field', *Acta Arith.* **12** (1966), 77–84.

[3] L.E. Dickson, *Linear Groups with an exposition of the Galois field theory* (Dover, New York, 1958).

[4] R. Lidl and G.L. Mullen, 'When does a polynomial over a finite field permute the elements of the field?', *Amer. Math. Monthly* **100** (1988), 243–246.

[5] R. Lidl and G.L. Mullen, 'When does a polynomial over a finite field permute the elements of the field? II', *Amer. Math. Monthly* **95** (1993), 71–74.

[6] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl. **20** (Addison-Wesley, Reading, MA, 1983).

[7] R. Matthews, 'Permutation properties of the polynomials over a finite field', *Proc. Amer. Math. Soc.* **120** (1994), 47–51.

[8] G.L. Mullen, 'Permutation polynomials: a matrix analog of Schur's conjecture and a survey of recent results', *Finite Fields Appl.* **1** (1995), 242–258.

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

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

[11] G. Turnwald, 'A new criterion for permutation polynomials', *Finite Fields Appl.* **1** (1995), 64–82.

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

Department of Mathematics
Kangwon National University
Chuncheon 200-701
Korea
e-mail: yhpark@math.kangwon.ac.kr

Department of Mathematics
Yonsei University
Seoul 120-749
Korea
e-mail: leejb@bubble.yonsei.ac.kr