BULL. AUSTRAL. MATH. SOC. 11T06
VOL. 57 (1998) [243-252]

PERMUTATION POLYNOMIALS WITH EXPONENTS IN AN ARITHMETIC PROGRESSION

YOUNG HO PARK AND JUNE BOK LEE

We examine the permutation properties of the polynomials of the type $h_{k,r,s}(x) = x^r\left(1 + x^s + \cdots + x^{sk}\right)$ over the finite field $\mathbb{F}_q$ of characteristic p. We give sufficient and necessary conditions in terms of k and r for $h_{k,r,1}(x)$ to be a permutation polynomial over $\mathbb{F}_q$ for $q = p$ or p^2. We also prove that if $h_{k,r,s}(x)$ is a permutation polynomial over $\mathbb{F}_q$, then $(k+1)^s = \pm 1$.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of $q = p^n$ elements of characteristic p. A polynomial $h(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (abbreviated to PP) over $\mathbb{F}_q$ if it induces a bijection on $\mathbb{F}_q$. In this article, we shall examine permutation properties of the polynomials

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

over $\mathbb{F}_q$, where k, r, s are positive integers. These are the generalisations of the polynomials of the type $h_k(x) = 1+x+\cdots+x^k$, whose permutation properties were completely characterised by Matthews when q is odd [**3**]:

THEOREM A. *For $q = p^n$ odd, $1 + x + \cdots + x^k$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $k \equiv 1 \pmod{p(q-1)}$.*

Let

$$d = \frac{q-1}{(s, q-1)}, \text{ and } S = \{x \in \mathbb{F}_q \mid x^s = 1\}.$$

There are two permuting classes as given in [**3**]. The proof of the following theorem is essentially the same as that given in [**3**], with a minor correction. We include it for the reader's convenience.

THEOREM B. *$h_{k,r,s}(x)$ is a permutation polynomial over $\mathbb{F}_q$ if one of the following conditions holds:*

(1) $k + 1 \equiv 1 \pmod{d}$, $k + 1 \in S$ *and* $(r, q-1) = 1$;
(2) $k + 1 \equiv -1 \pmod{d}$, $-(k+1) \in S$ *and* $(r - s, q-1) = 1$.

Received 14th July, 1997
This work is supported by BSRI-96-1423 and by Yonsei Academic Research Grant, 1996.

PROOF: Suppose (1). For any $a \in \mathbb{F}_q$, we have

$$h_{k,r,s}(a) = \begin{cases} a^r \dfrac{1 - a^{s(k+1)}}{1 - a^s} = a^r & \text{if } a^s \neq 1, \\ (k+1)a^r & \text{if } a^s = 1 \end{cases} \tag{1.1}$$

Since $k+1 \in S$ and $(r, q-1) = 1$, we see that $(k+1)x^r$ maps S onto S and x^r maps $\mathbb{F}_q - S$ onto inself.

Now suppose (2). Then

$$h_{k,r,s}(a) = \begin{cases} a^r \dfrac{1 - a^{s(k+1)}}{1 - a^s} = -a^{r-s} & \text{if } a^s \neq 1, \\ (k+1)a^r & \text{if } a^s = 1 \end{cases} \tag{1.2}$$

Since $-(k+1) \in S$ and $(r-s, q-1) = 1$, we see that $(k+1)x^r$ maps S onto $(-1)^s S$, and $-x^{r-s}$ maps $\mathbb{F}_q - S$ onto $\mathbb{F}_q - (-1)^s S$. $\square$

In his Ph.D dissertation Matthews has conjectured that the converse of Theorem B holds. We shall prove this conjecture for $q = p$ or p^2 (Theorem 4.6) and also prove that $\pm(k+1) \in S$ if $h_{k,r,s}(x)$ is a PP (Theorem 4.7). It is worth noting that, under the assumption that $h_{k,r,s}(x)$ is a permutation polynomial over $\mathbb{F}_q$, the conditions $k+1 \equiv 1 \pmod{d}$, $k+1 \in S$ force $(r, q-1) = 1$ and the conditions $k+1 \equiv -1 \pmod{d}$, $-(k+1) \in S$ imply $(r-s, q-1) = 1$. As a consequence of Theorem 4.7, it remains to show that $k+1 \equiv \pm 1 \pmod{d}$ to prove this conjecture.

The Hermite criterion will be used in the sequel [**2**];

THE HERMITE CRITERION. *$f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial over $\mathbb{F}_q$ if and only if the following conditions hold:*

(1) *f has exactly one root in $\mathbb{F}_q$;*
(2) *for each integer t with $1 \leqslant t \leqslant q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t \pmod{(x^q - x)}$ has degree $\leqslant q-2$.*

2. PRELIMINARY RESULTS.

Clearly, $h_{k,r,s}(x)$ and $h_{k,r',s}(x)$ are equal as functions on $\mathbb{F}_q$ if $r \equiv r' \pmod{q-1}$. For k, we have the following:

PROPOSITION 2.1. *If $k \equiv l \pmod{p(q-1)/(s, q-1)}$, then $h_{k,r,s}(a) = h_{l,r,s}(a)$ for all $a \in \mathbb{F}_q$.*

PROOF: If $a^s = 1$, then $h_{k,r,s}(a) = a^r(k+1) = a^r(l+1) = h_{l,r,s}(a)$. If $a^s \neq 1$, then

$$h_{k,r,s}(a) = a^r \frac{a^{s(k+1)} - 1}{a^s - 1} = a^r \frac{a^{s(l+1)} - 1}{a^s - 1} = h_{l,r,s}(a)$$

since $k \equiv l \pmod{(q-1)/(s,q-1)}$ if and only if $sk \equiv sl \pmod{q-1}$. $\square$

This Proposition justifies the following notational convention. For negative integers k, r, $h_{k,r,s}(x)$ will mean $h_{k',r',s}(x)$, where k', r' are positive integers with $k' \equiv k \pmod{p(q-1)/(s,q-1)}$ and $r' \equiv r \pmod{q-1}$.

Proposition 2.2. *If $h_{k,r,s}(x)$ is a PP over $\mathbb{F}_q$, then*

$$\left(k+1, \frac{p(q-1)}{s, q-1}\right) = 1.$$

Proof: Suppose $h_{k,r,s}(x)$ is a PP over $\mathbb{F}_q$. First, $h_{k,r,s}(1) = k+1 \neq h_{k,r,s}(0) = 0 \pmod{p}$, that is, $(k+1, p) = 1$. Since $h_{k,r,s}(a) = 0$ if and only if $a^r = 0$ or $1 + a^s + \cdots + a^{sk} = 0$, there is no a such that $a^s \neq 1$ and $1 + a^s + \cdots + a^{sk} = \left(a^{s(k+1)} - 1\right)/(a^s - 1) = 0$. Thus if we let $N_1 = \{a \mid a^s = 1\}$, $N_2 = \{a \mid a^{s(k+1)} = 1\}$, then $N_1 = N_2$. But $|N_1| = (s, q-1) = \left(s(k+1), q-1\right) = |N_2|$. Let $s = (s, q-1)s_0$, $q - 1 = (s, q-1)q_0$ with $(s_0, q_0) = 1$. Then $\left(s(k+1), q-1\right) = (s, q-1)\left((k+1)s_0, q_0\right) = (s, q-1)(k+1, q_0)$. Hence $(k+1, q_0) = 1$. Thus we have $1 = (k+1, pq_0) = \left(k+1, p(q-1)/(s, q-1)\right)$. $\square$

Proposition 2.3. *$h_{k,r,s}(x)$ is a PP if and only if $h_{-k-2,s-r,s}(x)$ is a PP.*

Proof: We show that $h_{k,r,s}(a) = -h_{-k-2,s-r,s}\left(a^{q-2}\right)$ for all $a \in \mathbb{F}_q$. If $a^s = 1$, then $h_{k,r,s}(a) = (k+1)a^r = -(-k-2+1)\left(a^{-1}\right)^{-r}\left(a^{-1}\right)^s = -h_{-k-2,-r+s,s}\left(a^{-1}\right)$. If $a^s \neq 0, 1$, then

$$-h_{-k-2,-r+s,s}\left(\frac{1}{a}\right) = -\left(\frac{1}{a}\right)^{(-r+s)} \frac{\left(\frac{1}{a}\right)^{s(-k-1)} - 1}{\left(\frac{1}{a}\right)^{s} - 1} = -a^r \frac{a^{s(k+1)} - 1}{1 - a^s} = h_{k,r,s}(a).$$

$\square$

Proposition 2.4. *$h_{k,r,s}(x)$ is a PP over $\mathbb{F}_q$ if and only if $h_{k,-r-ks,s}(x)$ is a PP over $\mathbb{F}_q$.*

Proof: We have $h_{k,r,s}\left(a^{q-2}\right) = h_{k,-r-ks,s}(a)$ for all $a \in \mathbb{F}_q$. $\square$

Let $(s, q-1) = s'$. We can choose an integer t relatively prime to $q-1$ such that $st \equiv s' \pmod{q-1}$. Since x^t is a PP, $h_{k,r,s}(x)$ is a PP if and only if the composition $h_{k,r,s}(x^t) = h_{k,rt,st}(x)$ is a PP. Now

$$h_{k,rt,st}(x) \equiv x^{rt}\left(1 + x^{s'} + \cdots + x^{s'k}\right) \equiv h_{k,rt,s'}(x) \pmod{(x^q - x)}$$

with $s' \mid (q-1)$. Thus it suffices to consider the polynomials $h_{k,r,s}(x)$ with $s \mid (q-1)$.

Now let $(r,s) = e$. If $(e, q-1) \neq 1$, then the equation $x^e = 1$ has $(e, q-1)$ solutions and $h_{k,r,s}(x)$ sends all solutions of $x^e = 1$ to $k+1$, so that $h_{k,r,s}(x)$ is not a PP. If $(e, q-1) = 1$, then x^e is a PP and $h_{k,r,s}(x) = h_{k,(r/e),(s/e)}(x^e)$ is a PP if and only if $h_{k,(r/e),(s/e)}(x)$ is a PP.

In conclusion, it is enough to consider the cases that $(r,s) = 1$ and $s \mid (q-1)$. From now on, we shall always assume that

$$(r,s) = 1 \text{ and } s \mid (q-1),$$

so that

$$d = \frac{q-1}{s}.$$

3. Circulant matrices.

We review elementary facts about circulant matrices. A circulant matrix of order n is an $n \times n$ matrix of the form

$$circ(c_0, c_1, \ldots, c_{n-1}) = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}$$

For a polynomial $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1}x^{n-1}$, $C_f = circ(c_0, c_1, \ldots, c_{n-1})$ is called the circulant matrix of f. It is well known that if a field F has a primitive nth root of unity ζ and $f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in F[x]$, then C_f can be put into a diagonalised form as follows [**1, 4**];

$$C_f \sim \begin{pmatrix} f(1) & & & & \\ & f(\zeta) & & & \\ & & f(\zeta^2) & & \\ & & & \ddots & \\ & & & & f(\zeta^{n-1}) \end{pmatrix}. \tag{3.1}$$

Suppose $f(x) = a_1 x + \cdots + a_{q-1}x^{q-1} \in \mathbb{F}_q$ is a PP over $\mathbb{F}_q$. The Hermite criterion implies $a_{q-1} = 0$. Considering the circulant matrix $M_f = circ(0, a_1, a_2, \ldots, a_{q-2})$ of order $q-1$, we then have

$$\det M_f = \prod_{a \in \mathbb{F}_q^*} f(a) = \prod_{a \in \mathbb{F}_q^*} a = -1. \tag{3.2}$$

For $a \in \mathbb{F}_q$ and positive integer m, we denote by $a_{(m)}$ the row vector $(a, a, \cdots, a)$ with m a's.

Let $C = circ\big(a_{(m)}, b_{(n-m)}\big)$ be an $n \times n$ circulant matrix with m a's and $(n-m)$ b's, where $a \neq b$. Then, using (3.1), it is not difficult to show

$$(3.3) \qquad \det C = \begin{cases} \big(ma + (n-m)b\big)(a-b)^{n-1} & \text{if } (m,n) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

It is also clear that

$$(3.4) \qquad \det circ(a_0, a_1, a_2, \dots, a_{n-1}) = (-1)^{n-1} \det circ(a_1, a_2, \dots, a_{n-1}, a_1).$$

4. Main Results

Returing to PP's, we first consider the case $s = 1$ and write $h_{k,r}(x)$ for $h_{k,r,1}(x)$. Assume $h_{k,r}(x)$ is a PP, and write

$$r + k = l(q-1) + m, \text{ where } 0 \leqslant m < q - 1.$$

Let $f(x) = h_{k,r}(x) \pmod{(x^q - x)}$ with $\deg(f) < q$. Then

$$f(x) = \begin{cases} l\big(x + \cdots + x^{r-1}\big) + (l+1)(x^r + \cdots + x^m) & \\ \qquad + l\big(x^{m+1} + \cdots + x^{q-1}\big), & \text{if } m \geqslant r \\ l(x + \cdots + x^m) + (l-1)\big(x^{m+1} + \cdots + x^{r-1}\big) & \\ \qquad + l\big(x^r + \cdots + x^{q-1}\big), & \text{if } m < r. \end{cases}$$

By the Hermite criterion, $l \equiv 0 \pmod{p}$, and hence

$$f(x) = \begin{cases} x^r + \cdots + x^m, & \text{if } m \geqslant r \\ -x^{m+1} - \cdots - x^{r-1}, & \text{if } m < r. \end{cases}$$

First consider the case $m \geqslant r$, and let

$$M_f = circ\big(0_{(r)}, 1_{(m-r+1)}, 0_{(q-2-m)}\big)$$

be the circulant matrix of $f(x)$ of order $(q-1) \times (q-1)$. Since

$$(4.1) \qquad m - r + 1 \equiv k + 1 \pmod{p(q-1)},$$

we have $(m - r + 1, q - 1) = 1$ by Propostion 2.2. Hence, by (3.3) and (3.4),

$$\det M_f = (-1)^{r(q-2)} \det circ\big(1_{(m-r+1)}, 0_{(q-2-m+r)}\big) = (-1)^{r(q-2)}(m - r + 1).$$

By (3.2) and (4.1) we thus have

$$(4.2) \quad k + 1 \equiv m - r + 1 \equiv (-1)^{r(q-2)} \det M_f \equiv (-1)^{r(q-2)-1} \equiv (-1)^{r-1} \pmod{p}.$$

Similar argument shows that (4.2) holds also when $m < r$. Thus we have proved:

https://doi.org/10.1017/S0004972700031622 Published online by Cambridge University Press

Theorem 4.1. *If $x^r(1+x+\cdots+x^k)$ is a PP over $\mathbb{F}_q$, then*

$$k+1 \equiv (-1)^{r-1} \pmod{p}.$$

Now we prove that the conjecture is true for $s=1$ and $q=p$.

Theorem 4.2. *$h_{k,r}(x) = x^r(1+x+\cdots+x^k)$ is a PP over $\mathbb{F}_p$ if and only if one of the following conditions holds:*

(1) $k+1 \equiv 1 \pmod{p(p-1)}$ *and* $(r, p-1) = 1$;
(2) $k+1 \equiv -1 \pmod{p(p-1)}$ *and* $(r-1, p-1) = 1$.

Proof: The claim is easy for $p=2$, so we assume that p is odd. By Proposition 2.1, we may assume that $1 \leqslant k \leqslant p(p-1)$. We may also assume that $1 \leqslant r \leqslant p-1$. As above, write

$$r+k = l(p-1)+m, \text{ with } 0 \leqslant m \leqslant p-2.$$

We know that $l \equiv 0 \pmod{p}$ and $m-r+1 \equiv \pm 1 \pmod{p}$. Since $-(p-2) \leqslant m-r+1 \leqslant p$, we must have $m-r+1 = 1, -1$ or $p-1$.

Case 1. $m-r+1 = 1$: Then $k = l(p-1) = p(p-1)$ and $h_{k,r}(a) = a^r(1+a+\cdots+a^{p(p-1)}) = a^r$ for all $a \in \mathbb{F}_p$. In this case, $h_{k,r}(x)$ is a PP over $\mathbb{F}_p$ if and only if $(r, q-1) = 1$.

Case 2. $m-r+1 = -1$: Then $k = l(p-1)-2 = p(p-1)-2$, and $h_{k,r}(a) = -a^{r-1}$ for all $a \in \mathbb{F}_p$. So $h_{k,r}(x)$ is a PP if and only if $(r-1, q-1) = 1$.

Case 3. $m-r+1 = p-1$: Then $k = l(p-1)+p-2 = p-2$ and, for $a \neq 0, 1$, we have $h_{k,r}(a) = a^r(1+a+\cdots+a^{p-2}) = a^r(a^{p-1}-1)/(a-1) = 0$. Thus $h_{k,r}(x)$ is not a PP over $\mathbb{F}_p$. ∎

Before we proceed to the case $q=p^2$, we need several observations.

Lemma 4.3. *Suppose $r<q$ and $k \leqslant p(q-1)$. If $h_{k,r}(x) = x^r(1+x+\cdots+x^k)$ is a PP over $\mathbb{F}_q$, then $r+k < q-1$ or $p(q-1) \leqslant r+k < (p+1)(q-1)$.*

Proof: The coefficient of x^{q-1} of $h_{k,r}(x) \pmod{x^q - x}$ is $[(r+k)/(q-1)]$. Hence, by the Hermite criterion, $[(r+k)/(q-1)] \equiv 0 \pmod{p}$. Since $r+k \leqslant q-1+p(q-1)$, we have $[(r+k)/(q-1)] = 0$ or p. ∎

Lemma 4.4. *Let $r<q$, q odd, and $k \leqslant p(q-1)$. If $(q-1)/2 \leqslant r+k < q-1$, and if $h_{k,r}(x)$ is a PP over $\mathbb{F}_q$, then $r \equiv 0 \pmod{p}$ or $r+k+1 \equiv 0 \pmod{p}$.*

Proof: We have

$$h_{k,r}(x)^2 = x^{2r}\left(1+2x+3x^2+\cdots+(k+1)x^k+kx^{k+1}+(k-1)x^{k+2}+\cdots+x^{2k}\right)$$

Hence, the coefficient of x^{q-1} in $h_{k,r}(x)^2$ is given by $(2k+1)-(q-1-2r) = 2k+2r+2-q$ if $2r+k < q-1$, or given by $(q-1-2r)+1 = q-2r$ if $2r+k \geqslant q-1$. By the Hermite criterion, the result follows. ∎

https://doi.org/10.1017/S0004972700031622 Published online by Cambridge University Press

Proposition 4.5. *Suppose q is odd and $1 \leqslant k \leqslant p(q-1)$. If $h_{k,r}(x)$ is a PP over $\mathbb{F}_q$, then*

$$k+1 = tp(p-1) \pm 1$$

for some integer t such that $1 \leqslant t \leqslant (q-p)/(p(p-1))$ or $(q/p) \leqslant t \leqslant (q-1)/(p-1)$.

Proof: We may assume that $1 \leqslant r \leqslant q-1$. By Lemma 4.3, we then have $1 \leqslant k < q-1$ or $(p-1)(q-1) \leqslant k \leqslant p(q-1)$. Since $k = tp(p-1)$ or $k = tp(p-1)-2$ for some t by Theorem 4.2, we have $1 \leqslant t \leqslant (q-1)/(p(p-1)) + (\delta/p(p-1))$ or $(q/p) - (1/p) + (\delta/p(p-1)) \leqslant t \leqslant (q-1)/(p-1) + (\delta/p(p-1))$, where $\delta = 0, 2$. Note that $(q-1)/(p(p-1)) + (\delta/p(p-1)) = (q/p-1)/(p-1) + (p-1+\delta)/(p(p-1))$, and $(q/p-1)/(p-1)$ is an integer. When q is odd, we have $(p-1+\delta)/(p(p-1)) < 1$, $-(1/p) + (\delta/p(p-1)) > -1$ and $(\delta/p(p-1)) < 1$ for $\delta = 0, 2$, and thus the claim follows. ∎

Theorem 4.6. *Let $q = p$ or $q = p^2$. Then $h_{k,r}(x) = x^r\left(1 + x + \cdots + x^k\right)$ is a PP over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) $k+1 \equiv 1 \pmod{p(q-1)}$ *and* $(r, q-1) = 1$;
(2) $k+1 \equiv -1 \pmod{p(q-1)}$ *and* $(r-1, q-1) = 1$.

Proof: Suppose $h_{k,r}(x)$ is a PP over $\mathbb{F}_q$. We may assume that $r < q$ and $k \leqslant p(q-1)$. Let $q = p^2$.

First we consider the case $q = 4$. By Theorem 4.1, $k = 2, 4$ or 6. $\mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ where $\alpha^2 = \alpha + 1$. If $k = 2$, $h_{k,r}(\alpha) = \alpha^r\left(1 + \alpha + \alpha^2\right) = 0$, and so $h_{k,r}(x)$ is not a PP over $\mathbb{F}_q$. If $k = 4$, then $h_{k,r}(a) = -a^{r-1}$ for $a \neq 1$ by (1.2) and thus $h_{k,r}(x)$ is a PP over $\mathbb{F}_q$ if and only if $(r-1, q-1) = 1$ (Case (1)). If $k = 6$, then $h_{k,r}(a) = a^r$ for $a \neq 0$ by (1.1) and then $h_{k,r}(x)$ is a PP over $\mathbb{F}_q$ if and only if $(r, q-1) = 1$ (Case (2)).

Now consider for odd $q = p^2$. By Proposition 4.5, $k+1 = tp(p-1) \pm 1$ for some t such that $1 \leqslant t \leqslant 1$ or $p \leqslant t \leqslant p+1$. So the possible values of t are 1, p or $p+1$. We shall show that $t \neq 1, p$

First, assume $t = 1$ so that $k = p(p-1)$ or $k = p(p-1) - 2$. If $r < p-1$, then

$$q-1 > r+k > k \geqslant p^2 - p - 2 \geqslant \frac{q-1}{2}.$$

Lemma 4.4 implies that $r \equiv 0 \pmod{p}$ or $r \pm 1 \equiv 0 \pmod{p}$. This is impossible since $r < p-1$. Thus $r \geqslant p-1$. If $k = p(p-1) - 2$ and $r = p-1$, then $q-1 > r+k = q-3 > (q-1)/2$. Again Lemma 4.4 implies $r = p-1 \equiv 0 \pmod{p}$ or $r+k+1 = q-2 \equiv 0 \pmod{p}$, which is absurd. If $k = p(p-1) - 2$ and $r = p$, then $(r-1, p-1) = p-1 \neq 1$, and thus $h_{k,r}(x)$ is not a PP by Theorem 4.2. Finally, if $p-1 \leqslant r \leqslant q-1$ with $k = p(p-1)$ or $p+1 \leqslant r \leqslant q-1$ with $k = p(p-1)-2$, then $q-1 \leqslant r+k \leqslant 2(q-1)$. So the coefficient of x^{q-1} in $h_{k,r}(x)$ (mod $(x^q - x)$) is nonzero. By the Hermite criterion, $h_{k,r}(x)$ is not a PP over $\mathbb{F}_q$.

Now consider the case $t = p$. Then $k = p^2(p-1)$ or $k = p^2(p-1) - 2$, so that $p(q-1) - k - 2$ is $p(p-1) - 2$ or $p(p-1)$, respectively. Recall that $h_{k,r}(x)$ is a PP if and only if $h_{p(q-1)-k-2,q-r}(x)$ is a PP (Proposition 2.3). Thus this case reduces to the case $t = 1$ and hence $h_{k,r}(x)$ is not a PP.

Therefore $t = p+1$ and $k+1 = p(q-1) \pm 1$. The remaining assertions are now clear by (1.1) and (1.2). ∎

The tensor product or Kronecker product $A \otimes B$ of two matrices A, B is defined by

$$A \otimes B = \begin{pmatrix} b_{11}A & b_{12}A & \dots & b_{1\nu}A \\ b_{21}A & b_{22}A & \dots & b_{2\nu}A \\ \vdots & \vdots & & \vdots \\ b_{\mu 1}A & b_{\mu 2}A & \dots & b_{\mu\nu}A \end{pmatrix}$$

where $B = (b_{ij})$ is a $\mu \times \nu$ matrix. It is well known that

$$\det A \otimes B = (\det A)^{\nu} (\det B)^{\mu}$$

if A is a $\mu \times \mu$ matrix, and B is a $\nu \times \nu$ matrix [4].

Towards the conjecture, we consider the general $s \mid (q-1)$.

Theorem 4.7. *If $h_{k,r,s}(x)$ is a PP over $\mathbb{F}_q$, then*

$$(k+1)^s \equiv (-1)^{r-1} \pmod{p}.$$

Furthermore,

$$k+1 \in S \text{ or } -(k+1) \in S.$$

Proof: Let $s \neq 1$. Write $r + ks = l(q-1) + m$, $0 \leqslant m < q-1$ as before, and let $r = l_0 s + r_0$ with $0 < r_0 < s$. Let $f(x) = h_{k,r,s}(x)$ (mod $(x^q - x)$) with $\deg(f) < q$. If $m \geqslant r$, then

$$f(x) = l\left(x^{r_0} + x^{r_0+s} + \dots + x^{r-s}\right) + (l+1)\left(x^r + x^{r+s} + \dots + x^m\right) \\ + l\left(x^{m+s} + x^{m+2s} + \dots + x^{q-1+r_0-s}\right),$$

and if $m < r$, then

$$f(x) = l\left(x^{r_0} + x^{r_0+s} + \dots + x^m\right) + (l-1)\left(x^{m+s} + x^{m+2s} + \dots + x^{r-s}\right) \\ + l\left(x^r + x^{r+s} + \dots + x^{q-1+r_0-s}\right).$$

https://doi.org/10.1017/S0004972700031622 Published online by Cambridge University Press

As before, let M_f be the circulant matrix of order $(q-1)\times(q-1)$ with the first row vector $(0, a_1, a_2, \ldots, a_{q-2})$ where $f(x) = a_1x + a_2x^2 + \cdots + a_{q-2}x^{q-2}$.

First, consider the case $m \geqslant r$. We have

$$\begin{aligned}\det M_f &= \det circ\big(0_{(r_0)}, l, 0_{(s-1)}, \ldots, l, 0_{(s-1)}, l+1, 0_{(s-1)}, \ldots, l+1, 0_{(s-1)},\\ &\qquad l, 0_{(s-1)}, \ldots, l, 0_{(s-1+s-r_0)}\big)\\ &= (-1)^{r_0(q-2)} \det circ\big(l, 0_{(s-1)}, \ldots, l, 0_{(s-1)}, l+1, 0_{(s-1)}, \ldots, l+1, 0_{(s-1)},\\ &\qquad l, 0_{(s-1)}, \ldots, l, 0_{(s-1)}\big)\\ &= (-1)^{r_0(q-2)} \det\Big(I_s \otimes circ\Big(\overbrace{l, l, \ldots, l}^{(r-r_0)/s}, \overbrace{l+1, \ldots, l+1}^{((m-r)/s)+1}, \overbrace{l, \ldots, l}^{d-((m-r_0)/s)-1}\Big)\Big)\\ &= (-1)^{r_0(q-2)} \Big[\det circ\Big(\overbrace{l, l, \ldots, l}^{(r-r_0)/s}, \overbrace{l+1, \ldots, l+1}^{((m-r)/s)+1}, \overbrace{l, \ldots, l}^{d-((m-r_0)/s)-1}\Big)\Big]^s,\end{aligned}$$

where I_s is the $s\times s$ identity matrix, and $d = (q-1)/s$. By (3.3) and (3.4),

$$\begin{aligned}&\det circ\Big(\overbrace{l, l, \ldots, l}^{(r-r_0)/s}, \overbrace{l+1, \ldots, l+1}^{((m-r)/s)+1}, \overbrace{l, \ldots, l}^{d-((m-r_0)/s)-1}\Big)\\ &=(-1)^{(r-r_0)(d-1)/s} \det circ\Big(\overbrace{l+1, \ldots, l+1}^{((m-r)/s)+1}, \overbrace{l, \ldots, l}^{d-((m-r)/s)-1}\Big)\\ &=(-1)^{(r-r_0)(d-1)/s}\left(dl + \frac{m-r}{s} + 1\right) = (-1)^{(r-r_0)(d-1)/s}(k+1).\end{aligned}$$

But, for odd q, we have

$$r_0(q-2) + \left[\frac{r-r_0}{s}(d-1)\right]s \equiv r_0 + l_0s(d-1) \equiv r_0 - l_0s \equiv r + l_0s = r \pmod 2.$$

Consequently, $(k+1)^s = (-1)^{r-1}$ by (3.2).

By a similar argument when $m < r$ we obtain

$$\det M_f = (-1)^{r_0(q-2)+(m-r_0+2s)(d-1)}(k+1)^s.$$

For odd q, a short calculation shows that $r_0(q-2) + (m - r_0 + 2s)(d-1) \equiv m \equiv r + sk \equiv r \pmod 2$. Here, the last congruence follows beause if s is odd, then d is even and then k is even by Proposition 2.2. Thus we always have $(k+1)^s = (-1)^{r-1}$.

Finally the last assertion of our Theorem is clear for even q. Assume q is odd. If r is odd, then $(k+1)^s = 1$ so that $k+1 \in S$. On the other hand, if r is even then s must be odd, because if r and s were both even, then $h_{k,r,s}(x)$ would be a polynomial in x^2 and then $h_{k,r,s}(x)$ could not be a PP. Thus if r is even, $(-(k+1))^s = 1$. $\square$

https://doi.org/10.1017/S0004972700031622 Published online by Cambridge University Press

References

[1] W.-S. Chou, *Permutation polynomials over finite dields and combinatorial applications*, (Ph.D. Dissertation) (The Pennsylvania State University, 1990).

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

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

[4] M. Marvin and H. Minc, *A survey of matrix theory and matrix inequalities* (Dover, New York, 1964).

Department of Mathematics
Kangwon National University
Chuncheon 200-701
Korea

Department of Mathematics
Yonsei University
Seoul 120-749
Korea