ON SOME PERMUTATION POLYNOMIALS OVER FINITE FIELDS

AMIR AKBARY AND QIANG WANG

Abstract. Let $p$ be prime, $q = p^m$ and $q - 1 = 7s$. We completely describe the permutation behavior of the binomial $P(x) = x^r(1 + x^e)$ ($1 \leq e \leq 6$) over a finite field $\mathbb{F}_q$ in terms of the sequence $\{a_n\}$ defined by the recurrence relation $a_n = a_{n-1} + 2a_{n-2} - a_{n-3}$ ($n \geq 3$) with initial values $a_0 = 3, a_1 = 1,$ and $a_2 = 5$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements with characteristic $p$. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if $P(x)$ induces a bijective map from $\mathbb{F}_q$ to itself. In general, finding classes of permutation polynomials of $\mathbb{F}_q$ is a difficult problem (see Chapter 7 of [2] for a survey of some known classes). An important class of permutation polynomials consists of permutation polynomials of the form $P(x) = x^r f(x^{q-1})$, where $l$ is a positive divisor of $q-1$ and $f(x) \in \mathbb{F}_q[x]$.

These polynomials were first studied by Rogers and Dickson for the case $f(x) = g(x)^l$ where $g(x) \in \mathbb{F}_q[x]$ ([2], Theorem 7.10). A very general result regarding these polynomials is given in [8]. In recent years, several authors have considered the case that $f(x)$ is a binomial (for example, [3], [9] and [1]).

Here we consider the binomial $P(x) = x^r + u^s$ with $r < u$. Let $s = (u - r, q - 1)$ and $l = \frac{q-1}{2}$. Then we can rewrite $P(x)$ as $P(x) = x^r(1 + x^{es})$ where $s = \frac{q-1}{2}$ and $(e, l) = 1$. If $P(x) = x^r(1 + x^{es})$ is a permutation binomial of $\mathbb{F}_q$, then $P(x)$ has exactly one root in $\mathbb{F}_q$ and thus $l$ is odd. When $l = 3, 5$, the permutation behavior of $P(x)$ was studied by L. Wang [9]. In the case $l = 5$, the permutation binomial $P(x)$ is determined in terms of the Lucas sequence $\{L_n\}$ where

$$L_n = \left(2 \cos \frac{\pi}{5}\right)^n + \left(-2 \cos \frac{2\pi}{5}\right)^n.$$ 

More precisely, it is proved that under certain conditions on $r$, $s = \frac{q-1}{2}$ and $e$, the binomial $P(x) = x^r(1 + x^{es})$ is a permutation binomial if and only if $L_s = 2$ in $\mathbb{F}_p$ ([9], Theorem 2).

In this paper, we consider the case $l = 7$ (see [1] for some results related to general $l$). Here we introduce a Lucas-type sequence $\{a_n\}$ by

$$a_n = \left(2 \cos \frac{\pi}{7}\right)^n + \left(-2 \cos \frac{2\pi}{7}\right)^n + \left(2 \cos \frac{3\pi}{7}\right)^n$$

2000 Mathematics Subject Classification. 11B39, 11T06.
Research of both authors partially supported by NSERC.
for integer $n \geq 0$. It turns out that $\{a_n\}_{n=0}^{\infty}$ is an integer sequence satisfying the
recurrence relation
\begin{equation}
a_n = a_{n-1} + 2a_{n-2} - a_{n-3}
\end{equation}
with initial values $a_0 = 3$, $a_1 = 1$, $a_2 = 5$ (see Lemma 2.1). This is the sequence
A094648 in Sloane’s Encyclopedia [6]. Next we extend the domain of $\{a_n\}_{n=0}^{\infty}$ to
include negative integers. For negative integer $-n$ we have
\[a_{-n} = \left(4 \cos \frac{\pi}{7} \cos \frac{2\pi}{7}\right)^n + \left(-4 \cos \frac{\pi}{7} \cos \frac{3\pi}{7}\right)^n + \left(4 \cos \frac{2\pi}{7} \cos \frac{3\pi}{7}\right)^n.
\]
Note that $\{a_n\}_{n=-\infty}^{\infty}$ is an integer sequence, so we can consider this sequence as
a sequence in $F_p$. Here we investigate the relation between this sequence in $F_p$ and
permutation properties of binomial $P(x) = x^r(1 + x^s)$ over a finite field $F_q = F_{p^m}$.
We have the following theorem.

**Theorem 1.1.** Let $q - 1 = 7s$ and $1 \leq e \leq 6$. Then $P(x) = x^r(1 + x^s)$ is a
permutation binomial of $F_q$ if and only if $(r, s) = 1$, $2^* \equiv 1 \pmod{p}$, $2r + es \neq
0 \pmod{7}$ and $\{a_n\}$ satisfies one of the following:
(a) $a_s = a_{-s} = 3$ in $F_p$;
(b) $a_{-cs-1} = -1 + \alpha$, $a_{-cs} = -1 - \alpha$ and $a_{-cs+1} = 1$ in $F_p$, where $\alpha$ is the inverse
of $s + 2\alpha \cos \frac{\pi}{7}$ modulo 7 and $\alpha^2 + \alpha + 2 = 0$ in $F_p$.

The sequence $\{a_n\}$ is called $s$-periodic over $F_p$ if $a_n = a_{n+ks}$ in $F_p$ for integers $k$
and $n$. Condition (a) in the above theorem is equivalent to $s$-periodicity of $a_n$ over
$F_p$ (see Lemma 2.4). Equivalently we can say $\{a_n\}$ is $s$-periodic over $F_p$ whenever
$\{a_n\} = \{a_n^0\}$ in $F_p$, where $\{a_n^0\}_{n=-\infty}^{\infty}$ is the unique sequence in $F_p$
defined by the recursion (2) and initial values $a_{-1}^0 = 2$, $a_0^0 = 3$ and $a_{1}^0 = 1$. Similarly condition
(b) can be written as $\{a_n\} = \{a_n^{c, \alpha}\}$ in $F_p$, where $\{a_n^{c, \alpha}\}_{n=-\infty}^{\infty}$ is the unique sequence in $F_p$
defined by the recursion (2) and initial values $a_{-cs-1} = -1 + \alpha$, $a_{-cs} = -1 - \alpha$
and $a_{-cs+1} = 1$. So Theorem 1.1 states that under certain conditions on $r, s = \frac{q-1}{7}$
and $e$ the binomial $P(x) = x^r(1 + x^s)$ is a permutation binomial of $F_p$ if and only if the Lucas-type sequence $\{a_n\}$ is equal to $\{a_n^0\}$ or $\{a_n^{c, \alpha}\}$ in $F_p$. (For more
explanation see Examples in Section 3).

It is clear that if Legendre symbol $\left(\frac{q}{7}\right) = -1$ then condition (b) in the above
theorem is never satisfied (the equation $x^2 + x + 2 = 0$ does not have any solution
in $F_p$). Moreover in this case we can show that condition (a) is always satisfied,
and so we have the following.

**Corollary 1.2.** Let $q - 1 = 7s$, $1 \leq e \leq 6$, and $p$ be a prime with $\left(\frac{q}{7}\right) = -1$.
Then $P(x) = x^r(1 + x^s)$ is a permutation binomial of $F_q$ if and only if $(r, s) = 1$, $2^* \equiv 1 \pmod{p}$
and $2r + es \neq 0 \pmod{7}$.

Theorem 1.1 gives a complete characterization of permutation binomials of the
form $P(x) = x^r(1 + x^{\frac{q-1}{7}})$. Moreover our theorem together with the above corollary
can lead to an efficient algorithm for constructing such permutation binomials.
Note that $\{a_n\}$ is a recursive sequence and therefore conditions (a) and (b) can be
quickly verified and so by employing the above theorem it is easy to find new
permutation binomials over certain $F_q$. Also by an argument similar to the proof
of Corollary 1.3 in [1], we can show that under the conditions of Theorem 1.1 on $q$,
there are exactly $3\phi(q - 1)$ permutation binomials $P(x) = x^r(1 + x^{\frac{q-1}{7}})$ of $F_q$.
Here, $\phi$ is the Euler totient function.
Proof. Note that $2 \cos \frac{\pi t}{7}$ be used in the proof of our theorem. Theorem 1.1 and Corollary 1.2 are proved in Section 3.

2. The Sequence $\{a_n\}$

We first show that $\{a_n\}$ appears in the closed expression for the lacunary sum of binomial coefficients $S(2n, 7, a) := \sum_{k=0}^{2n} \binom{2n}{k}$. 

**Lemma 2.1.** The sequence $\{a_n\}_{n=0}^{\infty}$ satisfies the recursion $a_n = a_{n-1} + 2a_{n-2} - a_{n-3}$ ($n \geq 3$), $a_0 = 3$, $a_1 = 1$, $a_2 = 5$ and we have 

$$S(2n, 7, a) = \begin{cases} 2^{2n} - 2^{2n+1} & \text{if } 2n - 2a \equiv 0 \pmod{7}; \\ 2^{2n} + 2a_{n-1} & \text{if } 2n - 2a \equiv 1, 6 \pmod{7}; \\ 2^{2n} - a_{n-1} & \text{if } 2n - 2a \equiv 2, 5 \pmod{7}; \\ 2^{2n} - a_{n+1} + a_{n-1} & \text{if } 2n - 2a \equiv 3, 4 \pmod{7}. \end{cases}$$

**Proof.** Note that $2 \cos \frac{\pi}{7}$, $-2 \cos \frac{2\pi}{7}$ and $2 \cos \frac{3\pi}{7}$ are the roots of the polynomial $g(x) = x^3 - x^2 - 2x + 1$, so $a_n$ satisfies the given recursion. 

We know that 

$$S(2n, 7, a) = \frac{2^{2n}}{7} + \frac{2}{7} \sum_{t=1}^{3} \left( 2 \cos \frac{\pi t}{7} \right) \frac{2^n}{7} \cos \frac{\pi t}{7} (2n - 2a),$$

(see [7], page 232, Lemma 1.3). This together with (1) and (2) imply the result. □

Next we have a general formula for the product $a_n a_m$.

**Lemma 2.2.** Let $m$ and $n$ be integers and $m \leq n$. Then 

$$a_n a_m = a_{m+n} + (-1)^m (a_{m} a_{n-m} - a_{n-2m}).$$

In particular, 

$$a_n^2 = a_{2n} + (-1)^n 2a_{n}.$$

**Proof.** Let $\delta = 2 \cos \frac{\pi}{7}$, $\eta = -2 \cos \frac{2\pi}{7}$, and $\epsilon = 2 \cos \frac{3\pi}{7}$. We have $a_n = \delta^n + \eta^n + \epsilon^n$ and $a_{-n} = (-\delta \eta)^n + (-\delta \epsilon)^n + (-\eta \epsilon)^n$. Considering these, a routine calculation implies the result. □

In the next two lemmas, we study the periodicity of $\{a_n\}$ over $\mathbb{F}_p$.

**Lemma 2.3.** Let $p \neq 2, 7$ be a prime. Then the sequence $\{a_n\}_{n=-\infty}^{\infty}$ is $7s$-periodic over $\mathbb{F}_p$.

**Proof.** We know that $g(x) = x^3 - x^2 - 2x + 1$ is the characteristic polynomial of the recursion associated to $a_n$. Let $\delta$, $\eta$ and $\epsilon$ be the roots of $g(x)$ in a splitting field $F$ of $g(x)$ over $\mathbb{F}_p$. Since $p \neq 2, 7$, we know that $a_n$ is $7s$-periodic in $\mathbb{F}_p$ if and only if $\delta^7 = \eta^7 = \epsilon^7 = 1$ in $F$.

We can show that $g(x)$ is either irreducible in $\mathbb{F}_p[x]$ or it splits in $\mathbb{F}_p[x]$. Now if $g(x)$ splits over $\mathbb{F}_p$, then $\delta^p - 1 = \eta^p - 1 = \epsilon^p - 1 = 1$ in $\mathbb{F}_p$ and therefore $a_n$ has period $7s = q - 1$. If $p = 7k + 1$ or 6, by Theorem 7 of [5], $g(x)$ splits over $\mathbb{F}_p$. If $p = 7k + 2$, 3, 4 or 5 and $g(x)$ is irreducible over $\mathbb{F}_p$, then, by Theorems 8.27 and 8.29 of [2], $a_n$ is periodic in $\mathbb{F}_p$ with the least period dividing $p^i - 1$. Also since
We continue by describing a necessary and sufficient condition under which the sequence \( \{a_n\}_{n=-\infty}^{\infty} \) will be a periodic sequence in \( \mathbb{F}_p \) with the even period \( s \).

**Lemma 2.4.** Let \( p \neq 2, 7 \) be a prime and \( s \) be a fixed even positive integer. Then \( \{a_n\} \) is \( s \)-periodic over \( \mathbb{F}_p \) if and only if \( a_s = a_{-s} = 3 \) in \( \mathbb{F}_p \).

**Proof.** With the notation in the proof of Lemma 2.3, we know that \( \{a_n\}_{n=-\infty}^{\infty} \) is \( s \)-periodic if and only if \( \text{diag}(\delta, \eta, \epsilon)^s = I \) in \( \mathbb{F} \). Here \( \text{diag}(\delta, \eta, \epsilon) \) is a diagonal matrix with entries \( \delta, \eta \) and \( \epsilon \) and \( I \) is the identity matrix. We know that a diagonal matrix is equal to the identity matrix if and only if \( (x-1)^3 \) is the characteristic polynomial of the diagonal matrix. By employing this fact, together with the identities \( a_n = \delta^n + \eta^n + \epsilon^n \) and \( a_{-n} = (-\delta \eta \epsilon)^n + (-\delta \eta )^n + (-\eta \epsilon)^n \) in \( \mathbb{F} \), we have

\[
\text{diag}(\delta, \eta, \epsilon)^s = I \text{ in } \mathbb{F} \iff a_s = a_{-s} = 3 \text{ in } \mathbb{F}_p.
\]

The following two lemmas play important roles in the proof of Theorem 1.1.

**Lemma 2.5.** Let \( p \neq 2, 7 \) be a prime, \( s = \frac{2^{c-1}}{7} \), and \( c \) (\( 1 \leq c \leq 6 \)) be a fixed integer. If the sequence \( \{a_n\}_{n=-\infty}^{\infty} \) satisfies \( a_{cs+1} = a_{2cs+1} = a_{3cs+1} = a_{4cs+1} = a_{5cs+1} = a_{6cs+1} = 1 \) in \( \mathbb{F}_p \), then

\[
a_{cs} = a_{2cs} = a_{4cs}, \text{ and } a_{3cs} = a_{5cs} = a_{6cs}
\]

in \( \mathbb{F}_p \).

**Proof.** From the recurrence relation of \( a_n \) we get

\[
a_{2cs+1} - a_{2cs+2} = 2a_{2cs} - a_{2cs+2}.
\]

So by the conditions of the lemma we have

(A) \( a_{2cs+1} = 1 \);
(B) \( (2a_{2cs} - a_{2cs+2})^2 = 1 \);
(C) \( (a_{4cs} - a_{4cs-1})^2 = 1 \).

We employ Lemmas 2.2 and 2.3 to deduce new identities from (A), (B) and (C).

For simplicity of our exposition we let \( a_{-(cs+1)} = \gamma \).

First of all (A) together with Lemma 2.2 imply

\[
a_{2cs+2} = 1 + 2\gamma.
\]

From (3) and \( 2a_{2cs} - a_{2cs+2} = 1 \), we have

\[
a_{2cs} = 1 + \gamma.
\]

Next from (B), (3), (4), Lemma 2.2 and \( a_{cs+1} = 1 \), we get

\[
1 = (2a_{2cs} - a_{2cs+2})^2
= 4a_{2cs}^2 - 4a_{2cs}a_{2cs+2} + a_{2cs+2}^2
= -4(1 + \gamma)^2 + a_{2cs+2}^2
= -4(1 + \gamma)^2 + a_{4cs+4} + 2a_{-(2cs+2)}
= -4(1 + \gamma)^2 + a_{4cs+4} + 2(\gamma^2 + 2).
\]

This implies

\[
a_{4cs+4} = 2(1 + \gamma)^2 - 5 = 2a_{2cs}^2 - 5.
\]

Note that \( a_{4cs} - a_{4cs-1} = 1 \) and the recurrence relation (2) imply

\[
a_{4cs+2} = a_{4cs+1} + a_{4cs} + 1,
\]

\[
a_{4cs+2} = a_{4cs+1} + a_{4cs} + 1,
\]
ON SOME PERMUTATION POLYNOMIALS OVER FINITE FIELDS

and

(7) \[ a_{4cs+3} = 3a_{4cs+1} + 1. \]

Now applying the recurrence relation \( a_{4cs+4} = a_{4cs+3} + 2a_{4cs+2} - a_{4cs+1} \) together with (6) and (7) to the left-hand side of (5) and applying Lemmas 2.2 and 2.3 to the right-hand side of (5) yield

(8) \[ a_{4cs+1} = a_{5cs} - 2. \]

Finally from (C) we have

\[ a_{4cs}^2 - 2a_{4cs}a_{4cs-1} + a_{4cs-1}^2 = 1. \]

Applying Lemma 2.2 and Lemma 2.3 on this equality yields

\[ a_{cs} + 2a_{3cs} - 2a_{cs-1} - 2a_{3cs+2} + a_{cs-2} = 1. \]

Now by employing the recurrence relation \( a_{cs+1} = a_{cs} + 2a_{cs-1} - a_{cs-2} \) in the previous identity and \( a_{cs+1} = 1 \), we obtain

(9) \[ a_{cs} = a_{3cs+2} - a_{3cs} + 1. \]

Since \( a_{3cs} - a_{3cs-1} = 1 \), from the recurrence relation (2) we have

\[ a_{3cs+2} = a_{3cs+1} + a_{3cs} + 1. \]

Applying this identity in (9) yields

(10) \[ a_{cs} = a_{3cs+1} + 2. \]

Now we are ready to finish the proof. Note that by changing \( s \) to \(-s\) all the above equations remain true, so by changing \( s \) to \(-s\) in (8) and applying Lemma 2.3 we have

\[ a_{3cs+1} = a_{2cs} - 2. \]

This together with (10) imply \( a_{cs} = a_{2cs} \). Changing \( s \) to \(-s\) in this equality yields \( a_{6cs} = a_{5cs} \). These identities together with Lemma 2.2 and Lemma 2.3 imply that

\[ a_{cs} = a_{2cs} = a_{4cs}, \quad a_{3cs} = a_{5cs} = a_{6cs}. \]

Lemma 2.6. Let \( p \neq 2, 7 \) be a prime, \( s = \frac{q-1}{2} \) and \( c (1 \leq c \leq 6) \) be a fixed integer. If the sequence \( \{a_n\}_{n=-\infty}^{\infty} \) satisfies

\[ a_{6cs-1} = -1 + \alpha, \quad a_{6cs} = -1 - \alpha, \quad \text{and} \quad a_{6cs+1} = 1, \]

where \( \alpha \) is a root of equation \( x^2 + x + 2 = 0 \) in \( \mathbb{F}_p \), then we have \( a_{cs} = a_{2cs} = a_{4cs} = \alpha, a_{3cs} = a_{5cs} = a_{6cs} = -1 - \alpha, a_{cs-1} = -2 - \alpha, a_{cs+1} = 1, a_{5cs-1} = 1 - 2\alpha, \) and \( a_{5cs+1} = -2\alpha \) in \( \mathbb{F}_p \).

Proof. From Lemmas 2.2 and 2.3 we have the following six identities.

\[
\begin{align*}
\{a_{6cs-1}^2 & = a_{5cs-2} - 2a_{cs+1} \\
a_{6cs-1}a_{6cs} & = a_{5cs-1} - a_1a_{cs+1} + a_{cs+2} \\
a_{6cs-1}a_{6cs+1} & = a_{5cs} - a_{2a_{cs+1} + a_{cs+3}} \\
a_{6cs}^2 & = a_{5cs} + 2a_{cs} \\
a_{6cs}a_{6cs+1} & = a_{5cs+1} + a_{cs} - a_{cs+1} \\
a_{6cs+1}^2 & = a_{5cs+2} - 2a_{cs-1} 
\end{align*}
\]
Replacing the known values of the variables in the above identities, writing $a_{5c_3-2}$ and $a_{5c_3+2}$ in terms of $a_{5c_3-1}$, $a_{5c_3}$ and $a_{5c_3+1}$, and writing $a_{cs+2}$ and $a_{cs+3}$ in terms of $a_{cs-1}$, $a_{cs}$ and $a_{cs+1}$ yield

\[
\begin{pmatrix}
(-1 + \alpha)^2 &=& 2a_{5c_3-1} + a_{5c_3} - a_{5c_3+1} - 2a_{cs+1} \\
1 - \alpha^2 &=& a_{5c_3-1} - a_{cs-1} + 2a_{cs} \\
-1 + \alpha &=& a_{5c_3} - a_{cs-1} + a_{cs} - 2a_{cs+1} \\
(1 + \alpha)^2 &=& a_{5c_3} + 2a_{cs} \\
-1 - \alpha &=& a_{5c_3+1} + a_{cs} - a_{cs+1} \\
1 &=& -a_{5c_3-1} + 2a_{5c_3} + a_{5c_3+1} - 2a_{cs-1}
\end{pmatrix}
\]

Solving this system of linear equations and noting that $\alpha^2 + \alpha + 2 = 0$ imply the desired values for $a_{cs-1}$, $a_{cs}$, $a_{cs+1}$, $a_{5c_3-1}$, $a_{5c_3}$ and $a_{5c_3+1}$. By setting up two similar systems of linear equations one can derive the desired values for $a_{2cs}$, $a_{3cs}$ and $a_{4cs}$.

3. Permutation Binomials and the Sequence \( \{a_n\} \)

The main tool in the proof of Theorem 1.1 is the following well known theorem of Hermite ([2], Theorem 7.4).

**Hermite’s Criterion** \( P(x) \) is a permutation polynomial of \( \mathbb{F}_q \) if and only if

(i) \( P(x) \) has exactly one root in \( \mathbb{F}_q \).

(ii) For each integer \( t \) with \( 1 \leq t \leq q-2 \) and \( t \not\equiv 0 \pmod{p} \), the reduction of \( [P(x)]^t \) \( \pmod{x^q - x} \) has degree less than or equal to \( q-2 \).

Finally we are ready to prove the main result of this paper.

**Proof of Theorem 1.1.** First we assume that \( P(x) \) is a permutation binomial. Then \( p \neq 2 \), since otherwise \( P(0) = P(1) = 0 \). Also, in this case, it is known that \( (r, s) = 1 \) ([8], Theorem 1.2) and \( 2^s \equiv 1 \pmod{p} \) ([4], Theorem 4.7). Next we note that the coefficient of \( x^{q-1} \) in the expansion of \( [P(x)]^{ks} \) is \( S(ks, 7, -ke^5r) \), so if \( P(x) \) is a permutation binomial then by Hermite’s Criterion \( S(ks, 7, -ke^5r) = 0 \) in \( \mathbb{F}_p \) for \( k = 1, \ldots, 6 \).

We next show that \( 2r + es \not\equiv 0 \pmod{7} \). Otherwise, \( 2r + es \equiv 0 \pmod{7} \) and Lemma 2.1 follows that

\[
S(ks, 7, -ke^5r) = \frac{2^{ks} + 2ak_s}{7}, \quad \text{in } \mathbb{F}_p
\]

for \( k = 1, \ldots, 6 \). From here if \( P(x) \) is a permutation binomial, we have

\[
a_s = a_{2s} = \cdots = a_{6s} = -\frac{1}{2} \text{ in } \mathbb{F}_p.
\]

Using Lemma 2.3 and Lemma 2.2, we have \( \frac{1}{2} = a_s^2 = a_{2s} + 2a_{6s} = 3a_s = -\frac{3}{2} \). Hence \( \frac{1}{2} (\frac{1}{2} + 3) = 0 \) in \( \mathbb{F}_p \) which is a contradiction since \( 7 \mid (q-1) \). Hence \( 2r + es \not\equiv 0 \pmod{7} \).

It remains to show that if \( P(x) \) is a permutation binomial then either (a) or (b) holds. Let \( c \) be the inverse of \( s + 2e^5r \) modulo 7. Hermite’s criterion together with Lemma 2.1 imply that

\[
\begin{align*}
a_{cs+1} &= 1, \quad a_{2cs-1} - a_{2cs+1} = 1, \quad a_{3cs} - a_{3cs-1} = 1, \\
a_{4cs} - a_{4cs-1} &= 1, \quad a_{5cs-1} - a_{5cs+1} = 1, \quad a_{6cs+1} = 1,
\end{align*}
\]
in \( \mathbb{F}_p \). So by Lemma 2.5, we have

\[(11) \quad a_{cs} = a_{2cs} = a_{4cs} = \alpha, \ a_{3cs} = a_{5cs} = a_{6cs} = \beta, \]

in \( \mathbb{F}_p \). From Lemma 2.2 and Lemma 2.3, we have

\[(12) \quad a^2_{cs} = a_{2cs} + 2a_{6cs} \text{ and } a^2_{6cs} = a_{5cs} + 2a_{cs}. \]

By subtracting these two equations and employing (11), we get

\[(13) \quad (a_{cs} - a_{6cs})(a_{cs} + a_{6cs} + 1) = 0 \quad \text{in } \mathbb{F}_p. \]

If \( \alpha = \beta \) in \( \mathbb{F}_p \), then by Lemma 2.2 and (11) we have \( a_{7cs} = a_{cs}a_{6cs} - a_{6cs}a_{5cs} + a_{4cs} = a_{4cs} \). Since by Lemma 2.3 \( a_{7cs} = 0 \) in \( \mathbb{F}_p \), we have \( a_{4cs} = 3 \) in \( \mathbb{F}_p \). This together with (11) and \( a_{cs} = a_{6cs} \) implies condition (a).

If \( \alpha \neq \beta \), then from (13) we have \( a_{cs} + a_{6cs} + 1 = 0 \). This together with (12) imply that \( \alpha \) and \( \beta \) are roots of the equation \( x^2 + x + 2 = 0 \) in \( \mathbb{F}_p \) and therefore \( \beta = -1 - \alpha \).

From Lemma 2.2 we have

\[ a_{cs}a_{cs+1} = a_{2cs+1} + a_{6cs-a1} - a_{6cs+1}. \]

This together with \( a_{cs} = \alpha \), \( a_{6cs} = -1 - \alpha \), and \( a_{cs+1} = a_{6cs+1} = 1 \) imply that \( a_{2cs+1} = 2\alpha + 2 \). Note that \( a_{2cs-1} = 1 + a_{2cs+1} \), and so \( a_{2cs-1} = 2\alpha + 3 \) and thus \( a_{2cs+2} = a_{2cs+1} + 2a_{2cs} - a_{2cs-1} = 2\alpha - 1 \). Finally by Lemma 2.2 we have \( a^2_{cs+1} = a_{2cs+2} - 2a_{6cs-1} \) which implies \( a_{6cs-1} = \alpha - 1 \). Hence, in this case, \( a_n \) satisfies condition (b).

Conversely we assume that the conditions in Theorem 1.1 are satisfied and we show that \( P(x) \) is a permutation binomial. First note that \( 2^r \equiv 1 \pmod{p} \) follows that \( p \) is odd. Hence it is obvious that \( P(x) \) has only one root in \( \mathbb{F}_q \). Since \( (r, s) = 1 \), the possible coefficient of \( x^{q-1} \) in the expansion of \( [P(x)]^t \) can only happen if \( t = ks \) for some \( k \in 1, \ldots, 6 \). So by Hermite’s criterion, it is sufficient to show that \( S(ks, 7, -ke^5r) = 0 \) in \( \mathbb{F}_p \) for \( k = 1, \ldots, 6 \).

Now if \( a_n \) satisfies condition (a), then by Lemma 2.4 \( a_n \) is \( s \)-periodic over \( \mathbb{F}_p \). Using the initial values of \( a_n \), \( 2r + cs \not\equiv 0 \pmod{7} \) and Lemma 2.1, we have \( S(ks, 7, -ke^5r) = 0 \) in \( \mathbb{F}_p \) and thus \( P(x) \) is a permutation binomial over \( \mathbb{F}_q \).

Next we assume that \( a_n \) satisfies condition (b). Then by Lemma 2.6, we also have

\[ a_{cs} = a_{2cs} = a_{4cs} = \alpha, \ a_{3cs} = a_{5cs} = a_{6cs} = -1 - \alpha, \]
\[ a_{cs-1} = -2 - \alpha, \ a_{cs+1} = 1, \ a_{5cs-1} = 1 - 2\alpha, \text{ and } a_{5cs+1} = -2\alpha. \]

By using \( 2^s = 1, \ a_{cs+1} = a_{6cs+1} = 1, \) and Lemma 2.1, we have
\[ S(ks, 7, -ke^5r) = 0 \text{ for } k = 1, \ldots, 6. \]

To demonstrate \( S(ks, 7, -ke^5r) = 0 \) for other \( k \)'s, it is sufficient to show that
\[ a_{2cs-1} - a_{2cs+1} = 1, \ a_{4cs} - a_{3cs-1} = 1, \]
\[ a_{4cs} - a_{4cs-1} = 1, \ a_{5cs-1} - a_{5cs+1} = 1. \]

From the values for \( a_{5cs-1} \) and \( a_{5cs+1} \) it is clear that \( a_{5cs-1} - a_{5cs+1} = 1 \). Next note that by considering appropriate systems of linear equations as described in the proof of Lemma 2.6 we can deduce that
\[ a_{2cs-1} = 2\alpha + 3, \ a_{2cs+1} = 2\alpha + 2, \ a_{3cs-1} = -\alpha - 2, \text{ and } a_{4cs-1} = \alpha - 1. \]
So \(a_{2k^3-1} - a_{2k^3+1} = a_{3k^3} - a_{2k^3-1} = a_{4k^3} - a_{4k^3-1} = 1\). These relations show that \(S(k, s, 7, -ke^3r) = 0\) in \(F_p\) for \(k = 1, \ldots, 6\). Hence \(P(x)\) is a permutation binomial of \(F_q\). □

Next we prove that if \((\frac{q}{r}) = -1\) then the sequence \(a_n\) is always \(s\)-periodic. That is, \(a_s = a_{-s} = 3\).

**Proof of Corollary 1.2.** Following the notation in the proof of Lemma 2.3, let \(\epsilon\) be a root of \(g(x) = x^s - x^2 - 2x + 1\) in an extension of \(F_p\). We need to prove that \(\epsilon^s = 1\). If \(p \equiv 6 \pmod{7}\) then by Theorem 7 of [5] we have \(\epsilon \in F_p\). Since \((p - 1, 7) = 1\), in this case \(\epsilon\) is a 7-th power in \(F_p\), and therefore \(\epsilon^s = 1\) in \(F_p\). To prove the result for \(p \equiv 3\) or \(5 \pmod{7}\), first of all note that \(g(x)\) is either irreducible in \(F_p[x]\) or it splits in \(F_p[x]\). If it splits over \(F_p\), then \(\epsilon\) is a 7-th power in \(F_p\) and so \(\epsilon^s = 1\) in \(F_p\). Otherwise \(g(x)\) splits over \(F_p^3\). Now since \(p \not\equiv 1, 2 \pmod{7}\) we have \((p^3 - 1, 7) = 1\), so \(\epsilon\) is a 7-th power in \(F_{p^3}\) and therefore \(\epsilon^s = 1\) in \(F_{p^3}\). Also since \(7 \mid (q - 1)\) we have \(6 \mid m\). This and \(\epsilon^s = 1\) in \(F_{p^3}\) imply that \(\epsilon^s = 1\) in \(F_p\). Hence \(\{a_n\}\) is \(s\)-periodic and so by Lemma 2.4, \(a_s = a_{-s} = 3\). Now Theorem 1.1 implies the result. □

**Examples** An algorithm for finding permutation binomials \(P(x) = x^r(1 + x^s)^{\alpha}\) of a given field \(F_q\) can be easily implemented by using Theorem 1.1 and Corollary 1.2. Moreover our theorem together with Lemma 2.4 and Lemma 2.6 imply that under certain conditions on \(r, s\) and \(\epsilon\) the binomial \(x^r(1 + x^s)^{\alpha}\) is a permutation polynomial over \(F_q\) if and only if the Lucas-type sequence \(\{a_n\}\) becomes one of the following four sequences over \(F_p\).

(I) \(a_{-s} = 2, a_{-s} = 3, a_{-s+1} = 1, a_{s-1} = 2, a_s = 3, a_{s+1} = 1\).

(II) \(a_{-s} = -1 + \alpha, a_{-s} = -1 - \alpha, a_{-s+1} = 1, a_{s-1} = -2 - \alpha, a_s = -2 + \alpha, a_{s+1} = 1\).

(III) \(a_{-s} = -1 + \alpha, a_{-s} = -1 - \alpha, a_{-s+1} = 1, a_{s-1} = -2 - \alpha, a_{s+1} = 1\).

(IV) \(a_{-s} = -1 + \alpha, a_{-s} = -1 - \alpha, a_{-s+1} = 1, a_{s-1} = -2 - \alpha, a_{s+1} = 1\).

Note that the sequence (I) is \(s\)-periodic and in (II), (III) and (IV), \(\alpha\) is a root of equation \(x^2 + x + 2 = 0\) in \(F_p\).

The following table gives some prime numbers \(p\) with \(p \equiv 1 \pmod{7}\) and \(2^{\frac{p-1}{2}} \equiv 1 \pmod{p}\) whose corresponding sequence \(\{a_n\}\) over \(F_p\) is in the form (I) ((II), (III), (IV), respectively).

<table>
<thead>
<tr>
<th>Type IV</th>
<th>Type III</th>
<th>Type II</th>
<th>Type I</th>
</tr>
</thead>
<tbody>
<tr>
<td>2731</td>
<td>4999</td>
<td>7309</td>
<td>874651</td>
</tr>
<tr>
<td>3389</td>
<td>18439</td>
<td>20063</td>
<td>941879</td>
</tr>
<tr>
<td>15583</td>
<td>20441</td>
<td>33587</td>
<td>1018879</td>
</tr>
<tr>
<td>62791</td>
<td>33503</td>
<td>37199</td>
<td>1036267</td>
</tr>
<tr>
<td>65899</td>
<td>55609</td>
<td>37339</td>
<td>1074277</td>
</tr>
</tbody>
</table>

Here \(p = 2731\) (4999, 7309, 874651 respectively) is the smallest prime \(p \equiv 1 \pmod{7}\) with \(2^{\frac{p-1}{2}} \equiv 1 \pmod{p}\) whose corresponding sequence \(\{a_n\}\) over \(F_p\) is in the form (IV) ((III), (II), (I), respectively). The following table gives examples of such permutation binomials over these four fields.
On some permutation polynomials over finite fields

\[ p = 2731 \]
\[ a_n = \begin{cases} 1001 & n = 3x - 1 \\ 760 & n = 2x - 1 \\ 3858 & n = x - 1 \\ 3 & n = x - 1 \end{cases} \]
\[ p = 4999 \]
\[ a_n = \begin{cases} 4237 & n = 2x - 1 \\ 3449 & n = x - 1 \\ 761 & n = x - 1 \end{cases} \]
\[ p = 7309 \]
\[ a_n = \begin{cases} 1727 & n = 3x - 1 \\ 4236 & n = x - 1 \\ 3448 & n = x - 1 \end{cases} \]
\[ p = 874651 \]
\[ a_n = \begin{cases} 1002 & n = 3x - 1 \\ 761 & n = x - 1 \\ 3859 & n = x - 1 \end{cases} \]

\[ (r, e, s) = (7, 1, 390) \]
\[ (23, 1, 390) \]
\[ (37, 1, 390) \]
\[ (49, 1, 390) \]
\[ (77, 1, 390) \]

\[ (7, 1, 1044) \]
\[ (19, 1, 1044) \]
\[ (23, 1, 1044) \]
\[ (41, 1, 1044) \]
\[ (49, 1, 1044) \]

\[ (1, 1, 124950) \]
\[ (11, 1, 124950) \]
\[ (13, 1, 124950) \]
\[ (19, 1, 124950) \]
\[ (23, 1, 124950) \]

\[ (1, 1, 124950) \]
\[ (11, 1, 124950) \]
\[ (13, 1, 124950) \]
\[ (19, 1, 124950) \]
\[ (23, 1, 124950) \]

References


[7] Z. H. Sun, The combinatorial sum \[ \sum_{k=0, k \equiv r \pmod{m}} (n \choose k) \] and its applications in number theory I (Chinese), Nanjing Daxue Xuebao Shuxue Bannian Kan 9 (1992), no. 2, 227–240.


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

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