ON SOME PERMUTATION POLYNOMIALS OVER FINITE FIELDS

AMIR AKBARY AND QIANG WANG

Received 8 March 2005 and in revised form 5 May 2005

Let p be prime, $q = p^m$, and $q - 1 = 7s$. We completely describe the permutation behavior of the binomial $P(x) = x^r(1 + x^{es})$ $(1 \le e \le 6)$ over a finite field $\mathbb{F}_q$ in terms of the sequence $\{a_n\}$ defined by the recurrence relation $a_n = a_{n-1} + 2a_{n-2} - a_{n-3}$ $(n \ge 3)$ 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 [3, Chapter 7] for a survey of some known classes). An important class of permutation polynomials consists of permutation polynomials of the form $P(x) = x^r f(x^{(q-1)/l})$, 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 $g(x) \in \mathbb{F}_q[x]$ [3, 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 (e.g., [2, 9] and [1]).

Here we consider the binomial $P(x) = x^r + x^u$ with $r < u$. Let $s = (u - r, q - 1)$ and $l = (q - 1)/s$. Then we can rewrite $P(x)$ as $P(x) = x^r(1 + x^{es})$, where $s = (q - 1)/l$ 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 Wang [9]. In the case $l = 5$, the permutation binomial $P(x)$ is determined in terms of the Lucas sequence $\{L_n\}$, where

$$L_n = \left(2\cos\frac{\pi}{5}\right)^n + \left(-2\cos\frac{2\pi}{5}\right)^n. \tag{1.1}$$

More precisely, it is proved that under certain conditions on r, $s = (q - 1)/5$, 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].

International Journal of Mathematics and Mathematical Sciences 2005:16 (2005) 2631–2640
DOI: 10.1155/IJMMS.2005.2631

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

$$a_n = \left(2\cos\frac{\pi}{7}\right)^n + \left(-2\cos\frac{2\pi}{7}\right)^n + \left(2\cos\frac{3\pi}{7}\right)^n \tag{1.2}$$

for integer $n \geq 0$. It turns out that $\{a_n\}_{n=0}^{\infty}$ is an integer sequence satisfying the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2} - a_{n-3} \tag{1.3}$$

with initial values $a_0 = 3$, $a_1 = 1$, and $a_2 = 5$ (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

$$a_{-n} = \left(4\cos\frac{\pi}{7}\cos\frac{2\pi}{7}\right)^n + \left(-4\cos\frac{\pi}{7}\cos\frac{3\pi}{7}\right)^n + \left(4\cos\frac{2\pi}{7}\cos\frac{3\pi}{7}\right)^n. \tag{1.4}$$

Note that $\{a_n\}_{n=-\infty}^{\infty}$ is an integer sequence, so we can consider this sequence as a sequence in $\mathbb{F}_p$. Here we investigate the relation between this sequence in $\mathbb{F}_p$ and permutation properties of binomial $P(x) = x^r(1 + x^{es})$ over a finite field $\mathbb{F}_q = \mathbb{F}_{p^m}$. We have the following Theorem.

Theorem 1.1. *Let $q - 1 = 7s$ and $1 \leq e \leq 6$. Then $P(x) = x^r(1 + x^{es})$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(r,s) = 1$, $2^s \equiv 1 \pmod{p}$, $2r + es \not\equiv 0 \pmod{7}$, and $\{a_n\}$ satisfies one of the following:*

(a) *$a_s = a_{-s} = 3$ in $\mathbb{F}_p$;*

(b) *$a_{-cs-1} = -1 + \alpha$, $a_{-cs} = -1 - \alpha$, and $a_{-cs+1} = 1$ in $\mathbb{F}_p$, where c is the inverse of $s + 2e^5 r$ modulo 7 and $\alpha^2 + \alpha + 2 = 0$ in $\mathbb{F}_p$.*

The sequence $\{a_n\}$ is called *s-periodic* over $\mathbb{F}_p$ if $a_n = a_{n+ks}$ in $\mathbb{F}_p$ for integers k and n. Condition (a) in the above theorem is equivalent to s-periodicity of a_n over $\mathbb{F}_p$ (see Lemma 2.4). Equivalently we can say $\{a_n\}$ is s-periodic over $\mathbb{F}_p$ whenever $\{a_n\} = \{a_n^0\}$ in $\mathbb{F}_p$, where $\{a_n^0\}_{n=-\infty}^{\infty}$ is the unique sequence in $\mathbb{F}_p$ defined by the recursion (1.3) and initial values $a_{s-1}^0 = 2$, $a_s^0 = 3$, and $a_{s+1}^0 = 1$. Similarly condition (b) can be written as $\{a_n\} = \{a_n^{c,\alpha}\}$ in $\mathbb{F}_p$, where $\{a_n^{c,\alpha}\}_{n=-\infty}^{\infty}$ is the unique sequence in $\mathbb{F}_p$ defined by the recursion (1.3) 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, $s = (q-1)/7$, and e the binomial $P(x) = x^r(1 + x^{es})$ is a permutation binomial of $\mathbb{F}_p$ if and only if the Lucas-type sequence $\{a_n\}$ is equal to $\{a_n^0\}$ or $\{a_n^{c,\alpha}\}$ in $\mathbb{F}_p$ (for more explanation, see Example 3.2).

It is clear that if the Legendre symbol $(\frac{p}{7}) = -1$, then condition (b) in the above theorem is never satisfied (the equation $x^2 + x + 2 = 0$ does not have any solution in $\mathbb{F}_p$). 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 let p be a prime with $(\frac{p}{7}) = -1$. Then $P(x) = x^r(1 + x^{es})$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(r,s) = 1$, $2^s \equiv 1 \pmod{p}$, and $2r + es \not\equiv 0 \pmod{7}$.*

Theorem 1.1 gives a complete characterization of permutation binomials of the form $P(x) = x^r(1+x^{e(q-1)/7})$. 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 $\mathbb{F}_q$. Also by an argument similar to the proof of [1, Corollary 1.3], we can show that under the conditions of Theorem 1.1 on q, there are exactly $3\phi(q-1)$ permutation binomials $P(x) = x^r(1+x^{e(q-1)/7})$ of $\mathbb{F}_q$. Here, ϕ is the Euler totient function.

In the next section, we study certain properties of the sequence $\{a_n\}$ that will 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

$$S(2n,7,a) := \sum_{\substack{k=0 \\ k\equiv a \,(\mathrm{mod}\,7)}}^{2n} \binom{2n}{k}. \tag{2.1}$$

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*

$$S(2n,7,a) = \begin{cases} \dfrac{2^{2n}+2a_{2n}}{7} & \text{if } 2n-2a \equiv 0 \,(\mathrm{mod}\,7), \\ \dfrac{2^{2n}-a_{2n+1}}{7} & \text{if } 2n-2a \equiv 1,6 \,(\mathrm{mod}\,7), \\ \dfrac{2^{2n}+a_{2n+1}-a_{2n-1}}{7} & \text{if } 2n-2a \equiv 2,5 \,(\mathrm{mod}\,7), \\ \dfrac{2^{2n}-a_{2n}+a_{2n-1}}{7} & \text{if } 2n-2a \equiv 3,4 \,(\mathrm{mod}\,7). \end{cases} \tag{2.2}$$

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

We know that

$$S(2n,7,a) = \frac{2^{2n}}{7} + \frac{2}{7}\left[\sum_{t=1}^{3}\left(2\cos\frac{\pi t}{7}\right)^{2n}\cos\frac{\pi t}{7}(2n-2a)\right], \tag{2.3}$$

(see [7, page 232, Lemma 1.3]). This together with (1.2) and (1.3) implies 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*

$$a_n a_m = a_{m+n} + (-1)^m (a_{-m} a_{n-m} - a_{n-2m}). \tag{2.4}$$

In particular,

$$a_n^2 = a_{2n} + (-1)^n 2a_{-n}. \tag{2.5}$$

Proof. Let $\delta = 2\cos(\pi/7)$, $\eta = -2\cos(2\pi/7)$, and $\epsilon = 2\cos(3\pi/7)$. 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 δ, η, and ϵ 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 $\delta^{7s} = \eta^{7s} = \epsilon^{7s} = 1$ 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 [5, Theorem 7], $g(x)$ splits over $\mathbb{F}_p$. If $p = 7k + 2, 3, 4$, or 5 and $g(x)$ is irreducible over $\mathbb{F}_p$, then, by [3, Theorems 8.27 and 8.29], a_n is periodic in $\mathbb{F}_p$ with the least period dividing $p^3 - 1$. Also since $q - 1 = p^m - 1 \equiv 0 \pmod 7$, in these cases, $3|m$. Hence, a_n is periodic in $\mathbb{F}_p$ with the least period dividing $7s = q - 1$. □

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 let s be a fixed even positive integer. Then*

$$\{a_n\} \text{ is } s\text{-periodic over } \mathbb{F}_p \Longleftrightarrow a_s = a_{-s} = 3 \text{ in } \mathbb{F}_p. \tag{2.6}$$

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 $\operatorname{diag}(\delta,\eta,\epsilon)^s = I$ in F. Here $\operatorname{diag}(\delta,\eta,\epsilon)$ is a diagonal matrix with entries δ, η, and ϵ 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 $a_{-n} = (-\delta\eta)^n + (-\delta\epsilon)^n + (-\eta\epsilon)^n$ in F, we have

$$\operatorname{diag}(\delta,\eta,\epsilon)^s = I \text{ in } F \Longleftrightarrow a_s = a_{-s} = 3 \text{ in } \mathbb{F}_p. \tag{2.7}$$

□

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, $s = (q-1)/7$, and let c $(1 \le c \le 6)$ be a fixed integer. If the sequence $\{a_n\}_{n=-\infty}^{\infty}$ satisfies $a_{cs+1} = a_{2cs-1} - a_{2cs+1} = a_{3cs} - a_{3cs-1} = a_{4cs} - a_{4cs-1} = a_{5cs-1} - a_{5cs+1} = a_{6cs+1} = 1$ in $\mathbb{F}_p$, then*

$$a_{cs} = a_{2cs} = a_{4cs}, \qquad a_{3cs} = a_{5cs} = a_{6cs} \tag{2.8}$$

in $\mathbb{F}_p$.

Proof. From the recurrence relation of a_n, we get $a_{2cs-1} - a_{2cs+1} = 2a_{2cs} - a_{2cs+2}$. So, by the conditions of the lemma, we have

(A) $a_{cs+1}^2 = 1$;
(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 implies

$$a_{2cs+2} = 1 + 2\gamma. \tag{2.9}$$

From (2.9) and $2a_{2cs} - a_{2cs+2} = 1$, we have

$$a_{2cs} = 1 + \gamma. \tag{2.10}$$

Next from (B), (2.9), (2.10), Lemma 2.2, and $a_{cs+1} = 1$, we get

$$\begin{aligned} 1 &= (2a_{2cs} - a_{2cs+2})^2 \\ &= 4a_{2cs}^2 - 4a_{2cs}a_{2cs+2} + a_{2cs+2}^2 \\ &= -4(1+\gamma)\gamma + a_{2cs+2}^2 \\ &= -4(1+\gamma)\gamma + a_{4cs+4} + 2a_{-(2cs+2)} \\ &= -4(1+\gamma)\gamma + a_{4cs+4} + 2(\gamma^2 + 2). \end{aligned} \tag{2.11}$$

This implies

$$a_{4cs+4} = 2(1+\gamma)^2 - 5 = 2a_{2cs}^2 - 5. \tag{2.12}$$

Note that $a_{4cs} - a_{4cs-1} = 1$ and the recurrence relation (1.3) imply

$$a_{4cs+2} = a_{4cs+1} + a_{4cs} + 1, \tag{2.13}$$

and

$$a_{4cs+3} = 3a_{4cs+1} + 1. \tag{2.14}$$

Now applying the recurrence relation $a_{4cs+4} = a_{4cs+3} + 2a_{4cs+2} - a_{4cs+1}$ together with (2.13) and (2.14) to the left-hand side of (2.12) and applying Lemmas 2.2 and 2.3 to the right-hand side of (2.12) yield

$$a_{4cs+1} = a_{5cs} - 2. \tag{2.15}$$

Finally, from (C), we have

$$a_{4cs}^2 - 2a_{4cs}a_{4cs-1} + a_{4cs-1}^2 = 1. \tag{2.16}$$

Applying Lemmas 2.2 and 2.3 on this equality yields

$$a_{cs} + 2a_{3cs} - 2a_{cs-1} - 2a_{3cs+2} + a_{cs-2} = 1. \tag{2.17}$$

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

$$a_{cs} = a_{3cs+2} - a_{3cs} + 1. \tag{2.18}$$

Since $a_{3cs} - a_{3cs-1} = 1$, from the recurrence relation (1.3), we have

$$a_{3cs+2} = a_{3cs+1} + a_{3cs} + 1. \tag{2.19}$$

Applying this identity in (2.18) yields

$$a_{cs} = a_{3cs+1} + 2. \tag{2.20}$$

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 (2.15) and applying Lemma 2.3, we have

$$a_{3cs+1} = a_{2cs} - 2. \tag{2.21}$$

This together with (2.20) implies $a_{cs} = a_{2cs}$. Changing s to $-s$ in this equality yields $a_{6cs} = a_{5cs}$. These identities together with Lemmas 2.2 and 2.3 imply that

$$a_{cs} = a_{2cs} = a_{4cs}, \qquad a_{3cs} = a_{5cs} = a_{6cs}. \tag{2.22}$$

□

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

$$a_{6cs-1} = -1 + \alpha, \qquad a_{6cs} = -1 - \alpha, \quad a_{6cs+1} = 1, \tag{2.23}$$

where α 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:

$$\begin{aligned} a_{6cs-1}^2 &= a_{5cs-2} - 2a_{cs+1}, \\ a_{6cs-1}a_{6cs} &= a_{5cs-1} - a_1 a_{cs+1} + a_{cs+2}, \\ a_{6cs-1}a_{6cs+1} &= a_{5cs} - a_2 a_{cs+1} + a_{cs+3}, \\ a_{6cs}^2 &= a_{5cs} + 2a_{cs}, \\ a_{6cs}a_{6cs+1} &= a_{5cs+1} + a_{cs} - a_{cs+1}, \\ a_{6cs+1}^2 &= a_{5cs+2} - 2a_{cs-1}. \end{aligned} \tag{2.24}$$

Replacing the known values of the variables in the above identities, writing a_{5cs-2} and a_{5cs+2} in terms of a_{5cs-1}, a_{5cs}, and a_{5cs+1}, and writing a_{cs+2} and a_{cs+3} in terms of a_{cs-1}, a_{cs}, and a_{cs+1} yield

$$\begin{aligned} (-1+\alpha)^2 &= 2a_{5cs-1} + a_{5cs} - a_{5cs+1} - 2a_{cs+1}, \\ 1 - \alpha^2 &= a_{5cs-1} - a_{cs-1} + 2a_{cs}, \\ -1 + \alpha &= a_{5cs} - a_{cs-1} + a_{cs} - 2a_{cs+1}, \\ (1+\alpha)^2 &= a_{5cs} + 2a_{cs}, \\ -1 - \alpha &= a_{5cs+1} + a_{cs} - a_{cs+1}, \\ 1 &= -a_{5cs-1} + 2a_{5cs} + a_{5cs+1} - 2a_{cs-1}. \end{aligned} \tag{2.25}$$

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_{5cs-1}, a_{5cs}, and a_{5cs+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 [3, Theorem 7.4].

Theorem 3.1 (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 $1 \le t \le q-2$ and $t \not\equiv 0 \pmod p$, the reduction of $[P(x)]^t \bmod (x^q - x)$ 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 $k=1,\dots,6$.

We next show that $2r+es \not\equiv 0 \pmod 7$. Otherwise, $2r+es \equiv 0 \pmod 7$ and Lemma 2.1 yields that

$$S(ks,7,-ke^5r) = \frac{2^{ks}+2a_{ks}}{7} \text{ in } \mathbb{F}_p \tag{3.1}$$

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

$$a_s = a_{2s} = \cdots = a_{6s} = -\frac{1}{2} \text{ in } \mathbb{F}_p. \tag{3.2}$$

Using Lemmas 2.3 and 2.2, we have $1/4 = a_s^2 = a_{2s} + 2a_{6s} = 3a_s = -3/2$. Hence, $(1/2)((1/2)+3)=0$ 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 implies that

$$\begin{aligned} &a_{cs+1}=1, \qquad a_{2cs-1}-a_{2cs+1}=1, \qquad a_{3cs}-a_{3cs-1}=1,\\ &a_{4cs}-a_{4cs-1}=1, \qquad a_{5cs-1}-a_{5cs+1}=1, \qquad a_{6cs+1}=1, \end{aligned} \tag{3.3}$$

in $\mathbb{F}_p$. So, by Lemma 2.5, we have

$$a_{cs}=a_{2cs}=a_{4cs}=\alpha, \qquad a_{3cs}=a_{5cs}=a_{6cs}=\beta, \tag{3.4}$$

in $\mathbb{F}_p$. From Lemmas 2.2 and 2.3, we have

$$a_{cs}^2 = a_{2cs}+2a_{6cs}, \qquad a_{6cs}^2 = a_{5cs}+2a_{cs}. \tag{3.5}$$

By subtracting these two equations and employing (3.4), we get

$$(a_{cs} - a_{6cs})(a_{cs} + a_{6cs} + 1) = 0 \text{ in } \mathbb{F}_p. \tag{3.6}$$

If $\alpha = \beta$ in $\mathbb{F}_p$, then by Lemma 2.2 and (3.4) we have $a_{7cs} = a_{cs}a_{6cs} - a_{6cs}a_{5cs} + a_{4cs} = a_{4cs}$. Since by Lemma 2.3 $a_{7cs} = a_0 = 3$ in $\mathbb{F}_p$, we have $a_{4cs} = 3$ in $\mathbb{F}_p$. This together with (3.4) and $a_{cs} = a_{6cs}$ implies condition (a).

If $\alpha \neq \beta$, then from (3.6) we have $a_{cs} + a_{6cs} + 1 = 0$. This together with (3.5) implies that α and β 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

$$a_{cs}a_{cs+1} = a_{2cs+1} + a_{6cs}a_1 - a_{6cs+1}. \tag{3.7}$$

This together with $a_{cs} = \alpha$, $a_{6cs} = -1 - \alpha$, and $a_{cs+1} = a_{6cs+1} = 1$ implies 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 $a_{cs+1}^2 = a_{2cs+2} - 2a_{6cs-1}$ 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 $2^s \equiv 1 \pmod p$ 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 $k = 1,\dots,6$. So by Hermite's criterion, it is sufficient to show that $S(ks,7,-ke^5r) = 0$ in $\mathbb{F}_p$ for $k = 1,\dots,6$.

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, $2r + es \not\equiv 0 \pmod 7$, 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

$$\begin{aligned} a_{cs} = a_{2cs} = a_{4cs} = \alpha, \quad & a_{3cs} = a_{5cs} = a_{6cs} = -1 - \alpha, \\ a_{cs-1} = -2 - \alpha, \quad a_{cs+1} = 1, \quad & a_{5cs-1} = 1 - 2\alpha, \quad a_{5cs+1} = -2\alpha. \end{aligned} \tag{3.8}$$

By using $2^s = 1$, $a_{cs+1} = a_{6cs+1} = 1$, and Lemma 2.1, we have

$$S(kcs,7,-kce^5r) = 0 \quad \text{for } k = 1,6. \tag{3.9}$$

To demonstrate $S(kcs,7,-kce^5r) = 0$ for other k's, it is sufficient to show that

$$\begin{aligned} a_{2cs-1} - a_{2cs+1} = 1, \qquad & a_{3cs} - a_{3cs-1} = 1, \\ a_{4cs} - a_{4cs-1} = 1, \qquad & a_{5cs-1} - a_{5cs+1} = 1. \end{aligned} \tag{3.10}$$

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

$$a_{2cs-1} = 2\alpha + 3, \qquad a_{2cs+1} = 2\alpha + 2, \qquad a_{3cs-1} = -\alpha - 2, \qquad a_{4cs-1} = \alpha - 1. \tag{3.11}$$

Table 3.1

Type IV	Type III	Type II	Type I
2731	4999	7309	874651
3389	18439	20063	941879
15583	20441	33587	1018879
62791	33503	37199	1036267
65899	55609	37339	1074277
⋮	⋮	⋮	⋮

So $a_{2cs-1} - a_{2cs+1} = a_{3cs} - a_{3cs-1} = a_{4cs} - a_{4cs-1} = 1$. These relations show that $S(ks,7,-ke^5r) = 0$ in $\mathbb{F}_p$ for $k = 1,\dots,6$. Hence, $P(x)$ is a permutation binomial of $\mathbb{F}_q$. □

Next we prove that if $(\frac{p}{7}) = -1$ 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 ϵ be a root of $g(x) = x^3 - x^2 - 2x + 1$ in an extension of $\mathbb{F}_p$. We need to prove that $\epsilon^s = 1$. If $p \equiv 6 \pmod 7$, then by [5, Theorem 7] we have $\epsilon \in \mathbb{F}_p$. Since $(p-1,7) = 1$, in this case, ϵ is a 7th power in $\mathbb{F}_p$ and therefore $\epsilon^s = 1$ in $\mathbb{F}_p$. To prove the result for $p \equiv 3$ or $5 \pmod 7$, first of all note that $g(x)$ is either irreducible in $\mathbb{F}_p[x]$ or it splits in $\mathbb{F}_p[x]$. If it splits over $\mathbb{F}_p$, then ϵ is a 7th power in $\mathbb{F}_p$ and so $\epsilon^s = 1$ in $\mathbb{F}_p$. Otherwise, $g(x)$ splits over $\mathbb{F}_{p^3}$. Now since $p \not\equiv 1$, 2 or $4 \pmod 7$, we have $(p^3-1,7) = 1$, so ϵ is a 7th power in $\mathbb{F}_{p^3}$ and therefore $\epsilon^{(p^3-1)/7} = 1$ in $\mathbb{F}_{p^3}$. Also since $7 \mid (q-1)$, we have $6 \mid m$. This and $\epsilon^{(p^3-1)/7} = 1$ in $\mathbb{F}_{p^3}$ implies that $\epsilon^s = 1$ in $\mathbb{F}_q$. Hence, $\{a_n\}$ is s-periodic and so by Lemma 2.4, $a_s = a_{-s} = 3$. Now Theorem 1.1 implies the result. □

Example 3.2. An algorithm for finding permutation binomials $P(x) = x^r(1 + x^{e(q-1)/7})$ of a given field $\mathbb{F}_q$ can be easily implemented by using Theorem 1.1 and Corollary 1.2. Moreover, our theorem together with Lemmas 2.4 and 2.6 implies that under certain conditions on r, s, and e the binomial $x^r(1 + x^{es})$ is a permutation polynomial over $\mathbb{F}_q$ if and only if the Lucas-type sequence $\{a_n\}$ becomes one of the following four sequences over $\mathbb{F}_p$:

(I) $a_{-s-1} = 2$, $a_{-s} = 3$, $a_{-s+1} = 1$, $a_{s-1} = 2$, $a_s = 3$, and $a_{s+1} = 1$;

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

(III) $a_{-2s-1} = -1+\alpha$, $a_{-2s} = -1-\alpha$, $a_{-2s+1} = 1$, $a_{2s-1} = -2-\alpha$, $a_{2s} = \alpha$, and $a_{2s+1} = 1$;

(IV) $a_{-3s-1} = -1+\alpha$, $a_{-3s} = -1-\alpha$, $a_{-3s+1} = 1$, $a_{3s-1} = -2-\alpha$, $a_{3s} = \alpha$, and $a_{3s+1} = 1$.

Note that the sequence (I) is s-periodic and in (II), (III), and (IV), α is a root of equation $x^2 + x + 2 = 0$ in $\mathbb{F}_p$.

Table 3.1 gives some prime numbers p with $p \equiv 1 \pmod 7$ and $2^{(p-1)/7} \equiv 1 \pmod p$ whose corresponding sequence $\{a_n\}$ over $\mathbb{F}_p$ is in the form (I) (resp., (II), (III), (IV)).

Here $p = 2731$ (resp., 4999, 7309, 874651) is the smallest prime $p \equiv 1 \pmod 7$ with $2^{(p-1)/7} \equiv 1 \pmod p$ whose corresponding sequence $\{a_n\}$ over $\mathbb{F}_p$ is in the form (IV) (resp., (III), (II), (I)). Table 3.2 gives examples of such permutation binomials over these four fields.

Table 3.2

	$p = 2731$	$p = 4999$	$p = 7309$	$p = 874651$
a_n	$a_{-3s-1} = 1001$	$a_{-2s-1} = 760$	$a_{-s-1} = 3858$	$a_{-s-1} = 2$
	$a_{-3s} = 1728$	$a_{-2s} = 4237$	$a_{-s} = 3449$	$a_{-s} = 3$
	$a_{-3s+1} = 1$	$a_{-2s+1} = 1$	$a_{-s+1} = 1$	$a_{-s+1} = 1$
	$a_{3s-1} = 1727$	$a_{2s-1} = 4236$	$a_{s-1} = 3448$	$a_{s-1} = 2$
	$a_{3s} = 1002$	$a_{2s} = 761$	$a_s = 3859$	$a_s = 3$
	$a_{3s+1} = 1$	$a_{2s+1} = 1$	$a_{s+1} = 1$	$a_{s+1} = 1$
(r,e,s)	$(7,1,390)$	$(5,1,714)$	$(7,1,1044)$	$(1,1,124950)$
	$(23,1,390)$	$(19,1,714)$	$(13,1,1044)$	$(11,1,124950)$
	$(37,1,390)$	$(23,1,714)$	$(35,1,1044)$	$(13,1,124950)$
	$(49,1,390)$	$(37,1,714)$	$(41,1,1044)$	$(19,1,124950)$
	$(77,1,390)$	$(47,1,714)$	$(49,1,1044)$	$(23,1,124950)$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Acknowledgments

Research of both authors was partially supported by NSERC.

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] J. B. Lee and Y. H. Park, *Some permuting trinomials over finite fields*, Acta Math. Sci. (English Ed.) **17** (1997), no. 3, 250–254.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[4] Y. H. Park and J. B. Lee, *Permutation polynomials with exponents in an arithmetic progression*, Bull. Austral. Math. Soc. **57** (1998), no. 2, 243–252.

[5] M. O. Rayes, V. Trevisan, and P. Wang, *Factorization of Chebyshev polynomials*, http://icm.mcs.kent.edu/reports/index1998.html.

[6] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/.

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

[8] D. Q. Wan and R. Lidl, *Permutation polynomials of the form* $x^r f(x^{(q-1)/d})$ *and their group structure*, Monatsh. Math. **112** (1991), no. 2, 149–163.

[9] L. Wang, *On permutation polynomials*, Finite Fields Appl. **8** (2002), no. 3, 311–322.

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

Qiang Wang: School of Mathematics and Statistics, Carleton University, Ottawa, ON, Canada K1S 5B6
E-mail address: wang@math.carleton.ca