Indian J Pure Appl Math (2026) 57:786–797
https://doi.org/10.1007/s13226-024-00716-y

ORIGINAL RESEARCH

A certain generalized Lucas sequence and its application to the permutation binomials over finite fields

Zhilin Zhang · **Hongjian Li** · **Delu Tian**

Received: 9 January 2023 / Accepted: 4 November 2024 / Published online: 29 November 2024

Abstract In this paper, we firstly present some basic properties of the certain generalized Lucas sequence. We subsequently describe a relationship between this sequence and the corresponding lacunary sums of binomial coefficients. Due to the relationship, we finally characterize a new class of permutation binomials over finite fields.

Keywords Generalized Lucas sequence · Permutation binomials · Finite fields

Mathematics Subject Classification 05A05 · 11T06 · 05A19

1 Introduction

Let $\mathbb{F}_q$ be a finite field of order q and let $\mathbb{F}_q[x]$ be the ring of polynomials in a single indeterminate x over $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called *a permutation polynomial on* $\mathbb{F}_q$ if it induces a map $f : \alpha \mapsto f(\alpha)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$.

The study of permutation polynomials has a long history and it started with Hermite [7] for prime fields in 1863, and later Dickson [5] for finite fields. Permutation polynomials over finite fields has been widely applied in many fields, for instance, combinatorial designs [6], cryptography [19,20] as well as coding theory [12]. There are numerous literatures on this topic and we refer readers to [4,8–10,14–17,22,27] for details.

Our work is partly motivated by the following open problem:

Communicated by B. Sury.

Supported by the National Natural Science Foundation of China(No:12001204)
Supported by the National Natural Science Foundation of China(No:12171163)
Supported by the National Natural Science Foundation of China(No:11801092)

Z. Zhang
School of Statistics and Mathematics, Guangdong University of Finance and Economics, Guangzhou 510320, Guangdong, P. R. China
E-mail: 20241032@gdufe.edu.cn

H. Li
School of Mathematics and Statistics, Guangdong University of Foreign Studies, Guangzhou 510006, Guangdong, P. R. China
E-mail: lhj@gdufs.edu.cn

D. Tian (✉)
Department of Mathematics, Guangdong University of Education, Guangzhou 510640, Guangdong, P. R. China
E-mail: tiandelu@gdei.edu.cn

Problem 1.1 (Lidl-Mullen *[16]) Let $\mathbb{F}_q$ be a finite field of order q. Determine conditions on k, r, and q so that*

$$P(x) = x^k + ax^r$$

permutes $\mathbb{F}_q$ with $a \in \mathbb{F}_q$.

The simplest type of polynomials is monomial and a monomial $kx^n \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $k \neq 0$ and $(n, q-1) = 1$. In this paper, we consider the permutation binomials $f(x)$ over $\mathbb{F}_q$ with the form $x^{\mu+\nu} + ax^{\mu}$. When $5 \mid q-1$ and $a = 1$, the permutation binomial $f(x)$ was determined by Wang [23] in terms of the Lucas sequence

$$\left\{\left(2cos\frac{\pi}{5}\right)^n + \left(-2cos\frac{\pi}{5}\right)^n\right\}_{n\in\mathbb{N}}.$$

When $7 \mid q-1$ and $a = 1$, with the help of Lucas-type sequence

$$\left\{\left(2cos\frac{\pi}{7}\right)^n + \left(-2cos\frac{2\pi}{7}\right)^n + \left(2cos\frac{3\pi}{7}\right)^n\right\}_{n\in\mathbb{N}},$$

the permutation behavior of $f(x)$ was studied by Akbary and Wang [1]. We refer the reader to [2,24] for a more general case.

In this paper, we characterize a new class of permutation binomials over finite fields as follows.

Theorem 1.2 *Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) = p$ and $3 \mid q-1$. Let $f(x) = x^{\mu+\nu} + 3x^{\mu} \in \mathbb{F}_q[x]$, where μ is a positive integer and $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$. Then $f(x)$ is a permutation binomail of $\mathbb{F}_q$ if and only if*

$$(\mu, \nu) = 1,$$

$$2^{\frac{4(q-1)}{3}} \equiv 7^{\frac{q-1}{3}} \pmod{p}$$

and one of the following holds:

(i) if $\nu = \frac{q-1}{3}$, then $\mu \equiv 2 \pmod 3$;
(ii) if $\nu = \frac{2(q-1)}{3}$, then $\mu \equiv 1 \pmod 3$.

Remark 1.3 Theorem 1.2 is significant because it provides a positive solution to Problem 1.1. For the sake of discussion, it may be convenient to write the binomial $x^k + ax^r$ as $x^{\mu+\nu} + ax^{\mu}$. It should be noted that we may assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q-1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$. That's why we will assume that $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$ in Theorem 1.2.

In this paper, we obtain an explicit class of permutation binomials over finite fields. To begin with, it is important to investigate the basic properties of the generalized Lucas sequences $\{U_n\}_{n\in\mathbb{N}}$ and two associated integer sequences. Secondly, we need to describe a relationship between these sequences and the corresponding lacunary sums of binomial coefficients. Based on this relationship, a sufficient and necessary condition of the binomials being the permutation binomials of finite fields should also be considered. At the end of this paper, we present some explicit examples of permutation binomials with the form $x^{\mu+\nu} + 3x^{\mu}$ to illustrate the details of Theorem 1.2. Meanwhile, we recognized that the application of $\{U_n\}^*_{n\in\mathbb{N}}$ will be discussed in greater detail in the another paper since it is beyond the present paper's topic.

2 Some useful auxiliary results

In this section, we introduce some prearrangement knowledge which will be used later, including the system of congruences and the classical Hermite's criterion.

Lemma 2.1 *Let p be a prime with $3 \mid p^n - 1$. Set $s = \frac{p^n-1}{3}$. If*

$$3 \cdot 2^{4s-3} \equiv -7^s \pmod{17},$$

then $s \equiv 5 \pmod{2^4}$, $p = 2$ and $n \geq 4$ is even.

Proof Since $2^3 \cdot (-2) \equiv 1 \pmod{17}$, it follows from $2^{-3} \equiv -2 \pmod{17}$ that

$$\begin{aligned} 3 \cdot 2^{4s-3} + 7^s &\equiv 3 \cdot (2^4)^s \cdot 2^{-3} + 7^s \\ &\equiv 3 \cdot (-1)^s \cdot 2^{-3} + 7^s \\ &\equiv (-6) \cdot (-1)^s + 7^s \\ &\equiv (-6) \cdot (-1)^s + (-10)^s \\ &\equiv (-6) \cdot (-1)^s + (-1)^s \cdot 10^s \\ &\equiv (-1)^s \cdot (10^s - 6) \pmod{17}. \end{aligned}$$

The case $s = 2k$ with $k \geq 1$. Observe that $17 \cdot 6 = 102$. Then

$$10^s = 10^{2k} = 100^k \equiv (-2)^k \equiv \begin{cases} (-1)^t \pmod{17}, if\ k = 4t; \\ (-2) \cdot (-1)^t \pmod{17}, if\ k = 4t+1; \\ 4 \cdot (-1)^t \pmod{17}, if\ k = 4t+2; \\ (-8) \cdot (-1)^t \pmod{17}, if\ k = 4t+3, \end{cases}$$

a desired contradiction. The case $s = 2k+1$ with $k \geq 1$. Then

$$10^s = 10^{2k+1} = 10 \cdot 100^k \equiv 10 \cdot (-2)^k \equiv \begin{cases} 10 \cdot (-1)^t \pmod{17}, if\ k = 4t; \\ (-3) \cdot (-1)^t \pmod{17}, if\ k = 4t+1; \\ 6 \cdot (-1)^t \pmod{17}, if\ k = 4t+2; \\ 5 \cdot (-1)^t \pmod{17}, if\ k = 4t+3. \end{cases}$$

So $k = 4t+2$ and t even. Let $t = 2m$. Then $s = 2k+1 = 16m+5$ implies that $s \equiv 5 \pmod{16}$.

Recall that $s = \frac{p^n-1}{3}$. By $s \equiv 5 \pmod{16}$, we have $\frac{p^n-1}{3} \equiv 5 \pmod{16}$ and so $p^n \equiv 0 \pmod{16}$. Thus, $p = 2$ and $n \geq 4$.

From $3 \mid 2^n - 1$, we get that $2^n \equiv (-1)^n \equiv 1 \pmod{3}$. So n is even. This completes the proof. □

One of the most useful characterizations of permutation polynomials is the following Hermite's criterion.

Lemma 2.2 (Hermite's criterion *[17, Theorem 7.4]) Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) = p$. Then $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions hold:*

(i) $f(x)$ has exactly one root in $\mathbb{F}_q$,
(ii) for each positive integer t with $t \leq q-2$ and $t \neq 0 \pmod{p}$, the reduction of

$$f(x)^t \pmod{x^q - x}$$

has degree $\leq q-2$.

Lemma 2.3 *Let $f(x) = x^{\mu+\nu} + ax^\mu \in \mathbb{F}_q[x]$ be a permutation binomial of $\mathbb{F}_q$. Then $char(\mathbb{F}_q) \neq 2$.*

Proof Assume on the contrary that $char(\mathbb{F}_q) = 2$. Then, by $a \neq 0$,

$$f(x) = x^{\mu+\nu} + ax^\mu = x^{\mu+\nu} + x^\mu. \tag{1}$$

Now (1) yields $f(0) = f(1) = 0$, which is contrary to the assumption that $f(x)$ is a permutation binomial. □

For the positive integer n, let $\pi(n)$ denote the set of all prime divisors of n.

Lemma 2.4 *Let a be a positive integer and let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) = p$. If $p \notin \pi(a^3+1)$, then $f(x) = x^{\mu+\nu} + ax^\mu$ has only one root in $\mathbb{F}_q$, where $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$.*

Proof Let $\alpha \in \mathbb{F}_q$ such that $f(\alpha) = \alpha^{\mu+\nu} + a \cdot \alpha^{\mu} = \alpha^{\mu}(\alpha^{\nu} + a) = 0$. Then $\alpha^{\nu} = -a$ or $\alpha = 0$. Assume that $\alpha^{\nu} = -a$. Now $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$ implies that

$$(q-1) \mid 3\nu$$

which implies that

$$\alpha^{3\nu} = 1 = (\alpha^{\nu})^3 = (-a)^3 = -a^3,$$

namely,

$$a^3 + 1 \equiv 0 \pmod{p}.$$

This means that $p \in \pi(a^3 + 1)$, a desired contradiction. □

Lemma 2.5 *Let $f(x) = x^{\mu+\nu} + ax^{\mu} \in \mathbb{F}_q[x]$ be a permutation binomial of $\mathbb{F}_q$ with $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$. Then $(\mu, \nu) = 1$.*

Proof It follows immediately from [22, Theorem 1.2], [23, Lemma 1] or [27, Theorem 1.2]. □

Lemma 2.6 *Let $f(x) = x^{\mu+\nu} + ax^{\mu} \in \mathbb{F}_q[x]$ with $(\mu, \nu) = 1$ and $\nu = \frac{q-1}{3}$ or $\frac{2(q-1)}{3}$. If $\frac{q-1}{3} \nmid t$, then the reduction of*

$$f(x)^t = \left(x^{\mu+\nu} + ax^{\mu}\right)^t \pmod{x^q - x}$$

has degree $\leq q - 2$.

Proof It follows immediately from [23, Lemma 3]. □

3 Generalized Lucas sequence

Let $\mathbb{N}$ be the set of non-negative integers and let α, β be the roots of

$$x^2 - Px + Q = 0 \tag{2}$$

where P, Q are relatively prime integers. The generalized Lucas sequences $\{U_n\}_{n\in\mathbb{N}}$ and $\{U_n^*\}_{n\in\mathbb{N}}$ which were defined by Lehmer [13] in 1930 as follows:

$$U_n = \alpha^n + \beta^n, \tag{3}$$

$$U_n^* = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \tag{4}$$

where $\alpha = \frac{P+\sqrt{P^2-4Q}}{2}$ and $\beta = \frac{P-\sqrt{P^2-4Q}}{2}$.

When $P = 1$ and $Q = -1$, U_n and U_n^* are called a Lucas sequence and a Fibonacci sequence respectively. It is widely known that the generalized Lucas sequences $\{U_n\}_{n\in\mathbb{N}}$ and $\{U_n^*\}_{n\in\mathbb{N}}$ satisfy the second-order linear recursive relations:

(i) $U_{n+2} = P \cdot U_{n+1} - Q \cdot U_n$ with initial values $U_0 = 2$ and $U_1 = P$;
(ii) $U_{n+2}^* = P \cdot U_{n+1}^* - Q \cdot U_n^*$ with initial values $U_0^* = 0$ and $U_1^* = 1$.

In the past hundred years, the applications of generalized Lucas sequences in exponential Diophantine equations, combinatorial mathematics, graph theory, cryptography, differential equations, numerical analysis, operations research, geometry and etc have been extensively studied, the interested reader can refer the relevant literature (for instance [11,18,21,25,26]) for detailed information about the basic properties and the applications mentioned above, we don't repeat here.

3.1 A certain generalized Lucas sequence

As the previous lines already suggest, we first show some basic properties of a certain generalized Lucas sequence $\{U_s\}_{s\in\mathbb{N}}$ with $P=-13$ and $Q=7^2$. What follows is to present two new integer sequences $\{V_s\}_{s\in\mathbb{N}}$ and $\{W_s\}_{s\in\mathbb{N}}$ which rely on $\{U_s\}_{s\in\mathbb{N}}$.

Lemma 3.1 *Let $\{U_s\}_{s\in\mathbb{N}}$ be a generalized Lucas sequence with $P=-13$ and $Q=7^2$. Then the following hold:*

(i) $\alpha=\frac{3\sqrt{3}i-13}{2}$ *and* $\beta=\frac{-3\sqrt{3}i-13}{2}$;
(ii) $U_s=(\frac{3\sqrt{3}i+1}{2})^{2s}+(\frac{3\sqrt{3}i-1}{2})^{2s}$;
(iii) $U_s\cdot U_t=U_{s+t}+7^{2t}\cdot U_{s-t}$ *for any* $s,t\in\mathbb{N}$ *with* $s\geq t$;
(iv) $(U_s)^2=U_{2s}+2\cdot 7^{2s}$;
(v) $U_{s+2}=-13\cdot U_{s+1}-7^2\cdot U_s$;
(vi) $\{U_s\}_{s\in\mathbb{N}}$ *is an integer sequence with initial values* $U_0=2$ *and* $U_1=-13$.

Proof Each follows immediately from the definition of $\{U_n\}_{n\in\mathbb{N}}$ (or see [18], Chapter 2). □

Lemma 3.2 *Let $s\in\mathbb{N}$ and let $V_s=\frac{\sqrt{3}i-1}{2}\cdot(\frac{3\sqrt{3}i+1}{2})^{2s}-\frac{\sqrt{3}i+1}{2}\cdot(\frac{3\sqrt{3}i-1}{2})^{2s}$. Then the following hold:*

(i) $V_s\cdot V_t=-V_{s+t}-U_{s+t}+7^{2t}\cdot U_{s-t}$ *for any* $s,t\in\mathbb{N}$ *with* $s\geq t$;
(ii) $(V_s)^2=-V_{2s}-U_{2s}+2\cdot 7^{2s}$;
(iii) $V_{s+2}=-8\cdot V_{s+1}+7^2\cdot U_s-U_{s+2}$;
(iv) $\{V_s\}_{s\in\mathbb{N}}$ *is an integer sequence with initial values* $V_0=-1$ *and* $V_1=2$.

Proof Since (ii)–(iv) follow from (i), we only need to give a proof of (i). It follows from Lemma 3.1 that

$$
\begin{aligned}
V_s\cdot V_t=&\left(\frac{\sqrt{3}i-1}{2}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2s}-\frac{\sqrt{3}i+1}{2}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2s}\right)\times\\
&\left(\frac{\sqrt{3}i-1}{2}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2t}-\frac{\sqrt{3}i+1}{2}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2t}\right)\\
=&(-1)\cdot\frac{\sqrt{3}i+1}{2}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}+\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2s}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2t}\\
&+\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2s}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2t}+\frac{\sqrt{3}i-1}{2}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\\
=&(-1)\cdot\Big(\frac{\sqrt{3}i-1}{2}+1\Big)\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}+\Big(\frac{\sqrt{3}i+1}{2}-1\Big)\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\\
&+\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2s}\cdot 7^{2t}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{-2t}+\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2s}\cdot 7^{2t}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{-2t}\\
=&(-1)\cdot\frac{\sqrt{3}i-1}{2}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}-(-1)\cdot\frac{\sqrt{3}i+1}{2}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\\
&+(-1)\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}+(-1)\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\\
&+7^{2t}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s-t)}+7^{2t}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s-t)}\\
=&(-1)\cdot\left(\frac{\sqrt{3}i-1}{2}\cdot\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}-\frac{\sqrt{3}i+1}{2}\cdot\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\right)\\
&+(-1)\cdot\left(\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s+t)}+\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s+t)}\right)\\
&+7^{2t}\cdot\left(\Big(\frac{3\sqrt{3}i+1}{2}\Big)^{2(s-t)}+\Big(\frac{3\sqrt{3}i-1}{2}\Big)^{2(s-t)}\right)\\
=&-V_{s+t}-U_{s+t}+7^{2t}\cdot U_{s-t},
\end{aligned}
$$

and we are done. □

Lemma 3.3 *Let $s \in \mathbb{N}$ and let $W_s = \frac{\sqrt{3}i-1}{2} \cdot (\frac{3\sqrt{3}i-1}{2})^{2s} - \frac{\sqrt{3}i+1}{2} \cdot (\frac{3\sqrt{3}i+1}{2})^{2s}$. Then the following hold:*

(i) $W_s \cdot W_t = -W_{s+t} - U_{s+t} + 7^{2t} \cdot U_{s-t}$;
(ii) $(W_s)^2 = -W_{2s} - U_{2s} + 2 \cdot 7^{2s}$;
(iii) $W_{s+2} = -11 \cdot W_{s+1} + 7^2 \cdot U_s - U_{s+2}$;
(iv) $\{W_s\}_{s\in\mathbb{N}}$ *is an integer sequence with initial values* $W_0 = -1$ *and* $W_1 = 11$.

Proof This can be proved as Lemma 3.2. □

3.2 The lacunary sums of binomial coefficients

In the following, we consider relationships between $\{U_s\}_{s\in\mathbb{N}}$, $\{V_s\}_{s\in\mathbb{N}}$ or $\{W_s\}_{s\in\mathbb{N}}$ and the lacunary sums of binomial coefficients respectively. It is worth noting that the relationship plays a fundamental role in this paper.

Theorem 3.4 *Let $s \in \mathbb{N}$ and let U_s, V_s and W_s be as in the preceding lemmas. Then the following hold:*

(i) $\sum_{i=0}^{[\frac{2s}{3}]} \binom{2s}{3i} \cdot 3^{3i} = \frac{4^{2s}+U_s}{3}$;

(ii) $\sum_{i=0}^{[\frac{2s-1}{3}]} \binom{2s}{3i+1} \cdot 3^{3i+1} = \frac{4^{2s}+V_s}{3}$;

(iii) $\sum_{i=0}^{[\frac{2s-2}{3}]} \binom{2s}{3i+2} \cdot 3^{3i+2} = \frac{4^{2s}+W_s}{3}$.

Proof Let $\alpha_0 = \frac{-1+\sqrt{3}i}{2}$ and $\beta_0 = \frac{-1-\sqrt{3}i}{2}$, where $i^2 = -1$. Then $\alpha_0^j + \beta_0^j = 2$ for $3 \mid j$ and $\alpha_0^j + \beta_0^j = -1$ for $3 \nmid j$. It follows from the binomial theorem that

$$\begin{aligned}
\sum_{i=0}^{[\frac{2s}{3}]} \binom{2s}{3i} \cdot 3^{3i} &= \frac{1}{3} \cdot \left(4^{2s} + 2 \cdot \sum_{3\mid j}^{2s} \binom{2s}{j} \cdot 3^j - \sum_{3\nmid j}^{2s} \binom{2s}{j} \cdot 3^j\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + 2 \cdot \sum_{3\mid j}^{2s} \binom{2s}{j} \cdot 3^j + (-1) \cdot \sum_{3\nmid j}^{2s} \binom{2s}{j} \cdot 3^j\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + (\alpha_0^j + \beta_0^j) \cdot \sum_{3\mid j}^{2s} \binom{2s}{j} \cdot 3^j + (\alpha_0^j + \beta_0^j) \cdot \sum_{3\nmid j}^{2s} \binom{2s}{j} \cdot 3^j\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + \sum_{3\mid j}^{2s} \binom{2s}{j} \cdot 3^j \cdot (\alpha_0^j + \beta_0^j) + \sum_{3\nmid j}^{2s} \binom{2s}{j} \cdot 3^j \cdot (\alpha_0^j + \beta_0^j)\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + \sum_{j=0}^{2s} \binom{2s}{j} \cdot 3^j \cdot (\alpha_0^j + \beta_0^j)\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + \sum_{j=0}^{2s} \binom{2s}{j} \cdot (3\alpha_0)^j + \sum_{j=0}^{2s} \binom{2s}{j} \cdot (3\beta_0)^j\right) \\
&= \frac{1}{3} \cdot \left(4^{2s} + (1+3\alpha_0)^{2s} + (1+3\beta_0)^{2s}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{3}\cdot\left(4^{2s} + (\frac{-1+3\sqrt{3}i}{2})^{2s} + (\frac{-1-3\sqrt{3}i}{2})^{2s}\right)\\
&= \frac{1}{3}\cdot\left(4^{2s} + (\frac{-1+3\sqrt{3}i}{2})^{2s} + (\frac{1+3\sqrt{3}i}{2})^{2s}\right)\\
&= \frac{1}{3}\cdot\left(4^{2s} + U_s\right).
\end{aligned}
$$

Similarly for (i), it suffices to show that (ii) and (iii) hold. This proves the theorem. □

3.3 The relationship between $\{U_s\}_{s\in\mathbb{N}}$, $\{V_s\}_{s\in\mathbb{N}}$ and $\{W_s\}_{s\in\mathbb{N}}$

At the end of this section, we will deal with the relationship between $\{U_s\}_{s\in\mathbb{N}}$, $\{V_s\}_{s\in\mathbb{N}}$ and $\{W_s\}_{s\in\mathbb{N}}$. Beforehand, a classical Pascal's formula is a must.

Lemma 3.5 (Pascal's formula *[3, Theorem 5.1.1]) Let n and k be integers. Then the following statements hold:*

(i) $\binom{n}{0} = 1$;
(ii) if $n < k$ *or* $k < 0$, *then* $\binom{n}{k} = 0$;
(iii) if $k \le n$, *then*

$$
\begin{aligned}
\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k}\\
&= \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}.
\end{aligned}
$$

Theorem 3.6 *Let* $s \in \mathbb{N}$ *and let* U_s, V_s *and* W_s *be as in the preceding lemmas. Then the following hold:*

(i) $U_{s+1} = U_s + \frac{1}{3}\cdot V_s + \frac{2}{9}\cdot W_s - \frac{130}{9}\cdot 4^{2s}$;
(ii) $V_{s+1} = V_s + 6\cdot U_s + 3^2\cdot W_s$;
(iii) $W_{s+1} = W_s + 6\cdot V_s + 3^2\cdot U_s$.

Proof It's trivial that we only need to prove (i). Similar calculations can be used to prove (ii) and (iii). Due to Pascal's formula and Theorem 3.4, we have

$$
\begin{aligned}
\frac{4^{2(s+1)} + U_{s+1}}{3} &= \sum_{i=0}^{[\frac{2(s+1)}{3}]}\binom{2(s+1)}{3i}\cdot 3^{3i}\\
&= \sum_{i=0}^{[\frac{2(s+1)}{3}]}\left(\binom{2s}{3i-2} + 2\cdot\binom{2s}{3i-1} + \binom{2s}{3i}\right)\cdot 3^{3i}\\
&= \frac{1}{3}\cdot\sum_{i=0}^{[\frac{2s-1}{3}]}\binom{2s}{3i+1}\cdot 3^{3i+1} + \frac{2}{9}\cdot\sum_{i=0}^{[\frac{2(s-1)}{3}]}\binom{2s}{3i+2}\cdot 3^{3i+2} + \sum_{i=0}^{[\frac{2s}{3}]}\binom{2s}{3i}\cdot 3^{3i}\\
&= \frac{1}{3}\cdot\frac{4^{2s}+V_s}{3} + \frac{2}{9}\cdot\frac{4^{2s}+W_s}{3} + \frac{4^{2s}+U_s}{3}.
\end{aligned}
$$

Thus, we get

$$
U_{s+1} = U_s + \frac{1}{3}\cdot V_s + \frac{2}{9}\cdot W_s - \frac{130}{9}\cdot 4^{2s},
$$

and we are done. □

4 The proof of Theorem 1.2

In the following, we begin to present the proof of Theorem 1.2, the main theorem of this paper.

Let $d = \frac{z(q-1)}{3}$ with $z = 1$ or 2. Then we have $d \leq q-2$ and

$$f(x)^d = (x^{\mu+\nu} + 3x^{\mu})^d = \sum_{i=0}^{d} \binom{d}{i} \cdot 3^i \cdot x^{\mu d+\nu d-\nu i}. \tag{5}$$

Let k be the degree of any term in the expansion of $f(x)^d \pmod{x^q - x}$. Then there is an integer ℓ such that

$$k = \mu d + \nu d - \nu i - \ell(q-1) \leq q-1.$$

Let us consider the special case where $k = q-1$. Then

$$\mu d + \nu d - \nu i - \ell(q-1) = q-1$$

implies that

$$\ell + 1 = \frac{\mu d + \nu d - \nu i}{q-1}. \tag{6}$$

Since ℓ is an integer, (6) implies that

$$(q-1) \mid (\mu d + \nu d - \nu i). \tag{7}$$

Let $\nu = \frac{(q-1)\nu_0}{3}$, where $\nu_0 = 1$ or 2. Now (7) and $d = \frac{(q-1)z}{3}$ imply that

$$3 \mid \mu z + \nu_0 z - \nu_0 i \tag{8}$$

which implies that

$$\mu z + \nu_0 z \equiv \nu_0 i \pmod 3, \tag{9}$$

and by $\nu_0 = 1$ or 2, we have $\nu_0^2 \equiv 1 \pmod 3$ and

$$\nu_0(\mu z + \nu_0 z) \equiv \nu_0^2 i \equiv i \pmod 3.$$

From

$$i \equiv \nu_0 z(\mu + \nu_0) \pmod 3,$$

we get that

$$f(x)^d \pmod{x^q - x} = \sum_{\substack{0 \leq i \leq d \\ i \equiv \nu_0 z(\mu+\nu_0) \pmod 3}} \binom{d}{i} \cdot 3^i \cdot x^{q-1} + \ldots \tag{10}$$

For necessity suppose that $f(x)$ is a permutation polynomial on $\mathbb{F}_q$. Then, by Lemma 2.2, we have

$$\sum_{\substack{0 \leq i \leq d \\ i \equiv \nu_0 z(\mu+\nu_0) \pmod 3}} \binom{d}{i} \cdot 3^i \equiv 0 \pmod p. \tag{11}$$

The case $\nu_0(\mu + \nu_0) \equiv 1 \pmod 3$. Then $2\nu_0(\mu + \nu_0) \equiv 2 \pmod 3$. From (11) and $d = \frac{(q-1)z}{3}$ with $z = 1$ or 2, we get

$$\sum_{\substack{0 \leq i \leq \frac{q-1}{3} \\ i \equiv 1 \pmod 3}} \binom{\frac{q-1}{3}}{i} \cdot 3^i \equiv 0 \pmod p \tag{12}$$

and

$$\sum_{\substack{0\le i\le \frac{2(q-1)}{3}\\ i\equiv 2 \pmod 3}} \binom{\frac{2(q-1)}{3}}{i} \cdot 3^i \equiv 0 \pmod p. \tag{13}$$

Let $s = \frac{q-1}{3}$. Since q is odd, s is even and Theorem 3.4 together with (12) and (13) yield

$$\frac{4^s + V_{\frac{s}{2}}}{3} \equiv 0 \pmod p \tag{14}$$

and

$$\frac{4^{2s} + W_s}{3} \equiv 0 \pmod p. \tag{15}$$

Then (14) and (15) imply that

$$V_{\frac{s}{2}} \equiv -4^s \pmod p \tag{16}$$

and

$$W_s \equiv -4^{2s} \pmod p. \tag{17}$$

By Lemma 3.2 (ii), we know that

$$(V_{\frac{s}{2}})^2 = -V_s - U_s + 2 \cdot 7^s.$$

This implies that

$$4^{2s} = -V_s - U_s + 2 \cdot 7^s. \tag{18}$$

Note that $(V_{\frac{s}{2}})^2 = 4^{2s} = -W_s$. Thus, by Theorem 3.6 (i), (ii), we have

$$45 \cdot 4^{2s} + 3 \cdot U_{s+1} = 2 \cdot 7^s + 2 \cdot U_s. \tag{19}$$

and

$$18 \cdot (4^{2s} - 7^s) + 3 \cdot U_s + 7^2 \cdot U_{s-1} = U_{s+1}. \tag{20}$$

Recall that $U_{s+1} = -13 \cdot U_s - 49 \cdot U_{s-1}$. Then (20) yields

$$18 \cdot (4^{2s} - 7^s) - 10 \cdot U_s - 2 \cdot U_{s+1} = 0. \tag{21}$$

Thus, by (19) and (21), we have

$$U_{s+1} = (-1) \cdot \frac{207 \cdot 4^{2s} + 8 \cdot 7^s}{17}. \tag{22}$$

Since $\{U_{s+1}\}_{s\in\mathbb{N}}$ is an integer sequence, this means that 17 divides $207 \cdot 4^{2s} + 8 \cdot 7^s$. Notice that

$$207 \cdot 4^{2s} + 8 \cdot 7^s = 8 \cdot (17 \cdot 12 \cdot 2^{4s-3} + 3 \cdot 2^{4s-3} + 7^s).$$

So

$$17 \mid 3 \cdot 2^{4s-3} + 7^s.$$

Now Lemma 2.1 yields $p = 2$ which leads to the contradiction. The case $\nu_0(\mu + \nu_0) \equiv 2 \pmod 3$. Then $2\nu_0(\mu + \nu_0) \equiv 1 \pmod 3$. From (11) and $d = \frac{(q-1)z}{3}$ with $z = 1$ or 2, we get

$$\sum_{\substack{0\le i\le \frac{q-1}{3}\\ i\equiv 2 \pmod 3}} \binom{\frac{q-1}{3}}{i} \cdot 3^i \equiv 0 \pmod p. \tag{23}$$

$$\sum_{\substack{0\le i\le \frac{2(q-1)}{3}\\ i\equiv 1 \pmod 3}} \binom{\frac{2(q-1)}{3}}{i} \cdot 3^i \equiv 0 \pmod p. \tag{24}$$

Let $s = \frac{q-1}{3}$. Since q is odd, it follows from s even, Theorem 3.4, (23) and (24) that

$$\frac{4^s + W_{\frac{s}{2}}}{3} \equiv 0 \pmod p \tag{25}$$

and

$$\frac{4^{2s} + V_s}{3} \equiv 0 \pmod p. \tag{26}$$

Then (25) and (26) imply that

$$W_{\frac{s}{2}} \equiv -4^s \pmod p \tag{27}$$

and

$$V_s \equiv -4^{2s} \pmod p. \tag{28}$$

By Lemma 3.3 (ii), we know that

$$(W_{\frac{s}{2}})^2 = -W_s - U_s + 2 \cdot 7^s.$$

This implies that

$$4^{2s} = -W_s - U_s + 2 \cdot 7^s. \tag{29}$$

Note that $(W_{\frac{s}{2}})^2 = 4^{2s} = -V_s$. Thus, by Theorem 3.6 (i), (iii), we have

$$135 \cdot 4^{2s} + 9 \cdot U_{s+1} = 4 \cdot 7^s + 7 \cdot U_s \tag{30}$$

and

$$3 \cdot U_s + 18 \cdot 4^{2s} + 7^2 \cdot U_{s-1} - U_{s+1} = 24 \cdot 7^s. \tag{31}$$

Recall that $U_{s+1} = -13 \cdot U_s - 49 \cdot U_{s-1}$. Then (31) yields

$$9 \cdot 4^{2s} - 12 \cdot 7^s - 5 \cdot U_s - U_{s+1} = 0. \tag{32}$$

Thus, by (30) and (32), we have

$$U_s = \frac{108 \cdot 4^{2s} - 61 \cdot 7^s}{26}. \tag{33}$$

Since $\{U_{s+1}\}_{s\in\mathbb{N}}$ is an integer sequence, it follows that 26 divides $108 \cdot 4^{2s} - 61 \cdot 7^s$. Notice that $2 \mid 108 \cdot 4^{2s}$. So $2 \mid 61 \cdot 7^s$, a desired contradiction.

The case$\nu_0 z(\mu + \nu_0) \equiv 0 \pmod 3$. Recall that $z = 1$ or 2. Since $\nu_0 = 1$ or 2, we have $\mu \equiv 2$ or $1 \pmod 3$ respectively.

From (11) and $d = \frac{(q-1)z}{3}$ with $z = 1$ or 2, we get that

$$\sum_{\substack{0\le i\le d\\ i\equiv 0 \pmod 3}} \binom{d}{i} \cdot 3^i = \frac{4^d + U_{\frac{d}{2}}}{3} \equiv 0 \pmod p. \tag{34}$$

Let $s = \frac{q-1}{3}$. Now (34) yields

$$U_{\frac{s}{2}} \equiv -4^s \pmod p \tag{35}$$

and

$$U_s \equiv -4^{2s} \pmod{p}. \tag{36}$$

Notice that $(U_{\frac{s}{2}})^2 = U_s + 2 \cdot 7^s$. Then (35) and (36) imply that

$$4^{2s} \equiv (U_{\frac{s}{2}})^2 = U_s + 2 \cdot 7^s \equiv -4^{2s} + 2 \cdot 7^s \pmod{p} \tag{37}$$

which implies that

$$4^{2s} \equiv 2^{4s} \equiv 7^s \pmod{p}. \tag{38}$$

In particular, from (38), we also have $p \neq 2$ or 7.

For sufficiency suppose that $(\mu, \nu) = 1$, $2^{4s} \equiv 7^s \pmod{p}$ and $\mu + \nu_0 \equiv 0 \pmod 3$ hold. Then Theorem 3.4, Lemma 2.4 and Lemma 2.6 together with Hermite's criterion (Lemma 2.2) imply that $f(x) = x^{\mu+\nu} + 3x^{\mu}$ is a permutation binomial of $\mathbb{F}_q$. Thus, Theorem 1.2 is proved. □

Remark 4.1 Using the approach of [22], we also can get Theorem 1.2.

At the end of this paper, we present some explicit examples of permutation binomials with the form $x^{\mu+\nu}+3x^{\mu}$ to illustrate the details of Theorem 1.2.

Example 4.2 Theorem 1.2 shows that the following permutation binomials hold:

(i) $f(x) = x^{13} + 3x^5$ is a permutation binomial of $\mathbb{F}_{5^2}$;
(ii) $f(x) = x^{107} + 3x^{11}$ is a permutation binomial of $\mathbb{F}_{17^2}$;
(iii) $f(x) = x^{23} + 3x^7$ is a permutation binomial of $\mathbb{F}_{5^2}$;
(iv) $f(x) = x^{47} + 3x^7$ is a permutation binomial of $\mathbb{F}_{61}$;
(v) $f(x) = x^{93} + 3x^{13}$ is a permutation binomial of $\mathbb{F}_{11^2}$.

The following example provides an infinite class of permutation binomials over $\mathbb{F}_{5^{2n}}$.

Example 4.3 Let $q = 5^{2n}$, $(\mu, \nu) = (5^{2m+1}, \frac{5^{2n}-1}{3})$ or $(5^{2m}, \frac{2\cdot(5^{2n}-1)}{3})$ with $n > m$ and $n \geq 1$. It can be shown that q, μ and ν satisfy the constraint conditions of Theorem 1.2. Thus, both

$$f_1(x) = x^{\frac{3\cdot 5^{2m+1}+5^{2n}-1}{3}} + 3x^{5^{2m+1}}$$

and

$$f_2(x) = x^{\frac{3\cdot 5^{2m}+2\cdot 5^{2n}-2}{3}} + 3x^{5^{2m}}$$

are permutation binomials of $\mathbb{F}_{5^{2n}}$.

Acknowledgements The authors would like to thank Professor Pingzhi Yuan at South China Normal University and the anonymous referees for corrections and valuable comments that led to the improvement of the paper.

Declarations

Conflict of interest The authors declare that there are no conflict of interests.

References

1. A. Akbary, Q. Wang, On some permutation polynomials, *Int. J. Math. Math. Sci.*, **16**(2005): 2631–2640.
2. A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.*, **134**(1)(2006): 15–22.
3. R. A. Brualdi, Introductory Combinatorics, 5nd ed., Pearson Education Asia Limited, 2009.
4. L. E. Dickson, History of the theory of numbers, vol.3, Carnegie Institute, Washington, D. C., 1923, Dover, New York, 2005.
5. L. E. Dickson, The analytic representation of substitutions on a power of prime numeber of letters with a discussion of the linear group, *Ann. Math.*, **11**(1-6)(1896/1897): 161–183.
6. C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Comb. Theory, Ser. A*, **113**(2006): 1526–1535.
7. C. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Pairs*, **57**(1863): 750–757.
8. X. Hou, V. P. Lavorante, New results on permutation binomials of finite fields, *Finite Fields Appl.*, **88**(2023), 102179.
9. X. Hou, Permutation polynomials over finite fields—A survey of recent advances, *Finite Fields Appl.*, **32**(2015): 82–119.
10. X. Hou, A survey of permutation binomials and trinomials over finite fields, in: Contemp. Math., Vol. 632, Amer. Math. Soc., Providence, RI, 2013, pp. 177–191.
11. T. Koshy, Fibonacci and Lucas Numbers with Applications, New York, Wiley-Interscience, 2001.
12. Y. Laigle–Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.*, **13**(2007): 59–70.
13. D. H. Lehmer, An Extended Theory of Lucas Functions, *Arm. Math.*, **31**(1930): 419–48.
14. K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Appl.*, **43**(2017): 69–85.
15. R. Lidl, G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly*, **95**(3)(1988): 243–246.
16. R. Lidl, G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly*, **100**(1)(1993): 71–74.
17. R. Lidl, H. Niederreiter, Finite fields, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
18. P. Ribenboim, The Book of Prime Number Records, New York, Springer-Verlag, 1989.
19. R. L. Rivest, A. Shamir, L. M. Adelman, A method for obtaining digital signatures and publi-key cryptosystems, *Commun. ACM*, **21**(1978): 120–126.
20. J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, *Electron. Lett.*, **34**(1998): 759–760.
21. S. Vajda, Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications, Dover Press, 2008.
22. D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.*, **112**(1991): 149–163.
23. L. Wang, On permutation polynomials, *Finite Fields Appl.*, **8**(2002): 311–322.
24. Q. Wang, On generalized Lucas sequences, Contemporary Mathematics, 2009.
25. P. Yuan, A note on the divisibility of the generalized Lucas sequences, *Fibonacci Quart.*, **40**(2)(2002): 153–156.
26. C. Zhou, P. Yuan, G. Xiao, Fibonacci-Lucas sequences and their applications, Harbin, Harbin Institute of Technology Press, 2016.
27. M. E. Zieve, On some permutation polynomials over F_q of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.*, **137**(2009): 2209–2216.