Combinatorics and Graphs: the twentieth anniversary conference of IPM, May 15-21, 2009,
Contemporary Mathematics 531 (2010), 127-141

On generalized Lucas sequences

Qiang Wang

This paper is dedicated to Professor G. B. Khosrovshahi on the occasion of his 70th birthday and to IPM on its 20th birthday.

Abstract. We introduce the notions of unsigned and signed generalized Lucas sequences and prove certain polynomial recurrence relations on their characteristic polynomials. We also characterize when these characteristic polynomials are irreducible polynomials over a finite field. Moreover, we obtain the explicit expressions of the remainders of Dickson polynomials of the first kind divided by the characteristic polynomial of generalized Lucas sequences. Using these remainders, we show an application of generalized Lucas sequences in the characterization of a class of permutation polynomials and their compositional inverses.

1. Introduction

Fibonacci numbers form an integer sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

which was well known in ancient India. To the western world, it became popular through the Italian Mathematician, Leonardo of Pisa known as Fibonacci (1170-1250), who considered the growth of an idealized (biologically unrealistic) rabbit population by using this sequence in his famous book *Liber Abaci (1202)*. In the language of recurrence relation, Fibonacci numbers $\{F_n\}_{n=0}^{\infty}$ satisfy a second order homogeneous recurrence relation given by

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2} \; for \; n \geq 2.$$

The so-called Lucas numbers $\{L_n\}_{n=0}^{\infty}$ have the same recurrence relation but different initial values, that is,

$$L_0 = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2} \; for \; n \geq 2.$$

1991 *Mathematics Subject Classification.* Primary 11B39; Secondary 11T06.

Key words and phrases. Lucas sequences, finite fields, Dickson polynomials, irreducible polynomials, permutation polynomials.

Research of the author was partially supported by NSERC of Canada. The author wants to thank Hadi Kharaghani for kind and continuous support, and generous hospitality during the visit to IPM. The author also wants to thank IPM, Behruz Tayfeh-Rezaie, and Saieed Akbari for their warm hospitality. Finally the author thanks the referee for helpful suggestions.

Nowadays, Lucas sequences are referred as a family of sequences with the similar structure. For a given pair of integers P, Q such that $\triangle = P^2 - 4Q$ is a non-square, there are two types of Lucas sequences. The first type is usually denoted by $\{V_n(P,Q)\}_{n=0}^{\infty}$ where

$$V_0(P,Q) = 2, V_1(P,Q) = P, V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q) \ for \ n \geq 2.$$

The second type of sequences $\{U_n(P,Q)\}_{n=0}^{\infty}$ is defined via

$$U_0(P,Q) = 0, U_1(P,Q) = 1, U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q) \ for \ n \geq 2.$$

We call $\{V_n(P,Q)\}_{n=0}^{\infty}$ the first type because we will see that they can be obtained from Dickson polynomials of the first kind. Similarly, the sequence $\{U_n(P,Q)\}_{n=0}^{\infty}$ can be obtained from Dickson polynomials of the second kind. Hence Fibonacci numbers and Lucas numbers are $\{U_n(1,-1)\}_{n=0}^{\infty}$ and $\{V_n(1,-1)\}_{n=0}^{\infty}$ respectively. When $P = 2$ and $Q = -1$, sequences $\{U_n(2,-1)\}_{n=0}^{\infty}$ and $\{V_n(2,-1)\}_{n=0}^{\infty}$ are called Pell numbers and Pell-Lucas numbers respectively.

It is well-known that $L_n = V_n(1,-1) = a^n + b^n$ where $a = \frac{1+\sqrt{5}}{2}$ and $b = \frac{1-\sqrt{5}}{2}$. Let η be a primitive 10-th root of unity, then we can rewrite $a = \eta + \eta^{-1}$, $b = \eta^3 + \eta^{-3}$, and thus $L_n = (\eta + \eta^{-1})^n + (\eta^3 + \eta^{-3})^n$. Hence this motivated us to introduce the following generalized notion of Lucas numbers in our previous work.

Definition 1.1. ([**4**]) For any integer $k \geq 1$ and η a fixed primitive $(4k+2)$-th root of unity, the generalized Lucas sequence (or unsigned generalized Lucas sequence) of order k is defined as $\{a_n\}_{n=0}^{\infty}$ such that

$$a_n = \sum_{\substack{t=1 \\ t \ odd}}^{2k} (\eta^t + \eta^{-t})^n = \sum_{t=1}^{k} ((-1)^{t+1}(\eta^t + \eta^{-t}))^n.$$

We note that the Lucas numbers are simply generalized Lucas sequences of order $k = 2$. Similarly, we can define

Definition 1.2. For any integer $k \geq 1$ and η a fixed primitive $(4k+2)$-th root of unity, the *signed (or alternating) generalized Lucas sequence* of order k is defined as $\{b_n\}_{n=0}^{\infty}$ such that

$$b_n = \sum_{\substack{t=1 \\ t \ even}}^{2k} (\eta^t + \eta^{-t})^n = \sum_{t=1}^{k} ((-1)^{t}(\eta^t + \eta^{-t}))^n.$$

In fact, we will see that all the coefficients of both characteristic polynomials of signed and unsigned generalized Lucas sequences of order k are integers and then using Waring's formula we can conclude that both sequences are integer sequences. Several examples of these families of integer sequences can be found in Sloan's On-Line Encyclopedia of Integer Sequences. For example, generalized Lucas sequence of order 4 is called an accelerator sequence for Catalan's constant (A094649). Similarly, the signed generalized sequences of order 3 and 5 are numbered as A094648 and A094650 respectively.

The following tables (Table 1, Table 2) contain initial values and recurrence relations of unsigned and signed generalized Lucas sequence of order k for small k's.

Table 1. Generalized Lucas sequences

k	*initial values*	*recurrence relations*
$k=1$	1	$a_{n+1}=a_n$
$k=2$	$2,1$	$a_{n+2}=a_{n+1}+a_n$
$k=3$	$3,1,5$	$a_{n+3}=a_{n+2}+2a_{n+1}-a_n$
$k=4$	$4,1,7,4$	$a_{n+4}=a_{n+3}+3a_{n+2}-2a_{n+1}-a_n$
$k=5$	$5,1,9,4,25$	$a_{n+5}=a_{n+4}+4a_{n+3}-3a_{n+2}-3a_{n+1}+a_n$

Table 2. Signed generalized Lucas sequences

k	*initial values*	*recurrence relations*
$k=1$	1	$b_{n+1}=-b_n$
$k=2$	$2,-1$	$b_{n+2}=-b_{n+1}+b_n$
$k=3$	$3,-1,5$	$b_{n+3}=-b_{n+2}+2b_{n+1}+b_n$
$k=4$	$4,-1,7,-4$	$b_{n+4}=-b_{n+3}+3b_{n+2}+2b_{n+1}-b_n$
$k=5$	$5,-1,9,-4,25$	$b_{n+5}=b_{n+4}+4b_{n+3}+3b_{n+2}-3b_{n+1}-b_n$

It is easy to see from the definition that the characteristic polynomial of generalized Lucas sequence of order $k \geq 1$ is

$$g_k(x) = \prod_{\substack{t=1 \\ t\ odd}}^{2k} (x - (\eta^t + \eta^{-t})).$$

Similarly, the characteristic polynomial of signed generalized Lucas sequence of order $k \geq 1$ is

$$f_k(x) = \prod_{\substack{t=1 \\ t\ even}}^{2k} (x - (\eta^t + \eta^{-t})).$$

It is easy to see that $f_1(x) = x+1$, $f_2(x) = x^2+x-1$, $g_1(x) = x-1$, and $g_2(x) = x^2-x-1$. By convention, we let $f_0(x) = g_0(x) = 1$.

In Section 2, we show that both characteristic polynomials of degree k satisfy interesting recurrence relations with characteristic polynomials of degree $k-1$ and $k-2$ (Theorem 2.1, Theorem 2.2). Namely,

$$f_0(x) = 1, f_1(x) = x+1, f_k(x) = xf_{k-1}(x) - f_{k-2}(x)\ for\ k \geq 2 \tag{1.1}$$

and

$$g_0(x) = 1, g_1(x) = x-1, g_k(x) = xg_{k-1}(x) - g_{k-2}(x)\ for\ k \geq 2. \tag{1.2}$$

These polynomial recurrence relations provide us an easy way to compute characteristic polynomials of the generalized Lucas sequences and signed generalized Lucas sequences even for large k. Hence it is quite fast to generate unsigned and signed generalized Lucas sequences. Moreover, we characterize when degree k polynomials

$f_k(x)$ and $g_k(x)$ are irreducible polynomials over a finite field $\mathbb{F}_q$. It turns out that $2k+1$ must be prime (Theorem 2.5). In Section 3, we use some divisibility properties of characteristic polynomials $g_k(x)$ to obtain the explicit expressions for the remainders $R_{n,k}(x)$ of Dickson polynomials $D_n(x)$ of the first kind divided by $g_k(x)$ (Theorem 3.2). As an application, we explain the connection between generalized Lucas sequences over a prime field, $R_{n,k}(x)$, and a class of permutation polynomials and their inverses over an extension field (Theorem 3.3 and Theorem 3.8, respectively).

2. Characteristic polynomials

For any integer $n \geq 1$ and a parameter a in a field $\mathbb{F}$, we recall that the Dickson polynomial of the first kind $D_n(x,a) \in \mathbb{F}[x]$ of degree n is defined by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}.$$

Similarly, the Dickson polynomial of the second kind $E_n(x,a) \in \mathbb{F}[x]$ of degree n is defined by

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}(-a)^i x^{n-2i}.$$

For $a \neq 0$, we write $x = y + a/y$ with $y \neq 0$ an indeterminate. Then the Dickson polynomials can often be rewritten (also referred as functional expression) as

$$D_n(x,a) = D_n\left(y + \frac{a}{y}, a\right) = y^n + \frac{a^n}{y^n},$$

and

$$E_n(x,a) = E_n\left(y + \frac{a}{y}, a\right) = \frac{y^{n+1} - a^{n+1}/y^{n+1}}{y - a/y},$$

for $y \neq \pm\sqrt{a}$; For $y = \pm\sqrt{a}$, we have $E_n(2\sqrt{a},a) = (n+1)(\sqrt{a})^n$ and $E_n(-2\sqrt{a},a) = (n+1)(-\sqrt{a})^n$. It is well known that $D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a)$ and $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$ for any $n \geq 2$. Here we also note that $V_n(P,Q) = D_n(P,Q)$ and $U_{n+1}(P,Q) = E_n(P,Q)$.

In the case $a = 1$, we denote Dickson polynomials of degree n of the first and the second kind by $D_n(x)$ and $E_n(x)$ respectively. It is well known that these Dickson polynomials are closely related to the Chebyshev polynomials by the connections $D_n(2x) = 2T_n(x)$ and $E_n(2x) = U_n(x)$, where $T_n(x)$ and $U_n(x)$ are Chebyshev polynomials of degree n of the first and the second kind, respectively. More information on Dickson polynomials can be found in [**11**].

For any $k \geq 1$, let η be a primitive $(4k+2)$-th root of unity. It is well known that $\eta^t + \eta^{-t}$ with $1 \leq t \leq 2k$ are all the roots of $E_{2k}(x)$. Hence the characteristic polynomials $f_k(x)$ and $g_k(x)$ of signed and unsigned generalized Lucas sequences are both factors of $E_{2k}(x)$. In fact, $E_{2k}(x) = f_k(x)g_k(x)$ because all three polynomials are monic.

Next we prove the following results on the polynomial recurrence relations on the characteristic polynomials $f_k(x)$ and $g_k(x)$.

Theorem 2.1. *Let* $g_k(x) = \prod_{\substack{t=1 \\ t\ odd}}^{2k} (x - (\eta^t + \eta^{-t}))$ *be the characteristic polynomial of generalized Lucas sequence of order* $k \geq 1$ *and* $g_0(x) = 1$. *Then*

(i) $g_k(x) = E_k(x) - E_{k-1}(x)$ *for* $k \geq 1$.

(ii) $g_k(x)$ *satisfies the following recurrence relation:*

$$g_0(x) = 1, g_1(x) = x - 1, g_k(x) = xg_{k-1}(x) - g_{k-2}(x) \ for \ k \geq 2.$$

(iii) *The generating function of the above recurrence is* $G(x;t) = \frac{1-t}{1-xt+t^2}$.

(iv) $g_k(x) = \sum_{i=0}^{k} (-1)^{\lceil \frac{i}{2} \rceil} \binom{k - \lceil \frac{i}{2} \rceil}{\lfloor \frac{i}{2} \rfloor} x^{k-i}$.

Proof. Let $G_k(x) = E_k(x) - E_{k-1}(x)$ for $k \geq 1$. Using the functional expression $E_k(y + y^{-1}) = \frac{y^{k+1} - y^{-(k+1)}}{y - y^{-1}}$, we can easily obtain $G_k(y + y^{-1}) = \frac{y^{(2k+1)}+1}{y^k(y+1)}$. In particular, let η be a primitive $(4k+2)$-th root of unity. Hence $\eta^{2k+1} = -1$ and thus $G_k(\eta^t + \eta^{-t}) = \frac{\eta^{(2k+1)t}+1}{\eta^{tk}(\eta^t+1)} = 0$ for all odd t. Hence all the roots of $g_k(x)$ are roots of $G_k(x)$. Moreover, $\deg(G_k(x)) = \deg(g_k(x)) = k$ and both $G_k(x)$ and $g_k(x)$ are monic, we conclude that (i) is satisfied. Using the recurrence relation $E_k(x) = xE_{k-1}(x) - E_{k-2}(x)$, one obtains (ii) immediately. Moreover, the generating function $G(x;t)$ of $g_k(x)$ can be derived from

$$\begin{aligned}
(1 - xt + t^2)G(x;t) &= (1 - xt + t^2) \sum_{k=0}^{\infty} g_k(x) t^k \\
&= \sum_{k=0}^{\infty} g_k(x) t^k - \sum_{k=0}^{\infty} x g_k(x) t^{k+1} + \sum_{k=0}^{\infty} g_k(x) t^{k+2} \\
&= 1 + (x-1)t - xt + \sum_{k=0}^{\infty} (g_{k+2}(x) - x g_{k+1}(x) + g_k(x)) t^{k+2} \\
&= 1 - t.
\end{aligned}$$

Finally, to prove (iv), we have

$$\begin{aligned}
g_k(x) &= E_k(x) - E_{k-1}(x) \\
&= \sum_{j=0}^{\lfloor k/2 \rfloor} (-1)^j \binom{k-j}{j} x^{k-2j} - \sum_{j=0}^{\lfloor (k-1)/2 \rfloor} (-1)^j \binom{k-1-j}{j} x^{k-1-2j} \\
&= \sum_{\substack{i=0 \\ i\ even}}^{k} (-1)^{\lceil i/2 \rceil} \binom{n - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i} - \sum_{\substack{i=0 \\ i\ odd}}^{k} (-1)^{\lfloor i/2 \rfloor} \binom{k - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i} \\
&= \sum_{i=0}^{k} (-1)^{\lceil i/2 \rceil} \binom{k - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i}.
\end{aligned}$$

□

Similarly, we have the following result for signed generalized Lucas sequences.

Theorem 2.2. *Let* $f_k(x) = \prod_{\substack{t=1\\ t\ even}}^{2k} (x - (\eta^t + \eta^{-t}))$ *be the characteristic polynomial of signed generalized Lucas sequence of order* $k \geq 1$ *and* $f_0(x) = 1$. *Then*

(i) $f_k(x) = E_k(x) + E_{k-1}(x)$ *for* $k \geq 1$.

(ii) $f_k(x)$ *satisfies the following recurrence relation:*

$$f_0(x) = 1, f_1(x) = x + 1, f_k(x) = xf_{k-1}(x) - f_{k-2}(x) \ for \ k \geq 2.$$

(iii) *The generating function of the above recurrence is* $F(x;t) = \frac{1+t}{1-xt+t^2}$.

(iv) $f_k(x) = \sum_{i=0}^{k} (-1)^{\lfloor \frac{i}{2} \rfloor} \binom{k - \lceil \frac{i}{2} \rceil}{\lfloor \frac{i}{2} \rfloor} x^{k-i}$.

Proof. Let $F_k(x) = E_k(x) + E_{k-1}(x)$ for $k \geq 1$. Using the functional expression of $E_n(x)$, we can easily obtain $F_k(y + y^{-1}) = \frac{y^{(2k+1)}-1}{y^k(y-1)}$. In particular, let η be a primitive $(4k+2)$-th root of unity. Hence $\eta^{2k+1} = -1$ and thus $F_k(\eta^t + \eta^{-t}) = \frac{\eta^{(2k+1)t}-1}{\eta^{tk}(\eta^t-1)} = 0$ for all even t. Hence all the roots of $f_k(x)$ are roots of $F_k(x)$. Moreover, $\deg(F_k(x)) = \deg(f_k(x)) = k$ and both $F_k(x)$ and $f_k(x)$ are monic. Hence we conclude that (i) is satisfied. Using the recurrence relation $E_k(x) = xE_{k-1}(x) - E_{k-2}(x)$, one obtains (ii) immediately. Moreover, the generating function $F(x;t)$ of $f_k(x)$ can be derived from

$$\begin{aligned}
(1 - xt + t^2)F(x;t) &= (1 - xt + t^2) \sum_{k=0}^{\infty} f_k(x) t^k \\
&= \sum_{k=0}^{\infty} f_k(x) t^k - \sum_{k=0}^{\infty} x f_k(x) t^{k+1} + \sum_{k=0}^{\infty} f_k(x) t^{k+2} \\
&= 1 + (x+1)t - xt + \sum_{k=0}^{\infty} (f_{k+2}(x) - xf_{k+1}(x) + f_k(x)) t^{k+2} \\
&= 1 + t.
\end{aligned}$$

Finally, to prove (iv), we have

$$\begin{aligned}
f_k(x) &= E_k(x) + E_{k-1}(x) \\
&= \sum_{j=0}^{\lfloor k/2 \rfloor} (-1)^j \binom{k-j}{j} x^{k-2j} + \sum_{j=0}^{\lfloor (k-1)/2 \rfloor} (-1)^j \binom{k-1-j}{j} x^{k-1-2j} \\
&= \sum_{\substack{i=0\\ i\ even}}^{k} (-1)^{\lfloor i/2 \rfloor} \binom{k - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i} + \sum_{\substack{i=0\\ i\ odd}}^{k} (-1)^{\lfloor i/2 \rfloor} \binom{k - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i} \\
&= \sum_{i=0}^{k} (-1)^{\lfloor i/2 \rfloor} \binom{k - \lceil i/2 \rceil}{\lfloor i/2 \rfloor} x^{k-i}.
\end{aligned}$$

□

The functional expressions of $f_k(x)$ and $g_k(x)$ are quite useful in the above proofs. We summarize them as follows:

$$(2.1) \quad f_k(y+y^{-1}) = \frac{y^{2k+1}-1}{y^k(y-1)} \ for \ y \neq 0, \pm 1, f_k(2) = 2k+1, \ and \ f_k(-2) = (-1)^k;$$

and
(2.2)

$$g_k(y+y^{-1}) = \frac{y^{2k+1}+1}{y^k(y+1)} \textit{ for } y \neq 0, \pm 1, g_k(2) = 1, \textit{ and } g_k(-2) = (-1)^k(2k+1).$$

Using these functional expressions, one can also easily obtain the following result (see also Exercise 2.11 in [**11**]).

Corollary 2.3. *Let $f_k(x)$ and $g_k(x)$ be characteristic polynomials of signed and unsigned generalized Lucas sequences of order k. Then we have*

(i) $f_{m+n}(x) = f_m(x)E_n(x) - f_{m-1}(x)E_{n-1}(x)$.
(ii) $g_{m+n}(x) = g_m(x)E_n(x) - g_{m-1}(x)E_{n-1}(x)$.
(iii) *If* $(2d+1) \mid (2k+1)$ *then* $f_d(x) \mid f_k(x)$ *and* $g_d(x) \mid g_k(x)$.

Next we will see some applications of $E_{2k}(x) = f_k(x)g_k(x)$. First, using $E_{2k}(x) = f_k(x)g_k(x)$, Theorem 2.1 and Theorem 2.2, it is obvious to obtain the following interesting combinatorial identity for any $0 \leq m \leq 2k$.

$$\sum_{\substack{i,j=0 \\ i+j=m}}^{k} (-1)^{\lceil \frac{i}{2} \rceil} \binom{k-\lceil \frac{i}{2} \rceil}{\lfloor \frac{i}{2} \rfloor} (-1)^{\lfloor \frac{j}{2} \rfloor} \binom{k-\lceil \frac{j}{2} \rceil}{\lfloor \frac{j}{2} \rfloor} = \begin{cases} 0 & \textit{if } m \textit{ is odd;} \\ (-1)^{\frac{m}{2}} \binom{2k-\frac{m}{2}}{\frac{m}{2}} & \textit{if } m \textit{ is even.} \end{cases}$$

Now we can characterize when $f_k(x)$ and $g_k(x)$ are irreducible polynomials over a finite field. Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) = p$. Since the factorization of $E_{2k}(x)$ over a finite field $\mathbb{F}_q$ is well known (see for example, [**6**] or [**8**]), we can obtain the factorization of $f_k(x)$ and $g_k(x)$ over $\mathbb{F}_q$ as well. Of course, it is enough to give the result for the case that $\gcd(2k+1, p) = 1$. Indeed, if $(2k+1) = p^r(2t+1)$ where $\gcd(2t+1, p) = 1$, then it is straightforward to obtain $f_k(x) = f_t(x)^{p^r}(x-2)^{\frac{p^r-1}{2}}$ and $g_k(x) = g_t(x)^{p^r}(x+2)^{\frac{p^r-1}{2}}$ by using the functional expressions of $f_k(x)$ and $g_k(x)$.

Theorem 2.4. *Let $\mathbb{F}_q$ be a finite field with $char(\mathbb{F}_q) = p$,* $\gcd(2k+1, p) = 1$, *and ϕ be Euler's totient function.*

(i) If q is even, then $f_k(x) = g_k(x)$ is a product of irreducible polynomials in $\mathbb{F}_q[x]$ which occur in cliques corresponding to the divisors d of $2k+1$ with $d > 1$. To each such d there correspond $\phi(d)/2k_d$ irreducible factors, each of which has the form

$$\prod_{i=0}^{k_d-1} (x - (\zeta_d^{q^i} + \zeta_d^{-q^i})).$$

where ζ_d is a primitive d-th root of unity and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

(ii) If q is odd, then $f_k(x)$ is a product of irreducible polynomials in $\mathbb{F}_q[x]$ which occur in cliques corresponding to the odd divisors d of $4k+2$ with $d > 2$. To each such d there correspond $\phi(d)/2k_d$ irreducible factors, each of which has the form

$$\prod_{i=0}^{k_d-1} (x - (\zeta_d^{q^i} + \zeta_d^{-q^i})).$$

where ζ_d is a primitive d-th root of unity and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

(iii) If q is odd, then $g_k(x)$ is a product of irreducible polynomials in $\mathbb{F}_q[x]$ which occur in cliques corresponding to the even divisors d of $4k+2$ with $d>2$. To each such d there correspond $\phi(d)/2k_d$ irreducible factors, each of which has the form

$$\prod_{i=0}^{k_d-1}(x-(\zeta_d^{q^i}+\zeta_d^{-q^i})).$$

where ζ_d is a primitive d-th root of unity and k_d is the least positive integer such that $q^{k_d}\equiv \pm 1 \pmod{d}$.

Proof. It is easy to see that $f_k(x)=g_k(x)$ for even q. Moreover, if q is odd and d is odd, then ζ_d is a even power of a primitive $(4k+2)$-th root of unity. Similarly, if q is odd and d is even then ζ_d is an odd power of a primitive $(4k+2)$-th root of unity. The rest of proof follows from [**6**] or [**8**]. □

If k_d is the least positive integer such that $q^{k_d}\equiv 1 \pmod{d}$, then we say the order of q modulo d is k_d which is denoted by $ord_d(q)=k_d$. Similarly, if k_d is the least positive integer such that $q^{k_d}\equiv -1 \pmod{d}$, then we say the order of q modulo d is $2k_d$ which is denoted by $ord_d(q)=2k_d$. Conversely, if $ord_d(q)=2k$ then, by the definition of k_d, we can obtain that $k_d=k$. However, if $ord_d(q)=k$, then k_d is not always equal to k. Indeed, if k is even, then $k_d=\frac{k}{2}$; otherwise, $k_d=k$. Now we have the following result which tells us when $f_k(x)$ and $g_k(x)$ are irreducible polynomials in $\mathbb{F}_q[x]$.

Theorem 2.5. *Let $\mathbb{F}_q$ be a finite field with $q=p^m$. If either $f_k(x)$ or $g_k(x)$ is irreducible in $\mathbb{F}_q[x]$, then $2k+1$ must be prime. Furthermore, the following are equivalent*

(i) *$f_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$;*
(ii) *$g_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$;*
(iii) *$k=1$, or $ord_{2k+1}(q)=2k$, or $ord_{2k+1}(q)=k$ and k is odd.*

Proof. First we consider $\gcd(2k+1,p)\neq 1$. In this case, $2k+1=p^r(2t+1)$ where $r\geq 1$ and $\gcd(2t+1,p)=1$. If $f_k(x)$ or $g_k(x)$ is irreducible, then $t=0$ and $\frac{p^r-1}{2}=1$ by using the comments before Theorem 2.4. Hence $k=1$ and $2k+1=3$ is prime. In fact, $f_1(x)$ and $g_1(x)$ are linear polynomials and they are always irreducible in $\mathbb{F}_q[x]$.

Now we assume that $\gcd(2k+1,p)=1$ and $k\geq 2$. If $2k+1$ is not prime, then there are more than one divisors d of $2k+1$ such that $d>1$. Hence by Theorem 2.4, neither $f_k(x)$ nor $g_k(x)$ is irreducible in $\mathbb{F}_q[x]$. When $2k+1$ is a prime number, by Theorem 2.4, there is only one possible choice for $d=2k+1$ when q is even, and only two possible choices for d (i.e., $d=2k+1$ for $f_k(x)$ and $d=4k+2$ for $g_k(x)$) if q is odd. Hence $\phi(d)=2k$. Therefore $\phi(d)/2k_d=1$ if and only if $k_d=k$.

If q is even, then $f_k(x)=g_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ if and only if $ord_{2k+1}(q)=2k$, or $ord_{2k+1}(q)=k$ and k is odd.

If q is odd, then $f_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ if and only if $ord_{2k+1}(q)=2k$, or $ord_{2k+1}(q)=k$ and k is odd; Similarly, $g_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ if and only if $ord_{4k+2}(q)=2k$, or $ord_{4k+2}(q)=k$ and k is odd. However, since q is odd, we have $(2k+1)\mid(q^i\pm 1)$ if and only if $(4k+2)\mid(q^i\pm 1)$ for any positive integer i. Hence $g_k(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ if and only if $ord_{2k+1}(q)=2k$, or $ord_{2k+1}(q)=k$ and k is odd. □

3. Permutation polynomials

Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements. In this section, we will explain an application of generalized Lucas sequence over the prime field $\mathbb{F}_p$ in the characterization of a class of permutation polynomials of $\mathbb{F}_q$ and their compositional inverses. We recall that a polynomial is a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ onto itself. The study of permutation polynomials of a finite field goes back to 19-th century when Hermite and later Dickson pioneered this area of research. In recent years, interests in permutation polynomials have significantly increased because of their potential applications in cryptography, coding theory, and combinatorics. For more background material on permutation polynomials we refer the reader to Chapter 7 of [**12**]. In [**10**], Lidl and Mullen proposed several open problems and conjectures involving permutation polynomials of finite fields. The following is one of the open problems.

Problem 3.1 (**Lidl-Mullen**). *Determine conditions on k, r, and q so that $P(x) = x^k + ax^r$ permutes $\mathbb{F}_q$ with $a \in {\mathbb{F}_q}^*$.*

Note that we may assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q-1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$. There are many papers on permutation binomials published in the past twenty years. In particular, different types of characterizations were given. We refer the reader to [**3**], [**4**], [**5**], [**7**], [**13**], [**14**], [**15**], [**18**], [**19**], [**20**], [**21**], [**22**], [**23**], [**24**] [**25**], [**26**], [**28**], [**29**], among others.

In this section, we follow the approach from [**3**], [**4**], and [**26**] in terms of generalized Lucas sequences. We will refine a result of the characterization of PPs in [**26**] by studying the remainders of Dickson polynomials of the first kind divided by the characteristic polynomial of the associated generalized Lucas sequences. First, let us rewrite $P(x) = x^k + ax^r = x^r(x^{k-r} + a)$ and let $s = \gcd(k-r, q-1)$ and $\ell = \frac{q-1}{s}$ (here ℓ is called the index of $P(x)$, see [**2**]). Then $P(x) = x^r(x^{es} + a)$ for some e such that $(e, \ell) = 1$. If $a = b^s$ for some $b \in \mathbb{F}_q$, then $x^r(x^{es} + a)$ is a PP of $\mathbb{F}_q$ if and only if $x^r(x^{es} + 1)$ is a PP of $\mathbb{F}_q$. Hence we only concentrate on polynomials of the form $P(x) = x^r(x^{es} + 1)$ such that $\gcd(e, \ell) = 1$ from now on. Obviously, q must be odd. Otherwise, $P(0) = P(1) = 0$, a contradiction. It is quite easy to see it is necessary that $\gcd(r, s) = 1$, $\gcd(2e, \ell) = 1$ and $2^s = 1$ for $P(x) = x^r(x^{es} + 1)$ to be a PP of $\mathbb{F}_q$ ([**26**]). Moreover, $\gcd(2r + es, \ell) = 1$. Otherwise, if $\gcd(2r + es, \ell) = d > 1$, then, for a primitive ℓ-th root of unity ζ,

$$\begin{aligned} (\zeta^{\ell-\frac{\ell}{d}})^r(\zeta^{(\ell-\frac{\ell}{d})e}+1)^s &= \zeta^{-\frac{\ell}{d}r}\zeta^{-\frac{\ell}{d}es}(\zeta^{\frac{\ell}{d}e}+1)^s \\ &= \zeta^{-\frac{\ell}{d}(2r+es)}\zeta^{\frac{\ell}{d}r}(\zeta^{\frac{\ell}{d}e}+1)^s \\ &= \zeta^{\frac{\ell}{d}r}(\zeta^{\frac{\ell}{d}e}+1)^s. \end{aligned}$$

By Theorem 1 (f) [**26**] (or Lemma 2.1 in [**28**]), $P(x) = x^r(x^{es} + 1)$ is not a permutation polynomial of $\mathbb{F}_q$. Therefore $\gcd(2r + es, \ell) = 1$.

Now we collect all these necessary conditions for $P(x) = x^r(x^{es} + 1)$ to be a PP as follows:

$$\gcd(r, s) = 1, \gcd(2e, \ell) = 1, \gcd(2r + es, \ell) = 1, \text{ and } 2^s = 1. \tag{3.1}$$

For $\ell = 3$, the conditions in (3.1) are sufficient to determine $P(x)$ is a PP of $\mathbb{F}_q$. However, for $\ell \geq 3$, it turns out not to be the case (for example, see [**3**], [**4**]). For general ℓ, a characterization of PPs of the form $x^r(x^{es} + 1)$ in terms of generalized Lucas sequence of order $k := \frac{\ell-1}{2}$ is given in [**26**]. In the following we study the remainders of Dickson polynomials of the first kind divided by characteristic polynomials of generalized Lucas sequences and then improve the result in [**26**].

Let $k \geq 1$ and $R_{n,k}(x)$ be the remainder of degree n Dickson polynomial $D_n(x)$ of the first kind divided by $g_k(x)$. Because all roots of $g_k(x)$ are of form $\eta^t + \eta^{-t}$ where $1 \leq t \leq 2k$ is odd and η is a fixed primitive $(4k+2)$-th root of unity, it is clear that $R_{4k+2+n,k}(x) = R_{n,k}(x)$. We now give an explicit description of $R_{n,k}(x)$ for any $0 \leq n \leq 4k+1$ by using certain divisibility properties of $g_k(x)$.

THEOREM 3.2. *Let $k \geq 1$ and $R_{n,k}(x)$ be the remainder of degree n Dickson polynomial $D_n(x)$ of the first kind divided by $g_k(x)$. Then we have*

$$R_{n,k}(x) = \begin{cases} D_n(x), & if\ 0 \leq n \leq k-1; \\ g_{k-1}(x), & if\ n = k; \\ -R_{2k+1-n,k}(x), & if\ k+1 \leq n \leq 2k+1; \\ R_{4k+2-n,k}(x), & if\ 2k+2 \leq n \leq 4k+1; \end{cases}$$

PROOF. If $k = 1$, then $g_1(x) = x - 1$ and it is easy to compute directly that $R_{0,1}(x) = 2$, $R_{1,1}(x) = 1$, $R_{2,1}(x) = -1$, $R_{3,1}(x) = -2$, $R_{4,1}(x) = -1$, and $R_{5,1}(x) = 1$. Hence the results hold for $k = 1$. So we assume that $k \geq 2$. Because $\deg(D_n(x)) = n$ and $\deg(g_k(x)) = k$, we have $R_{n,k}(x) = D_n(x)$ for $1 \leq n \leq k-1$.

Next we prove that $D_k(x) = g_k(x) + g_{k-1}(x)$. We first show that all roots of $g_{k-1}(x)$ are roots of $D_k(x) - g_k(x)$. Indeed, let θ be a primitive $(4k-2)$-th root of unity. Then for any odd t, $D_k(\theta^t + \theta^{-t}) - g_k(\theta^t + \theta^{-t}) = \theta^{kt} + \theta^{-kt} - \frac{\theta^{2kt+1}+1}{\theta^{kt}(\theta^t+1)} = \frac{\theta^{2kt}+\theta^t}{\theta^{kt}(\theta^t+1)} = 0$. Since $\deg(D_k(x) - g_k(x)) = \deg(g_{k-1}(x))$ and both $D_k(x) - g_k(x)$ and $g_{k-1}(x)$ are monic, we have $D_k(x) = g_k(x) + g_{k-1}(x)$ and thus $R_{k,k}(x) = g_{k-1}(x)$.

Now we prove that $R_{n,k}(x) = -R_{2k+1-n,k}(x)$ for all $k+1 \leq n \leq 2k+1$. Equivalently, we prove that $R_{k+i,k}(x) = -R_{k-i+1,k}(x)$ for all $1 \leq i \leq k+1$, namely, $g_k(x) \mid (D_{k+i}(x) + D_{k-i+1}(x))$. Indeed, for any odd t such that $1 \leq t \leq 2k-1$ and a fixed primitive $(4k+2)$-th root of unity η, we have $D_{k+i}(\eta^t + \eta^{-t}) + D_{k-i+1}(\eta^t + \eta^{-t}) = \eta^{(k+i)t} + \eta^{-(k+i)t} + \eta^{(k-i+1)t} + \eta^{-(k-i+1)t} = \eta^{-(k-i+1)t}(\eta^{(2k+1)t} + 1) + \eta^{(k-i+1)t}(\eta^{-(2k+1)t} + 1) = 0$. Hence all roots of $g_k(x)$ are roots of $D_{k+i}(x) + D_{k-i+1}(x)$.

Similarly we can show that $g_k(x) \mid (D_{2k+1+i}(x) - D_{2k+1-i}(x))$ for all $1 \leq i \leq 2k$ and thus $R_{n,k}(x) = R_{4k+2-n,k}(x)$ for all $2k+2 \leq n \leq 4k+1$. □

Table 3 gives a list of $R_{n,k}(x)$'s for small $k \geq 2$'s. We note that the degree of $R_{n,k}(x)$ is at most $k-1$. Any remainder is either a Dickson polynomial of degree $\leq k-1$ or $g_{k-1}(x)$ or a negation of the above. Therefore, for the last two columns, we only list the partial information. The rest entries can be found by following the same symmetry pattern as in the first two columns.

Let L be left shift operator on the generalized Lucas sequence $\mathbf{a} = (a_0, a_1, \ldots)$ (see [**9**] for more information on LFSR sequences and shift operators). Namely, $L\mathbf{a} = (a_1, a_2, \ldots)$. For any $f(x) = x^n - c_{n-1}x^{n-1} - \ldots - c_0$, we write $f(L) = L^n - c_{n-1}L^{n-1} - \ldots - c_0 I$ where $I = L^0$ such that $I\mathbf{a} = \mathbf{a}$. Because $g_k(x)$ is a characteristic polynomial of generalized Lucas sequence $\mathbf{a}$, we obtain $g_k(L)\mathbf{a} = 0$. This means that $g_k(L)(a_i) = 0$ for each $i = 0, 1, \ldots$. Since $R_{n,k}(x)$ is the remainder of degree n Dickson polynomial $D_n(x)$ of the first kind divided by $g_k(x)$, we also obtain that $R_{n,k}(L)\mathbf{a} = D_n(L)\mathbf{a}$ and thus $R_{n,k}(L)(a_i) = D_n(L)(a_i)$ for each $i =$

TABLE 3. $R_{n,k}(x)$ for small k's

$R_{n,k}(x)$	$k=2$	$k=3$	$k=4$	$k=5$
$n=0$	2	2	2	2
$n=1$	x	x	x	x
$n=2$	$x-1$	x^2-2	x^2-2	x^2-2
$n=3$	$-x+1$	x^2-x-1	x^3-3x	x^3-3x
$n=4$	$-x$	$-(x^2-x-1)$	x^3-x^2-2x+1	x^4-4x^2+2
$n=5$	-2	$-(x^2-2)$	$-(x^3-x^2-2x+1)$	$x^4-x^3-3x^2+2x+1$
$n=6$	$-x$	$-x$	$-(x^3-3x)$	$-(x^4-x^3-3x^2+2x+1)$
$n=7$	$-x+1$	-2	$-(x^2-2)$	$-(x^4-4x^2+2)$
$n=8$	$x-1$	$-x$	$-x$	$-(x^3-3x)$
$n=9$	x	$-(x^2-2)$	-2	$-(x^2-2)$
$n=10$		$-(x^2-x-1)$		$-x$
$n=11$		x^2-x-1		-2
$n=12$		x^2-2		
$n=13$		x		

$0, 1, \ldots$. Hence we have the following characterization of permutation polynomials of the form $x^r(x^{es}+1)$ over $\mathbb{F}_q$.

THEOREM 3.3. *Let $q = p^m$ be an odd prime power and $q-1 = \ell s$ with $\ell \geq 3$ and $\gcd(e, \ell) = 1$. Let $k := \frac{\ell-1}{2}$. Then $P(x) = x^r(x^{es}+1)$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(r, s) = 1$, $\gcd(2r + es, \ell) = 1$, $2^s = 1$, and*

$$R_{j_c,k}(L)(a_{cs}) = -1 \text{ for all } c = 1, \ldots, \ell-1, \tag{3.2}$$

where a_{cs} is the cs-th term of the generalized Lucas sequence $\{a_i\}_{i=0}^{\infty}$ of order k over $\mathbb{F}_p$, $j_c = c(2e^{\phi(\ell)-1}r + s) \bmod 2\ell$, $R_{j_c,k}(x)$ is the remainder of Dickson polynomial $D_{j_c}(x)$ of the first kind divided by $g_k(x)$. In particular, all j_c are distinct even numbers between 1 and 2ℓ.

PROOF. As we discussed earlier, it is necessary to have $\gcd(r, s) = 1, \gcd(2r + es, \ell) = 1$, and $2^s = 1$ for $P(x)$ to be a PP of $\mathbb{F}_q$. Under these conditions, by Corollary 3 of [**26**], we have $P(x) = x^r(x^{es}+1)$ is a PP of $\mathbb{F}_q$ if and only if

$$\sum_{j=0}^{j_c} t_j^{(j_c)} a_{cs+j} = -1, \tag{3.3}$$

for all $c = 1, \ldots, \ell-1$, where $t_j^{(j_c)}$ is the coefficient of x^j in $D_{j_c}(x)$. Moreover, Equation (3.3) is equivalent to $D_{j_c}(L)(a_{cs}) = -1$ for all $c = 1, \ldots, \ell-1$. However, $D_{j_c}(L)(a_{cs}) = R_{j_c,k}(L)(a_{cs})$, hence we are done. □

REMARK 3.4. We emphasize that j_c' s are *all distinct even* numbers from 2 and $4k$. Since we obtained explicit and simple expressions for $R_{j_c,k}(x)$ in Theorem 3.2, the coefficients of $R_{j_c,k}(x)$ can be obtained easily. Moreover, the above result has significant advantage over Corollary 3 in [**26**] since j_c can be as large as $4k$ while all the degrees of $R_{j_c,k}(x)$ are less than k. Abusing the notation $t_j^{(j_c)}$, we can rewrite the condition (3.2) as

$$\sum_{j} t_j^{(j_c)} a_{cs+j} = -1 \text{ for all } c = 1, \ldots, \ell-1 \tag{3.4}$$

where $t_j^{(j_c)}$ represents the coefficient of x^j in $R_{j_c,k}(x)$.

Remark 3.5. In [**4**], we proved that if $p \equiv -1 \pmod{\ell}$ or $p \equiv 1 \pmod{\ell}$ and $\ell \mid m$ then $P(x) = x^r(x^{es}+1)$ is a PP of $\mathbb{F}_q$ where $q = p^m$ if and only if $\gcd(2e, \ell) = 1$, $\gcd(r, s) = 1$, $2^s = 1$, $\gcd(2r + es, \ell) = 1$. In particular, in the case that $p \equiv 1 \pmod{\ell}$ and $\ell \mid m$, the condition $\gcd(2r + es, \ell) = 1$ is redundant ([**1**]). Furthermore, the period of the generalized Lucas sequence $\mathbf{a}$ over $\mathbb{F}_p$ divides s. Hence in this case, we always have $R_{2c,k}(L)(k) = -1$ for all $c = 1, 2, \ldots, \ell - 1$.

Finally we consider a related question which is to find the compositional inverse polynomial $Q(x) = \sum_{i=0}^{q-2} b_i x^i$ of a given permutation polynomial $P(x)$. In 1991, Mullen propose the following problem ([**16**]).

Problem 3.6 (**Mullen**). *Compute the coefficients of the inverse polynomial of a permutation polynomial efficiently.*

It is well-known that

$$\sum_{s\in\mathbb{F}_q} s^{q-1-n}Q(s) = \sum_{s\in\mathbb{F}_q} s^{q-1-n}\sum_{i=0}^{q-2} b_i s^i = \sum_{i=0}^{q-2} b_i \sum_{s\in\mathbb{F}_q} s^{q-1+i-n} = -b_n,$$

for each $0 \le n \le q-2$. Since $P(x)$ is a permutation polynomial of $\mathbb{F}_q$,

$$b_n = -\sum_{P(s)\in\mathbb{F}_q} (P(s))^{q-1-n} Q(P(s)) = -\sum_{s\in\mathbb{F}_q} sP(s)^{q-1-n}.$$

Set $P(x)^{q-1-n} \pmod{x^q - x} = c_0 + c_1 x + \ldots + c_{q-1}x^{q-1}$, we have

$$b_n = -\sum_{s\in\mathbb{F}_q} sP(s)^{q-1-n} = -\sum_{s\in\mathbb{F}_q} s\sum_{i=0}^{q-1} c_i s^i = c_{q-2}. \tag{3.5}$$

Using Equation (3.5), Muratović-Ribić [**17**] described the inverse polynomial of $P(x) = x^r f(x^s)^{\frac{q-1}{s}} \in \mathbb{F}_q[x]$ recently. In [**27**], we generalized the result to the inverse polynomials of permutation polynomials of the form $x^r f(x^s)$. In particular, for binomials $x^r(x^{es}+1)$, we have given the following characterization of the inverse in terms of generalized Lucas sequences (Theorem 3.1 and Equation (5) in [**27**]).

Theorem 3.7. *Let p be an odd prime and $q = p^m$, $\ell \ge 3$ is odd, $q - 1 = \ell s$, and $\gcd(e, \ell) = 1$. If $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1 x + \cdots + b_{q-2}x^{q-2}$ is the inverse polynomial of $P(x)$ modulo $x^q - x$, then there are at most ℓ nonzero coefficients b_n. These n's satisfy $n \equiv r^{-1} \pmod{s}$. Let $\bar{r} = r^{-1} \bmod s$ and $n_c = q - 1 - cs - \bar{r} = (\ell - c)s - \bar{r}$ with $c = 0, 1, \cdots, \ell - 1$. Then*

$$b_{q-1-n_c} = \frac{1}{\ell}\left(2^{n_c} + \sum_{j=0}^{u_c} t_j^{(u_c)} a_{n_c+j}\right), \tag{3.6}$$

where $u_c = 2(cr + \frac{r\bar{r}-1}{s})e^{\phi(\ell)-1} + cs + \bar{r} \bmod 2\ell$, $t_j^{(u_c)}$ is the coefficient of x^j of Dickson polynomial $D_{u_c}(x)$ of the first kind, and $\{a_i\}_{i=0}^{\infty}$ is the generalized Lucas sequence of order $\frac{\ell-1}{2}$.

Here we improve this result by replacing $D_{u_c}(x)$ with $R_{u_c,k}(x)$ where $k := \frac{\ell-1}{2}$ and $\ell = \frac{q-1}{s}$.

Theorem 3.8. *Let p be an odd prime and $q = p^m$, $\ell \geq 3$ is odd, $q-1 = \ell s$, and $\gcd(e,\ell) = 1$. Let $k := \frac{\ell-1}{2}$. If $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1x + \ldots + b_{q-2}x^{q-2}$ is the inverse polynomial of $P(x)$ modulo $x^q - x$, then there are at most ℓ nonzero coefficients b_n. These n's satisfy $n \equiv r^{-1} \pmod{s}$. Let $\bar{r} = r^{-1} \bmod s$ and $n_c = q-1-cs-\bar{r} = (\ell-c)s - \bar{r}$ with $c = 0, 1, \ldots, \ell-1$. Then*

$$b_{cs+\bar{r}} = \frac{1}{\ell}(2^{s-\bar{r}} + R_{u_c,k}(L)(a_{n_c})), \tag{3.7}$$

where a_{n_c} is the n_c-th term of the generalized Lucas sequence $\{a_i\}_{i=0}^{\infty}$ of order k over $\mathbb{F}_p$, $u_c = c(2re^{\phi(\ell)-1}+s) + 2(\frac{r\bar{r}-1}{s})e^{\phi(\ell)-1} + \bar{r} \bmod 2\ell$, $R_{u_c,k}(x)$ is the remainder of Dickson polynomial $D_{u_c}(x)$ of the first kind divided by $g_k(x)$.

Proof. Equation (3.6) in Theorem 3.7 can be rewritten as

$$b_{q-1-n_c} = \frac{1}{\ell}\left(2^{n_c} + D_{u_c}(L)(a_{n_c})\right). \tag{3.8}$$

Since $D_{u_c}(L)(a_i) = R_{u_c,k}(L)(a_i)$ and $q-1-n_c = cs+\bar{r}$, we are done. □

Remark 3.9. Again the advantage of this version over Theorem 3.1 in [**27**] is that the degrees of $R_{u_c,k}(x)$ are less than k and thus there are much fewer terms involved in the summation of $R_{u_c,k}(L)(a_{n_c})$. We also note that u_c's are all distinct odd numbers from 1 to $2\ell - 1$ for $c = 0, \ldots, \ell-1$.

In particular, if $\mathbf{a}$ is periodic with period dividing s, then the above result reduces to

Corollary 3.10. *Let p be an odd prime and $q = p^m$, $\ell \geq 3$ is odd, $q-1 = \ell s$, and $\gcd(e,\ell) = 1$. If $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1x + \ldots + b_{q-2}x^{q-2}$ is the inverse polynomial of $P(x)$ modulo $x^q - x$. Assume the period of the generalized Lucas sequence $\mathbf{a} = \{a_i\}_{i=0}^{\infty}$ of order $k := \frac{\ell-1}{2}$ over $\mathbb{F}_p$ divides s. Then*

$$b_{cs+\bar{r}} = \frac{1}{\ell}(2^{s-\bar{r}} + R_{u_c,k}(L)(a_{s-\bar{r}})), \ \textit{for}\ c = 0, 1, \ldots, \ell-1. \tag{3.9}$$

where $\bar{r} = r^{-1} \bmod s$, $u_c = c(2re^{\phi(\ell)-1}+s) + 2(\frac{r\bar{r}-1}{s})e^{\phi(\ell)-1} + \bar{r} \bmod 2\ell$, $R_{u_c,k}(x)$ is the remainder of Dickson polynomial $D_{u_c}(x)$ of the first kind divided by $g_k(x)$.

Example 3.11. Let $\ell = 3$ and $\gcd(e,3) = 1$. In this case, $k = 1$ and $g_1(x) = x - 1$. So $\{a_i\}_{i=0}^{\infty}$ is the constant sequence $1, 1, \ldots$. Moreover, by Theorem 3.2, we have $R_{2,1}(x) = -1$ and $R_{4,1}(x) = -1$. Hence $R_{2,1}(L)(a_{cs}) = R_{4,1}(L)(a_{cs}) = -a_{cs} = -1$ is automatically satisfied. Therefore, by Theorem 3.3, binomial $x^r(x^{es}+1)$ is a PP of $\mathbb{F}_q$ iff $\gcd(r,s) = 1$, $\gcd(2r+es, 3) = 1$, and $2^s = 1$.

Again, by Theorem 3.2, we obtain that $R_{1,1}(x) = 1$, $R_{3,1}(x) = -2$, $R_{5,1}(x) = 1$. Let $\bar{r} = r^{-1} \bmod s$ and $u_c = c(2re+s) + 2\frac{r\bar{r}-1}{s}e + \bar{r}$. Then we have

$$R_{u_c,1}(L)(a_{s-\bar{r}}) = \begin{cases} a_{s-\bar{r}} = 1, & if\ u_c = 1, 5; \\ -2a_{s-\bar{r}} = -2, & if\ u_c = 3. \end{cases}$$

Moreover, by Theorem 3.8, we obtain

$$b_{cs+\bar{r}} = \begin{cases} \frac{1}{3}(2^{s-\bar{r}} + 1), & if\ u_c = 1, 5; \\ \frac{1}{3}(2^{s-\bar{r}} - 2), & if\ u_c = 3. \end{cases}$$

Example 3.12. Let $\ell = 5$ and $\gcd(e,5)=1$. In this case, we have that $k=2$, $g_2(x) = x^2 - x - 1$ and $\{a_i\}_{i=0}^{\infty}$ is the ordinary Lucas sequence. It is easy to see from Theorem 3.2 that $R_{2,2}(x) = x-1$, $R_{4,2}(x) = -x$, $R_{6,2}(x) = -x$, and $R_{8,2}(x) = x-1$. Hence

$$R_{j_c,2}(L)(a_{cs}) = \begin{cases} a_{cs+1} - a_{cs}, & if\ j_c = 2, 8; \\ -a_{cs+1}, & if\ j_c = 4, 6. \end{cases}$$

Under the conditions $\gcd(r,s)=1$, $\gcd(e,5)=1$, $\gcd(2r+es,5)=1$, and $2^s = 1$, we obtain from Theorem 3.3 that $R_{j_c,2}(L)(a_{cs}) = -1$ iff either $a_{s+1} - a_s = a_{4s+1} - a_{4s} = -1$ and $a_{2s+1} = a_{3s+1} = 1$ or $a_{2s+1} - a_{2s} = a_{3s+1} - a_{3s} = -1$ and $a_{s+1} = a_{4s+1} = 1$. By a useful property of Lucas sequence, i.e., $a_m a_n = a_{m+n} + (-1)^n a_{m-n}$ (in particular, $a_n^2 = a_{2n} + (-1)^n 2$), we can easily deduce that $R_{j_c,2}(L)(a_{cs}) = -1$ iff $a_s = 2$. In particular, $\{a_n\}$ is s-periodic (see Lemma 6 in [**25**]).

Moreover, we obtain from Theorem 3.2 that $R_{1,2}(x) = x$, $R_{3,2}(x) = 1-x$, $R_{5,2}(x) = -2$, $R_{7,2}(x) = 1-x$, and $R_{9,2}(x) = x$. Let $\bar{r} = r^{-1} \bmod s$ and $u_c = c(2re^3 + s) + 2\frac{r\bar{r}-1}{s}e^3 + \bar{r}$. Therefore

$$R_{u_c,2}(L)(a_{s-\bar{r}}) = \begin{cases} a_{s-\bar{r}+1}, & if\ u_c = 1, 9; \\ a_{s-\bar{r}} - a_{s-\bar{r}+1}, & if\ u_c = 3, 7; \\ -2a_{s-\bar{r}}, & if\ u_c = 5; \end{cases}$$

and we obtain from Theorem 3.8 that

$$b_{cs+\bar{r}} = \begin{cases} \frac{1}{5}(2^{s-\bar{r}} + a_{s-\bar{r}+1}), & if\ u_c = 1, 9; \\ \frac{1}{5}(2^{s-\bar{r}} + a_{s-\bar{r}} - a_{s-\bar{r}+1}), & if\ u_c = 3, 7; \\ \frac{1}{5}(2^{s-\bar{r}} - 2a_{s-\bar{r}}), & if\ u_c = 5. \end{cases}$$

Example 3.13. For $\ell = 7$ and $\gcd(e,7) = 1$, we have that $k=3$ and $g_3(x) = x^3 - x^2 - 2x + 1$. We refer the reader to [**3**] for a complete description of generalized Lucas sequences when $P(x) = x^r(x^{es}+1)$ is a permutation polynomial of $\mathbb{F}_q$. In this case, $\{a_n\}_{n=0}^{\infty}$ is not always s-periodic. By Theorem 3.8 again, the inverse $Q(x)$ of $P(x)$ satisfies

$$b_{cs+\bar{r}} = \begin{cases} \frac{1}{7}(2^{n_c} + a_{n_c+1}), & if\ u_c = 1, 13; \\ \frac{1}{7}(2^{n_c} - a_{n_c} - a_{n_c+1} + a_{n_c+2}), & if\ u_c = 3, 11; \\ \frac{1}{7}(2^{n_c} + 2a_{n_c} - a_{n_c+2}), & if\ u_c = 5, 9; \\ \frac{1}{7}(2^{n_c} - 2a_{n_c}), & if\ u_c = 7; \end{cases}$$

where $\bar{r} = r^{-1} \bmod s$, $n_c = (7-c)s - \bar{r}$ and $u_c = c(2re^5 + s) + 2\frac{r\bar{r}-1}{s}e^5 + \bar{r} \bmod 14$.

References

[1] A. Akbary, S. Alaric, and Q. Wang, *On some classes of permutation polynomials*, *Int. J. Number Theory* **4** (2008), no. 1, 121–133

[2] A. Akbary, D. Ghioca, and Q. Wang, *On permutation polynomials of prescribed shape*, Finite Fields Appl. **15** (2009), 207-213.

[3] A. Akbary and Q. Wang, *On some permutation polynomials*, Int. J. Math. Math. Sci., **16** (2005), 2631-2640.

[4] A. Akbary and Q. Wang, *A generalized Lucas sequence and permutation binomials*, Proc. Amer. Math. Soc., **134** (2006), no 1, 15-22.

[5] A. Akbary and Q. Wang, *On polynomials of the form* $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci. (2007), Art. ID 23408, 7 pp.

[6] M. Bhargava and M. E. Zieve, *Factorizing Dickson polynomials over finite fields*, Finite Fields Appl. **5** (1999), 103-111.

[7] W. S. Chou, *Binomial permutations of finite fields*, Bull. Austral. Math. Soc. **38** (1988), 325-327.

[8] W. S. Chou, *The factorization of Dickson polynomials over finite fields*, Finite Fields Appl. **3** (1997), 84-96.

[9] S. W. Golomb and G. Guang, *Signal Design for Good Correlation*, Cambridge University Press, 2005.

[10] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* **100** (1993), 71-74.

[11] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Longman Scientific and Technical, 1993.

[12] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[13] A. Masuda, D. Panario, and Q. Wang, *The number of permutation binomials over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes*, Electron. J. Combin. **13** (2006), no 1, Research paper 65, 15pp.

[14] A. Masuda and M. E. Zieve, *Permutation binomials over finite fields*, Trans. Amer. Math. Soc. **361** (2009), no. 8, 4169–4180.

[15] R. A. Mollin and C. Small, *On permutation polynomials over finite fields* , Internat. J. Math. Math. Sci. **10** (1987), no. 3, 535–543.

[16] G. L. Mullen, *Permutation polynomials over finite fields*, in: Finite fields, Coding Theory, and Advances in Communication and Computing, Las Vegas, NY, 1991, pp. 131-151.

[17] A. Muratović-Ribić, *A note on the coefficients of inverse polynomials*, Finite Fields Appl. **13** (2007), no. 4, 977-980.

[18] H. G. Park, *On certain binomials over finite fields*, J. Appl. Math. & Computing **18** (2005), no. 1-2, 679-684.

[19] C. Small, *Permutation binomials*, Internat. J. Math. & Math. Sci. **13** (1990), no. 2, 337-342.

[20] C. Small, *Arithmetic of finite fields*, Monographs and Textbooks in Pure and Applied Mathematics, 148. Marcel Dekker, Inc., New York, 1991.

[21] G. Turnwald, *Permutation polynomials of binomial type*, Contributions to general algebra **6**, 281-286.

[22] D. Wan, *Permutation polynomials over finite fields*, Acta Mathematica Sinica (New Series), Vol. 3, **1** (1987), 1-5.

[23] D. Wan, *Permutation polynomials over finite fields*, Acta Mathematica Sinica (New Series), Vol. 10, **1** (1994), 30-35.

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

[25] L. Wang, *On permutation polynomials*, Finite Fields and Their Applications **8** (2002), 311–322.

[26] Q. Wang, *Cyclotomic mapping permutation polynomials*, Sequences, Subsequences, and Consequences 2007 (Los Angeles), Lecture Notes in Computer Science 4893, pp. 119-128.

[27] Q. Wang, *On inverse permutation polynomials*, Finite Fields Appl. **15** (2009), 207-213.

[28] M. E. Zieve, *Some families of permutation binomials over finite fields*, Int. J. Number Theory **4** (2008), no. 5, 851–857.

[29] M. E. Zieve, *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$*, Proc. Amer. Math. Soc. **137** (2009), no. 7, 2209-2216.

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

E-mail address: `wang@math.carleton.ca`