Finite Fields and Their Applications 15 (2009) 207–213

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On inverse permutation polynomials ☆

Qiang Wang

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6, Canada

ARTICLE INFO

Article history:
Received 18 June 2008
Revised 30 September 2008
Available online 24 December 2008
Communicated by Gary L. Mullen

Keywords:
Permutation polynomials
Inverse polynomials
Generalized Lucas sequence
Finite fields

ABSTRACT

We give an explicit formula of the inverse polynomial of a permutation polynomial of the form $x^r f(x^s)$ over a finite field $\mathbb{F}_q$ where $s \mid q-1$. This generalizes results in [A. Muratović-Ribić, A note on the coefficients of inverse polynomials, Finite Fields Appl. 13 (4) (2007) 977–980] where $s=1$ or $f = g^{\frac{q-1}{s}}$ were considered respectively. We also apply our result to several interesting classes of permutation polynomials.

1. Introduction

Let p be prime, $q=p^m$, and $\mathbb{F}_q$ be a finite field of order q. Let $P(x)$ be a permutation polynomial (PP) over $\mathbb{F}_q$ and $Q(x)$ be the compositional inverse polynomial of $P(x)$. By the modulo reduction $x^q - x$, we only need to consider polynomials of degree less than or equal to $q-1$. Because a permutation polynomial can not have degree $q-1$, we let $P(x) = a_0 + a_1 x + \cdots + a_{q-2}x^{q-2}$ be a permutation polynomial of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1 x + \cdots + b_{q-2}x^{q-2}$ be the inverse polynomial of $P(x)$ modulo $x^q - x$. In [5], G.L. Mullen posed the problem of computing the coefficients of the inverse polynomial of a permutation polynomial efficiently (Problem 10). Recently Muratović-Ribić [6] characterized all the coefficients of the inverse polynomial of a permutation polynomial of the form $x^r f(x^s)^{(q-1)/s}$ as follows:

Theorem 1.1 *(Muratović-Ribić). Let $P(x) = x^r f(x^s)^{\frac{q-1}{s}} \in \mathbb{F}_q[x]$ where $r \geqslant 1$ is an integer with $\gcd(r, q-1) = 1$, s is a divisor of $q-1$ and $f(x) \in \mathbb{F}_q[x]$ is a polynomial without roots in $\mathbb{F}_q$. Denote by $Q(x) = b_0 + b_1 x + \cdots + b_{q-2}x^{q-2}$ the inverse of permutation polynomial $P(x)$ modulo $x^q - x$. Let k_0 be the*

☆ Research is partially supported by NSERC of Canada.

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

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.12.003

least positive integer for which there exists a positive integer l_0 such that $l_0 s = k_0 r + 1$ and

$$f\left(x^s\right)^{\frac{q-1}{s}k_0} \equiv \sum_{i=0}^{(q-1)/s} d_i x^{is} \pmod{x^q - x}.$$

Then $b_n \neq 0$ only if $s \mid rn-1$. Moreover, if $b_n \neq 0$, then the following holds:

(i) *If $rn \not\equiv 1 \pmod{q-1}$ and $i \equiv \frac{rn-1}{s} \pmod{\frac{q-1}{s}}$ then $b_n = d_i$.*
(ii) *If $rn \equiv 1 \pmod{q-1}$ then $b_n = d_0 + d_{(q-1)/s}$.*

The method used in the proof of Theorem 1.1 is based on Eq. (3) in [6] which applies to more general polynomial $P(x)$, for example, $P(x) = x^r f(x^s)$ where $s = 1$.

It is well known that any nonconstant polynomial $h(x) \in \mathbb{F}_q[x]$ can be written as $ax^r f(x^s) + b$ where $a \neq 0$ and $s \mid q-1$ (see for example [1]). To find the inverse of $h(x)$, it is enough to find the inverse of permutation polynomial $x^r f(x^s)$. We refer to [4] or [8] for some general characterization of permutation polynomials $P(x) = x^r f(x^s)$. For $s = 1$, an explicit formula of the inverse of permutation polynomial $x^r f(x)$ is obtained directly from Eq. (3) in [6]. In this paper, we use the similar method as in [6] to give an explicit formula of the inverse polynomial of a permutation polynomial of the form $x^r f(x^s)$ over a finite field $\mathbb{F}_q$ for any $s \mid q-1$ (Theorem 2.1). We also apply Theorem 2.1 to several interesting classes of permutation polynomials considered in [4]. These results (Corollaries 2.3, 2.4) are presented in Section 2. Finally we explore the connection (Theorem 3.1) between inverse polynomials of permutation binomials of the form $x^r(x^{es}+1)$ over $\mathbb{F}_q$ and so-called generalized Lucas sequences over $\mathbb{F}_p$. Some examples of inverse polynomials of permutation binomials are also provided in Section 3.

2. General results

Let us assume that $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$. It is well known that if $P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ then we must have $(r, s) = 1$. Hence the inverse of r modulo s exists and we denote it by $\bar{r} = r^{-1} \bmod s$. The notation $a = b \bmod c$ means that a is an integer such that $0 \leqslant a < c$ and $a \equiv b \pmod{c}$. We will use this notation and the fact $\bar{r} = r^{-1} \bmod s$ frequently later on.

First we show that the inverse polynomial $Q(x)$ of $P(x) = x^r f(x^s)$ has at most $\ell := \frac{q-1}{s}$ nonzero coefficients and give the explicit formula to compute these coefficients. We assume that $\ell \geqslant 2$ in this paper since $\ell = 1$ is the trivial case.

Theorem 2.1. *Let $P(x) = x^r f(x^s) \in \mathbb{F}_q[x]$ be a permutation polynomial of $\mathbb{F}_q$ where $r \geqslant 1$, $s = \frac{q-1}{\ell}$, $\ell \geqslant 2$ is a divisor of $q-1$. Denote by $Q(x) = b_0 + b_1 x + \cdots + b_{q-2}x^{q-2}$ the inverse polynomial of $P(x)$ modulo $x^q - x$. Then the following holds.*

(i) *If $b_n \neq 0$, then $s \mid (rn-1)$. In particular, there are at most ℓ such nonzero b_n's such that $0 \leqslant n \leqslant q-2$ and $n \equiv r^{-1} \pmod{s}$. That is, $n = is + \bar{r}$ where $i = 0, \ldots, \ell-1$ and $\bar{r} = r^{-1} \bmod s$.*
(ii) *Let $\bar{a} \equiv \frac{r\bar{r}-1}{s} \pmod{\ell}$. Then*

$$b_{is+\bar{r}} = \frac{1}{\ell}\sum_{t=0}^{\ell-1} \zeta^{-(ir+\bar{a})t} f\left(\zeta^t\right)^{q-1-\bar{r}-is}, \quad i = 0, \ldots, \ell-1,$$

where ζ is a primitive ℓth root of unity.
(iii) *For each $i = 0, \ldots, \ell-1$, let $f(x^s)^{q-1-\bar{r}-is} \equiv \sum_{j=0}^{\ell} d_{i,j} x^{js} \pmod{x^q - x}$ and $m_i = ir + \bar{a} \bmod \ell$. Then $b_{is+\bar{r}} = d_{i,m_i}$ if $m_i \neq 0$ and $b_{is+\bar{r}} = d_{i,0} + d_{i,\ell}$ if $m_i = 0$.*

Proof. By Eq. (3) in [6],

$$b_n = -\sum_{x\in\mathbb{F}_q} xP(x)^{q-1-n} = -\sum_{x\in\mathbb{F}_q} x\sum_{i=0}^{q-1} c_i x^i = c_{q-2},$$

where $P(x)^{q-1-n} \pmod{x^q - x} = c_0 + c_1x + \cdots + c_{q-1}x^{q-1}$. If b_n is nonzero, then the coefficient of x^{q-2} in the expansion of $P(x)^{q-1-n}$ is nonzero. Hence there exists some j such that $js + r(q-1) - rn \equiv q-2 \pmod{q-1}$ and thus $js \equiv rn - 1 \pmod{q-1}$. Therefore, $s \mid (rn-1)$. That is, $rn \equiv 1 \pmod{s}$. Because $(r,s) = 1$, we have $n \equiv r^{-1} \pmod{s}$. Therefore there are at most ℓ nonzero coefficients in the inverse polynomial $Q(x)$ corresponding to $n \equiv r^{-1} \pmod{s}$. Hence $n = is + \bar{r}$ for $i = 0,\dots,\ell-1$ where $\bar{r} = r^{-1} \bmod s$. It is therefore straightforward to obtain $b_{is+\bar{r}} = -\sum_{x\in\mathbb{F}_q} xP(x)^{q-1-is-\bar{r}} = \frac{1}{\ell}\sum_{t=0}^{\ell-1} \zeta^{-(ir+\bar{a})t} f(\zeta^t)^{q-1-\bar{r}-is}$.

Finally, $q-1 = \ell s$ implies that $-s$ and $\frac{1}{\ell}$ are the same in $\mathbb{F}_q$. Since $m_i = ir + \bar{a} \bmod \ell$, we have

$$\begin{aligned}\frac{1}{\ell}\sum_{t=0}^{\ell-1} \zeta^{-(ir+\bar{a})t} f\left(\zeta^t\right)^{q-1-\bar{r}-is} &= -s\sum_{t=0}^{\ell-1} \zeta^{-(ir+\bar{a})t} f\left(\zeta^t\right)^{q-1-\bar{r}-is} \\ &= -\sum_{x\in\mathbb{F}_q} x^{q-1-m_i s} f\left(x^s\right)^{q-1-\bar{r}-is}.\end{aligned}$$

However, the last term is equal to d_{i,m_i} if $m_i \neq 0$ and is equal to $d_{i,0} + d_{i,\ell}$ otherwise. $\square$

Remark. For positive integers n, ℓ, a, the lacunary sum for the coefficient $C(n,j,k)$ of x^j in the polynomial expansion of $f(x)^n = (f_0 + f_1x + f_2x^2 + \cdots + f_kx^k)^n$ is defined as

$$S(n,\ell,a,k+1) = \sum_{\substack{j=0 \\ j\equiv a \pmod{\ell}}}^{nk} C(n,j,k),$$

where

$$C(n,j,k) = \sum_{\substack{n_0+n_1+\cdots+n_k=n \\ n_1+2n_2+\cdots+kn_k=j}} \frac{n!}{n_0!n_1!\cdots n_k!} f_0^{n_0} f_1^{n_1}\cdots f_k^{n_k}.$$

Using

$$\sum_{\substack{j=0 \\ j\equiv a \pmod{\ell}}}^{nk} C(n,j,k) = \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-at}\sum_{j=0}^{nk} C(n,j,k)\zeta^{jt} = \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-at} f\left(\zeta^t\right)^n, \tag{1}$$

we obtain that

$$S(n,\ell,a,k+1) = \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-at} f\left(\zeta^t\right)^n. \tag{2}$$

Hence (ii) of Theorem 2.1 can also be written as

$$b_{is+\bar{r}} = S(q-1-\bar{r}-is, \ell, ir+\bar{a}, k+1), \quad i = 0,\dots,\ell-1. \tag{3}$$

From the above theorem, we need to compute ℓ different powers of $f(x^s)$ in order to find all the coefficients of the inverse polynomial of $P(x)$. We note that it is not efficient to find all the coefficients of the inverse polynomial if $s=1$. However, if s is big (i.e., ℓ is small), it is quite efficient to compute the inverse polynomial by using the above theorem. For example, for odd q, it is well known that $P(x)=x^r f(x^{(q-1)/2})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r,(q-1)/2)=1$ and $(f(-1)f(1))^{\frac{q-1}{2}}=(-1)^{r+1}$. The next result gives the explicit format of the inverse polynomial of such permutation polynomial by applying Theorem 2.1.

Corollary 2.2. *For odd q and $s=\frac{q-1}{2}$, the inverse polynomial $Q(x)$ of the permutation polynomial $P(x)=x^r f(x^s)$ is given by $b_{\bar r}x^{\bar r}+b_{s+\bar r}x^{s+\bar r}$ with $b_{\bar r}=\frac{1}{2}(f(1)^{q-1-\bar r}+(-1)^{\bar a}f(-1)^{q-1-\bar r})$ and $b_{s+\bar r}=\frac{1}{2}(f(1)^{s-\bar r}+(-1)^{\bar a'}f(-1)^{s-\bar r})$, where $\bar r=r^{-1} \bmod s$, $\bar a\equiv\frac{r\bar r-1}{s} \pmod 2$, $\bar a'\equiv\bar a+r \pmod 2$.*

Next we show in certain cases, we can also simplify this process by computing only one fixed power of each $f(x^s)$ even for large ℓ. The following theorem is one of such examples which also generalizes Theorem 1.1. Indeed, if $f(x)=g(x)^\ell$ then $f(x)^s=1$.

Corollary 2.3. *Let $q-1=\ell s$ and $P(x)=x^r f(x^s)\in\mathbb{F}_q[x]$ be a permutation polynomial of $\mathbb{F}_q$ where $r\geqslant 1$ and $s=\frac{q-1}{\ell}$. Denote by $Q(x)=b_0+b_1x+\cdots+b_{q-2}x^{q-2}$ its inverse polynomial modulo x^q-x. Assume that $f(\zeta^t)^s=1$ for a primitive ℓth root of unity ζ and any $t=0,\ldots,\ell-1$. Let $\bar r=r^{-1} \bmod s$ and $\bar a\equiv\frac{r\bar r-1}{s} \pmod{\ell}$. Then, for all possible nonzero coefficients b_n corresponding to $n=is+\bar r$ where $i=0,\ldots,\ell-1$, we have*

$$b_{is+\bar r}=\frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-(ir+\bar a)t}f\left(\zeta^t\right)^{q-1-\bar r}.$$

In particular, assume $f(x^s)^{q-1-\bar r}\equiv\sum_{j=0}^{\ell}d_jx^{js} \pmod{x^q-x}$ and $m_i=ir+\bar a \bmod \ell$. Then $b_n=d_{m_i}$ if $m_i\neq 0$, and $b_n=d_0+d_\ell$ if $m_i=0$.

Proof. The first part follows immediately from Theorem 2.1 and $f(\zeta^t)^s=1$. Because $q-1=\ell s$, $-s$ and $\frac{1}{\ell}$ are the same in $\mathbb{F}_q$. Hence $\frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-(ir+\bar a)t}f(\zeta^t)^{q-1-\bar r}=-s\sum_{t=0}^{\ell-1}\zeta^{-(ir+\bar a)t}f(\zeta^t)^{q-1-\bar r}=-\sum_{x\in\mathbb{F}_q}x^{q-1-(ir+\bar a)s}f(x^s)^{q-1-\bar r}$. However, the last term is equal to d_{m_i} if $m_i\neq 0$ and is equal to d_0+d_ℓ otherwise. Hence the proof is complete. □

By using a similar proof, we obtain

Corollary 2.4. *Let $q-1=\ell s$ and $P(x)=x^r f(x^s)\in\mathbb{F}_q[x]$ be a permutation polynomial of $\mathbb{F}_q$ where $r\geqslant 1$ and $s=\frac{q-1}{\ell}$. Denote by $Q(x)=b_0+b_1x+\cdots+b_{q-2}x^{q-2}$ its inverse polynomial modulo x^q-x. Let $\bar r=r^{-1} \bmod s$ and $\bar a\equiv\frac{r\bar r-1}{s} \pmod{\ell}$. Assume that $f(\zeta^t)^s=\zeta^{kt}$ for a primitive ℓth root of unity ζ and any $t=0,\ldots,\ell-1$. Then, for all possible nonzero coefficients b_n corresponding to $n=is+\bar r$ where $i=0,\ldots,\ell-1$, we have*

$$b_{is+\bar r}=\frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{-(ir+\bar a+ik)t}f\left(\zeta^t\right)^{q-1-\bar r}.$$

In particular, assume $f(x^s)^{q-1-\bar r}\equiv\sum_{j=0}^{\ell}d_jx^{js} \pmod{x^q-x}$ and $m_i=ir+\bar a+ik \bmod \ell$. Then $b_n=d_{m_i}$ if $m_i\neq 0$, and $b_n=d_0+d_\ell$ if $m_i=0$.

We refer the readers to [4] for several interesting classes of permutation polynomials which satisfy the assumptions of Corollaries 2.3 and 2.4.

3. Binomials and sequences

In this section, we consider the inverse polynomial of a permutation binomial $f(x) = x^r(x^{es} + 1)$ over $\mathbb{F}_q$ where $q = p^m$, $q - 1 = \ell s$ for some positive integers ℓ, s and $(e, \ell) = 1$. We note that the characterization of permutation polynomials of the form $x^r(x^{es} + 1)$ have been studied by Akbary and the author in [2,3] and [9]. In particular, if $f(x) = x^r(x^{es} + 1)$ is a permutation polynomial over $\mathbb{F}_q$ then p must be odd. Otherwise, $P(0) = P(1) = 0$. Since $\ell \mid q - 1$, let $\zeta \in \mathbb{F}_q$ be a primitive ℓth root of unity. Moreover, we must have $\zeta^{ei} \neq -1$ for $i = 0, \ldots, \ell - 1$. Hence ℓ must be odd and then s must be even. So we can assume that $\ell \geqslant 3$ as $\ell = 1$ is trivial. Because both p and ℓ are odd, there exists $\eta \in \mathbb{F}_q$ such that $\eta^2 = \zeta$. Hence η is a primitive 2ℓth root of unity in $\mathbb{F}_q$.

We define the sequence $\{a_n\}_{n=0}^{\infty}$ by

$$a_n = \sum_{t=1}^{\frac{\ell-1}{2}} \left((-1)^{t+1}\left(\eta^t + \eta^{-t}\right)\right)^n = \sum_{\substack{t=1 \\ t \text{ odd}}}^{\ell-1} \left(\eta^t + \eta^{-t}\right)^n.$$

The sequence $\{a_n\}_{n=0}^{\infty}$ is called *generalized Lucas sequence of order* $\frac{\ell-1}{2}$ because $\{a_n\}_{n=0}^{\infty} = \{L_n\}_{n=0}^{\infty}$ when $\ell = 5$, where the sequence $\{L_n\}_{n=0}^{\infty}$ is the so-called Lucas sequence satisfying the recurrence relation $L_{n+2} - L_{n+1} - L_n = 0$ and $L_0 = 2$ and $L_1 = 1$.

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

$$D_n(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-1)^i x^{n-2i}.$$

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

$$E_n(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}(-1)^i x^{n-2i}.$$

We consider the Dickson polynomial $E_{\ell-1}(x)$ of the second kind with degree $\ell - 1$. It is well known that $\eta^t + \eta^{-t}$ with $1 \leqslant t \leqslant \ell - 1$ are all the roots of $E_{\ell-1}(x)$ where η is a primitive 2ℓth root of unity. Let

$$E_{\ell-1}^{\text{odd}}(x) = \prod_{\substack{t=1 \\ \text{odd}\, t}}^{\ell-1} \left(x - \left(\eta^t + \eta^{-t}\right)\right).$$

Then the characteristic polynomial of the sequence $\{a_n\}_{n=0}^{\infty}$ is $E_{\ell-1}^{\text{odd}}(x)$ and $\{a_n\}_{n=0}^{\infty}$ is a sequence over the prime field $\mathbb{F}_p$.

Now we prove the following result which gives the explicit format of the inverse polynomials of permutation binomials of the form $x^r(x^{e(q-1)/\ell} + 1)$ in terms of generalized Lucas sequence of order $\frac{\ell-1}{2}$.

Theorem 3.1. *Let p be odd prime and $q = p^m$. Assume that ℓ, s, r, e are positive integers such that $\ell \geqslant 3$ is odd, $q - 1 = \ell s$, and $(e, \ell) = 1$. 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 the following holds.*

(i) *If $b_n \neq 0$, then $n \equiv r^{-1} \pmod{s}$. Hence $Q(x)$ has at most ℓ nonzero coefficients b_n corresponding to $n = is + \bar{r}$ where $\bar{r} = r^{-1} \bmod s$ and $i = 0, \ldots, \ell - 1$.*

(ii)
$$b_n = \frac{1}{\ell}\left(2^{q-1-n} + \sum_{i=0}^{\lfloor u_n/2\rfloor} t_i^{(u_n)} a_{q-1-n+u_n-2i}\right), \tag{4}$$

where $\bar{n} = \frac{rn-1}{s} \bmod \ell$, $u_n = 2\bar{n}e^{\phi(\ell)-1} + n \bmod 2\ell$, $t_i^{(u_n)} = \frac{u_n}{u_n-i}\binom{u_n-i}{i}(-1)^i$, *and* $\{a_n\}_{n=0}^{\infty}$ *is the generalized Lucas sequence of order* $\frac{\ell-1}{2}$.

Proof. By Theorem 2.1, $Q(x)$ has at most ℓ nonzero coefficients b_n with $n \equiv r^{-1} \pmod s$ and $1 \leqslant n \leqslant q-2$. Then $n = is + \bar{r}$ where $\bar{r} = r^{-1} \bmod s$ and $i = 0, \ldots, \ell-1$. Moreover, $\bar{n} \equiv \frac{rn-1}{s} \equiv ir + \bar{a} \pmod \ell$ where $\bar{a} \equiv \frac{r\bar{r}-1}{s} \pmod \ell$.

Let $\xi = \zeta^e$. Since $(e, \ell) = 1$, ξ is also a primitive ℓth root of unity. Moreover, because $2\ell \mid q-1$, then there exists $\eta \in \mathbb{F}_q$ such that $\eta^2 = \xi$. Because ζ^{-1} is also a primitive ℓth root of unity, by Theorem 2.1, we obtain

$$\begin{aligned}
b_n &= \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{\bar{n}t} f\left(\zeta^{-t}\right)^{q-1-n} \\
&= \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^{\bar{n}t}\left(\zeta^{-et}+1\right)^{q-1-n} \\
&= \frac{1}{\ell}\sum_{t=0}^{\ell-1}\xi^{\bar{n}e^{\phi(\ell)-1}t}\left(\xi^{-t}+1\right)^{q-1-n} \\
&= \frac{1}{\ell}\left(2^{q-1-n} + \sum_{t=1}^{\ell-1}\eta^{2\bar{n}e^{\phi(\ell)-1}t-(q-1-n)t}\left(\eta^{-t}+\eta^{t}\right)^{q-1-n}\right) \\
&= \frac{1}{\ell}\left(2^{q-1-n} + \sum_{t=1}^{\frac{\ell-1}{2}}\left(\eta^{(2\bar{n}e^{\phi(\ell)-1}+n)t} + \eta^{-(2\bar{n}e^{\phi(\ell)-1}+n)t}\right)\left(\eta^{-t}+\eta^{t}\right)^{q-1-n}\right),
\end{aligned}$$

where the last identity holds because q, n are odd and $\eta^{\ell} = -1$. Hence the result follows from the definition of $\{a_n\}_{n=0}^{\infty}$ and the fact

$$\eta^{u_n t} + \eta^{-u_n t} = D_{u_n}\left(\eta^t + \eta^{-t}\right) = \sum_{i=0}^{\lfloor u_n/2\rfloor}\frac{u_n}{u_n-i}\binom{u_n-i}{i}(-1)^i\left(\eta^t+\eta^{-t}\right)^{u_n-2i}.$$

This completes the proof. □

We note that Eq. (4) can also be written as

$$b_{q-1-n} = \frac{1}{\ell}\left(2^n + \sum_{j=0}^{u_n} c_j^{(u_n)} a_{n+j}\right), \tag{5}$$

where $c_j^{(u_n)}$ is the coefficient of x^j in the expansion of the Dickson polynomial of the first kind $D_{u_n}(x)$ of degree $u_n = 2\hat{n}e^{\phi(\ell)-1} + (q-1-n) \pmod{2\ell}$ and $\hat{n} = \frac{(q-1-n)r-1}{s} \pmod \ell$. Moreover, all the coefficients of the inverse polynomial $Q(x)$ in Theorem 3.1 are in $\mathbb{F}_p$. Because the coefficients $t_i^{(u_n)}$ and the general term of generalized Lucas sequence $\{a_n\}_{n=0}^{\infty}$ over $\mathbb{F}_p$ are quite easy to find, one can generate many examples of inverse polynomials by applying Theorem 3.1. For example, if $\ell = 3$ and $s = (q-1)/3$, then $\{a_n\}_{n=0}^{\infty}$ is a constant sequence $1, 1, \ldots$. Hence $b_n = \frac{1}{3}(2^{-\bar{r}} + D_{u_n}(1))$ because $P(x) = x^r(x^{es}+1)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(r, s) = 1$, $2^s \equiv 1 \pmod p$, and

Table 1
Permutation binomials $x^r(x^{\frac{e(q-1)}{7}}+1)$ and inverse polynomials over $\mathbb{F}_{13^2}$.

PP	Inverse of PP
$x+x^{25}$	$7x+7x^{25}+6x^{49}+7x^{73}+6x^{97}+7x^{121}+6x^{145}$
x^5+x^{29}	$2x^5+9x^{29}+7x^{53}+8x^{77}+8x^{101}+7x^{125}+9x^{149}$
x^7+x^{31}	$5x^7+5x^{55}+10x^{79}+x^{103}+x^{127}+10x^{151}$
$x^{11}+x^{35}$	$x^{59}+x^{131}$
$x^{13}+x^{37}$	$7x^{13}+6x^{37}+7x^{61}+7x^{85}+6x^{109}+6x^{133}+7x^{157}$
$x^{17}+x^{41}$	$9x^{17}+9x^{41}+8x^{65}+7x^{89}+2x^{113}+7x^{137}+8x^{161}$
$x^{19}+x^{43}$	$10x^{43}+x^{67}+5x^{91}+5x^{115}+x^{139}+10x^{163}$
...	...

Table 2
Permutation binomials $x^r(x^{\frac{e(q-1)}{9}}+1)$ and inverse polynomials over $\mathbb{F}_{17^2}$.

PP	Inverse of PP
$x+x^{33}$	$9x+9x^{33}+8x^{65}+9x^{97}+8x^{129}+9x^{161}+8x^{193}+9x^{225}+8x^{257}$
x^3+x^{35}	$x^{11}+5x^{43}+10x^{75}+10x^{107}+5x^{139}+x^{171}$
x^7+x^{39}	$16x^{23}+9x^{55}+7x^{87}+2x^{119}+7x^{151}+9x^{183}+16x^{215}+2x^{247}+2x^{279}$
x^9+x^{41}	$4x^{25}+x^{57}+7x^{89}+7x^{153}+x^{185}+4x^{217}+x^{249}+x^{281}$
$x^{13}+x^{45}$	$5x^5+12x^{37}+3x^{69}+7x^{101}+5x^{133}+5x^{165}+7x^{197}+3x^{229}+12x^{261}$
$x^{15}+x^{47}$	$x^{47}+x^{111}$
$x^{19}+x^{51}$	$x^{27}+5x^{59}+10x^{91}+10x^{123}+5x^{155}+x^{187}$
...	...

$(2r+es,\ell)=1$. In the case $\ell=5$ and $s=(q-1)/5$, the corresponding sequence $\{a_n\}_{n=0}^{\infty}$ is the Lucas sequence. In this case, $P(x)=x^r(x^{es}+1)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(r,s)=1$, $2^s\equiv 1 \pmod p$, $(2r+es,\ell)=1$, $a_s=2$. In particular, $\{a_n\}_{n=0}^{\infty}$ is periodic with a period s. Hence we can use s-periodicity of $\{a_n\}_{n=0}^{\infty}$ and $2^s\equiv 1 \pmod p$ to simplify the computation of Eq. (4) or Eq. (5). We observe that explicit formulas of inverse polynomials of permutation binomials for the cases $\ell=3,5$ have also been obtained recently by Muratović-Ribić in [7] without using sequences. The formulas in [7] are similar to Eq. (3) for $\ell=3,5$. When $\ell\geqslant 7$, generalized Lucas sequences were introduced so that we can evaluate the lacunary sums. Here we give some examples of inverse polynomials of permutation binomials with $\ell\geqslant 7$ (see Tables 1 and 2).

Acknowledgments

The author would like to thank Amir Akbary for helpful suggestions. He also wants to thank the referee for useful comments, in particular, for pointing out explicit formulas of inverse polynomials of permutation binomials for the cases $\ell=3,5$ in [7].

References

[1] A. Akbary, D. Ghioca, Q. Wang, On permutation polynomials of prescribed shape, Finite Fields Appl. (2009), doi:10.1016/j.ffa.2008.12.001, in press.
[2] A. Akbary, Q. Wang, On some permutation polynomials, Int. J. Math. Math. Sci. 16 (2005) 2631–2640.
[3] A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, Proc. Amer. Math. Soc. 134 (1) (2006) 15–22.
[4] A. Akbary, Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci. (2007) 7, Art. ID 23408.
[5] G.L. Mullen, Permutation polynomials over finite fields, in: Finite Fields, Coding Theory, and Advances in Communication and Computing, Las Vegas, 1991, in: Lect. Notes Pure Appl. Math., vol. 141, Dekker, New York, 1993, pp. 131–151.
[6] A. Muratović-Ribić, A note on the coefficients of inverse polynomials, Finite Fields Appl. 13 (4) (2007) 977–980.
[7] A. Muratović-Ribić, Inverse of some classes of permutation binomials, Discrete Appl. Math., in press.
[8] 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.
[9] Q. Wang, Cyclotomic mapping permutation polynomials, in: Sequences, Subsequences, and Consequences, Los Angeles, 2007, in: Lecture Notes in Comput. Sci., vol. 4893, Springer, 2007, pp. 119–128.