A NOTE ON THE PERMUTATION BEHAVIOUR OF THE POLYNOMIAL $g_{n,q}$

Neranga Fernando
Department of Mathematics, Northeastern University, Boston, Massachusetts
w.fernando@northeastern.edu

Received: 5/11/18, Revised: 8/17/18, Accepted: 12/13/18, Published: 1/5/19

Abstract

Let $q = 4$ and k be an even positive integer. In this note, we present a class of permutation polynomials over $\mathbb{F}_{q^{3k}}$. We also present a generalization.

1. Introduction

Let p be a prime and q a power of p. Let $\mathbb{F}_q$ denote the finite field with q elements, Char$\mathbb{F}_q$ denote the characteristic of $\mathbb{F}_q$, and e be a positive integer. A permutation polynomial (PP) of $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ such that the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Permutation polynomials over finite fields have important applications in coding theory, cryptography, finite geometry, combinatorics and computer science, among other fields. Most studies on PPs have been over finite fields. However, several authors have studied PPs over finite commutative rings. We refer the reader to [9], [4] and references therein for further details on PPs over finite commutative rings.

For each integer $n \geq 0$, there is a polynomial $g_{n,q} \in \mathbb{F}_p[x]$ defined by the functional equation

$$\sum_{c \in \mathbb{F}_q} (x + c)^n = g_{n,q}(x^q - x). \tag{1}$$

The polynomial $g_{n,q}$ was introduced in [5], and its permutation property was studied in [2, 6]. The objective is to determine the triples $(n, e; q)$ of positive integers for which $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$. We call a triple of integers $(n, e; q)$ *desirable* if $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Define

$$S_{m,q} = x + x^q + \cdots + x^{q^{m-1}} \in \mathbb{F}_p[x],$$

where m is a positive integer and $p = \text{Char}\mathbb{F}_q$. When q is fixed, we write $S_{m,q} = S_m$. Note that S_m is a particular type of linearized polynomial and $S_e = \text{Tr}_{q^e/q}$, where $\text{Tr}_{q^e/q}$ is the *trace* function from $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$. The polynomial $g_{n,q}$ can be expressed in

terms of polynomials of the form S_m when the integer n takes certain forms. PPs arising from polynomials $g_{n,q}$ that involve S_m were studied in [3].

Desirable triples obtained from computer searches were presented in [1, 2, 6]. Table 1 in the Appendix of the present paper contains PPs over $\mathbb{F}_{q^e}$ defined by the polynomial $g_{n,q}$ when $q = 4$ and $e = 6$. In [1], Hou and the author of the present paper discovered several new classes of PPs which explained several entries of Table 3 in [2]. But, as a whole, determining the permutation behaviour of the polynomial $g_{n,q}$ appears to be a difficult problem. We refer the reader to [6] for more background of the polynomial $g_{n,q}$, and to [1] for a complete table of desirable triples when $q = 4$.

PPs over $\mathbb{F}_{q^{3k}}$, where q is a power of 2, have appeared in the literature; see [2, 7, 10]. In [7], Hou confirmed a class of PPs over $\mathbb{F}_{4^{3k}}$ that was conjectured in [2]. In [10], Yuan and Ding generalized Hou's result and obtained several more classes of PPs of the form $L(x)+S_{2k}^a+S_{2k}^b$ over $\mathbb{F}_{q^{3k}}$, where q is a power of 2. In this paper, we present a new class of PPs over $\mathbb{F}_{q^{3k}}$ defined by the polynomial $g_{n,q}$, where $q = 4$ and $k > 0$ is an even integer, which explains another entry, $n = 65921$, of Table 1 in the Appendix.

The note is organized as follows. In Section 2, we present the main result of the paper, Theorem 1, which gives a new class of PPs over $\mathbb{F}_{4^{3k}}$. In Section 3, we explain an entry of Table 1 in the Appendix using the results obtained in Section 2. In Section 4, we present a generalization. In Section 2 and Section 3, we assume that $q = 4$ and use $e = 3k$ for some even k unless otherwise specified.

2. A Class of Permutation Polynomials Over $\mathbb{F}_{q^{3k}}$

We recall two facts:

Fact 1. ([8, Theorem 7.7]) *Let $f \in \mathbb{F}_q[x]$. Then f is a PP of $\mathbb{F}_q$ if and only if for all $a \in \mathbb{F}_q^*$, $\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(af(x))} = 0$, where $p = \mathrm{Char}\mathbb{F}_q$ and $\zeta_p = e^{2\pi i/p}$.*

Fact 2. ([2, Lemma 6.13]) *Let p be a prime and $f\colon \mathbb{F}_p^n \to \mathbb{F}_p$ a function. If there exists a $y \in \mathbb{F}_p^n$ such that $f(x+y)-f(x)$ is a nonzero constant for all $x \in \mathbb{F}_p^n$, then $\sum_{x\in\mathbb{F}_p^n} \zeta_p^{f(x)} = 0$.*

Lemma 1. *Let k be a positive integer, q a power of 2, $b \in \mathbb{F}_{q^{3k}}^*$ and $y \in \mathbb{F}_{q^k}^*$. Then $Tr_{q^{3k}/2}\big(b\,(y + y^q + \cdots + y^{q^{k-2}})\big) = Tr_{q^{3k}/2}\big(y\,(b^{q^{3k}} + b^{q^{3k-1}} + \cdots + b^{q^{2k+2}})\big)$.*

Proof. We write $\mathrm{Tr} = \mathrm{Tr}_{q^{3k}/2}$. We have

$$\begin{aligned}\mathrm{Tr}\big(b\,(y+y^q+\cdots+y^{q^{k-2}})\big) &= \mathrm{Tr}\big(by+by^q+\cdots+by^{q^{k-2}}\big)\\ &= \mathrm{Tr}\big(by\big)+\mathrm{Tr}\big(by^q\big)+\cdots+\mathrm{Tr}\big(by^{q^{k-2}}\big)\\ &= \mathrm{Tr}\big(b^{q^{3k}}y^{q^{3k}}\big)+\mathrm{Tr}\big(b^{q^{3k-1}}y^{q^{3k}}\big)+\cdots+\mathrm{Tr}\big(b^{q^{2k+2}}y^{q^{3k}}\big)\\ &= \mathrm{Tr}\big(b^{q^{3k}}y\big)+\mathrm{Tr}\big(b^{q^{3k-1}}y\big)+\cdots+\mathrm{Tr}\big(b^{q^{2k+2}}y\big)\\ &= \mathrm{Tr}\big(yb^{q^{3k}}+yb^{q^{3k-1}}+\cdots+yb^{q^{2k+2}}\big)\\ &= \mathrm{Tr}\big(y\,(b^{q^{3k}}+b^{q^{3k-1}}+\cdots+b^{q^{2k+2}})\big).\end{aligned}$$

□

Lemma 2. *Let k be a positive integer, q a power of 2, $x \in \mathbb{F}_{q^{3k}}$ and $c \in \mathbb{F}_{q^{3k}} \setminus \mathbb{F}_{q^k}$. Then $Tr_{q^{3k}/2}\big(c(x+x^q+\cdots+x^{q^{2k-1}})\big) = Tr_{q^{3k}/2}\big(x(c^{q^{3k}}+c^{q^{3k-1}}+\cdots+c^{q^{k+1}})\big)$.*

Proof. We write $\mathrm{Tr} = \mathrm{Tr}_{q^{3k}/2}$. We have

$$\begin{aligned}\mathrm{Tr}\big(c(x+x^q+\cdots+x^{q^{2k-1}})\big) &= \mathrm{Tr}\big(cx+cx^q+\cdots+cx^{q^{2k-1}}\big)\\ &= \mathrm{Tr}\big(cx\big)+\mathrm{Tr}\big(cx^q\big)+\cdots+\mathrm{Tr}\big(cx^{q^{2k-1}}\big)\\ &= \mathrm{Tr}\big(c^{q^{3k}}x^{q^{3k}}\big)+\mathrm{Tr}\big(c^{q^{3k-1}}x^{q^{3k}}\big)+\cdots+\mathrm{Tr}\big(c^{q^{k+1}}x^{q^{3k}}\big)\\ &= \mathrm{Tr}\big(c^{q^{3k}}x\big)+\mathrm{Tr}\big(c^{q^{3k-1}}x\big)+\cdots+\mathrm{Tr}\big(c^{q^{k+1}}x\big)\\ &= \mathrm{Tr}\big(xc^{q^{3k}}+xc^{q^{3k-1}}+\cdots+xc^{q^{k+1}}\big)\\ &= \mathrm{Tr}\big(x\,(c^{q^{3k}}+c^{q^{3k-1}}+\cdots+c^{q^{k+1}})\big).\end{aligned}$$

□

The following theorem is the main theorem of this paper.

Theorem 1. *Let $q = 4$, $e = 3k$, where $k > 0$ is an even integer. Then $g = S_{k+1}^2 + S_{2k}^{q^k+1}$ is a PP of $\mathbb{F}_{q^e}$.*

Proof. By Fact 1, it suffices to show that

$$\sum_{x\in\mathbb{F}_{q^e}} (-1)^{\mathrm{Tr}_{q^e/2}(ag(x))} = 0$$

for all $0 \neq a \in \mathbb{F}_{q^e}$. We write $\mathrm{Tr} = \mathrm{Tr}_{q^e/2}$. We consider two cases, where $\mathrm{Tr}_{q^e/q^k}(a) \neq 0$ and $\mathrm{Tr}_{q^e/q^k}(a) = 0$.

`Case 1.` Assume $\mathrm{Tr}_{q^e/q^k}(a) \neq 0$. By Fact 2, it suffices to show that there exists $y \in \mathbb{F}_{q^e}$ such that $\mathrm{Tr}\big(ag(x+y)-ag(x)\big)$ is a nonzero constant for all $x \in \mathbb{F}_{q^e}$.

Let $y \in \mathbb{F}_{q^k}^*$. Then for $x \in \mathbb{F}_{q^e}$, we have

$$\begin{aligned}
&\mathrm{Tr}\big(ag(x+y) - ag(x)\big)\\
&= \mathrm{Tr}\big[a\big(S_{k+1}^2(x+y) + S_{2k}^{q^k+1}(x+y) - S_{k+1}^2(x) - S_{2k}^{q^k+1}(x)\big)\big]\\
&= \mathrm{Tr}(a\, S_{k+1}^2(y)) && (S_{2k}(y) = 0 \text{ since } y \in \mathbb{F}_{q^k})\\
&= \mathrm{Tr}(a\,(y + y^q + \cdots + y^{q^{k-1}} + y^{q^k})^2)\\
&= \mathrm{Tr}(a\,(y + y^q + \cdots + y^{q^{k-1}} + y)^2)\\
&= \mathrm{Tr}(a\,(y^q + y^{q^2} + \cdots + y^{q^{k-1}})^2)\\
&= \mathrm{Tr}(a\,(y + y^q + \cdots + y^{q^{k-2}})^{2q})\\
&= \mathrm{Tr}(a\, S_{k-1}^{2q}(y))\\
&= \mathrm{Tr}(a^{2q^{e-2}}\, S_{k-1}(y))\\
&= \mathrm{Tr}(b\, S_{k-1}(y)) && (a^{2q^{e-2}} = b, \text{ i.e. } a = b^{2q})\\
&= \mathrm{Tr}\big(b\,(y + y^q + \cdots + y^{q^{k-2}})\big)\\
&= \mathrm{Tr}\big(y\,(b^{q^{3k}} + b^{q^{3k-1}} + \cdots + b^{q^{2k+2}})\big) && (\text{Lemma 1})\\
&= \mathrm{Tr}_{q^k/2}\big(y\,(c^{q^{2k+2}} + \cdots + c^{q^{3k}})\big), && \text{where } c = \mathrm{Tr}_{q^e/q^k}(b) \neq 0.
\end{aligned}$$

Now consider $\gcd(\mathtt{x}^{q^{2k+2}} + \mathtt{x}^{q^{2k+3}} + \cdots + \mathtt{x}^{q^{3k}},\ \mathtt{x}^{q^k} + \mathtt{x})$. By [8, Theorem 3.62], we only need to consider $\gcd(\mathtt{x}^{2k+2} + \mathtt{x}^{2k+3} + \cdots + \mathtt{x}^{3k},\ \mathtt{x}^k + 1)$.

Since k is even, $\gcd(\mathtt{x}^{2k+2}+\mathtt{x}^{2k+3}+\cdots+\mathtt{x}^{3k},\ \mathtt{x}^k+1) = \gcd(1+\mathtt{x}+\cdots+\mathtt{x}^{k-2},\ \mathtt{x}^k+1) = 1$, which implies $c^{q^{2k+2}} + \cdots + c^{q^{3k}} \neq 0$, and hence there exists $y \in \mathbb{F}_{q^k}$ such that $\mathrm{Tr}\big(ag(x+y) - ag(x)\big) = \mathrm{Tr}_{q^k/2}\big(y\,(c^{q^{2k+2}} + \cdots + c^{q^{3k}})\big)$ is a nonzero constant, which is 1.

`Case 2.` Assume $\mathrm{Tr}_{q^e/q^k}(a) = 0$. Then $a = b + b^{q^k}$ for some $b \in \mathbb{F}_{q^e}$. Since $a \neq 0$, we have $b \notin \mathbb{F}_{q^k}$. For $x \in \mathbb{F}_{q^e}$, we have

$$\begin{aligned}
\mathrm{Tr}\big(ag(x)\big) &= \mathrm{Tr}\big(bg(x) + b^{q^k} g(x)\big)\\
&= \mathrm{Tr}\big(bg(x)\big) + \mathrm{Tr}\big(b^{q^k} g(x)\big)\\
&= \mathrm{Tr}\big(bg(x)\big) + \mathrm{Tr}\big(bg(x)^{q^{2k}}\big)\\
&= \mathrm{Tr}\big(bg(x) + bg(x)^{q^{2k}}\big)\\
&= \mathrm{Tr}\big(b(g(x) + g(x)^{q^{2k}})\big).
\end{aligned}$$

Note that $S_{2k}^{q^k} + S_{2k}^{q^{2k}} \equiv S_{2k} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}$ and

$$S_{k+1}^2 + S_{k+1}^{2q^{2k}} \equiv x^2 + x^{2q^k} + S_{2k}^2 + S_{2k}^{2q^k} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

Then we have

$$\begin{aligned} g(\mathtt{x})+g(\mathtt{x})^{q^{2k}} &\equiv S_{k+1}^2+S_{2k}^{q^k+1}+S_{k+1}^{2q^{2k}}+S_{2k}^{q^{2k}+1} \pmod{\mathtt{x}^{q^e}-\mathtt{x}} \\ &= S_{k+1}^2+S_{k+1}^{2q^{2k}}+S_{2k}\cdot(S_{2k}^{q^k}+S_{2k}^{q^{2k}}) \\ &\equiv x^2+x^{2q^k}+S_{2k}^2+S_{2k}^{2q^k}+S_{2k}^2 \pmod{\mathtt{x}^{q^e}-\mathtt{x}} \\ &= (\mathtt{x}+\mathtt{x}^{q^k}+S_{2k}^{q^k})^2 \\ &= (S_{3k}+S_k^q)^2 \\ &\equiv (S_{2k}^{q^{k+1}})^2 \pmod{\mathtt{x}^{q^e}-\mathtt{x}}. \end{aligned} \tag{2}$$

So for $x\in\mathbb{F}_{q^e}$,

$$\begin{aligned} \mathrm{Tr}\big(ag(x)\big) &= \mathrm{Tr}\big(bS_{2k}(x)^{2q^{k+1}}\big) \\ &= \mathrm{Tr}\big(cS_{2k}(x)\big) \qquad\qquad (b=c^{2q^{k+1}}) \\ &= \mathrm{Tr}\big(c(x+x^q+\cdots+x^{q^{2k-1}})\big) \\ &= \mathrm{Tr}\big(x(c^{q^{3k}}+c^{q^{3k-1}}+\cdots+c^{q^{k+1}})\big) \qquad \text{(Lemma 2)}. \end{aligned}$$

Now consider $\gcd(\mathtt{x}^{q^{k+1}}+\mathtt{x}^{q^{k+2}}+\cdots+\mathtt{x}^{q^{3k}},\ \mathtt{x}^{q^{3k}}+\mathtt{x})$. By [8, Theorem 3.62], we only need to consider $\gcd(\mathtt{x}^{k+1}+\mathtt{x}^{k+2}+\cdots+\mathtt{x}^{3k},\ \mathtt{x}^{3k}+1)$.

Since $\gcd(\mathtt{x}^{k+1}+\mathtt{x}^{k+2}+\cdots+\mathtt{x}^{3k},\ \mathtt{x}^{3k}+1)=\gcd(1+\mathtt{x}+\cdots+\mathtt{x}^{2k-1},\ \mathtt{x}^{3k}+1)=\mathtt{x}^k+1$, we see that for $z\in\mathbb{F}_{q^{3k}}$, we have $z^{q^{3k}}+z^{q^{3k-1}}+\cdots+z^{q^{k+1}}=0$ if and only if $z\in\mathbb{F}_{q^k}$. Since $c\notin\mathbb{F}_{q^k}$, we have $c^{q^{3k}}+c^{q^{3k-1}}+\cdots+c^{q^{k+1}}\neq 0$. Therefore

$$\sum_{x\in\mathbb{F}_{q^e}}(-1)^{\mathrm{Tr}(ag(x))}=\sum_{x\in\mathbb{F}_{q^e}}(-1)^{\mathrm{Tr}(x(c^{q^{3k}}+c^{q^{3k-1}}+\cdots+c^{q^{k+1}}))}=0. \qquad \square$$

3. Polynomial $g_{n,q}$

We first recall a fact:

Fact 3. ([2, Theorem 6.1]) *Let $q\geq 4$ be even, and let*

$$n=1+q^{a_1}+q^{b_1}+\cdots+q^{a_{q/2}}+q^{b_{q/2}},$$

where $a_i,b_i\geq 0$ are integers. Then

$$g_{n,q}=\sum_i S_{a_i}S_{b_i}+\sum_{i<j}(S_{a_i}+S_{b_i})(S_{a_j}+S_{b_j}).$$

Corollary 1. *Let $q=4$, $e=6$, and $n=65921=1+2q^3+q^4+q^8$. Then*

$$g_{n,q}\equiv S_3^2+S_4^{q^2+1} \pmod{\mathtt{x}^{q^e}-\mathtt{x}},$$

and $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proof. We write g_n for $g_{n,q}$. Let $a_1 = b_1 = 3, a_2 = 4$ and $b_2 = 8$ in Fact 3. Then we have

$$\begin{aligned} g_n &= S_3^2 + S_4 S_8 \\ &\equiv S_3^2 + S_4(S_6 + S_2) \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \\ &= S_3^2 + S_4 S_4^{q^2} \\ &= S_3^2 + S_4^{q^2+1}. \end{aligned}$$

Let $k = 2$ in Theorem 1. Then it follows from Theorem 1 that g_n is a PP of $\mathbb{F}_{q^e}$. □

Remark 1. Let k be odd and consider $g = S_{k+1}^2 + S_{2k}^{q^k+1}$. Note that g consists of even number of powers of x since S_{k+1} and S_{2k} consist of even number of powers of x. Thus the polynomial g defined in Theorem 1 is never a PP over $\mathbb{F}_{4^{3k}}$ when k is odd since $g(0) = g(1)$.

4. A Generalization

The following theorem is a generalization of Theorem 1.

Theorem 2. *Let q be a power of 2. Let $L \in \mathbb{F}_{q^{3k}}[x]$ be a 2-linearized polynomial such that*

(i) L permutes $\mathbb{F}_{q^k}$, and

(ii) $L + L^{q^{2k}} \equiv S_{2k}^2 + S_{2k}^{2q^{k+1}} \pmod{\mathtt{x}^{q^{3k}} - \mathtt{x}}$.

Then $L + S_{2k}^{q^k+1}$ is a PP of $\mathbb{F}_{q^{3k}}$.

Proof. Let $g = L + S_{2k}^{q^k+1}$. As in Case 1 in Theorem 1, assume $\mathrm{Tr}_{q^{3k}/q^k}(a) \neq 0$. By Fact 2, it suffices to show that there exists $y \in \mathbb{F}_{q^{3k}}$ such that $\mathrm{Tr}_{q^{3k}/2}\big(ag(x+y) - ag(x)\big)$ is a nonzero constant for all $x \in \mathbb{F}_{q^{3k}}$. We write $\mathrm{Tr} = \mathrm{Tr}_{q^{3k}/2}$.

Let $y \in \mathbb{F}_{q^k}^*$. Then for $x \in \mathbb{F}_{q^{3k}}$, we have

$$\begin{aligned} &\mathrm{Tr}\big(ag(x+y) - ag(x)\big) \\ &= \mathrm{Tr}\big[a\big(L(x+y) + S_{2k}^{q^k+1}(x+y) - L(x) - S_{2k}^{q^k+1}(x)\big)\big] \\ &= \mathrm{Tr}(a\,L(y)) \qquad\qquad (S_{2k}(y) = 0 \text{ since } y \in \mathbb{F}_{q^k}) \\ &= \mathrm{Tr}_{q^k/2}\big(L(y)\,\mathrm{Tr}_{q^{3k}/q^k}(a)\big). \end{aligned}$$

Since L permutes $\mathbb{F}_{q^k}$ and $y \in \mathbb{F}_{q^k}^*$, $L(y) \neq 0$. Thus we choose $y \in \mathbb{F}_{q^k}$ such that $\mathrm{Tr}_{q^k/2}\big(L(y)\,\mathrm{Tr}_{q^{3k}/q^k}(a)\big) \neq 0$. In Case 2 in Theorem 1, (2) still holds because of condition 2. □

Note. Let $q = 4$, k be even and $L = S_{k+1}^2$. Then $L = x^2 \circ S_{k+1}$. Since $\gcd(2, q^k - 1) = 1$, x^2 permutes $\mathbb{F}_{q^k}$. For $x \in \mathbb{F}_{q^k}$, we have $S_{k+1} = x^q + x^{q^2} + \cdots + x^{q^{k-1}}$. Note that when k is odd S_{k+1} does not permute $\mathbb{F}_{q^k}$ since $S_{k+1}(0) = S_{k+1}(1)$.

Now consider $\gcd(\mathtt{x}^q + \mathtt{x}^{q^2} + \cdots + \mathtt{x}^{q^{k-1}},\ \mathtt{x}^{q^k} + 1)$. By [8, Theorem 3.62], we only need to consider $\gcd(\mathtt{x}+\mathtt{x}^2+\cdots+\mathtt{x}^{k-1},\ \mathtt{x}^k+1)$. Since $\gcd(\mathtt{x}+\mathtt{x}^2+\cdots+\mathtt{x}^{k-1},\ \mathtt{x}^k+1) = 1$, S_{k+1} permutes $\mathbb{F}_{q^k}$. Thus L satisfies condition (i) in Theorem 2.

For (ii), we have

$$\begin{aligned} L + L^{q^{2k}} &= S_{k+1}^2 + \left(S_{k+1}^2\right)^{q^{2k}} \\ &= (x + x^q + x^{q^2} + \cdots + x^{q^k})^2 + (x^2 + x^{2q} + x^{2q^2} + \cdots + x^{2q^k})^{q^{2k}} \\ &= (x + x^q + x^{q^2} + \cdots + x^{q^k})^2 + (x^{q^{2k}} + x^{q^{2k+1}} + x^{q^{2k+2}} + \cdots + x^{q^{3k}})^2 \\ &= (x + x^q + x^{q^2} + \cdots + x^{q^k} + x^{q^{2k}} + x^{q^{2k+1}} + x^{q^{2k+2}} + \cdots + x^{q^{3k}})^2 \\ &\equiv S_{2k}^2 + S_{2k}^{2q^{k+1}} \pmod{x^{q^{3k}} - x}. \end{aligned}$$

Acknowledgement. The author is grateful to the referee and the editor for useful comments and suggestions.

References

[1] N. Fernando and X. Hou, From r-linearized polynomial equations to r^m-linearized polynomial equations, *Finite Fields Appl.* **37** (2016), 14 – 27.

[2] N. Fernando, X. Hou, and S. D. Lappano, A new approach to permutation polynomials over finite fields, II, *Finite Fields Appl.* **22** (2013), 122 – 158.

[3] N. Fernando, X. Hou, and S. D. Lappano, Permutation polynomials over finite fields involving $x + x^q + \cdots + x^{q^{a-1}}$, *Discrete Math.* **315** (2014), 173 – 184.

[4] D. Görcsös, G. Horváth, and A. Mészáros, Permutation polynomials over finite rings, *Finite Fields Appl.* **49** (2018), 198 – 211.

[5] X. Hou, Two classes of permutation polynomials over finite fields, *J. Combin. Theory Ser. A* **118** (2011), 448 – 454.

[6] X. Hou, A new approach to permutation polynomials over finite fields, *Finite Fields Appl.* **18** (2012), 492 – 521.

[7] X. Hou, Proof of a conjecture on permutation polynomials over finite fields, *Finite Fields Appl.* **24** (2013) 192 – 195.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[9] R. L. Rivest, Permutation polynomials modulo 2^w, *Finite Fields Appl.* **7** (2001), no. 2, 287 – 292.

[10] P. Yuan and C. Ding, Permutation polynomials of the form $L(x)+S_{2k}^a+S_{2k}^b$ over $\mathbb{F}_{q^{3k}}$, *Finite Fields Appl.* **29** (2014), 106 – 117.

Appendix

The following table is a part of [1, Table 1] of desirable triples $(n, e; q)$ with $q = 4$, $e = 6$ and $w_4(n) > 4$, where $w_4(n)$ is the base 4 weight of n.

Table 1: Desirable triples $(n, 6; 4)$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
6	4361	1,2,0,0,1,0,1	[2, Theorem 6.12]
6	6161	1,0,1,0,0,2,1	[2, Theorem 6.12]
6	6401	1,0,0,0,1,2,1	[2, Theorem 6.12]
6	8227	3,0,2,0,0,0,2	[2, Theorem 6.10]
6	8707	3,0,0,0,2,0,2	[2, Theorem 6.11]
6	12299	3,2,0,0,0,0,3	[2, Theorem 6.6]
6	12307	3,0,1,0,0,0,3	[2, Theorem 6.8]
6	14339	3,0,0,0,0,2,3	[2, Theorem 6.6]
6	37121	1,0,0,0,1,0,1,2	[2, Theorem 6.12]
6	65801	1,2,0,0,1,0,0,0,1	[2, Corollary 6.16]
6	65921	1,0,0,2,1,0,0,0,1	Theorem 1
6	66307	3,0,0,0,3,0,0,0,1	[7, Theorem 1.1]
6	135209	1,2,2,0,0,0,1,0,2	
6	135217	1,0,3,0,0,0,1,0,2	[1, Proposition 3.4]
6	135457	1,0,2,0,1,0,1,0,2	[1, Proposition 3.7]
6	137249	1,0,2,0,0,2,1,0,2	
6	8388607	3,3,3,3,3,3,3,3,3,3,3,3,1	[6, Proposition 3.1]