Results on permutation polynomials of shape $X^t + \gamma \operatorname{Tr}_{q^n/q}(X^k)$

Daniel Gerike and Gohar M. Kyureghyan

The maps of shape $T(x) = x^t + \operatorname{Tr}_{q^n/q}(x^k)$ combine in an interesting way the additive and multiplicative structures of $\mathbb{F}_{q^n}$ and serve as a source for maps with special properties required in different areas of applications. In this paper we briefly survey known results on such permutations and continue their study. We prove that if $T(x)$ is bijective on $\mathbb{F}_{q^n}$ then necessarily $\gcd(t, q^n - 1) = 1$. We show that $F(x) = x^{q^2+q+1} + \operatorname{Tr}_{q^3/q}(x)$ has very special properties on $\mathbb{F}_{q^3}$ by determining explicitly its iterates, the inverse map, the set of fixed points and its cycle structure.

Keywords. permutation polynomial, iterates, cycle structure, compositional inverse, switching construction, trace, sparse polynomials over finite fields.

1 Introduction

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Given a univariate polynomial $F(X) \in \mathbb{F}_q[X]$, its *associated map* F is defined by

$$F : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto F(x).$$

The associated maps of polynomials $F(X)$ and $G(X)$ are equal on $\mathbb{F}_q$ if and only if $F(X) \equiv G(X) \pmod{X^q - X}$. In particular, the associated maps of two different polynomials of degree less than q are different. The number of different maps of $\mathbb{F}_q$ into itself is q^q, which is also the number of different polynomials of degree less than q in $\mathbb{F}_q[X]$. This shows that any map g of $\mathbb{F}_q$ into itself is the associated map of a unique polynomial over $\mathbb{F}_q$ of degree less than q, which is called the reduced polynomial of g. The *degree* of the map g is the degree of its reduced polynomial.

A polynomial over $\mathbb{F}_q$ is called a *permutation polynomial* of $\mathbb{F}_q$ if it induces a permutation on $\mathbb{F}_q$. The degree of a permutation on $\mathbb{F}_q$ and the non-zero terms in its reduced polynomial form are basic algebraic characteristics of it, which are important parameters for its implementation costs. The cycle decomposition of a permutation provides information on both algebraic as well as combinatorial properties of it. One of the main

current challenges in the research on permutations of finite fields is finding connections between their polynomial representations and combinatorial properties. At present, this is studied for very few families of permutation polynomials [1, 3, 6, 11, 13, 15, 17, 18]. A brief summary on classes of permutation polynomials with known cycle structure is given in [18]. The latter reference describes also an application of permutation polynomials with known cycle structure in coding theory. Inverses of permutations used in coding theory or cryptology must often satisfy some special requirements [2, 18]. Since for a generic permutation it is difficult to obtain relevant informations on its inverse, it is significant to have constructions of permutation polynomials, for which the inverse polynomial is also explicitly known.

2 Permutation polynomials of form $X^t + \gamma \operatorname{Tr}_{q^n/q}(X^k)$

An interesting class of permutation polynomials, which need to be better understood is that of shape $X^t + \operatorname{Tr}_{q^n/q}(X^k)$, where $\gamma \in \mathbb{F}_{q^n}^*$ and $1 \leq t, k \leq q^n - 1$ are integers. These polynomials combine the multiplicative and additive structure of the field $\mathbb{F}_{q^n}$ in a simple manner, so that there could be a good chance to describe special properties of induced permutations.

Permutations $x^t + \operatorname{Tr}_{q^n/q}(x^k)$ were first considered for a prime q in [4, 5, 10]. In [11] several families of such permutations were found when q is odd. A further class of such permutations is described for $q = 3^r, r \geq 2$, in [14]. The case q even is treated in detail in [12].

The next theorem shows that in search for permutation polynomials of shape $X^t + \operatorname{Tr}_{q^n/q}(X^k)$ only exponents $1 \leq t \leq q^n - 1$ which are coprime with $q^n - 1$ need to be considered.

Theorem 2.1. *Let $n \geq 1$, $1 \leq t \leq q^n - 1$, $\gamma \in \mathbb{F}_{q^n}$ and $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be an arbitrary map. If the map $F(x) = x^t + \gamma f(x)$ is a permutation of $\mathbb{F}_{q^n}$, then $\gcd(t, q^n - 1) = 1$.*

Proof. Let α be a fixed nonzero element in $\mathbb{F}_{q^n}$ with $\operatorname{Tr}_{q^n/q}(\alpha\gamma) = 0$. Consider the map $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined by

$$g(x) = \operatorname{Tr}_{q^n/q}(\alpha F(x)) = \operatorname{Tr}_{q^n/q}(\alpha(x^t + \gamma f(x)))$$

Since F is a permutation of $\mathbb{F}_{q^n}$, every $y \in \mathbb{F}_q$ has q^{n-1} preimages in $\mathbb{F}_{q^n}$ under g, i. e. $\left|g^{-1}(y)\right| = q^{n-1}$. Further observe that

$$g(x) = \operatorname{Tr}_{q^n/q}(\alpha(x^t + \gamma f(x))) = \operatorname{Tr}_{q^n/q}(\alpha x^t) + f(x) \operatorname{Tr}_{q^n/q}(\alpha\gamma) = \operatorname{Tr}_{q^n/q}(\alpha x^t),$$

due to the choice of α. Let $d = \gcd(t, q^n - 1)$. Then the power map $x \mapsto x^t$ is d-to-1 on $\mathbb{F}_{q^n}^*$. This shows that d must divide $\left|g^{-1}(y)\right| = q^{n-1}$ if $y \neq 0$, completing the proof. □

The above proof works for a larger class of maps on $\mathbb{F}_{q^n}$. Recall that $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called balanced if for every $y \in \mathbb{F}_q$, the cardinality of $\{x \in \mathbb{F}_{q^n} : f(x) = y\}$ is q^{n-1}.

Theorem 2.2. *Let $G, H : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. Suppose there exists an element $\alpha \in \mathbb{F}_{q^n}^*$ such that the map $h(x) = \mathrm{Tr}_{q^n/q}(\alpha H(x))$ is constant on $\mathbb{F}_{q^n}$ and the map $g(x) = \mathrm{Tr}_{q^n/q}(\alpha G(x))$ is not balanced. Then the sum $G + H$ is not a permutation of $\mathbb{F}_{q^n}$.*

Proof. The proof follows from the observation, that if $G + H$ is a permutation of $\mathbb{F}_{q^n}$, then necessarily the map $\mathrm{Tr}_{q^n/q}(\alpha(G(x) + H(x))) = g(x) + h(x)$ is balanced. □

Observe that $\mathrm{Tr}_{q^n/q}(\alpha H(x))$ is constant on $\mathbb{F}_{q^n}$ if and only if the image set of H is contained in a coset of the hyperplane $\mathcal{H}_\alpha = \{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{q^n/q}(\alpha x) = 0\}$. In particular such an α exists if $H(X)$ is an affine q-polynomial with a nontrivial kernel.

The next result demonstrates a specific application of Theorem 2.2.

Corollary 2.3. *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a q-linear map with an image set contained in $\mathcal{H}_\alpha$ for some $\alpha \in \mathbb{F}_{q^n}^*$. Furthermore, let t be a positive integer with $\gcd(t, q^n - 1) > 1$, $P : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ a permutation and $K : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ arbitrary. Then $P(x)^t + L(K(x))$ is not a permutation on $\mathbb{F}_{q^n}$.*

Remark 2.1. Arguments similar to ours in the proofs of Theorem 2.1 and Theorem 2.2 are used in [16], where permutation polynomials $X^t + L(X)$ are studied, where $L(X)$ is a linearized polynomial.

By Theorem 2.1, any permutation polynomial $T(X) = X^t + \mathrm{Tr}_{q^n/q}(X^k)$ satisfies $\gcd(t, q^n - 1) = 1$. Let t^{-1} be the inverse of t modulo $q^n - 1$. Then $T(X^{t^{-1}}) = X + \gamma \mathrm{Tr}_{q^n/q}(X^{k \cdot t^{-1}})$ is a permutation polynomial as well. Hence to characterize all permutation polynomials of shape $X^t + \mathrm{Tr}_{q^n/q}(X^k)$ it is enough to consider those with $t = 1$. Note that if k defines such a permutation then the same permutation can be obtained with $k \cdot q$ too, because of $\mathrm{Tr}_{q^n/q}(x^{q \cdot k}) = \mathrm{Tr}_{q^n/q}(x^k)$. The next theorem lists the currently known permutation polynomials of type $X + \mathrm{Tr}_{q^n/q}(X^k)$ for q odd. The cases (a)-(i) are from [10], and (j) from [14]. The case (k) can be obtained for example using results on permutations constructed via linear translators from [11]. For the case q even we refer to [12].

Theorem 2.4. *Let $q = p^s$, where p is an odd prime and $s \geq 1$. Then*

$$F(X) = X + \gamma \mathrm{Tr}_{q^n/q}(X^k) \in \mathbb{F}_{q^n}[X]$$

is a permutation polynomial in each of the following cases.

(a) $n = 2$, $q \equiv \pm 1 \pmod 6$, $\gamma = -1/3$, $k = 2q - 1$,

(b) $n = 2$, $q \equiv 5 \pmod 6$, $\gamma^3 = -1/27$, $k = 2q - 1$,

(c) $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$,

(d) $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q + 1)^2/4$,

(e) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 - Q + 1$,

(f) $n = 2$, $q = Q^2$, $\gamma = -1$, $k = Q^3 + Q^2 - Q$,

(g) $n = 3$, $\gamma = 1$, $k = (q^2+1)/2$,

(h) $n = 3$, $\gamma = -1/2$, $k = q^2 - q + 1$,

(i) $n = 2lr$, $\gamma^{q^{2l}-1} = -1$, $k = q^l + 1$, *where* l, r *are positive integers,*

(j) $n = 2$, $q = 3^s$, $s \geq 2$, $\gamma^{(q-1)/2} = (\gamma - 1)^{(q-1)/2}$, $k = 3^{2s-1} + 3^s - 3^{s-1}$,

(k) $n \geq 2$, $(-\operatorname{Tr}_{q^n/q}(\gamma))^{(q-1)/(p^d-1)} \neq 1$, $k = p^i$, *where* $1 \leq i \leq s$ *and* $d = \gcd(i, s)$.

Remark 2.2. It can be easily checked that $k = 2q - 1$ satisfies $\gcd(k, q^2 - 1) = 1$ if $q \equiv 1 \pmod 3$ and $\gcd(k, q^2 - 1) = 3$ if $q \equiv -1 \pmod 3$. This observation with Theorem 2.4(a) show that in contrast to t the exponent k need not be coprime with $q^n - 1$ if $x^t + \gamma \operatorname{Tr}_{q^n/q}(x^k)$ is a permutation on $\mathbb{F}_{q^n}$. For all exponents k appearing in Theorem 2.4 the numbers $\gcd(k, q^n - 1)$ are explicitly determined in [8].

For a permutation polynomial $P(X)$ on $\mathbb{F}_q$ and an integer $1 \leq \ell \leq q-1$ with $\gcd(\ell q - 1) = 1$, the polynomial $P(X^\ell)$ induces a permutation on $\mathbb{F}_q$ as well. In general, the connections between cycle decompositions of permutations $P(X)$ and $P(X^\ell)$ are not straightforward. Section 3 shows that the permutation $C(x^{q^2+q+1})$ with $C(x)$ as in Theorem 2.4(g) has a very special cycle structure.

3 Permutation $X^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(X)$ on $\mathbb{F}_{q^3}$

In this section, we consider the reduced permutation polynomial $F(X)$ on $\mathbb{F}_{q^3}$ associated to the map given by

$$F(x) = (x + \operatorname{Tr}_{q^3/q}(x^{(q^2+1)/2})) \circ (x^{q^2+q-1}),$$

which is obtained by composing the permutation described in case (g) of Theorem 2.4 with the permutation $x \mapsto x^{q^2+q-1}$. We describe explicitly the iterates of F and then use this to determine its cycle structure and the polynomial representation of its inverse map.

It is easy to check that

$$(q^2 + q - 1) \cdot \frac{q^2+1}{2} = \frac{(q^3-1)(q+1)}{2} + q \equiv q \pmod{q^3 - 1}$$

and therefore

$$F(X) = X^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(X).$$

Further, for $x \neq 0$, we have

$$F(x) = \frac{x^{q^2+q} + x(x + x^q + x^{q^2})}{x} = x + \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x},$$

and hence

$$F(x) = \begin{cases} x + \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x}, & x \in \mathbb{F}_{q^3}^* \\ 0, & x = 0. \end{cases}$$

In the remaining part of this section, we use the convention $0/0 = 0$ and write

$$F(x) = x + \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} \text{ for all } x \in \mathbb{F}_{q^3}.$$

The following two lemmas describe computational connections in $\mathbb{F}_{q^3}$, which are fundamental for the results of this section.

Lemma 3.1. *Any $x \in \mathbb{F}_{q^3}$ satisfies*

$$x^3 - \mathrm{Tr}_{q^3/q}(x)x^2 + \mathrm{Tr}_{q^3/q}(x^{q+1})x - \mathrm{N}_{q^3/q}(x) = 0, \tag{1}$$

where $N_{q^3/q}(x) = x^{1+q+q^2}$ is the norm of x *over $\mathbb{F}_q$.*

Proof. Any $x \in \mathbb{F}_q$ clearly fulfils (1). Let hence $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $m(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of x over $\mathbb{F}_q$. Since $m(X) = (X - x)(X - x^q)(X - x^{q^2})$ in $\mathbb{F}_{q^3}[X]$, we get

$$m(X) = X^3 - \mathrm{Tr}_{q^3/q}(x)X^2 + \mathrm{Tr}_{q^3/q}(x^{q+1})X - \mathrm{N}_{q^3/q}(x),$$

implying the statement. □

Lemma 3.2. *Let $x \in \mathbb{F}_{q^3}^*$. Then we have*

(a) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{\mathrm{N}_{q^3/q}(x)}$;

(b) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) = \frac{\mathrm{Tr}_{q^3/q}(x)}{\mathrm{N}_{q^3/q}(x)}$;

(c) $\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q-1}}\right) + \mathrm{Tr}_{q^3/q}(x^{q-1}) = \mathrm{Tr}_{q^3/q}(x^{q+1})\,\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) - 3.$

Proof. Property (a) follows from

$$\mathrm{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \frac{1}{x} + \frac{1}{x^q} + \frac{1}{x^{q^2}} = \frac{x^{q^2+q} + x^{q^2+1} + x^{q+1}}{x^{1+q+q^2}} = \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{\mathrm{N}_{q^3/q}(x)}.$$

This also shows that

$$\mathrm{Tr}_{q^3/q}(x) = \frac{\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right)}{\mathrm{N}_{q^3/q}\left(\frac{1}{x}\right)} = \mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right)\mathrm{N}_{q^3/q}(x),$$

from which (b) follows. For (c), note that

$$\begin{aligned}
\mathrm{Tr}_{q^3/q}(x^{q+1})\,\mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q+1}}\right) &= \mathrm{Tr}_{q^3/q}\left(\frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x^{q+1}}\right) \\
&= \mathrm{Tr}_{q^3/q}\left(\frac{x^{q+1} + x^{q^2+q} + x^{q^3+q^2}}{x^{q+1}}\right) \\
&= \mathrm{Tr}_{q^3/q}(1 + x^{q^2-1} + x^{q^2-q}) \\
&= 3 + \mathrm{Tr}_{q^3/q}\left(\frac{1}{x^{q-1}}\right) + \mathrm{Tr}_{q^3/q}(x^{q-1}).
\end{aligned}$$

□

Theorem 3.3. *Let*

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : F(x) = x\}$$

be the set of fixed points of $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$. *Then we have*

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{q^3/q}(x^{q+1}) = 0\} = \{0\} \cup \{x \in \mathbb{F}_{q^3}^* : \mathrm{Tr}_{q^3/q}(x^{-1}) = 0\}.$$

In particular, $|\mathrm{Fix}(F)| = q^2$.

Proof. By definition of F, it is straightforward, that

$$\mathrm{Fix}(F) = \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{q^3/q}(x^{q+1}) = 0\}.$$

Lemma 3.2(a) completes the proof. □

Claim. For an integer $n \geq 0$, set

$$\begin{aligned} a_n &= \frac{4^n + (-2)^n - 2}{9}, \\ b_n &= \frac{(-2)^n - 1}{3}, \\ c_n &= a_{n+1} - a_n = \frac{4^n - (-2)^n}{3}, \\ d_n &= b_{n+1} - b_n = -(-2)^n. \end{aligned}$$

Then all these numbers are integers and they satisfy

$$b_n^2 + 2a_n - b_n = c_n \tag{2}$$

$$-(c_n b_n + d_n a_n) = c_n \tag{3}$$

$$d_n b_n = -c_n \tag{4}$$

Proof. Equations (2)–(4) can be easily checked by the following direct calculations:

$$\begin{aligned} b_n^2 + 2a_n - b_n &= \frac{((-2)^n - 1)^2}{9} + \frac{2 \cdot 4^n + 2 \cdot (-2)^n - 4}{9} - \frac{(-2)^n - 1}{3} \\ &= \frac{4^n - 2(-2)^n + 1 + 2 \cdot 4^n + 2(-2)^n - 4}{9} - \frac{(-2)^n - 1}{3} \\ &= \frac{4^n - 1 - ((-2)^n - 1)}{3} = \frac{4^n - (-2)^n}{3}; \\ -(c_n b_n + d_n a_n) &= -\left(\frac{4^n - (-2)^n}{3} \cdot \frac{(-2)^n - 1}{3} - (-2)^n \cdot \frac{4^n + (-2)^n - 2}{9}\right) \\ &= -\frac{(4^n - (-2)^n)((-2)^n - 1) - (-2)^n(4^n + (-2)^n - 2)}{9} \\ &= -\frac{4^n(-2)^n - 4^n - 4^n + (-2)^n - 4^n(-2)^n - 4^n + 2(-2)^n}{9} \\ &= -\frac{(-2)^n - 4^n}{3} = \frac{4^n - (-2)^n}{3}; \\ d_n b_n &= -(-2)^n \cdot \frac{(-2)^n - 1}{3} = -\frac{4^n - (-2)^n}{3}. \end{aligned}$$

Note that

$$b_n = \begin{cases} (2^n - 1)/3, & n \text{ even}, \\ -(2^n + 1)/3, & n \text{ odd}. \end{cases}$$

Recall that $3 = 2^2 - 1$ divides $2^n - 1$ if and only if n is even. Consequently, 3 divides $2^n + 1$ if and only if n is odd. These observations show, that b_n is an integer. Since $c_n = -d_n b_n$ and $2a_n = c_n - b_n^2 + b_n$, these numbers are also integers. □

Remark 3.1. By abuse of notation, we use the same symbol a for an integer number a and an element a mod p of a prime field $\mathbb{F}_p$. In the remainder of this chapter, we use $a/3$ to denote elements in $\mathbb{F}_p$ not only for $p \geq 5$ but also in $\mathbb{F}_3$. In the latter case, we assume that the integer a is divisible by 3 and the quotient $a/3$ is computed in the ring of integers.

For an integer $n \geq 0$, set

$$F^n(x) = (\underbrace{F \circ F \circ \cdots \circ F}_{n})(x)$$

to denote the nth iterate of F.

Theorem 3.4. *Let q be a power of an odd prime and*

$$F(x) = x + \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x}$$

on $\mathbb{F}_{q^3}$. Then for $n \geq 0$, we have

$$F^n(x) = a_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - b_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x, \tag{5}$$

where $a_n = (4^n + (-2)^n - 2)/9$ and $b_n = ((-2)^n - 1)/3$.

Proof. For $n \geq 0$, we put $c_n = a_{n+1} - a_n = (4^n - (-2)^n)/3$ and $d_n = b_{n+1} - b_n = -(-2)^n$ and define

$$F_n(x) = a_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - b_n \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x.$$

We aim to prove that $F^n(x) = F_n(x)$.

First, consider $x \in \mathbb{F}_q$. Then we have $\mathrm{Tr}_{q^3/q}(x^{q+1}) = 3x^2$ and $\mathbb{N}_{q^3/q}(x) = x^3$, implying

$$F(x) = x + \frac{3x^2}{x} = 4x,$$

and

$$\begin{aligned} F_n(x) &= a_n \frac{9x^4}{x^3} - b_n \frac{3x^2}{x} + x = (9a_n - 3b_n + 1)x \\ &= (4^n + (-2)^n - 2 - (-2)^n + 1 + 1)x = 4^n x = F^n(x). \end{aligned}$$

The statement is obviously true also for $x \in \mathrm{Fix}(F)$, since in this case $\mathrm{Tr}_{q^3/q}(x^{q+1}) = 0$. We apply induction on n to prove the identity for the remaining cases. Hence let $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and $\mathrm{Tr}_{q^3/q}(x^{q+1}) \neq 0$. The statement is true for $n = 0$ and $n = 1$. Our goal is to show that

$$F_{n+1}(x) = F^{n+1}(x) = F(F^n(x)) = F(F_n(x)) = F_n(x) + \frac{\mathrm{Tr}_{q^3/q}(F_n(x)^{q+1})}{F_n(x)},$$

or equivalently

$$(F_{n+1}(x) - F_n(x)) \cdot F_n(x) = \mathrm{Tr}_{q^3/q}(F_n(x)^{q+1}),$$

holds, if $F^n(x) = F_n(x)$. In the rest of the proof, we use the following abbreviations:

$$\begin{aligned} L(x) &= (F_{n+1}(x) - F_n(x)) \cdot F_n(x) \\ R(x) &= \mathrm{Tr}_{q^3/q}(F_n(x)^{q+1}) \end{aligned}$$

and $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(x) = \mathrm{Tr}_{q^3/q}(x^{q+1})$. Our goal is to show $L(x) = R(x)$ for all $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ with $u(x) \neq 0$. First, observe that $R(x)$ can be written as follows:

$$\begin{aligned} R(x) &= \mathrm{Tr}\left[\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)^q \cdot \left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\right] \\ &= \mathrm{Tr}\left[\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x^q} + x^q\right) \cdot \left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\right] \\ &= \mathrm{Tr}\left[a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2\frac{u(x)^2}{x^{q+1}} - a_nb_n\frac{u(x)^3}{\mathrm{N}(x)}\left(\frac{1}{x} + \frac{1}{x^q}\right) + a_n\frac{u(x)^2}{\mathrm{N}(x)}(x + x^q)\right. \\ &\qquad \left. -b_nu(x)\left(x^{q-1} + \frac{1}{x^{q-1}}\right) + x^{q+1}\right] \\ &= 3a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2u(x)^2\,\mathrm{Tr}\left(\frac{1}{x^{q+1}}\right) - 2a_nb_n\frac{u(x)^3}{\mathrm{N}(x)}\,\mathrm{Tr}\left(\frac{1}{x}\right) + 2a_n\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) \\ &\quad - b_nu(x)\left(\mathrm{Tr}(x^{q-1}) + \mathrm{Tr}\left(\frac{1}{x^{q-1}}\right)\right) + u(x). \end{aligned}$$

Applying Lemma 3.2(a), (b) and (c) to the last expression, we get

$$\begin{aligned} R(x) &= 3a_n^2\frac{u(x)^4}{\mathrm{N}(x)^2} + b_n^2u(x)^2\frac{\mathrm{Tr}(x)}{\mathrm{N}(x)} - 2a_nb_n\frac{u(x)^3}{\mathrm{N}(x)} \cdot \frac{u(x)}{\mathrm{N}(x)} + 2a_n\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) \\ &\quad - b_nu(x)\left(u(x)\frac{\mathrm{Tr}(x)}{\mathrm{N}(x)} - 3\right) + u(x). \\ &= (3a_n^2 - 2a_nb_n)\frac{u(x)^4}{\mathrm{N}(x)^2} + (b_n^2 + 2a_n - b_n)\frac{u(x)^2}{\mathrm{N}(x)}\,\mathrm{Tr}(x) + (3b_n + 1)u(x), \end{aligned}$$

and hence

$$\frac{R(x)}{u(x)} = (3a_n^2 - 2a_nb_n)\frac{u(x)^3}{\mathrm{N}(x)^2} + (b_n^2 + 2a_n - b_n)\frac{u(x)}{\mathrm{N}(x)}\,\mathrm{Tr}(x) + 3b_n + 1.$$

We compute now $L(x)/u(x)$:

$$\begin{aligned}\frac{L(x)}{u(x)} &= \left(c_n\frac{u(x)}{\mathrm{N}(x)} - d_n\frac{1}{x}\right)\left(a_n\frac{u(x)^2}{\mathrm{N}(x)} - b_n\frac{u(x)}{x} + x\right)\\ &= c_n a_n\frac{u(x)^3}{\mathrm{N}(x)^2} - (c_n b_n + d_n a_n)\frac{u(x)^2}{\mathrm{N}(x)x} + d_n b_n\frac{u(x)}{x^2} + c_n\frac{u(x)x}{\mathrm{N}(x)} - d_n.\end{aligned}$$

Because

$$3a_n^2 - 2a_n b_n = a_n(3a_n - 2b_n) = a_n\frac{4^n + (-2)^n - 2 - 2(-2)^n + 2}{3} = a_n c_n$$

and

$$3b_n + 1 = (-2)^n = -d_n,$$

to prove $R(x)/u(x) = L(x)/u(x)$ it is enough to show that

$$c_n\frac{u(x)x}{\mathrm{N}(x)} - (b_n^2 + 2a_n - b_n)\frac{u(x)}{\mathrm{N}(x)}\operatorname{Tr}(x) - (c_n b_n + d_n a_n)\frac{u(x)^2}{\mathrm{N}(x)x} + d_n b_n\frac{u(x)}{x^2} = 0$$

Or equivalently, by multiplying with $\mathrm{N}(x)x^2/u(x) \neq 0$,

$$c_n x^3 - (b_n^2 + 2a_n - b_n)\operatorname{Tr}(x)x^2 - (c_n b_n + d_n a_n)u(x)x + d_n b_n\,\mathrm{N}(x) = 0. \tag{6}$$

Using (2)–(4), we reduce (6) to

$$c_n x^3 - c_n\operatorname{Tr}(x)x^2 + c_n\operatorname{Tr}(x^{q+1})x - c_n\,\mathrm{N}(x) = 0,$$

for $n \geq 1$, also $c_n \geq 1$ and we can further reduce to

$$x^3 - \operatorname{Tr}(x)x + \operatorname{Tr}(x^{q+1})x - \mathrm{N}(x) = 0,$$

which is satisfied for any $x \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ by Lemma 3.1. □

Remark 3.2. The iterate $F^n(x)$ in (5) can be written in polynomial form

$$F^n(X) = a_n\operatorname{Tr}_{q^3/q}(X^{q^2+q-1}) + (2a_n - b_n)\operatorname{Tr}_{q^3/q}(X) - b_n X^{q^2+q-1} + (b_n + 1)X,$$

using the following identities in $\mathbb{F}_{q^3}$:

$$\begin{aligned}\frac{\operatorname{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} &= \operatorname{Tr}_{q^3/q}(x^{q+1})\operatorname{Tr}_{q^3/q}\left(\frac{1}{x}\right) = \operatorname{Tr}_{q^3/q}\left(\frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x}\right)\\ &= \operatorname{Tr}_{q^3/q}\left(\frac{x^{q+1} + x^{q^2+q} + x^{q^2+1}}{x}\right)\\ &= \operatorname{Tr}_{q^3/q}(x^q) + \operatorname{Tr}_{q^3/q}(x^{q^2+q-1}) + \operatorname{Tr}_{q^3/q}(x^{q^2})\\ &= \operatorname{Tr}_{q^3/q}(x^{q^2+q-1}) + 2\operatorname{Tr}_{q^3/q}(x)\end{aligned}$$

and

$$F(x) = \frac{\operatorname{Tr}_{q^3/q}(x^{q+1})}{x} + x = x^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(x).$$

Theorem 3.5. *Let $q = p^s$ where $p \geq 5$ and $m = \mathrm{ord}_p(4)$. Then the permutation F on $\mathbb{F}_{q^3}$ defined by $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$ satisfies the following properties:*

(a) *If $\mathrm{ord}_p(-2) = \mathrm{ord}_p(4)$, then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} m^{(q^3-q^2)/m}.$$

(b) *If $\mathrm{ord}_p(-2) = 2 \cdot \mathrm{ord}_p(4)$, then the cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} m^{(q-1)/m} (2m)^{(q^3-q^2-q+1)/(2m)}.$$

The cycles of length m partition the set of nonzero elements of the subfield $\mathbb{F}_q$, i. e.

$$\mathrm{CS}_{\mathbb{F}_q}(F) = 1^1 m^{(q-1)/m}.$$

(c) *The permutation F has order $\mathrm{ord}_p(-2)$ in the symmetric group of permutations on $\mathbb{F}_{q^3}$.*

Proof. Clearly, (c) is a direct consequence of (a) and (b). Let $y \in \mathbb{F}_{q^3}$ and $y \notin \mathrm{Fix}(F)$, i. e. $u(y) \neq 0$. Let $t \geq 2$ be the minimal integer with $F^t(y) = y$, i. e. $t = \ell(F, y)$, the length of the cycle containing y in the cycle decomposition of F. Recall the abbreviations $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(y) = \mathrm{Tr}_{q^3/q}(y^{q+1})$. Then

$$F^t(y) - y = a_t \frac{u(y)^2}{\mathrm{N}(y)} - b_t \frac{u(y)}{y} = 0,$$

implying

$$a_t \cdot u(y) = b_t \cdot \frac{\mathrm{N}(y)}{y} = b_t \cdot y^{q^2+q}. \tag{7}$$

Then necessarily it holds

$$\mathrm{Tr}(a_t \cdot u(y)) = \mathrm{Tr}(b_t \cdot y^{q^2+q}),$$

or equivalently

$$3 \cdot a_t \cdot u(y) = b_t \cdot u(y),$$

and hence

$$\frac{4^t + (-2)^t - 2}{3} = 3 \cdot a_t = b_t = \frac{(-2)^t - 1}{3},$$

which is equivalent to $4^t = 1$. This shows that t must be divisible by $\mathrm{ord}_p(4)$, and in particular

$$t \geq \mathrm{ord}_p(4). \tag{8}$$

Let $r = \mathrm{ord}_p(-2)$. Then $a_r = b_r = 0$ and, therefore

$$t \leq \mathrm{ord}_p(-2). \tag{9}$$

Hence if $\mathrm{ord}_p(4) = \mathrm{ord}_p(-2)$, the statement in (a) follows from (8) and (9). Suppose now $r = 2 \cdot \mathrm{ord}_p(4)$, then $t \in \{m, 2m\}$ and we have to determine for which y, the integer $t = m$. For $t = m$, the equation (7) reduces to

$$u(y) = 3 \cdot y^{q^2+q},$$

since in this case $a_t = -2/9$ and $b_t = -2/3$. In particular, y^{q^2+q} then belongs to the subfield $\mathbb{F}_q$, since $u(y)$ does. This yields

$$y^{q^2+1} = (y^{q^2+q})^q = y^{q^2+q},$$

which is equivalent to $y \in \mathbb{F}_q$. This proves (b). □

Theorem 3.6. *Let $q = p^s$, where $p \geq 5$. The inverse map of*

$$F(x) = x + \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} = x^{q^2+q-1} + \mathrm{Tr}_{q^3/q}(x)$$

on $\mathbb{F}_{q^3}$ is $F^k(x)$, where $k = \mathrm{ord}_p(-2) - 1$. More precisely, it holds

$$\begin{aligned} F^{-1}(x) &= -\frac{1}{4} \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} + \frac{1}{2} \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x \\ &= -\frac{1}{4} \cdot \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + \frac{1}{2} \cdot x^{q^2+q-1} + \frac{1}{2}x. \end{aligned}$$

Proof. Theorem 3.5(c) yields $F^{-1}(x) = F^k(x)$, where $k = \mathrm{ord}_p(-2) - 1$. It remains to note that $a_k = -1/4$ and $b_k = -1/2$. The polynomial form is obtained using the identities from Remark 3.2. □

In [7] it is shown, that the inverse map of a permutation $x + \gamma \,\mathrm{Tr}_{q^n/q}(x^k)$ has the form $x + \gamma g(x)$, with $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$. In general, an explicit description of g is a difficult problem. The inverse of the permutation $F_{16}(x) = x + \mathrm{Tr}_{q^3/q}(x^{(q^2+1)/2})$ can be determined using Theorem 3.6 and he fact that $F(x) = F_{16}(x^{q^2+q-1})$:

Corollary 3.7. *Let $q = p^s$, where $p \geq 5$. The inverse map of the permutation $F_{16}(x) = x + \mathrm{Tr}_{q^3/q}(x^{(q^2+1)/2}))$ on $\mathbb{F}_{q^3}$ is given by*

$$F_{16}^{-1}(x) = \left(-\frac{1}{4} \cdot \mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) + \frac{1}{2} \cdot x^{q^2+q-1} + \frac{1}{2}x \right)^{q^2+q-1}.$$

The next theorem presents results on $F(x)$ in the case $p = 3$.

Theorem 3.8. *Let $q = 3^s$, with $s \geq 1$, and F be the permutation on $\mathbb{F}_{q^3}$ given by $F(x) = x + (\mathrm{Tr}_{q^3/q}(x^{q+1}))/x$. Then F has the following properties:*

(a) *The order of F is* 3.

(b) *The cycle structure of F is*

$$\mathrm{CS}(F) = 1^{q^2} 3^{(q^3-q^2)/3}.$$

(c) *The inverse map of F is given by*

$$\begin{aligned} F^{-1}(x) &= 2 \cdot \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})^2}{\mathrm{N}_{q^3/q}(x)} - \frac{\mathrm{Tr}_{q^3/q}(x^{q+1})}{x} + x \\ &= -\mathrm{Tr}_{q^3/q}(x^{q^2+q-1}) - x^{q^2+q-1} - x. \end{aligned}$$

Proof. Recall the abbreviations $\mathrm{Tr} = \mathrm{Tr}_{q^3/q}$, $\mathrm{N} = \mathrm{N}_{q^3/q}$, $u(y) = \mathrm{Tr}_{q^3/q}(y^{q+1})$. Let id_{q^3} be the identity function on $\mathbb{F}_{q^3}$. Using formula (5) and computing $a_2 = 2$, $b_2 = 1$, $a_3 = 0$, $b_3 = 0$, it is easy to see that $F^2 \neq \mathrm{id}_{q^3}$, whereas $F^3 = \mathrm{id}_{q^3}$, proving (a). To verify (b), note that by (a) the cycles of F have length at most 3. To show that there are no cycles of length 2, we prove that if $F^3(y) = y$ for $y \in \mathbb{F}_{q^3}$, then $y \in \mathrm{Fix}(F)$. Indeed, if

$$F^2(y) = 2 \cdot \frac{u(y)^2}{\mathrm{N}(y)} - \frac{u(y)}{y} + y = y,$$

it follows that

$$2 \cdot u(y) = y^{q^2+q},$$

and then

$$0 = \mathrm{Tr}(2 \cdot u(y)) = \mathrm{Tr}(x^{q^2+q}) = u(y),$$

i. e. $y \in \mathrm{Fix}(F)$. Theorem 3.3 completes the proof. The statement in (c) follows from (a), which implies that $F^{-1}(x) = F^2(x)$. □

Aknowledgments. We thank Lukas Kölsch for interesting discussions leading to Corollary 2.3 and for pointing us to reference [16].

Remark. This is a preprint of [9].

References

[1] Shair Ahmad. Cycle Structure of Automorphisms of Finite Cyclic Groups. In: *J. Comb. Theory* 6.4 (1969), pp. 370–374.

[2] Christina Boura and Anne Canteaut. On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$. In: *IEEE Trans. Inf. Theory* 59 (2013), pp. 691–702.

[3] Ayça Çeşmelioğlu, Wilfried Meidl, and Alev Topuzoğlu. On the cycle structure of permutation polynomials. In: *Finite Fields Appl.* 14.3 (2008), pp. 593–614.

[4] Pascale Charpin and Gohar Kyureghyan. Monomial functions with linear structure and permutation polynomials. In: *Contemp. Math.* 518 (2010), pp. 99–111.

[5] Pascale Charpin and Gohar M. Kyureghyan. On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$. In: *Sequences and Their Applications - SETA 2008*. Ed. by Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof. Lect. Notes Comput. Sci. 5203. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 368–376.

[6] Pascale Charpin, Sihem Mesnager, and Sumanta Sarkar. Involutions Over the Galois Field $\mathbb{F}_{2^n}$. In: *IEEE Trans. Inf. Theory* 62.4 (2016), pp. 2266–2276.

[7] Mikayel G. Evoyan, Gohar M. Kyureghyan, and Melsik K. Kyuregyan. On k-Switching of Mappings on Finite Fields. In: *Math. Probl. Comput. Sci.* 39 (2013), pp. 5–12.

[8] Daniel Gerike. PhD Thesis, Otto-von-Guericke University of Magdeburg. in preparation.

[9] Daniel Gerike and Gohar M. Kyureghyan. Results on permutation polynomials of shape $x^t + \gamma \operatorname{Tr}_{q^n/q}(x^d)$. In: *Combinatorics and Finite Fields*. Ed. by Kai-Uwe Schmidt and Arne Winterhof. Radon Ser. Comput. Appl. Math. 23. Berlin, Boston: De Gruyter, 2019, pp. 67–78.

[10] Gohar Kyureghyan and Michael Zieve. Permutation polynomials of the form $X + \gamma \operatorname{Tr}(X^k)$. In: *Contemporary Developments in Finite Fields and Applications*. Ed. by Anne Canteaut, Gove Effinger, Sophie Huczynska, Daniel Panario, and Leo Storme. Singapore: World Scientific, 2016, pp. 178–194.

[11] Gohar M. Kyureghyan. Constructing permutations of finite fields via linear translators". In: *J. Comb. Theory*. Ser. A 118.3 (2011), pp. 105–1061.

[12] Kangquan Li, Longjiang Qu, Xi Chen, and Chao Li. Permutation polynomials of the form $cx + \operatorname{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic. In: *Cryptogr. Commun.* 10.3 (2018), pp. 531–554.

[13] Rudolf Lidl and Gary L. Mullen. Cycle Structure of Dickson Permutation Polynomials. In: *Math. J. Okayama Univ.* 33 (1991), pp. 1–11.

[14] Jingxue Ma and Gennian Ge. A note on permutation polynomials over finite fields. In: *Finite Fields Appl.* 48 (2017), pp. 261–270.

[15] Gary L. Mullen and Theresa P. Vaughan. Cycles of Linear Permutations Over a Finite Field. In: *Linear Algebra Appl.* 108 (1988), pp. 63–82.

[16] Enes Pasalic and Pascale Charpin. Some results concerning cryptographically significant mappings over GF(2^n). In: *Des. Codes Cryptogr.* 57.3 (2010), pp. 257–269.

[17] Ivelisse M. Rubio and Carlos J. Corrada-Bravo. Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials. In: *Finite Fields and Applications*. Ed. by Gary L. Mullen, Alain Poli, and Henning Stichtenoth. Lect. Notes Comput. Sci. 2948. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 254–261.

[18] Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Cycle structure of permutation functions over finite fields and their applications. In: *Adv. Math. Commun.* 6.3 (2012), pp. 347–361.

Author information

Daniel Gerike, Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany.
E-mail: daniel.gerike@ovgu.de

Gohar M. Kyureghyan, University of Rostock, Institute of Mathematics, Ulmenstrasse 69, Haus 3, 18057 Rostock, Germany.
E-mail: gohar.kyureghyan@uni-rostock.de