Designs, Codes and Cryptography (2020) 88:1723–1740
https://doi.org/10.1007/s10623-020-00721-2

Permutations on finite fields with invariant cycle structure on lines

Daniel Gerike[1] · **Gohar M. Kyureghyan**[2]

Received: 3 September 2019 / Revised: 31 December 2019 / Accepted: 16 January 2020 /
Published online: 14 February 2020

Abstract
We study the cycle structure of permutations $F(x) = x + \gamma f(x)$ on $\mathbb{F}_{q^n}$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. We show that for a 1-homogeneous function f the cycle structure of F can be determined by calculating the cycle structure of certain induced mappings on parallel lines of $\gamma \mathbb{F}_q$. Using this observation we describe explicitly the cycle structure of two families of permutations over $\mathbb{F}_{q^2}$: $x + \gamma \operatorname{Tr}(x^{2q-1})$, where $q \equiv -1 \pmod 3$ and $\gamma \in \mathbb{F}_{q^2}$, with $\gamma^3 = -\frac{1}{27}$ and $x + \gamma \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$, where $q = 2^s$, s odd and $\gamma \in \mathbb{F}_{q^2}$, with $\gamma^{(q+1)/3} = 1$.

Keywords Permutation polynomials · Cycle structure · Switching construction · Subspaces

Mathematics Subject Classification 11T06 · 05A05 · 11T71 · 12Y05

A permutation can be expressed as a unique product of disjoint cycles (up to reordering). The cycle decomposition of a permutation on a finite field provides information on both algebraic as well as combinatorial properties of the permutation. Much of that information is retained in the *cycle structure* of the permutation, which lists the lengths of the cycles and their frequencies in the cycle decomposition. Two permutations have the same cycle structure exactly if they lie in the same conjugacy class of the symmetric group. One of the main current challenges in the research on permutations of finite fields is finding the cycle structure for interesting families of permutation polynomials, and vice versa, given a conjugacy class of the symmetric group over a finite field, find a nice member of it. At present, the cycle structure is studied for very few families of permutation polynomials. In [1] the cycle structure of monomials x^k over $\mathbb{F}_q$ is determined. It directly depends on the multiplicative order of the exponent k modulo the divisors of $q-1$. In [10] formulas for

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography 2019".

✉ Daniel Gerike
daniel.gerike@ovgu.de

Gohar M. Kyureghyan
gohar.kyureghyan@uni-rostock.de

1 Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany

2 University of Rostock, Ulmenstraße 69, Haus 3, 18057 Rostock, Germany

the cycle structure of Dickson polynomials $D_n(x, a)$ with parameter $a = 1$ or $a = -1$ are given. The cycle structure of Dickson polynomials is similar to the cycle structure of monomials. In [12] the cycle structure of q-linearized polynomials over $\mathbb{F}_{q^n}$ is considered. The authors give a formula for the cycle structure of the restriction of a linearized polynomial to certain subspaces of $\mathbb{F}_{q^n}$. Further they show how to combine these results to get the cycle structure on the whole field. Applying this method to a given family of linearized permutation polynomials is often challenging. However it can be used to compute the cycle structure of an explicitly given linearized permutation polynomial using a computer algebra system, e. g. SAGE or MAGMA. In [13] functional graphs of mappings of finite fields are considered. This approach leads to a refinement of the results obtained in [12]. In [2] the authors show that any permutation polynomial P_n with Carlitz rank n can be written as $P_n = C_n \circ R_n$, where C_n is a single cycle of length n and R_n is a Möbius transformation. They use this fact to determine the cycle structure of permutation polynomials with low Carlitz rank.

In this paper we study the cycle structure of permutation polynomials of shape $x + \gamma f(x)$ on $\mathbb{F}_{q^n}$, where $\gamma \in \mathbb{F}_{q^n}^*$ and $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. In particular we show that if f is 1-homogeneous, then it suffices to consider the induced permutations on certain lines. We use this observation to describe the cycle structure of two families of permutations on $\mathbb{F}_{q^2}$: $x + \gamma\,\mathrm{Tr}(x^{2q-1})$, where $q \equiv -1 \pmod 3$, $\gamma \in \mathbb{F}_{q^2}$, $\gamma^3 = -\frac{1}{27}$ and $x + \gamma\,\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$, where $q = 2^s$, s odd and $\gamma \in \mathbb{F}_{q^2}$, with $\gamma^{(q+1)/3} = 1$.

1 Induced permutations on lines and subspaces

Let $q = p^s$ with p a prime number and $s \in \mathbb{N}$. In this paper we consider $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space. Similarly all mentioned vector spaces are over $\mathbb{F}_q$. The following result is straightforward.

Lemma 1 *Let $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}$. Then F maps every line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$ into itself.*

Proof Let $\alpha + \gamma u \in \alpha + \gamma\mathbb{F}_q$, then

$$F(\alpha + \gamma u) = \alpha + \gamma u + \gamma f(\alpha + \gamma u) = \alpha + \gamma(u + f(\alpha + \gamma u)) \in \alpha + \gamma\mathbb{F}_q.$$

So F maps $\alpha + \gamma\mathbb{F}_q$ into itself. □

The next lemma shows that the converse of the above lemma is also true.

Lemma 2 *Let $\gamma \in \mathbb{F}_{q^n}^*$. If $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ maps every line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^n}$ into itself, then $F(x) = x + \gamma f(x)$ for an appropriate mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$.*

Proof By assumption, for any $\alpha \in \mathbb{F}_{q^n}$ there exists a mapping $f_\alpha : \mathbb{F}_q \to \mathbb{F}_q$ such that

$$F(\alpha + \gamma u) = \alpha + \gamma(u + f_\alpha(u)) = \alpha + \gamma u + \gamma f_\alpha(u)$$

for $u \in \mathbb{F}_q$. Let now A be a system of representatives for the cosets of the line $\gamma\mathbb{F}_q$ in $\mathbb{F}_{q^n}$. Then every $x \in \mathbb{F}_{q^n}$ can be uniquely written as $\alpha + \gamma u$ with $\alpha \in A$, $u \in \mathbb{F}_q$. For $x = \alpha + \gamma u$ with $\alpha \in A$ and $u \in \mathbb{F}_q$ we define $f(x) = u + f_\alpha(u)$. Then clearly

$$F(x) = F(\alpha + \gamma u) = \alpha + \gamma u + \gamma f_\alpha(u) = x + \gamma f(x),$$

where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, with $f(x) = u + f_\alpha(u)$. □

Remark 1 Let $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. Further let L be a subspace of $\mathbb{F}_{q^n}$ containing γ. Then $\gamma\mathbb{F}_q \subseteq L$ and $L = \bigcup_{\alpha \in L}(\alpha + \gamma\mathbb{F}_q)$ is a union of cosets of $\gamma\mathbb{F}_q$. Hence any coset $\beta + L = \bigcup_{\alpha \in L}(\alpha + \beta + \gamma\mathbb{F}_q)$. Since F maps any of those lines into themselves it also maps any coset of L into itself.

As an immediate corollary of Lemma 1 we get the following result.

Theorem 1 *Let $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $F(x) = x + \gamma f(x)$, where $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. Then F permutes $\mathbb{F}_{q^n}$ if and only if it permutes every line $\alpha + \gamma\mathbb{F}_q$ with $\alpha \in \mathbb{F}_{q^n}$.*

The next observation follows directly from Theorem 1.

Proposition 1 *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}^*$. If $F(x) = x + \gamma f(x)$ is a permutation of $\mathbb{F}_{q^n}$, then every cycle in its cycle decomposition has a length not exceeding q.*

Let S_A denote the symmetric group of a set A. Two permutations $\pi : A \to A$ and $\pi' : B \to B$ are called *conjugate*, if there exists a bijection $\varphi : A \to B$, with $\pi = \varphi^{-1} \circ \pi' \circ \varphi$. The next well known fact is used often in the sequel.

Proposition 2 *Let A, B be finite sets with $|A| = |B|$ and $F \in S_A$ and $G \in S_B$. Then F and G have the same cycle structure if and only if there exists a bijection $\varphi : A \to B$, with $F = \varphi^{-1} \circ G \circ \varphi$.*

Recall that a mapping $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called *homogeneous* of degree 1 or 1-*homogeneous*, if $g(ux) = ug(x)$ for any $u \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$. Next we consider a special class of permutations $F(x) = x + \gamma f(x)$, where f is homogeneous of degree 1. The following theorem shows that the cycle structure of such permutations has an interesting regularity.

Theorem 2 *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be 1-homogeneous and $\gamma \in \mathbb{F}_{q^n}^*$. Further let L and M be subspaces of $\mathbb{F}_{q^n}$ such that $\gamma \in L$, $L \subsetneq M$ and $\dim(L) = \dim(M) - 1$. If $F(x) = x + \gamma f(x)$ permutes $\mathbb{F}_{q^n}$, then F has the same cycle structure on all cosets $m + L \neq L$ of L in M.*

Proof Let $\alpha \in M \setminus L$ be fixed. Then for any $m \in M \setminus L$, the coset $m + L$ can be represented as $\alpha t + L$ with $t \in \mathbb{F}_q^*$. By Remark 1, the mapping F is a permutation on the coset $t\alpha + L$. Let now $l \in L$. Then for a fixed t, we get

$$F(t\alpha + l) = t\alpha + l + \gamma f(t\alpha + l) = t\alpha + G_t(l)$$

with $G_t(l) : L \to L$, $G_t(l) = l + \gamma f(t\alpha + l)$. Since $G_t(l) = F(t\alpha + l) - t\alpha = \tau^{-1} \circ F \circ \tau$, where $\tau : L \to t\alpha + L$, with $\tau(l) = l + t\alpha$, Proposition 2 shows that $G_t(l)$ is a permutation of L that has the same cycle structure as F on $t\alpha + L$. To complete the proof, it remains to show, that the cycle structure of G_t is independent of t. Since f is homogeneous of degree 1, we have

$$\begin{aligned} t^{-1}G_t(tl) &= t^{-1}(tl + \gamma f(t\alpha + tl)) = t^{-1}(tl + \gamma f(t(\alpha + l)) \\ &= t^{-1}(tl + t\gamma f(\alpha + l)) = l + \gamma f(\alpha + l) = G_1(l). \end{aligned}$$

This shows that G_t and G_1 are conjugate permutations in the symmetric group S_L and consequently have the same cycle structure. □

For the choice $L = \gamma\mathbb{F}_q$ and M any two dimensional subspace of $\mathbb{F}_{q^n}$ containing γ, Theorem 2 implies that the cycle structure of the permutation $F(x) = x + \gamma f(x)$ is the same on all parallel lines $m + \gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ contained in M. This is a key observation for understanding the cycle structure of permutations of shape $x + \gamma f(x)$ which we summarize in the following theorem.

Theorem 3 *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be 1-homogeneous and $\gamma \in \mathbb{F}_{q^n}^*$. Suppose $F(x) = x + \gamma f(x)$ is a permutation on $\mathbb{F}_{q^n}$. Then the following holds:*

(a) *If M is a two dimensional subspace of $\mathbb{F}_{q^n}$ containing γ, then the cycle structure of F is the same on every line $m + \gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ lying in M.*
(b) *There are at most $1 + (q^{n-1} - 1)/(q - 1)$ lines in $\mathbb{F}_{q^n}$ such that the cycle structure of F is pairwise different on them.*

Proof The statement follows from Theorem 2 with M of dimension 2 and the observation that $\frac{q^{n-1}-1}{q-1}$ is the number of pairwise different two dimensional subspaces containing γ. We need to consider the cycle structure of F on the line $\gamma\mathbb{F}_q$ separately. □

Remark 2 Example 1 shows that there are permutations $x + \gamma\, \mathrm{Tr}_{q^n/q}(x^k)$, for which there exist two dimensional subspaces M of $\mathbb{F}_{q^n}$, such that the cycle structure of F is not the same on every line $m + \gamma\mathbb{F}_q \neq \gamma\mathbb{F}_q$ lying in M.

The following permutations are from [8], they do not belong to a known infinite family.

Example 1 Let $q = 9$, $n = 3$, $k \in \{11, 19\}$ and $\gamma \in \mathbb{F}_q$, where $\gamma^4 = -1$. Let $F(x) = x + \gamma\, \mathrm{Tr}_{q^3/q}(x^k)$. Then the cycle structure of F on $\gamma\mathbb{F}_q$ is 1^9. And for the 80 lines $l \parallel \gamma\mathbb{F}_q$, $l \neq \gamma\mathbb{F}_q$, it holds, that

on 8 the cycle structure of F is 3^3,
on 36 the cycle structure of F is $1^1 4^2$,
on 36 the cycle structure of F is $1^1 8^1$.

Since a two dimensional subspace of $\mathbb{F}_{9^3}$, containing $\gamma\mathbb{F}_9$, contains 8 further lines and $8 \nmid 36$, there exists a two dimensional subspace of $\mathbb{F}_{9^3}$, containing $\gamma\mathbb{F}_q$, that contains at least two lines with different cycle structures.

In the next sections we demonstrate applications of Theorem 3.

2 The case $F(x) = x + \gamma\, \mathrm{Tr}_{q^n/q}(x^k)$

In this section we consider the case $f(x) = \mathrm{Tr}_{q^n/q}(x^k)$ with $k \in \mathbb{N}$ and $\mathrm{Tr}_{q^n/q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$, where $\mathrm{Tr}_{q^n/q}(x) = x + x^q + \cdots + x^{q^{n-1}}$ is the trace mapping. The study of permutations $x + \gamma\, \mathrm{Tr}_{q^n/q}(x^k)$ was originated in [3], where the complete characterization of such permutations for $q = 2$ is achieved. Several families of such permutations are found in [4,8,9,11]. In this paper we concentrate on the cases $n = 2$ and $n = 3$. The currently known families of such non-linear permutations for $n = 2$ and $n = 3$ are given in Theorem 4. Cases 1-5 for odd q and cases 6, 16 and 17 are from [8]. Cases 1-5 for even q and cases 7-14 are from [9]. Case 15 is from [11].

Theorem 4 *The polynomial $F(x) = x + \gamma\, \mathrm{Tr}_{q^n/q}(x^k)$ is a permutation polynomial over $\mathbb{F}_{q^n}$ in each of the following cases.*

1. $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = -1/3$, $k = 2q - 1$,
2. $n = 2$, $q \equiv -1 \pmod 3$, $\gamma^3 = -1/27$, $k = 2q - 1$,
3. $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$,
4. $n = 2$, $q = Q^2$, $Q > 0$, $\gamma = -1$, $k = Q^3 - Q + 1$,
5. $n = 2$, $q = Q^2$, $Q > 0$, $\gamma = -1$, $k = Q^3 + Q^2 - Q$,

6. $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q+1)^2/4$,
7. $n = 2$, $q = 2^s$, s even, $\gamma^3 = 1$, $k = (3q-2)(q^2+q+1)/3$,
8. $n = 2$, $q = 2^s$, s odd, $\gamma^3 = 1$, $k = (3q^2-2)(q+4)/5$,
9. $n = 2$, $q = 2^s$, $\gamma \in \mathbb{F}_q$, s.t. $x^3 + x + \gamma^{-1}$ has no root in $\mathbb{F}_q$, $k = 2^{2s-2} + 3 \cdot 2^{s-2}$,
10. $n = 2$, $q = 2^s$, $s \equiv 1 \pmod 3$, $\gamma = 1$, $k = (2q^2-1)(q+6)/7$,
11. $n = 2$, $q = 2^s$, $s \equiv -1 \pmod 3$, $\gamma = 1$, $k = -(q^2-2)(q+6)/7$,
12. $n = 2$, $q = 2^s$, s odd, $\gamma^{(q+1)/3} = 1$, $k = (2^{2s-1} + 3 \cdot 2^{s-1} + 1)/3$,
13. $n = 2$, $q = 2^s$, s even, $\gamma = 1$, $k = (q^2 - 2q + 4)/3$,
14. $n = 2$, $q = Q^2$, $Q = 2^s$, $\gamma \in \mathbb{F}_Q^*$, $k = 2^{4s-1} - 2^{3s-1} + 2^{2s-1} + 2^{s-1}$,
15. $n = 2$, $q = 3^s$, $s \geq 2, \gamma^{(q-1)/2} = (\gamma-1)^{(q-1)/2}$, $k = 3^{2s-1} + 3^s - 3^{s-1}$,
16. $n = 3$, q odd, $\gamma = 1$, $k = (q^2+1)/2$,
17. $n = 3$, q odd, $\gamma = -1/2$, $k = q^2 - q + 1$.

It can be easily seen that in all cases of Theorem 4 the integers k and n satisfy $k \equiv 1 \pmod{q-1}$, implying.

Proposition 3 *If q and k appear in one of the cases of Theorem 4, then $x^k = x$ for any $x \in \mathbb{F}_q$, and hence the function $\mathrm{Tr}_{q^n/q}(x^k)$ is homogeneous of degree 1.*

Consequently every permutation listed in Theorem 4 fulfills the conditions of Theorem 3. Thus to determine the cycle structure of these permutations, it is enough to find the cycle structure of the induced permutations on lines parallel to $\gamma\mathbb{F}_q$. By Theorem 3(b), for $n = 2$ there are at most two lines with different cycle structure, and for $n = 3$ there are at most $q + 2$ such lines. One of the lines for which we need to compute the cycle structure is $\gamma\mathbb{F}_q$.

Remark 3 Let $F(x) = x + \gamma\,\mathrm{Tr}_{q^n/q}(x^k)$ be one of the cases appearing in Theorem 4. Then the cycle structure of F on $\gamma\mathbb{F}_q$ is easy to determine. Indeed, for any $\gamma u \in \gamma\mathbb{F}_q$ it holds $F(\gamma u) = \gamma(1 + \mathrm{Tr}_{q^n/q}(\gamma^k))u$, and hence the cycle containing γu has length equal to the multiplicative order of $(1 + \mathrm{Tr}_{q^n/q}(\gamma^k))$ in $\mathbb{F}_q$.

Note that in several of the cases listed in Theorem 4 there are multiple choices for γ defining permutations. However in some of these cases the choice of γ does not impact the cycle structure of permutations.

Proposition 4 *Let $i \in \{2, 6, 8, 12\}$ be fixed and $F_{i,\gamma}$ be a permutation of $\mathbb{F}_{q^2}$ described in case i of Theorem 4. Further let $\gamma_1, \gamma_2 \in \mathbb{F}_{q^2}$ be such, that F_{i,γ_1} and $\mathbb{F}_{i,\gamma_2}$ are permutations. Then F_{i,γ_1} and $\mathbb{F}_{i,\gamma_2}$ are conjugate in the symmetric group over $\mathbb{F}_{q^2}$ and hence they have the same cycle structure. Further the cycle structure of F_{i,γ_1} on $\gamma_1\mathbb{F}_q$ is the same as the cycle structure of F_{i,γ_2} on $\gamma_2\mathbb{F}_q$ and for any $\alpha_1 \in \mathbb{F}_{q^2} \setminus \gamma_1\mathbb{F}_q$, $\alpha_2 \in \mathbb{F}_{q^2} \setminus \gamma_2\mathbb{F}_q$, the cycle structure of F_{i,γ_1} on $\alpha_1 + \gamma_1\mathbb{F}_q$ is the same as the cycle structure of F_{i,γ_2} on $\alpha_2 + \gamma_2\mathbb{F}_q$.*

Since the proofs are similar, we present only a proof for case 2.

Proof $F_{2,\gamma}(x) = x + \gamma\,\mathrm{Tr}_{q^2/q}(x^{2q-1})$, where $\gamma^3 = -\frac{1}{27}$. One possible choice for γ is $-\frac{1}{3}$. Set $F^*(x) = x - \frac{1}{3}\mathrm{Tr}_{q^2/q}(x^{2q-1})$. In the following we proceed similar to the proof of Theorem 3.2 from [8]. Let $\omega := -3\gamma$, then $\omega^3 = 1$ and consequently $\omega^{2q-1} = 1$. Then

$$\begin{aligned} F_{2,\gamma}(\omega x) &= \omega x - \frac{1}{3}\omega\,\mathrm{Tr}_{q^2/q}(\omega^{2q-1}x^{2q-1}) = \omega(x - \frac{1}{3}\mathrm{Tr}_{q^2/q}(x^{2q-1})) \\ &= \omega F^*(x). \end{aligned} \tag{1}$$

This shows that $F_{2,\gamma}$ is a conjugate of F^* for any γ with $\gamma^3 = -\frac{1}{27}$, that is the cycle structure of $F_{2,\gamma}$ is the same for every γ, such that $F_{2,\gamma}$ is a permutation.

Since $\varphi : \mathbb{F}_q \to \gamma\mathbb{F}_q, \varphi(x) = \omega x$ is a bijection, (1) also shows, that the cycle structure of $F_{2,\gamma}$ on $\gamma\mathbb{F}_q$ is the same as the cycle structure of F^* on $\mathbb{F}_q$.

Let $\beta_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be fixed and $\alpha_0 = \omega\beta_0 \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$. Then $\varphi_0 : \beta_0 + \mathbb{F}_q \to \alpha_0 + \gamma\mathbb{F}_q, \varphi_0(x) = \omega x$ is one-to-one. Consequently (1) also shows, that the cycle structure of $\mathbb{F}_{2,\gamma}$ on $\alpha_0 + \gamma\mathbb{F}_q$ is the same as the cycle structure of F^* on $\beta_0 + \mathbb{F}_q$. By Theorem 3 for any $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the cycle structure of $F_{2,\gamma}$ on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of $F_{2,\gamma}$ on $\alpha_0 + \gamma\mathbb{F}_q$. These two facts together show that for any $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the cycle structure of $F_{2,\gamma}$ on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of F^* on $\beta_0 + \mathbb{F}_q$. □

Tables 1 and 2 contain numerical results on the cycle structure on affine lines l parallel to $\gamma\mathbb{F}_q$ and $l \neq \gamma\mathbb{F}_q$ for permutations obtained by Theorem 4. Let $m_1^{r_1} m_2^{r_2} \ldots m_i^{r_i}$ denote the cycle structure of a permutation with r_1 cycles of length m_1, r_2 cycles of length m_2, …and r_i cycles of length m_i, where $m_1 < m_2 < \cdots < m_i$.

Recall that Theorem 3 shows that for $n = 3$, there are at most $q + 2$ different kinds of lines, where "different" means, that on those lines the considered permutation has different cycle structures. One of those lines is $\gamma\mathbb{F}_q$, which we do not consider in the tables. So the upper bound for different lines in the tables is $q + 1$. Observe that Table 2 shows in particular that in cases 16 and 17 of Theorem 4 this upper bound $q + 1$ is not achieved. Instead for $q = 81$ there are only 8 different lines in case 16, and 9 different lines in case 17; and for $q = 125$ there are 9 different lines in case 16, and 14 different lines in case 17.

The cycle structures marked with ∗∗ in Table 1 look particularly simple. Based on our numerical results we believe that the following statements hold.

Conjecture *Permutations listed in Theorem 4 fulfill:*

1. *For fixed q, the cycle structures of the permutations in case 1 are the same as the cycle structures of the permutations in case 3.*
2. *Let F_γ be as described in case 9 and m be the largest integer with $2^m \leq s$. Then there exists an element γ, such that F_γ has $2^{s-(m+1)}$ cycles of length 2^{m+1} on every line $\alpha + \gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.*
   If $2^m = s$, then this is the case for $\gamma = 1$. For this special case, we have a technical proof which will be published in [5].
3. *Let F_γ be as described in case 14. If $4 \nmid s$, then there exists an element γ, such that F_γ has 4 cycles of length 2^{s-2} on every line $\alpha + \gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.*
4. *Let F_γ be as described in case 15. Then there exists an element γ, such that F_γ has 1 fixed point and 1 cycle of length $q - 1$ on every line $\alpha + \gamma\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.*

For the permutations considered in the previous conjecture, it is easy to describe their cycle structure on the line $\gamma\mathbb{F}_q$. We state this in the next proposition. Note that in cases 9, 14 and 15, $\gamma \in \mathbb{F}_q$ and thus $\gamma\mathbb{F}_q = \mathbb{F}_q$.

Proposition 5 *Let* $\mathrm{ord}(x)$ *be the multiplicative order of x in* $\mathbb{F}_q$.

(a) *In cases 1 and 3 the permutations have q fixed points on $\gamma\mathbb{F}_q$, if q is even, and 1 fixed point and* $(q-1)/\mathrm{ord}(3)$ *cycles of length* $\mathrm{ord}(3)$ *on $\gamma\mathbb{F}_q$, if q is odd.*
(b) *In cases 9 and 14 the permutation F_γ reduces to the identity mapping on $\gamma\mathbb{F}_q$ and consequently has q fixed points on $\gamma\mathbb{F}_q$.*
(c) *In case 15 the permutation F_γ reduces to $F(u) = (2\gamma + 1)u$ on $\gamma\mathbb{F}_q$ and consequently has one fixed point and* $(q-1)/\mathrm{ord}(2\gamma + 1)$ *cycles of length* $\mathrm{ord}(2\gamma + 1)$ *on $\gamma\mathbb{F}_q$.*

Table 1 Examples of cycle structure on lines for $n = 2$

Case	q	γ	Cycle struct. on any line $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$
1	289		$1^1 4^2 28^{10}$
	1024		$4^1 8^{25} 20^1 40^{20}$
2*	125		$1^3 2^1 30^4$
	1103		$1^3 18^2 28^2 252^4$
3	289		$1^1 4^2 28^{10}$
	1024		$4^1 8^{25} 20^1 40^{20}$
4	289		$1^1 4^1 12^2 14^2 28^1 62^2 80^1$
	1024		$4^1 140^1 880^1$
5	289		$1^5 8^1 19^4 52^1 148^1$
	1024		$1^4 140^2 240^1 500^1$
6	289		$1^{145} 4^1 28^5$
	2197		$1^{1099} 3^2 52^3 156^6$
7	1024	1	$1^4 11^{20} 19^{20} 42^{10}$
		$\neq 1$	$1^4 30^2 70^2 80^2 260^1 400^1$
	4096	1	$8^2 72^6 120^6 144^2 440^6$
		$\neq 1$	$4^1 6^1 212^2 30^2 252^1 360^4\ 561^4$
8	2048		$1^2 20^{11} 22^1 44^1\ 66^5 88^5 110^1 132^2\ 176^1 198^1 242^1$
	8192		$1^2 7^{78} 26^6 39^{10} 52^5 65^4\ 91^{16} 104^{14} 117^4 130^4\ 143^2 156^6 208^4 260^1\ 364^1$
9	1024	1	$4^1 60^{17}$
		a	$2^1 6^5 62^1 186^5$
		a^{99}	16^{64} $**$
10	1024		$1^4 10^2 20^5 35^4 60^6\ 400^1$
	8192		$2^1 26^2 52^2 390^2\ 1014^1 2574^1 3666^1$
11	2048		$2^1 22^4 55^2 138^{11} 165^2$
	16384		$1^4 28^3 40^7 42^2 553^4\ 1141^4 4572^2$
12*	2048		$1^{682} 2^1 22^{62}$
	32768		$1^{10922} 6^1 30^{728}$
13	1024		$2^2 4^5 30^2 80^1 320^1 540^1$
	16384		$2^2 14^2 56^1 170^{14} 308^1\ 3402^4$
14	1024	1	$4^1 12^5 20^6 36^5 60^5 180^2$
		b	256^4 $**$
15	243	c	$1^1 242^1$ $**$
		c^4	$1^1 2^1 6^1 13^2 26^2\ 78^2$

Here a is a root of $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$ in $\mathbb{F}_{1024}$, b is a root of $x^5 + x^2 + 1$ in $\mathbb{F}_{32}$ and c is a root of $x^5 - x + 1$ in $\mathbb{F}_{243}$. $*$We determine the cycle structure for these cases completely in Theorems 7 and 10

Table 2 Examples of cycle structure on lines for $n = 3$

Case	q	A	B
16	81	$3^1 6^1 9^4 12^3$	1
		$1^1 2^6 4^6 11^4$	3
		$1^1 2^1 3^1 5^3 6^5 15^2$	6
		$1^1 2^1 4^1 10^1 11^4 20^1$	12
		$1^1 2^1 9^1 11^1 22^1 36^1$	12
		$1^1 3^1 9^1 27^1 41^1$	12
		$1^1 5^3 9^1 10^3 35^1$	12
		$1^1 3^1 5^1 14^1 28^1 30^1$	24
	125	$1^2 2^1 3^2 4^1 6^2 12^3 21^1\ 42^1$	9
		$2^1 11^1 34^2 44^1$	9
		$2^1 7^9 10^1 50^1$	9
		$2^1 14^5 53^1$	9
		$5^1 6^1 18^3 60^1$	9
		$14^4 69^1$	9
		$3^2 4^2 9^1 18^3 24^2$	18
		$1^2 7^9 10^2 20^2$	27
		$1^2 2^1 3^2 4^1 6^1 9^1 12^5 36^1$	27
17	81	$3^1 6^1 9^4 12^3$	1
		$1^3 2^3 6^6 12^3$	3
		$4^2 9^1 32^2$	6
		$1^3 3^1 4^1 7^1 9^1 22^1 33^1$	12
		$1^3 3^1 6^1 7^1 27^1 35^1$	12
		$2^1 3^1 7^1 10^1 14^1 45^1$	12
		$2^1 36^1 43^1$	12
		$18^1 63^1$	12
		$19^1 62^1$	12
	125	$1^1 2^2 3^1 7^1 9^1 13^1 15^1\ 20^1 53^1$	9
		$1^1 3^1 4^1 7^1 18^1 39^1 53^1$	9
		$2^2 3^1 8^1 48^1 62^1$	9
		$1^2 5^1 9^1 46^1 63^1$	9
		$1^2 11^1 16^1 30^1 66^1$	9
		$6^1 8^1 44^1 67^1$	9
		$1^4 2^2 5^1 12^1 29^1 71^1$	9
		$25^1 26^1 74^1$	9
		$8^1 41^1 76^1$	9
		$2^2 3^2 8^1 26^1 81^1$	9
		$2^2 5^1 33^1 83^1$	9
		$1^1 2^2 3^1 4^2 8^1 15^1 86^1$	9
		$1^1 2^2 7^1 8^1 9^1 96^1$	9
		$1^2 8^1 115^1$	9

Here column A contains the cycle structure on lines $l \parallel \gamma\mathbb{F}_q,\ l \neq \gamma\mathbb{F}_q$ and B the number of planes $P > \gamma\mathbb{F}_q$ with such lines

Remark 4 At present we have no explanation for the cycle structure of case 16. In [6] we describe explicitly the cycle structure of the composition of this mapping with x^{q^2+q-1}, that is for $x^{q^2+q-1} + \mathrm{Tr}_{q^3/q}(x)$. The possible cycle lengths are only 1, the multiplicative order of 4 modulo p and twice the multiplicative order of 4 modulo p, where p is the characteristic of $\mathbb{F}_q$.

3 Determining the cycle structure of $x + \gamma\,\mathrm{Tr}_{q^2/q}(x^{2q-1})$.

Numerical results for case 2 of Theorem 4 show that the cycle structure of these permutations on lines $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$ is the same as the cycle structure of x^3 on $\mathbb{F}_q$. The next Theorem by Ahmad describes the cycle structure of permutation polynomials x^k. We denote by $\mathrm{ord}_t(k)$ the order of k modulo t, i. e. the smallest positive integer m with $k^m \equiv 1 \pmod t$.

Theorem 5 ([1]) *The polynomial x^k, $\gcd(k, q-1) = 1$, permuting $\mathbb{F}_q^*$ has a cycle of length t if and only if $t = \mathrm{ord}_m(k)$, where $m \mid (q-1)$. The number N_t of t-cycles satisfies*

$$t \cdot N_t = \gcd(k^t - 1, q-1) - \sum_{i|t, i\neq t} i \cdot N_i \text{ and } N_1 = \gcd(k-1, q-1).$$

Remark 5 On $\mathbb{F}_q$, x^k has the additional fixed point $x = 0$ and thus $N_1 + 1$ fixed points in total.

Let $\mathrm{Tr}(x) = \mathrm{Tr}_{q^2/q}(x) = x + x^q$ be the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. We use this notation for the remainder of the paper. In this section we determine the cycle structure of case 2 of Theorem 4, which is $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ on $\mathbb{F}_{q^2}$, where $q \equiv -1 \pmod 3$ and $\gamma^3 = -\frac{1}{27}$. We do this by showing, that indeed the cycle structure of $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ on lines $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$ is the same as the cycle structure of x^3 on $\mathbb{F}_q$.

By Proposition 4 for all admissible choices of γ the cycle structure of F as well as its cycle structure on the lines parallel to $\gamma\mathbb{F}_q$ is the same. Hence we consider the case $\gamma = -\frac{1}{3}$, for which $\gamma\mathbb{F}_q = \mathbb{F}_q$ holds, because in this case $\gamma \in \mathbb{F}_q$.

First we determine the cycle structure of F on $\mathbb{F}_q$.

Lemma 3 *Let $q \equiv -1 \pmod 3$ and p be the characteristic of $\mathbb{F}_q$. Then*

(a) *If q is even, the permutation $F(x) = x - \frac{1}{3}\mathrm{Tr}(x^{2q-1})$ reduces to $F(x) = x$ on the line $\mathbb{F}_q$. Consequently it has q fixed points on $\mathbb{F}_q$.*
(b) *If q is odd, the permutation $F(x) = x - \frac{1}{3}\mathrm{Tr}(x^{2q-1})$ reduces to $F(x) = \frac{1}{3}x$ on the line $\mathbb{F}_q$. Consequently, it has one fixed point and $\frac{q-1}{\mathrm{ord}_p(3)}$ cycles of length $\mathrm{ord}_p(3)$ on $\mathbb{F}_q$.*

Proof If q is even and $x \in \mathbb{F}_q$, then clearly $F(x) = x$. If otherwise q is odd and $x \in \mathbb{F}_q$, then

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

So $x = 0$ is a fixed point and the m-th iterate of F is $\left(\frac{1}{3}\right)^m x$. Therefore if $x \neq 0$ it is contained in the cycle $\left(x, \frac{1}{3}x, \ldots, \left(\frac{1}{3}\right)^{k-1} x\right)$ where $k = \mathrm{ord}_p\left(\frac{1}{3}\right) = \mathrm{ord}_p(3)$. □

To determine the cycle structure of F on the other lines parallel to $\mathbb{F}_q$, by Theorem 3, we only need to pick one of them and find the cycle structure on it. The following claim will be used for a suitable choice of this line.

Claim 1 If $q \equiv 5 \pmod 6$, then $-\frac{1}{3}$ is a non-square of $\mathbb{F}_q$.

Proof Let $q = p^s$ with p prime. Then $p \equiv 5 \pmod 6$ and s is odd. Hence $-\frac{1}{3}$ is a non-square of $\mathbb{F}_q$ if and only if $-\frac{1}{3}$ is a non-square in $\mathbb{F}_p$. The rest follows from the observation that $-\frac{1}{3}$ is a non-square in a prime field $\mathbb{F}_p$ with $p \equiv 5 \pmod 6$. The latter follows directly from the Quadratic Reciprocity Law. □

Now we are ready to determine the rest of the cycle structure of F.

Theorem 6 *Let $q \equiv -1 \pmod 3$ and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then the permutation $F(x) = x - \frac{1}{3}\operatorname{Tr}(x^{2q-1})$ has the same cycle structure on $\alpha + \mathbb{F}_q$ as the permutation x^3 on $\mathbb{F}_q$.*

Proof According to Theorem 3 the cycle structure of F on the line $\alpha + \mathbb{F}_q$ does not depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As in the proof of Theorem 2 for any α and $l \in \mathbb{F}_q$ the following holds: $F(\alpha + l) = \alpha + G_\alpha(l)$ and $G_\alpha(l) := l + \gamma \operatorname{Tr}((\alpha + l)^{2q-1})$ permutes $\mathbb{F}_q$ and has the same cycle structure as F on $\alpha + \mathbb{F}_q$. Next we show that for a particular choice of α, and thus for any choice of α by Theorem 3, the permutation G_α is a conjugate of $m(x) = x^3$ in $S_{\mathbb{F}_q}$.

If q is *even*, then $\gamma = -\frac{1}{3} = 1 \in \mathbb{F}_2$. Let $\alpha \in \mathbb{F}_4 \le \mathbb{F}_{q^2}$, $\alpha \notin \mathbb{F}_2$. Since $q = 2^s$, with s odd, $\alpha \notin \mathbb{F}_{2^s}$. This α satisfies

$$\alpha^2 = \alpha + 1, \quad \alpha^3 = 1, \qquad \operatorname{Tr}(\alpha) = \alpha^q + \alpha = \alpha^2 + \alpha = 1,$$
$$\operatorname{Tr}(\alpha^2) = \operatorname{Tr}(\alpha + 1) = \operatorname{Tr}(\alpha) = 1, \qquad \operatorname{Tr}(\alpha^3) = \operatorname{Tr}(1) = 0$$

and

$$\begin{aligned}(\alpha + l)^{q+1} &= (\alpha + l)(\alpha^q + l) = (\alpha + l)(\alpha + 1 + l)\\ &= \alpha^2 + \alpha + \alpha l + \alpha l + l + l^2 = l^2 + l + 1.\end{aligned}$$

Using the above equations we get

$$\begin{aligned}G_\alpha(l) &= l + \operatorname{Tr}((\alpha + l)^{2q-1}) = l + \operatorname{Tr}\left(\frac{(\alpha^q + l)^2}{\alpha + l}\right)\\ &= l + \frac{(\alpha^q + l)^2}{\alpha + l} + \frac{(\alpha + l)^2}{\alpha^q + l} = l + \frac{(\alpha^q + l)^3 + (\alpha + l)^3}{(\alpha + l)(\alpha^q + l)}\\ &= l + \frac{\operatorname{Tr}((\alpha + l)^3)}{(\alpha + l)^{q+1}} = l + \frac{2l^3 + 3l^2\operatorname{Tr}(\alpha) + 3l\operatorname{Tr}(\alpha^2) + \operatorname{Tr}(\alpha^3)}{l^2 + l + 1}\\ &= l + \frac{l^2 + l}{l^2 + l + 1} = \frac{l^3 + l^2 + l + l^2 + l}{l^2 + l + 1} = \frac{l^3}{l^2 + l + 1}.\end{aligned}$$

Now we can show that $G_\alpha = \varphi^{-1} \circ m \circ \varphi$, or equivalently $\varphi \circ G_\alpha = m \circ \varphi$ for the permutation

$$\varphi(l) := l^{q-2} + 1 = \begin{cases}\frac{1}{l} + 1, & l \neq 0,\\ 1, & l = 0.\end{cases}$$

We have

$$(\varphi \circ G_\alpha)(0) = f(0) = 1 = m(1) = (m \circ \varphi)(0).$$

If $l \neq 0$ then

$$(\varphi \circ G_\alpha)(l) = \frac{l^2 + l + 1}{l^3} + 1 = \frac{1}{l^3} + \frac{1}{l^2} + \frac{1}{l} + 1 = \left(\frac{1}{l} + 1\right)^3 = (m \circ \varphi)(l).$$

This proves the theorem for even q.

If q is *odd*, then by Claim 1, $-\frac{1}{3}$ is a non-square of $\mathbb{F}_q$, so there is $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^2 = -\frac{1}{3}$. This α satisfies $(\alpha^q)^2 = (\alpha^2)^q = \alpha^2$ and thus

$$\alpha^q = -\alpha, \qquad \mathrm{Tr}(\alpha) = \mathrm{Tr}(-\alpha) = 0, \qquad \mathrm{Tr}(\alpha^2) = 2\alpha^2, \qquad \mathrm{Tr}(\alpha^3) = \alpha^2\,\mathrm{Tr}(\alpha) = 0.$$

Using these equations we obtain

$$\begin{aligned} G_\alpha(l) &= l - \frac{1}{3}\mathrm{Tr}((\alpha+l)^{2q-1}) = l - \frac{1}{3}(\alpha+l)^{2(q+1)}\,\mathrm{Tr}\left(\frac{1}{(\alpha+l)^3}\right) \\ &= l - \frac{1}{3}\left[(\alpha^q+l)(\alpha+l)\right]^2\left(\frac{1}{(\alpha+l)^3} + \frac{1}{(\alpha^q+l)^3}\right) \\ &= l - \frac{1}{3}(l^2-\alpha^2)^2 \cdot \frac{(\alpha+l)^3 + (\alpha^q+l)^3}{(l^2-\alpha^2)^3} = l - \frac{1}{3}\cdot\frac{\mathrm{Tr}((l+\alpha)^3)}{l^2-\alpha^2} \\ &= l - \frac{1}{3}\cdot\frac{2l^3 + 3l^2\,\mathrm{Tr}(\alpha) + 3l\,\mathrm{Tr}(\alpha^2) + \mathrm{Tr}(\alpha^3)}{l^2-\alpha^2} \\ &\overset{*}{=} l - \frac{1}{3}\cdot\frac{2l^3 + 6l\alpha^2}{l^2-\alpha^2} = l - \frac{1}{3}\cdot\frac{2l^3-2l}{l^2+1/3} \\ &= l - \frac{l(2l^2-2)}{3l^2+1} = \frac{l(3l^2+1) - l(2l^2-2)}{3l^2+1} = \frac{l(l^2+3)}{3l^2+1}, \end{aligned}$$

where $*$ follows from $\alpha^2 = -\frac{1}{3}$. Next we show that $G_\alpha = \varphi^{-1} \circ m \circ \varphi$, or equivalently $\varphi \circ G_\alpha = m \circ \varphi$ for the permutation

$$\varphi(l) := \left(\frac{1}{2}l + \frac{1}{2}\right)^{q-2} - 1 = \begin{cases} \frac{1-l}{1+l}, & l \neq -1, \\ -1, & l = -1. \end{cases}$$

We have

$$(\varphi \circ G_\alpha)(-1) = \varphi\left(\frac{-1(1+3)}{3+1}\right) = \varphi(-1) = -1 = m(-1) = (m \circ \varphi)(-1).$$

If $l \neq -1$ then

$$(\varphi \circ G_\alpha)(l) = \frac{1 - \frac{l(l^2+3)}{3l^2+1}}{1 + \frac{l(l^2+3)}{3l^2+1}} = \frac{1 - 3l + 3l^2 - l^3}{1 + 3l + 3l^2 + l^3} = \left(\frac{1-l}{1+l}\right)^3 = (m \circ \varphi)(l).$$

Consequently F has the same cycle structure on $\alpha + \mathbb{F}_q$ as x^3 on $\mathbb{F}_q$. □

We summarize the results of this section by describing explicitly the cycle structure of F in the general case.

Theorem 7 *Let $q \equiv -1 \pmod 3$, p be the characteristic of $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^3 = -\frac{1}{27}$. Let N_t be defined by the following recursion*

$$N_1 = \gcd(2, q-1)$$

and

$$t \cdot N_t = \gcd(3^t - 1, q-1) - \sum_{i \mid t, i \neq t} i \cdot N_i.$$

1. *Let q be even. Then the permutation $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ of $\mathbb{F}_{q^2}$ has q fixed points on $\gamma\mathbb{F}_q$. Further, on any affine line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the permutation $F(x)$ has $N_1 + 1 = 2$ fixed points and N_t cycles of length t for every $t > 1$, such that $t = \mathrm{ord}_m(3)$ for a divisor m of $q-1$.*
2. *Let q be odd. Then the permutation $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ of $\mathbb{F}_{q^2}$ has one fixed point and $\frac{q-1}{\mathrm{ord}_p(3)}$ cycles of length $\mathrm{ord}_p(3)$ on $\gamma\mathbb{F}_q$. Further, on any affine line $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$, the permutation $F(x)$ has $N_1 + 1 = 3$ fixed points and N_t cycles of length t for every $t > 1$, such that $t = \mathrm{ord}_m(3)$ for a divisor m of $q-1$.*

Proof The theorem follows from Lemma 3 and Theorems 6 and 5. □

Corollary 1 *Let $q \equiv -1 \pmod 3$ and $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^3 = -\frac{1}{27}$. Then the permutation $F(x) = x + \gamma\,\mathrm{Tr}(x^{2q-1})$ has $3q-2$ fixed points on $\mathbb{F}_{q^2}$.*

Proof If q is even, there are q fixed points on $\gamma\mathbb{F}_q$ and 2 fixed points on any of the $q-1$ affine lines $\alpha + \gamma\mathbb{F}_q$, so in this case F has $q + 2(q-1) = 3q-2$ fixed points in total.

If q is odd, there is 1 fixed point on $\gamma\mathbb{F}_q$ and there are 3 fixed points on any of the $q-1$ affine lines $\alpha + \gamma\mathbb{F}_q$, so in this case F has $1 + 3(q-1) = 3q-2$ fixed points in total.

4 Determining the cycle structure of $x + \gamma\,\mathrm{Tr}_{q^2/q}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$.

In this section we determine the cycle structure of case 12 of Theorem 4, which is $F(x) = x + \gamma\,\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ on $\mathbb{F}_{q^2}$, where $q = 2^s$, s odd and $\gamma^{(q+1)/3} = 1$. Recall, that by $\mathrm{Tr}(x)$, we denote $\mathrm{Tr}_{q^2/q}(x) = x^q + x$. By Proposition 4 for all admissible choices of γ the cycle structure of F as well as its cycle structure on the lines parallel to $\gamma\mathbb{F}_q$ is the same. Hence it is enough to consider $\gamma = 1$, for which $\gamma\mathbb{F}_q = \mathbb{F}_q$ holds.

We first determine the number of fixed points of F on $\mathbb{F}_{q^2}$.

Lemma 4 *Let $q = 2^s$ and s be odd. Then the permutation*

$$F(x) = x + \mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$$

of $\mathbb{F}_{q^2}$ has $\frac{q^2-1}{3} + 1$ fixed points.

Proof Note that x is a fixed point of F if and only if $\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right) = 0$. Since

$$\frac{2^{2s-1} + 3\cdot 2^{s-1} + 1}{3} = (2^{s-1}+1)\frac{q+1}{3} \text{ and } \gcd(2^{s-1}+1, 2^{2s}-1) = 1,$$

$\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has the same number of zeros as $\mathrm{Tr}\left(x^{\frac{q+1}{3}}\right)$. Clearly 0 is a zero of $\mathrm{Tr}\left(x^{\frac{q+1}{3}}\right)$. If $x \neq 0$, then

$$\mathrm{Tr}\left(x^{\frac{q+1}{3}}\right) = x^{\frac{q+1}{3}} + x^{\frac{q+1}{3}q} = 0$$

if and only if

$$1 + x^{\frac{q^2-1}{3}} = 0.$$

Since $1+x^{\frac{q^2-1}{3}}$ splits completely over $\mathbb{F}_{q^2}$, this shows that $\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has $\frac{q^2-1}{3}+1$ zeros, and consequently F has $\frac{q^2-1}{3}+1$ fixed points in $\mathbb{F}_{q^2}$. □

The next lemma describes the cycle structure of F on the line $\mathbb{F}_q$.

Lemma 5 *Let $q = 2^s$ and s be odd. Then the permutation*

$$F(x) = x + \mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$$

reduces to the identity on the line $\mathbb{F}_q$. Consequently it has q fixed points on $\mathbb{F}_q$.

Proof Clearly $F(x) = x$ for $x \in \mathbb{F}_q$. □

Lemma 6 *Let $q = 2^s$ and s be odd. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then the permutation $F(x) = x + \mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has $\frac{2^s-2}{3}$ fixed points on the line $\alpha + \mathbb{F}_q$.*

Proof By Lemma 4 F has $\frac{q^2-1}{3}+1$ fixed points and by Lemma 5 we have that q of them are on the line $\mathbb{F}_q$. By Theorem 3, the permutation F has the same number of fixed points on every line $\alpha + \mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So on any of those lines the number of fixed points is

$$\left(\frac{2^{2s}-1}{3} + 1 - 2^s\right)/(2^s-1) = \frac{2^s-2}{3}.$$

□

To determine the cycle structure of F on the lines parallel but not equal to $\mathbb{F}_q$, by Theorem 3 it suffices to pick one of them and find the cycle structure on it.

Theorem 8 *Let $q = 2^s$ and s be odd. Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\beta \in (\mathbb{F}_4 \setminus \mathbb{F}_2) \subseteq (\mathbb{F}_{q^2} \setminus \mathbb{F}_q)$. Then the permutation $F(x) = x+\mathrm{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ has the same cycle structure on $\alpha+\mathbb{F}_q$ as the permutation $G_\beta(x) = x + P_s(x)(x^{2^{s-1}} + x + 1)$ on $\mathbb{F}_q$, where $P_s(x) = \mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)$. In particular $G_\beta(x)$ has $\frac{2^s-2}{3}$ fixed points.*

Proof By Theorem 3 the cycle structure of F on the line $\alpha + \mathbb{F}_q$ does not depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Here we choose $\alpha = \beta$ and as in Theorem 6 conclude, that the considered cycle structure is the same as that of

$$G_\beta : \mathbb{F}_q \to \mathbb{F}_q, \quad G_\beta(x) = x + \mathrm{Tr}\left((x+\beta)^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right).$$

Since $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have that

$$\beta^2 = \beta + 1, \qquad \beta^3 = 1, \qquad \beta^4 = \beta, \qquad \beta^q = \beta^2.$$

Note that

$$\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}=2^{s-1}+4^{s-1}-\frac{4^{s-1}-1}{3}=2^{s-1}+4^{s-1}-\sum_{k=0}^{s-2}4^k,$$

and therefore

$$G_\beta(x)=x+\mathrm{Tr}\left(\frac{(x+\beta)^{2^{s-1}}(x+\beta)^{4^{s-1}}}{\prod_{k=0}^{s-2}(x^{4^k}+\beta)}\right).$$

Since for $x\in\mathbb{F}_q$

$$\begin{aligned}\prod_{k=0}^{s-1}(x^{4^k}+\beta)&=\prod_{k=0}^{(s-1)/2}(x^{2^{2k}}+\beta)\prod_{k=(s-1)/2+1}^{s-1}(x^{2^{2k}}+\beta)\\&=\prod_{k=0}^{(s-1)/2}(x^{2^{2k}}+\beta)\prod_{k=1}^{(s-1)/2}(x^{2^{2k-1}}+\beta)=\prod_{k=0}^{s-1}(x^{2^k}+\beta),\end{aligned}$$

we get

$$\prod_{k=0}^{s-2}(x^{4^k}+\beta)=\frac{\prod_{k=0}^{s-1}(x^{2^k}+\beta)}{x^{4^{s-1}}+\beta}$$

and

$$\begin{aligned}G_\beta(x)&=x+\mathrm{Tr}\left(\frac{x^{2^{s-1}}+\beta^2}{\prod_{k=0}^{s-2}(x^{2^k}+\beta)}\right)=x+\frac{x^{2^{s-1}}+\beta}{\prod_{k=0}^{s-2}(x^{2^k}+\beta^2)}+\frac{x^{2^{s-1}}+\beta^2}{\prod_{k=0}^{s-2}(x^{2^k}+\beta)}\\&=x+\frac{\prod_{k=0}^{s-1}(x^{2^k}+\beta)+\prod_{k=0}^{s-1}(x^{2^k}+\beta^2)}{\prod_{k=0}^{s-2}(x^{2^k}+\beta^2)(x^{2^k}+\beta)}=x+\frac{\mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right)}{\prod_{k=0}^{s-2}((x^2+x)^{2^k}+1)}.\end{aligned}$$

Further, note that

$$\prod_{k=0}^{s-2}((x^2+x)^{2^k}+1)=\sum_{j=0}^{2^{s-1}-1}(x^2+x)^j=\frac{(x^2+x)^{2^{s-1}}+1}{x^2+x+1}=\frac{x^{2^{s-1}}+x+1}{x^2+x+1}$$

and hence

$$G_\beta(x)=x+\frac{(x^2+x+1)P_s(x)}{x^{2^{s-1}}+x+1}=x+P_s(x)(x^{2^{s-1}}+x+1),$$

where $P_s(x)=\mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right)$. □

The following properties of $P_s(x)$ will allow us to determine the cycle structure of G_β explicitly. For $s=3^m\cdot l$, where $3\nmid l$, we define $\nu_3(s):=m$.

Lemma 7 *Let $\beta\in\mathbb{F}_4\setminus\mathbb{F}_2$, $x\in\mathbb{F}_{2^s}$ and s be odd. Let $t\mid s$, $u\in\mathbb{F}_{2^t}$ and $G_\beta(x)=x+P_s(x)(x^{2^{s-1}}+x+1)$, where $P_s(x)=\mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right)$. Then*

(a) $P_s(x) \in \mathbb{F}_2$,

(b) $P_s(u) = \begin{cases} 0, & 3 \mid (s/t) \\ P_t(u), & 3 \nmid (s/t) \end{cases}$

(c) $G_\beta(x) = x$ *if and only if* $P_s(x) = 0$,

(d) $\#\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\} = \frac{2^s-2}{3}$,

(e) $\#\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 1\} = \frac{2^{s+1}+2}{3}$,

(f) $\#\{u \in \mathbb{F}_{2^t} | P_s(u) = 1\} = \begin{cases} 0, & \nu_3(t) < \nu_3(s), \\ \frac{2^{t+1}+2}{3}, & \nu_3(t) = \nu_3(s). \end{cases}$

Proof The fact that

$$\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right)^4 = \prod_{k=0}^{s-1}(x^{4\cdot 2^k}+\beta) = \prod_{k=0}^{s-1}(x^{2^k}+\beta), \text{ shows that } \prod_{k=0}^{s-1}(x^{2^k}+\beta) \in \mathbb{F}_4.$$

Thus

$$P_s(x) = \mathrm{Tr}_{2^{2s}/2^s}\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right) = \mathrm{Tr}_{4/2}\left(\prod_{k=0}^{s-1}(x^{2^k}+\beta)\right) \in \mathbb{F}_2,$$

which is (a). Further note that $u^{2^k}+\beta \neq 0$ and

$$\prod_{k=0}^{s-1}(u^{2^k}+\beta) = \left(\prod_{k=0}^{t-1}(u^{2^k}+\beta)\right)^{s/t} = \begin{cases} 1, & s/t \equiv 0 \pmod 3 \\ \prod_{k=0}^{t-1}(u^{2^k}+\beta), & s/t \equiv 1 \pmod 3 \\ \prod_{k=0}^{t-1}(u^{2^k}+\beta^2), & s/t \equiv 2 \pmod 3 \end{cases}$$

and, because $\beta^q = \beta^2$,

$$\mathrm{Tr}_{q^2/q}\left(\prod_{k=0}^{t-1}(u^{2^k}+\beta^2)\right) = \mathrm{Tr}_{q^2/q}\left(\prod_{k=0}^{t-1}(u^{2^k}+\beta)\right) = P_t(u).$$

This shows (b). Since s is odd, $x^{2^{s-1}}+x+1$ has no root in $\mathbb{F}_{2^s}$, which implies (c). By Theorem 8, the permutation G_β has $\frac{2^s-2}{3}$ fixed points. With (c), we see that $\#\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\} = \frac{2^s-2}{3}$, which is (d). By (a), we know that $P_s(x) \in \mathbb{F}_2$, so

$$\#\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 1\} = 2^s - \#\{x \in \mathbb{F}_{2^s} \mid P_s(x) = 0\} = 2^s - \frac{2^s-2}{3} = \frac{2^{s+1}+2}{3}.$$

This is (e). With (b) we obtain

$$\#\{u \in \mathbb{F}_{2^t} | P_s(u) = 1\} = \begin{cases} 0, & 3 \mid (s/t) \\ \#\{u \in \mathbb{F}_{2^t} | P_t(u) = 1\}, & 3 \nmid (s/t) \end{cases}$$
$$= \begin{cases} 0, & 3 \mid (s/t) \\ \frac{2^{t+1}+2}{3}, & 3 \nmid (s/t) \end{cases}.$$

Since $3 \nmid (s/t)$ if and only if $\nu_3(t) = \nu_3(s)$, (f) follows. □

Now we are ready to determine the cycle structure of G_β.

Theorem 9 *Let $q = 2^s$ with s odd and $\beta \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Let $P_s(x) = \mathrm{Tr}\left(\prod_{k=0}^{s-1}(x^{2^k} + \beta)\right)$. Then the permutation $G_\beta(x) = x + P_s(x)(x^{2^{s-1}} + x + 1)$ of $\mathbb{F}_q$ has $\frac{q-2}{3}$ fixed points and N_t cycles of length $2t$ for every $t \mid s$ with $\nu_3(t) = \nu_3(s)$. The numbers N_t are positive and satisfy $2tN_t = \dfrac{2^{t+1}+2}{3} - \sum_{\substack{d\mid t, d<t,\\ \nu_3(d)=\nu_3(s)}} 2dN_d$ and $2 \cdot 3^m N_{3^m} = \frac{2^{3^m+1}+2}{3}$, where $m = \nu_3(s)$.*

Proof By Lemma 7(c), $x \in \mathbb{F}_q$ is a fixed point of G_β if and only if $P_s(x) = 0$ and then Lemma 7(d) shows that G_β has $\frac{q-2}{3}$ fixed points. Let $G_\beta^n = \underbrace{G \circ \cdots \circ G}_{n}$ denote the n-th iterate of G_β.

Consider now an $x_0 \in \mathbb{F}_q$ that is not fixed by G_β, i.e. an $x_0 \in \mathbb{F}_q$ with $P_s(x_0) \neq 0$. Then $P_s(x_0) = 1$ by Lemma 7(a). Consequently on the cycle containing x_0 the permutation G_β reduces to

$$G_\beta(x) = x + x^{2^{s-1}} + x + 1 = x^{2^{s-1}} + 1$$

and thus has its inverse given by

$$G_\beta^{-1}(x) = x^2 + 1.$$

As a result an even number of iterations of G_β^{-1} yields

$$G_\beta^{-2t}(x) = x^{2^{2t}},$$

while an odd number of iterations gives

$$G_\beta^{-(2t+1)}(x) = x^{2^{2t+1}} + 1.$$

Since s is odd, $x^{2^{2t+1}} + x + 1$ has no roots in $\mathbb{F}_q$, so

$$x_0 \neq x_0^{2^{2t+1}} + 1 = G_\beta^{-(2t+1)}(x_0), \quad \text{and thus} \quad G_\beta^{2t+1}(x_0) \neq x_0.$$

Hence the cycle length is even, say $2t$. Since t is minimal with $x_0 = G_\beta^{-2t}(x_0) = (x_0^{2^t})^{2^t}$, it must hold that $x_0 \in \mathbb{F}_{2^t}$. This forces $t \mid s$.

Suppose now $t \mid s$ and G_β has N_t cycles of length $2t$. Then it must hold that

$$\begin{aligned} 2tN_t &= \#\{u \in \mathbb{F}_{2^t} \mid P_s(u) = 1 \text{ and } u \text{ is not in a subfield of } \mathbb{F}_{2^t}\} \\ &= \#\{u \in \mathbb{F}_{2^t} \mid P_s(u) = 1\} - \sum_{\substack{d\mid t\\ d<t}} \#\left\{u \in \mathbb{F}_{2^d} \;\middle|\; \begin{array}{c} P_s(u) = 1 \text{ and } u \text{ is not} \\ \text{in a subfield of } \mathbb{F}_{2^d} \end{array}\right\}. \end{aligned}$$

Combining this with Lemma 7(f), we get

$$2tN_t = \begin{cases} 0, & \nu_3(t) < \nu_3(s) \\ \frac{2^{t+1}+2}{3} - \sum_{\substack{d\mid t\\ d<t}} 2dN_d, & \nu_3(t) = \nu_3(s). \end{cases}$$

Note that $2dN_d = 0$ if $d \mid s$ with $\nu_3(d) < \nu_3(s)$. Finally observe that for any $t \mid s$ with $\nu_3(t) = \nu_3(s)$, the number N_t is positive. Indeed, by Lemma 7 (e) there are proper elements u of $\mathbb{F}_{2^t}$ with $P_s(u) = 1$. These numbers satisfy then

$$2tN_t = \frac{2^{t+1}+2}{3} - \sum_{\substack{d|t, d<t,\\ \nu_3(d)=\nu_3(s)}} 2dN_d.$$

For $t = 3^m$ with $m = \nu_3(s)$, the sum is empty and thus $2 \cdot 3^m N_{3^m} = \frac{2^{3^m+1}+2}{3}$. □

We summarize the results of this section by describing explicitly the cycle structure of F in the general case.

Theorem 10 *Let $q = 2^s$ and s be odd. Let $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^{(q+1)/3} = 1$. For $t \mid s$, with $\nu_3(t) = \nu_3(s)$, let N_t be defined by the following recursion*

$$N_{3^m} = \frac{2^{3^m+1}+2}{2 \cdot 3^{m+1}}, \text{ for } m = \nu_3(s)$$

and

$$2tN_t = \frac{2^{t+1}+2}{3} - \sum_{\substack{d|t, d<t,\\ \nu_3(d)=\nu_3(s)}} 2dN_d.$$

Then the permutation $F(x) = x + \gamma \operatorname{Tr}\left(x^{\frac{2^{2s-1}+3\cdot 2^{s-1}+1}{3}}\right)$ of F_{q^2} has

1. *q fixed points on $\gamma\mathbb{F}_q$ and*
2. *$\frac{q-2}{3}$ fixed points and N_t cycles of length $2t$ on every affine line $\alpha+\gamma\mathbb{F}_q$ with $\alpha \in \mathbb{F}_{q^2}\setminus\gamma\mathbb{F}_q$, where t is an arbitrary divisor of s satisfying $\nu_3(t) = \nu_3(s)$.*

Proof Part 1 follows from Lemma 5 and part 2 follows from Theorems 8 and 9. □

Acknowledgements Open Access funding provided by Projekt DEAL. We thank the referees for the comments which helped us to improve the presentation of this paper.

References

1. Ahmad S.: Cycle structure of automorphisms of finite cyclic groups. J. Comb. Theory **6**, 370–374 (1969).
2. Çeşmelioğlu A., Meidl W., Topuzoğlu A.: On the cycle structure of permutation polynomials. Finite Fields Appl. **14**, 593–614 (2008).
3. Charpin P., Kyureghyan G.: On a class of permutation polynomials over $\mathbb{F}_{2^n}$. Proc. SETA. Lect. Notes Comput. Sci. **5203**, 368–376 (2008).
4. Charpin P., Kyureghyan G.: Monomial functions with linear structure and permutation polynomials. Finite fields: theory and applications. Contemp. Math. **518**, 99–111 (2010).
5. Gerike, D.: PhD Thesis, Otto-von-Guericke University of Magdeburg, In preparation
6. Gerike D., Kyureghyan G.M.: Results on permutation polynomials of Shape $x^t + \mathrm{Tr}_{q^n/q}(x^d)$, combinatorics and finite fields. Radon Ser. Comput. Appl. Math. **23**, 67–78 (2019).
7. Kyureghyan G.M.: Constructing permutations of finite fields via linear translators. J. Comb. Theory A **118**, 1052–1061 (2011).

8. Kyureghyan, G.M., Zieve, M.E.: Permutation polynomials of the form $X + \gamma \mathrm{Tr}(X^k)$. Contemp. Dev. Finite Fields Appl. 178–194 (2016)
9. Li K., Qu L., Chen X., Li C.: Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic. Cryptogr. Commun. **10**(3), 531–554 (2018).
10. Lidl R., Mullen G.L.: Cycle structure of Dickson permutation polynomials. Math. J. Okayama Univ. **33**, 1–11 (1991).
11. Ma J., Ge G.: A note on permutation polynomials over finite fields. Finite Fields Appl. **48**, 261–270 (2017).
12. Mullen G.L., Vaughan T.P.: Cycles of linear permutations over a finite field. Linear Algebra Appl. **108**, 63–82 (1988).
13. Panario D., Reis L.: The functional graph of linear maps over finite fields and applications. Des. Codes Cryptogr. **87**, 437–453 (2019).
14. Rubio I., Corrada-Bravo C.J.: Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials, Finite Fields and Applications, LNCS 2948, pp. 254–261. Springer-Verlag, Berlin (2004).