Permutations on $\mathbb{F}_{q^n}$ with Invariant Cycle Structure on Certain Lines

Daniel Gerike[1] and Gohar M. Kyureghyan[2]

[1] Otto-von-Guericke University of Magdeburg, daniel.gerike@ovgu.de
[2] University of Rostock, gohar.kyureghyan@uni-rostock.de

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 permutations $x + \gamma \operatorname{Tr}(x^{2q-1})$ over $\mathbb{F}_{q^2}$, where $q \equiv -1 \pmod 3$, $\gamma \in \mathbb{F}_{q^2}$ and $\gamma^3 = -\frac{1}{27}$.

Keywords: permutation polynomials, cycle structure, switching construction, subspaces

A permutation can be expressed as a unique product of disjoint cycles (up to reordering). Such a cycle decomposition 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. 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. At present, this is studied for very few families of permutation polynomials, like monomial, linearized or Dickson polynomials. In this paper we consider the class 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 will 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 permutations $x + \gamma \operatorname{Tr}(x^{2q-1})$ over $\mathbb{F}_{q^2}$, where $q \equiv -1 \pmod 3$, $\gamma \in \mathbb{F}_{q^2}$ and $\gamma^3 = -\frac{1}{27}$.

1 Induced Permutations on Lines and Subspaces

The following result is straightforward:

Lemma 1.1. *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 1.2. *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 of the lemma 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 $f(x) = f_\alpha(u)$. Then clearly

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

where $f : \mathbb{F}_q \to \mathbb{F}_q$. □

Remark 1.3. 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. Since every coset of a subspace L in $\mathbb{F}_{q^n}$ is a union of lines $\alpha + \gamma\mathbb{F}_q$ for certain $\alpha \in \mathbb{F}_{q^n}$, the mapping F maps any coset of L into itself.

As an immediate corollary of Lemma 1.1 we get:

Theorem 1.4. *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 1.4:

Proposition 1.5. *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 1.6. *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 1.7. *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 $\gamma \in L$, $L < M$ 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 1.3, the mapping F is a permutation on the coset $t\alpha + L$. Let now $l \in L$. Then

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

with $G_t(l) : L \to L$, $G_t(l) = l + \gamma f(t\alpha + l)$. Since $G_t(l) = F(t\alpha + l) - t\alpha$ and adding $t\alpha$ is a bijection from L to $t\alpha+L$, $G_t(l)$ is a permutation of L that has the same cycle structure as F on $t\alpha + L$ by Theorem 1.6. Hence it remains to show, that the cycle structure of G_t is independent of t. Since $t \in \mathbb{F}_q^*$, multiplying by t is a permutation of L. 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 1.7 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 1.8. *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 properties hold:*

(a) *Let M be any two dimensional subspace of $\mathbb{F}_{q^n}$ containing γ. Then the cycle structure of F is the same on any 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 1.7 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. □

In the next sections we demonstrate applications of Theorem 1.8.

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 $x+\gamma\operatorname{Tr}_{q^n/q}(x^k)$ 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], [7], [8] and [10]. In this paper we concentrate on the cases $n=2$ and $n=3$. The following theorem lists the known families of such non-linear permutations for $n=2$ and $n=3$:

Theorem 2.1. *The polynomial $F(x)=x+\gamma\operatorname{Tr}_{q^n/q}(x^k)$ is a permutation polynomial over $\mathbb{F}_{q^n}$ in each of the following cases:*

1. $n=2$, $q\equiv\pm1 \pmod 3$, $\gamma=-1/3$, $k=2q-1$,
2. $n=2$, $q\equiv-1 \pmod 3$, $\gamma^3=-1/27$, $k=2q-1$,
3. $n=2$, $q\equiv1 \pmod 3$, $\gamma=1$, $k=(q^2+q+1)/3$,
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. $n=2$, $q\equiv1 \pmod 4$, $(2\gamma)^{(q+1)/2}=1$, $k=(q+1)^2/4$,
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* $\mathbb{F}_q$, $k=2^{2s-2}+3\cdot2^{s-2}$,
10. $n=2$, $q=2^s$, $s\equiv1 \pmod 3$, $\gamma=1$, $k=(2q^2-1)(q+6)/7$,
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*, $\gamma^{(q+1)/3}=1$, $k=(2^{2s-1}+3\cdot2^{s-1}+1)/3$,
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. $n=2$, $q=3^s$, $s\geq2$,$\gamma^{(q-1)/2}=(\gamma-1)^{(q-1)/2}$, $k=3^{2s-1}+3^s-3^{s-1}$,
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 2.1 the integers k and n satisfy $k\equiv1 \pmod{q-1}$, implying:

Proposition 2.2. *If q and k appear in one of the cases of Theorem 2.1, then $x^k=x$ for any $x\in\mathbb{F}_q$, and hence the function $\operatorname{Tr}_{q^n/q}(x^k)$ is homogeneous of degree 1.*

Consequently every permutation listed in Theorem 2.1 fulfills the conditions of Theorem 1.8. 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 1.8 (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 2.3. Let $F(x)=x+\gamma\operatorname{Tr}_{q^n/q}(x^k)$ be one of the cases appearing in Theorem 2.1. 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 $F(\gamma u)=\gamma(1+\operatorname{Tr}_{q^n/q}(\gamma^k))u$, and hence the cycle containing γu has length equal to the multiplicative order of $(1+\operatorname{Tr}_{q^n/q}(\gamma^k))$ in $\mathbb{F}_q$.

In some of the cases listed in Theorem 2.1 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 2.4. *Let γ_1 and γ_2 define permutations F_{γ_1} and F_{γ_2} appearing in one of the cases 2, 6, 8 and 12 of Theorem 2.1. Then F_{γ_1} and F_{γ_2} are conjugate and hence they have the same cycle structure.*

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

Proof. Let $F(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{2q-1})$, where $\gamma^3 = -\frac{1}{27}$. One possible choice for γ is $-\frac{1}{3}$. Let $F^*(x) = x - \frac{1}{3} \operatorname{Tr}_{q^2/q}(x^{2q-1})$. In the following we proceed similar to the proof of Theorem 3.2 from [7]: Let $\omega := -3\gamma$, then $\omega^3 = 1$ and consequently $\omega^{2q-1} = 1$, s. t.

$$\begin{aligned} F(\omega x) &= \omega x - \frac{1}{3}\omega \operatorname{Tr}_{q^2/q}(\omega^{2q-1}x^{2q-1}) = \omega(x - \frac{1}{3}\operatorname{Tr}_{q^2/q}(x^{2q-1})) \\ &= \omega F^*(x) \end{aligned}$$

It follows that F is a conjugate of F^* for any admissible γ, that is the cycle structure of F is the same for every such γ. □

Remark 2.5. With notation from the proof of Proposition 2.4 and $\alpha = \omega\beta$, the mapping $\varphi : \beta + \mathbb{F}_q \to \alpha + \gamma\mathbb{F}_q$ given by $\varphi(x) = \omega x$ is a bijection. Consequently the cycle structure of F on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of F^* on $\beta + \mathbb{F}_q$. This shows that for all possible choices of γ the cycle structure on lines parallel to $\gamma\mathbb{F}_q$ is the same as well.

Tables 1 and 2 describe numerical results on the cycle structure on affine lines l parallel to $\gamma\mathbb{F}_q$ and $l \neq \gamma\mathbb{F}_q$ for some of the permutations from Theorem 2.1. If a permutation has r_1 cycles of length m_1, r_2 cycles of length m_2, ... and r_i cycles of length m_i, where $m_1 < m_2 < \cdots < m_i$, we denote its cycle structure by $m_1^{r_1} m_2^{r_2} \ldots m_i^{r_i}$.

Table 2 shows in particular that in cases 16 and 17 the upper bound $q + 1$ from Theorem 1.8 for different cycle structures on lines is not achieved. Instead for $q = 25$ there are only 6 in both cases and for $q = 125$ there are 9 in case 16 and 14 in case 17.

Remark 2.6. Although the cycle structure of $F(x) = x + \operatorname{Tr}_{q^3/q}(x^{(q^2+1)/2})$, which is case 16 of Theorem 2.1, seems to be complex, this is not the case for the cycle structure of $F \circ (x^{q^2+q-1}) = x^{q^2+q-1} + \operatorname{Tr}_{q^3/q}(x)$. The latter is explicitly determined in [5].

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

Table 1. Examples of cycle structure on lines for $n = 2$. 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 $\mathbb{F}_{243}$.

case	q	γ	cycle structure on any line $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$
1	289		$1^1 4^2 28^{10}$
2	125		$1^3 2^1 30^4$
3	289		$1^1 4^2 28^{10}$
4	289		$1^1 4^1 12^2 14^2 28^1 62^2 80^1$
5	289		$1^5 8^1 19^4 52^1 148^1$
6	289		$1^{145} 4^1 28^5$
7	1024	1	$1^4 11^{20} 19^{20} 42^{10}$
		$\neq 1$	$1^4 30^2 70^2 80^2 260^1 400^1$
8	2048		$1^2 20^{11} 22^1 44^1 66^5 88^5 110^1$ $132^2 176^1 198^1 242^1$
9	1024	1	$4^1 60^{17}$
		a	$2^1 6^5 62^1 186^5$
10	1024		$1^4 10^2 20^5 35^4 60^6 400^1$
11	2048		$2^1 22^4 55^2 138^{11} 165^2$
12	2048		$1^{682} 2^1 22^{62}$
13	1024		$2^2 4^5 30^2 80^1 320^1 540^1$
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	$1^1 2^1 6^1 13^2 26^2 78^2$

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

case	q	A	B
16	25	$1^1 3^1 5^3 6^1$	2
		$1^4 2^1 3^3 10^1$	3
		$2^1 3^1 4^2 12^1$	3
		$1^1 5^3 9^1$	6
		$1^1 2^1 3^1 9^1 10^1$	6
		$11^1 14^1$	6
	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	25	$1^1 3^1 5^3 6^1$	2
		$1^1 2^1 3^2 4^1 6^1$	3
		$1^3 2^5 12^1$	3
		$1^2 6^1 17^1$	6
		$2^1 4^1 19^1$	6
		25^1	6
	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

Theorem 2.7 ([1]). *The polynomial* x^k , $\gcd(k, q-1) = 1$, *permuting* $\mathbb{F}_q^*$ *has a cycle of length* m *if and only if* $m = \operatorname{ord}_t(k)$, *where* $t \mid (q-1)$. *The number* N_m *of those cycles satisfies*

$$m \cdot N_m = \gcd(k^m - 1, q-1) - \sum_{i \mid m, i \neq m} i \cdot N_i, \;\; N_1 = \gcd(k-1, q-1).$$

Remark 2.8. On $\mathbb{F}_q$, x^k has the additional fixed point $x = 0$.

In the next section we show, that in case 2 the cycle structure on lines $l \parallel \gamma\mathbb{F}_q, l \neq \gamma\mathbb{F}_q$ is indeed the same as the cycle structure of x^3 on $\mathbb{F}_q$.

3 Determining the Cycle Structure of $x + \gamma \operatorname{Tr}_{q^2/q}(x^{2q-1})$.

We write $\operatorname{Tr}(x) = x + x^q$ for the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. In this section we determine the cycle structure of $F(x) = x + \gamma \operatorname{Tr}(x^{2q-1})$, where $q \equiv -1 \pmod 3$ and $\gamma^3 = -\frac{1}{27}$.

By Proposition 2.4 and Remark 2.5 for all admissible choices of γ the cycle structure of F as well as its cycle structure on 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.

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

Lemma 3.1. *Let* $q \equiv -1 \pmod 3$ *and* p *be the characteristic of* $\mathbb{F}_q$. *Then the permutation* $F(x) = x - \frac{1}{3}\operatorname{Tr}(x^{2q-1})$ *reduces to* $F(x) = \frac{1}{3}x$ *on the line* $\mathbb{F}_q$. *Consequently, it has one fixed point and* $\frac{q-1}{\operatorname{ord}_p(3)}$ *cycles of length* $\operatorname{ord}_p(3)$ *on* $\mathbb{F}_q$.

Proof. Let $x \in \mathbb{F}_q$, then

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

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

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

Lemma 3.2. *If* $q \equiv -1 \pmod 3$ *and odd, then* $-\frac{1}{3}$ *is a nonsquare of* $\mathbb{F}_q$.

Proof. Let p be the characteristic of $\mathbb{F}_q$, then $p \equiv -1 \pmod 3$ and $q = p^n$, where p and n are odd. $-\frac{1}{3}$ is a nonsquare of $\mathbb{F}_q$ if and only if $x^2 + \frac{1}{3}$ is irreducible in $\mathbb{F}_q[x]$. Since $q = p^n$ with odd n, $x^2 + \frac{1}{3}$ is irreducible in $\mathbb{F}_q[x]$ if and only if it is irreducible in $\mathbb{F}_p[x]$. $x^2 + \frac{1}{3}$ is irreducible in $\mathbb{F}_p[x]$ if and only if $-\frac{1}{3}$ is a nonsquare in $\mathbb{F}_p$. Consequently it suffices to show that $-\frac{1}{3}$ is a nonsquare of the prime field $\mathbb{F}_p$, where $p \equiv -1 \pmod 3$ and odd. Obviously $-\frac{1}{3}$ is nonsquare if and only if

-3 is nonsquare. The rest follows from the law of quadratic reciprocity for the Legendre symbol:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

Now we consider two cases.
For $p \equiv 1 \pmod 4$, we have

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1, \text{ s.t. } \left(\frac{-3}{p}\right) = 1 \cdot (-1) = -1.$$

For $p \equiv 3 \pmod 4$, we have

$$\left(\frac{-1}{p}\right) = -1, \left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1, \text{ s.t. } \left(\frac{-3}{p}\right) = (-1)\cdot 1 = -1.$$

In both cases $\left(\frac{-3}{p}\right) = -1$, implying -3 and so $-\frac{1}{3}$ are nonsquares of $\mathbb{F}_p$. □

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

Theorem 3.3. *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 Corollary 1.8 the cycle structure of F on a line $\alpha + \mathbb{F}_q$ is the same for any choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As in the proof of Theorem 1.7 for any α and $l \in \mathbb{F}_q$ the following holds: $F(\alpha + l) = \alpha + G_\alpha(l)$ where $G_\alpha(l) := l + \gamma \operatorname{Tr}((\alpha + l)^{2q-1})$ permutes $\mathbb{F}_q$ and has the same cycle structure as F on $\alpha + \mathbb{F}_q$. Next we show that for a suitable choice of α, the permutation G_α is a conjugate of $m(x) = x^3$ in $S_{\mathbb{F}_q}$. This choice depends on the parity of q.

If q is *even*, then $G_\alpha(l) = l + \operatorname{Tr}((\alpha + l)^{2q-1})$. Since $q = p^n$ with n odd, $x^2 + x + 1$ is irreducible over $\mathbb{F}_q$. This means we find $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^2 = \alpha + 1$. Consequently

$$\begin{aligned} &\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 1, && \operatorname{Tr}(\alpha) = \alpha^q + \alpha = \alpha^{3j+2} + \alpha = \alpha^2 + \alpha = 1, \\ &\operatorname{Tr}(\alpha^2) = \operatorname{Tr}(\alpha + 1) = \operatorname{Tr}(\alpha) = 1, && \operatorname{Tr}(\alpha^3) = \operatorname{Tr}(1) = 0 \end{aligned}$$

and

$$(\alpha+l)^{q+1} = (\alpha+l)(\alpha^q+l) = (\alpha+l)(\alpha+1+l) = \alpha^2+\alpha+\alpha l+\alpha l+l+l^2 = l^2+l+1.$$

Using these equations we see that

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

Now we can show that $G_\alpha = f^{-1} \circ m \circ f$ for

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

by the following computations.

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

If $l \neq 0$ then

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

If q is *odd*, then $-\frac{1}{3}$ is a nonsquare of $\mathbb{F}_q$ (according to Lemma 3.2) and we find $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^2 = -\frac{1}{3}$. Consequently $(\alpha^q)^2 = (\alpha^2)^q = \alpha^2$ and thus

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

Using these equations we see that

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

Now we can show that $G_\alpha = f^{-1} \circ m \circ f$ for

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

by the following computations.

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

If $l \neq -1$ then

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

We now see that in any case there is an $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, such that G_α is a conjugate of x^3 on $S_{\mathbb{F}_q}$. Consequently f has the same cycle structure on $\alpha + L$ as x^3 on $\mathbb{F}_q$ and since F has the same cycle structure on any one of these lines the assertion follows. □

We conclude by describing explicitly the cycle structure of F in the general case $\gamma^3 = -\frac{1}{27}$:

Theorem 3.4. *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_m be defined by the following recursion:*

$$m \cdot N_m = \gcd(3^m - 1, q-1) - \sum_{i|m, i \neq m} i \cdot N_i, \;\; N_1 = \gcd(2, q-1) = \begin{cases} 1, & q \textit{ even} \\ 2, & q \textit{ odd} \end{cases}.$$

Then $F(x) = x + \gamma \operatorname{Tr}(x^{2q-1})$ permuting $\mathbb{F}_{q^2}$ has

1. *one fixed point and $\frac{q-1}{\operatorname{ord}_p(3)}$ cycles of length $\operatorname{ord}_p(3)$ on $\gamma\mathbb{F}_q$ and*
2. *one fixed point and N_m cycles of lenght m for any $m = \operatorname{ord}_t(3)$, where $t \mid (q-1)$, on any of the $q-1$ affine lines $\alpha + \gamma\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^2} \setminus \gamma\mathbb{F}_q$.*

Proof. As we mentioned at the beginning of this section, the choice of γ is irrelevant for the cycle structure of F and for the cycle structure on lines parallel to $\gamma\mathbb{F}_q$, so we can w. l. o. g. choose $\gamma = -\frac{1}{3}$. In this case we get $\gamma\mathbb{F}_q = \mathbb{F}_q$. Then part 1 is Lemma 3.1 and part 2 follows in this way: According to Theorem 3.3 the cycle structure of F on $\alpha + \gamma\mathbb{F}_q$ is the same as the cycle structure of x^3 on $\mathbb{F}_q$, which is known (see Theorem 2.7). □

If we count the fixed points of F we get:

For $p = 2$, there are q fixed points on $\gamma\mathbb{F}_q$ and $1 + \gcd(3-1, q-1) = 2$ fixed points on any of the $q-1$ affine line $\alpha + \gamma\mathbb{F}_q$, in total $q + 2(q-1) = 3q - 2$.

For $p \neq 2$, there is 1 fixed point on $\gamma\mathbb{F}_q$ and $1 + \gcd(3-1, q-1) = 3$ fixed points on any of the $q-1$ affine lines $\alpha + \gamma\mathbb{F}_q$, in total $1 + 3(q-1) = 3q - 2$.

Corollary 3.5. *Let $q \equiv -1 \pmod 3$ and $\gamma \in \mathbb{F}_{q^2}$ with $\gamma^3 = -\frac{1}{27}$. Then the permutation $F(x) = x + \gamma \operatorname{Tr}(x^{2q-1})$ has $3q-2$ fixed points on $\mathbb{F}_{q^2}$.*

References

1. Shair Ahmad: Cycle Structure of Automorphisms of Finite Cyclic Groups, J. Combin. Theory, 6 (1969) 370-374.
2. Ayça Çeşmelioğlu, Wilfried Meidl, Alev Topuzoğlu: On the cycle structure of permutaion polynomials, Finite Fields and Their Applications, 14 (2008) 593-614.
3. Pascale Charpin and Gohar Kyureghyan: On a class of permutation polynomials over $\mathbb{F}_{2^n}$, *Proceedings of SETA 2008*, Lecture Notes in Comput. Sci. 5203, (2008) 368–376.

4. Pascale Charpin and Gohar Kyureghyan: Monomial functions with linear structure and permutation polynomials, *Finite fields: theory and applications*, Contemp. Math. 518, (2010) 99-111.
5. Daniel Gerike, Gohar M. Kyureghyan: Results on Permutation Polynomials of Shape $x^t + \mathrm{Tr}_{q^n/q}(x^d)$, to appear in the proceedings of the Workshop on Pseudo-Randomness and Finite Fields of the RICAM special semester on "Multivariate Algorithms and Their Foundations in Number Theory".
6. Gohar M. Kyureghyan: Constructing permutations of finite fields via linear translators, J. Combin. Theory, Ser. A 118 (2011) 1052-1061.
7. Gohar M. Kyureghyan, Michael E. Zieve: Permutation Polynomials of the Form $X+\gamma\,\mathrm{Tr}(X^k)$, Contemporary developments in finite fields and applications, (2016) 178-194.
8. Kangquan Li, Longjiang Qu, Xi Chen, Chao Li: Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic, Cryptography and Communications: Special Issue on SETA 2016, 10(3) (2018) 531-554.
9. Rudolf Lidl, Gary L. Mullen: Cycle Structure of Dickson Permutation Polynomials, Math. J. Okayama Univ., 33 (1991) 1-11.
10. Jingxue Ma, Gennian Ge: A note on permutation polynomials over finite fields, Finite Fields and their Applications, 48 (2017) 261-270.
11. Gary L. Mullen, Theresa P. Vaughan: Cycles of Linear Permutations Over a Finite Field, Linear Algebra and its Applications, 108 (1988) 63-82.
12. Ivelisse Rubio, Carlos J. Corrada-Bravo: Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials, Finite Fields and Applications, LNCS 2948, Seiten 254-261, Springer-Verlag, 2004.