On components of vectorial permutations of $\mathbb{F}_q^n$

Nurdagül Anbar[1], Canan Kaşıkcı[2], Alev Topuzoğlu[2]

[1]*Johannes Kepler University,*
Altenbergerstrasse 69, 4040-Linz, Austria
Email: nurdagulanbar2@gmail.com
[2]*Sabancı University,*
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
Email: canank@sabanciuniv.edu
Email: alev@sabanciuniv.edu

Abstract

We consider vectorial maps

$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n,$$

which induce permutations of $\mathbb{F}_q^n$. We show that the degrees of the components $f_1, f_2, \dots, f_n \in \mathbb{F}_q[x_1, \dots, x_n]$ are at least 2 when $2 \le \deg(F) = d < \sqrt{q}$ and $d|(q-1)$. Our proof uses an absolutely irreducible curve over $\mathbb{F}_q$ and the number of rational points on it that we relate to the cardinality of the value set of a polynomial.

1 Introduction

Let q be a power of a prime p and $\mathbb{F}_q$ be the finite field with q elements. For an integer $n \ge 2$, the ring of polynomials in n indeterminates over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[x_1, \dots, x_n]$. It is well-kown that any map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ can be uniquely represented as $f \in \mathbb{F}_q[x_1, \dots, x_n]$ such that $\deg_{x_j}(f) < q$ for all $j = 1, \dots, n$, where $\deg_{x_j}(f)$ is the degree of $f \in \mathbb{F}_q[x_1, \dots, x_n]$, when it is considered as a polynomial over $\mathbb{F}_q[x_1, \dots, x_{j-1}, x_{j+1} \dots, x_n]$, see [3]. The degree of $f = \sum a_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ is defined as $\deg(f) = \max\{i_1 + \cdots + i_n \ , \ a_{i_1,\dots,i_n} \neq 0\}$.

An element $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is a *permutation polynomial* in n variables if the equation $f(x_1, \ldots, x_n) = a$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $a \in \mathbb{F}_q$. A classification of permutation polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ of degree at most two is given in [6].

A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is called a *local permutation polynomial* if for each i, $1 \leq i \leq n$, the polynomial $f(a_1, \ldots a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ is a permutation polynomial in x_i, for all choices of $a_1, \ldots a_{i-1}, a_{i+1}, \ldots, a_n \in \mathbb{F}_q$. The author of [4] and [5] gives necessary and sufficient conditions for polynomials in two or three variables to be local permutation polynomials over prime fields. Relevence of local permutation polynomials for the study of Latin squares or cubes are also described in [4] and [5]. Furthermore, it is shown in [1] that the degree of a local permutation polynomial in $\mathbb{F}_q[x_1, x_2]$ is at most $2q - 4$, and that this bound is sharp.

Any map $F : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ can be represented by

$$F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)), \tag{1.1}$$

where $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg_{x_j}(f_i) < q$ for all $i, j = 1, \ldots, n$, see [3, Lemma 7.40]. The degree of F is defined as $\deg(F) = \max\limits_{1 \leq i \leq n} \{\deg(f_i)\}$. A map $F : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ is called a *vectorial permutation* if it induces a permutation on $\mathbb{F}_q^n$. In what follows, we consider the *class* $\mathcal{F}$ of vectorial permutations F as in (1.1) with $\deg_{x_j}(f_i) < q$ for all $i, j = 1, \ldots, n$.

We consider a natural extension of the concept of local permutation polynomials to maps $F : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$. We define

$$F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

to be a *vectorial local permutation* if all polynomials $f_i(x_1, \ldots, x_n)$, $1 \leq i \leq n$, are local permutations. We denote this class of maps by $\mathcal{F}_L$.

Here we focus on the degrees of components of maps in $\mathcal{F}$. It turns out that the vectorial permutations, which are not vectorial local permutations yield a subclass of maps $F = (f_1, \ldots, f_n) \in \mathcal{F}$ (with additional properties), that satisfy $\deg(f_i) \geq 2$ for $1 \leq i \leq n$. This note is organized as follows. In Section 2, we give preliminary results on maps in $\mathcal{F}$. The main results are presented in Section 3. In particular, given a map $F = (f_1, \ldots, f_n) \in \mathcal{F} \setminus \mathcal{F}_L$, the conditions are obtained for f_i to be of degree ≥ 2 for $1 \leq i \leq n$.

2 Preliminaries

We start by pointing out the well-known connection between vectorial permutations and orthogonal systems of equations.

Lemma 2.1. *A map $F = (f_1, \ldots, f_n) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ is in $\mathcal{F}$ if and only if for any $1 \leq m \leq n$ and $a_1, \ldots, a_m \in \mathbb{F}_q$, the system of equations*

$$f_{i_1}(x_1, \ldots, x_n) = a_1 \ , \ldots \ , f_{i_m}(x_1, \ldots, x_n) = a_m \tag{2.1}$$

has exactly q^{n-m} solution with $i_1 < \ldots < i_m$.

Lemma 2.1 is a direct consequence of Theorem 2 in [7].

Lemma 2.2. *Let $F = (f_1, \ldots, f_n)$ be as in* (1.1)*, with* $\deg(F) \geq 1$*. Then there exist $i, j \in \{1, \ldots, n\}$ and $\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n \in \mathbb{F}_q$ such that the polynomial $f_i(\alpha_1, \ldots, \alpha_{j-1}, x_j, \alpha_{j+1}, \ldots, \alpha_n)$ is not constant in the variable x_j.*

Proof. For the proof we need to show the following. Suppose $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ is of degree ≥ 0. Then there exists $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ such that $f(\alpha_1, \ldots, \alpha_n) \neq 0$. We use induction on n. The argument holds for $n = 1$ since f in this case is a polynomial of degree $d < q$. Suppose the argument holds for all $1 \leq k < n$. We can assume without loss of generality that $\deg_{x_1}(f) = d > 0$. That is, we can write f as

$$f = x_1^d f_d + \cdots + x_1 f_1 + f_0$$

for some $f_i \in \mathbb{F}_q[x_2, \ldots, x_n]$ with $f_d \neq 0$. By the induction hypothesis there exists $(\alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^{n-1}$ such that $f_d(\alpha_2, \ldots, \alpha_n) \neq 0$. Hence, $f(x, \alpha_2, \ldots, \alpha_n)$ is a polynomial of degree $d < q$ and there exists $\alpha_1 \in \mathbb{F}_q$ with $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$. □

We recall that two vectorial maps $F_1(x_1, \ldots, x_n)$ and $F_2(x_1, \ldots, x_n)$ are said to be equivalent if

$$F_2(x_1, \ldots, x_n) = L_2\left(F_1\left(L_1(x_1, \ldots, x_n) + (c_1, \ldots, c_n)\right)\right) + (d_1, \ldots, d_n)$$

for nonsingular linear transformations $L_1, L_2 : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ and $(c_1, \ldots, c_n)$, $(d_1, \ldots, d_n) \in \mathbb{F}_q^n$. In other words, F_1 and F_2 are equivalent, if one can be transformed to the other by non-singular transformations and shifts. Obviously equivalent maps have the same permutation behaviour.

In what follows we sometimes use equivalent maps in $\mathcal{F}$ interchangeably. In particular, we assume without loss of generality that $i = j = 1$ in Lemma 2.2, i.e., we deduce that if $F = (f_1, \ldots, f_n) \in \mathcal{F}$ has positive degree, then $g(x) := f_1(x, \alpha_2, \ldots, \alpha_n)$ is a polynomial of degree $d > 0$ for some $\alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$.

Lemma 2.3. *Let $F = (f_1, \ldots, f_n) \in \mathcal{F}$ and suppose that $g(x) = f_1(x, \alpha_2, \ldots, \alpha_n)$ has degree $d > 0$ for some $(\alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^{n-1}$. If $g(x)$ is not a permutation of $\mathbb{F}_q$, then there exits $j \in \{2, \ldots, n\}$ such that $f_j(x, \alpha_2, \ldots, \alpha_n)$ is not a constant polynomial.*

Proof. Suppose that $f_j(x, \alpha_2, \ldots, \alpha_n) = a_j$ for $a_j \in \mathbb{F}_q$, $j = 2, \ldots, n$. The system

$$f_2(x_1, \ldots, x_n) = a_2 \ , \ldots \ , f_n(x_1, \ldots, x_n) = a_n$$

has q solutions by Lemma 2.1, namely the solution set is $S = \{(x, \alpha_2, \ldots, \alpha_n) \,|\, x \in \mathbb{F}_q\}$. Then for any $y \in \mathbb{F}_q$, the system

$$f_1(x_1, \ldots, x_n) = y \ , f_2(x_1, \ldots, x_n) = a_2 \ , \ldots \ , f_n(x_1, \ldots, x_n) = a_n$$

has a unique solution in the set S. This implies that $f_1(x, \alpha_2, \ldots, \alpha_n)$ is a permutation, which contradicts our assumption. □

We also need the following lemma in Section 3.

Lemma 2.4. *Let g be a separable polynomial over $\mathbb{F}_q$ of degree $d < q$. Then there exists $c \in \mathbb{F}_q$ such that $\gcd(g(x) + c, g'(x)) = 1$.*

Proof. The fact that g is a separable polynomial implies that $g'(x) \neq 0$. Now we prove that $g(x) + c$ and $g'(x)$ have no common root in the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$ for some $c \in \mathbb{F}_q$. Note that $g'(x)$ is a polynomial of degree $t \leq d - 1$. Let $\beta_1, \ldots, \beta_t$ be the roots of $g'(x)$ in $\bar{\mathbb{F}}_q$. Let $c_1, \ldots, c_t$ be elements of $\bar{\mathbb{F}}_q$ such that $g(x) + c_i$ has a zero at β_i for $i = 1, \ldots, t$. Then we have $\mathbb{F}_q \setminus \{c_1, \ldots, c_t\} \neq \emptyset$, and hence $g(x) + c$ and $g'(x)$ have no common root for any element $c \in \mathbb{F}_q \setminus \{c_1, \ldots, c_t\}$. □

3 Main Results

In this section we investigate the component polynomials $f_1, \ldots, f_n$ of $F = (f_1, \ldots, f_n) \in \mathcal{F}$ with $\deg(F) \geq 2$. As above, we take $g(x) = f_1(x, \alpha_2, \ldots, \alpha_n)$ of $\deg(g) > 0$, and relate g to some $f_i(x, \alpha_2, \ldots, \alpha_n)$, $2 \leq i \leq n$, via an affine equation, which defines an absolutely irreducible curve over $\mathbb{F}_q$. By using the cardinality of the value set of a polynomial, and the number of rational points of the curve, we obtain sufficient conditions for $f_2, \ldots, f_n$ to be non-linear.

Let F be a function field over $\mathbb{F}_q$ of genus $g(F)$. One calls $\mathbb{F}_q$ the full constant field of F if $\mathbb{F}_q$ is algebraically closed in F. In this case, the well-known Hasse–Weil bound states that the number $N(F)$ of rational places of F satisfies

$$q + 1 - 2g(F)\sqrt{q} \leq N(F) \leq q + 1 + 2g(F)\sqrt{q} \ , \tag{3.1}$$

see [9, Theorem 5.2.3]. When F is a rational function field, say $F = \mathbb{F}_q(z)$ for some $z \in F$, we denote the places of $\mathbb{F}_q(z)$ corresponding to zero and the pole of $z - \alpha$ by $(z = \alpha)$ and $(z = \infty)$. Now we consider a function field F as a compositum of rational function fields over a rational function field to obtain a bound on its genus as follows.

Lemma 3.1. *Let g, h be separable polynomials in $\mathbb{F}_q[T]$ with positive degrees d_1 and d_2. Let $F = \mathbb{F}_q(x, y)$ be the function field defined by the equation $g(x) = 1/h(y)$. If $\gcd(g(T), g'(T)) = 1$, then F is a function field with the full constant field $\mathbb{F}_q$ of genus $g(F) \leq (d_1 - 1)(d_2 - 1)$.*

Proof. Let $\mathbb{F}_q(z)$ be a rational function field. We consider the rational function field extensions $\mathbb{F}_q(x)/\mathbb{F}_q(z)$ and $\mathbb{F}_q(y)/\mathbb{F}_q(z)$ defined by the equations $z = g(x)$ and $z = 1/h(y)$, respectively. Then F is the compositum of $\mathbb{F}_q(x)$ and $\mathbb{F}_q(y)$, see Figure 1. Note that $\mathbb{F}_q(x)/\mathbb{F}_q(z)$ is an extension of degree d_1 and the place $(z = \infty)$ is totally ramified in $\mathbb{F}_q(x)$. Also, $\mathbb{F}_q(y)/\mathbb{F}_q(z)$ is an extension of degree d_2 and $(z = 0)$ is totally ramified in $\mathbb{F}_q(y)$. In other words, the place $(x = \infty)$ of $\mathbb{F}_q(x)$ (resp. $(y = \infty)$ of $\mathbb{F}_q(y)$) is the unique place lying over $(z = \infty)$ (resp. $(z = 0)$). Since $(z = \infty)$ and $(z = 0)$ are totally ramified, the function fields $\mathbb{F}_q(x)$ and $\mathbb{F}_q(y)$ are defined over $\mathbb{F}_q$. Moreover, the assumption $\gcd(g(T), g'(T)) = 1$ implies that $(z = 0)$ is unramified in $\mathbb{F}_q(x)/\mathbb{F}_q(z)$. Hence, by Abhyankar's Lemma (see [9, Theorem 3.9.1]), any place of $\mathbb{F}_q(x)$ lying over $(z = 0)$ is totally ramified. This proves that the full constant field of F is $\mathbb{F}_q$. Moreover, by Castelnuovo's Inequality (see [9, Theorem 3.11.3]), the genus $g(F)$ of F satisfies

$$g(F) \leq (d_1 - 1)(d_2 - 1) \ .$$

□

Corollary 3.2. *Let g, h be separable polynomials in $\mathbb{F}_q[T]$ with positive degrees d_1 and d_2. If $\gcd(g(T), g'(T)) = 1$, then the polynomial $p(X, Y) = g(X)h(Y) - 1 \in \mathbb{F}_q[X, Y]$ is absolutely irreducible over $\mathbb{F}_q$. Therefore, the zero set of $p(X, Y)$ defines an absolutely irreducible curve over $\mathbb{F}_q$.*

$$\begin{tikzcd}
 & F=\mathbb{F}_q(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_q(x) \arrow[dr, dash, "z=g(x)"'] & & \mathbb{F}_q(y) \arrow[dl, dash, "z=1/h(y)"] \\
 & \mathbb{F}_q(z) &
\end{tikzcd}$$

Figure 1: Compositum of rational function fields

Lemma 3.3. *Let $\mathcal{X}$ be the projective curve over $\mathbb{F}_q$ defined by the affine equation $p(X,Y)=g(X)h(Y)-1$, where g,h are polynomials over $\mathbb{F}_q$ given as in Lemma 3.1. Then the number N of affine rational points of $\mathcal{X}$ satisfies*

$$q-(d_1+d_2-1)-2(d_1-1)(d_2-1)\left(\sqrt{q}+\frac{d_1+d_2}{2}\right)\leq N\ .$$

Proof. By Lemma 3.1, we see that $F=\mathbb{F}_q(x,y)$ with $g(x)=1/h(y)$ is the function field of $\mathcal{X}$ with the full constant field $\mathbb{F}_q$. Then the fact that $g(F)\leq(d_1-1)(d_2-1)$ together with Equation (3.1) implies that the number $N(F)$ of rational places of F satisfies

$$q+1-2(d_1-1)(d_2-1)\sqrt{q}\leq N(F)\leq q+1+2(d_1-1)(d_2-1)\sqrt{q}\ . \quad (3.2)$$

It is a well-known fact that each non-singular rational point of $\mathcal{X}$ corresponds to a unique rational place of F, see [2, 8]. Next we find the rational points at infinity, and obtain an approximation to the number of singular rational points. This enables us to approximate the number of rational places corresponding to them.

We first consider the points of $\mathcal{X}$ at infinity, i.e., the ones $(X:Y:0)$ for which $P(X:Y:0)=0$, where $P(X:Y:Z)=Z^{d_1+d_2}(g(X/Z)h(Y/Z)-1)$. Since $P(X:Y:0)=X^{d_1}Y^{d_2}$, there are only two points at infinity, namely $Q_1=(1:0:0)$ and $Q_2=(0:1:0)$, which are rational. The number of places corresponding to Q_1 and Q_2 are determined by the factorization of the homogeneous polynomials $Z^{d_2}h(Y/Z)$ and $Z^{d_1}g(X/Z)$, respectively. Hence there exist at most d_2 and d_1 rational places corresponding to points Q_1 and Q_2, respectively.

An affine point $(X,Y)\in\overline{\mathbb{F}}_q^2$ is a singular point of $\mathcal{X}$ if and only if the following equality holds.

$$g'(X)h(Y)=h'(Y)g(X)=h(Y)g(X)-1=0\ .$$

Note that we have $P(X,Y) = -1$ for any $X, Y \in \overline{\mathbb{F}}_q$ with $g(X) = 0$ or $h(Y) = 0$. This shows that if (X,Y) is a singular point of $\mathcal{X}$ then $g'(X) = 0$ and $h'(Y) = 0$. Therefore, there are at most $d_1 - 1$ choices for X and $d_2 - 1$ choices for Y. In particular, $\mathcal{X}$ can have at most $(d_1-1)(d_2-1)$ singular affine rational points. Since $\mathcal{X}$ is a degree $d_1 + d_2$ curve, there exist at most $(d_1-1)(d_2-1)(d_1+d_2)$ rational places corresponding to these singular points. Therefore, we conclude that there exist at least

$$N(F) - (d_1 + d_2) - (d_1-1)(d_2-1)(d_1+d_2) \tag{3.3}$$

rational places corresponding to the rational affine points. Then equations (3.2) and (3.3) give the desired result. □

Theorem 3.4. *Let* $F = (f_1, \ldots, f_n) \in \mathcal{F}$ *and* $\deg(F) \geq 2$. *Suppose* F *is not a vectorial local permutation, so that there exist* $\alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ *where* $g(x) = f_1(x, \alpha_2, \ldots, \alpha_n)$ *is not a permutation. If we have* $0 < \deg(g) < \sqrt{q}$, *then* $\deg(f_i) \geq 2$ *for any* $i = 2, \ldots, n$ *unless* $f_i(x, \alpha_2, \ldots, \alpha_n)$ *is constant.*

Proof. We set $d_1 = \deg(g)$. By Lemma 2.3, there exists i, $2 \leq i \leq n$, such that $\deg(f_i(x, \alpha_2, \ldots, \alpha_n)) = d_2 > 0$. Set $h(x) = f_i(x, \alpha_2, \ldots, \alpha_n)$. We assume without loss of generality that g, h are separable polynomials. Otherwise, we can replace g, h by other separable polynomials $\tilde{g}, \tilde{h}$ over $\mathbb{F}_q$, where $g(x) = \tilde{g}(x)^{p^n}$ and $h(x) = \tilde{h}(x)^{p^m}$ for some integers $n, m \geq 0$. Note that since $g(x)$ is not a permutation polynomial, the degrees of g and $\tilde{g}$ are at least 2. We suppose that g has no root in $\mathbb{F}_q$. We also suppose by Lemma 2.4 that $\gcd(g(T), g'(T)) = 1$.

We denote the value set of g by V_g, i.e., $V_g = \{u = g(a) \mid a \in \mathbb{F}_q\}$. In [10], Wan gives bounds for the cardinality of V_g;

$$\frac{q-1}{d_1} + 1 \leq \# V_g \leq q - \frac{q-1}{d_1} \ . \tag{3.4}$$

Let $S \subset \mathbb{F}_q^2$ be the set consisting of elements (x,y) such that $(g(x), h(y)) = (t, 1/t)$ for $t \in \mathbb{F}_q^*$. Then by Equation (3.4) we conclude that

$$\# S \leq \left(q - \frac{q-1}{d_1} \right) d_2 \ . \tag{3.5}$$

Hence any affine point (x,y) of $\mathcal{X}$ defined by the equation $p(X,Y) = g(X)h(Y) - 1$ corresponds to a solution of the system

$$g(x) = t \quad \text{and} \quad h(y) = 1/t$$

for some $t \in \mathbb{F}_q$. Therefore by Lemma 3.3 and Equation (3.5) we conclude that

$$q-(d_1+d_2-1)-2(d_1-1)(d_2-1)\left(\sqrt{q}+\frac{d_1+d_2}{2}\right)\leq\left(q-\frac{q-1}{d_1}\right)d_2\ .$$

This shows that if $d_2 = 1$, then we have $d_1^2 \geq q-1$, which contradicts the fact that $d_1 < \sqrt{q}$. □

Example 3.5. (i) Let $F_1 : \mathbb{F}_{2^6}^2 \mapsto \mathbb{F}_{2^6}^2$ be the map defined by $(x,y) \mapsto (f_1(x,y), f_2(x,y))$ where $f_1(x,y) = x^2(y^3+\zeta)+\zeta y^2$ and $f_2(x,y) = x^2(y^3+\zeta)+y^5+\zeta y^2$, where ζ is a primitive element of $\mathbb{F}_{2^6}$. It is straightforward to show that $F_1(x,y) = L_2 \circ F_2 \circ L_1(x,y)$, where $F_2 : \mathbb{F}_{2^6}^2 \mapsto \mathbb{F}_{2^6}^2$ is defined by $F_2(x,y) = (x^5, (x^3+\zeta)y^2)$ and L_1, L_2 are linear permutations of $\mathbb{F}_{2^6}^2$, defined by $L_1(x,y) = (y, x+y)$, $L_2(x,y) = (x+y, y)$. Note that F_2 is a vectorial permutation since the system $x^5 = a$, $(x^3+\zeta)y^2 = b$ has a unique solution for all $(a,b) \in \mathbb{F}_{2^6}^2$. This follows from $\gcd(5,63) = 1$ so that x^5 permutes $\mathbb{F}_{2^6}$, and the polynomial $T^3+\zeta$ not having a root in $\mathbb{F}_{2^6}$. By Hermite's criterion, for $\alpha \in \mathbb{F}_{2^6}^*$ the polynomial $\alpha^2(T^3+\zeta)+\zeta T^2$ is not a permutation of $\mathbb{F}_{2^6}$. Hence Theorem 3.4 applies, and indeed $\deg f_2(\alpha, y) = 5$.

(ii) Let $F_2 : \mathbb{F}_{2^6}^2 \mapsto \mathbb{F}_{2^6}^2$ be the map defined by $(x,y) \mapsto (f_1(x,y), f_2(x,y))$ where $f_1(x,y) = y^5+x^2y^3$ and $f_2(x,y) = yx^4+x^3$. For $\alpha \in \mathbb{F}_{2^6}^*$, the polynomial $T^5+\alpha^2T^3$ has two distinct roots in $\mathbb{F}_{2^6}$, namely $T = 0$ and $T = \alpha$. That is, $f_1(\alpha, y)$ is not a permutation of $\mathbb{F}_{2^6}$. Since $\deg f_2(\alpha, y) = 1$, by Theorem 3.4 we conclude that F_2 is not a vectorial permutation.

Theorem 3.6. *Let $F = (f_1, \ldots, f_n) \in \mathcal{F}$. If $1 < \deg(F) = d < \sqrt{q}$ and $d|q-1$, then $\deg(f_i) \geq 2$ for any $i = 1, \ldots, n$.*

Proof. We assume without loss of generality that $\deg(f_1) = d$. We first show that f_1 is equivalent to a polynomial of the form $f = cx_1^d + h$, where $h \in \mathbb{F}_q[x_1, \ldots, x_n]$ and $c \in \mathbb{F}_q^*$. Put

$$f_1(x_1,\ldots,x_n)=x_1^{e_1^1}\cdots x_n^{e_n^1}+\cdots+x_1^{e_1^k}\cdots x_n^{e_n^k}+g(x_1,\ldots,x_n)\ ,$$

where $\sum_{i=1}^n e_i^j = d$ for all $j = 1, \ldots, k$ and $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree at most $d-1$. Consider the change of variable $x_i \mapsto x_i + c_ix_1$ for some $c_i \in \mathbb{F}_q$, $i = 2, \ldots, n$. Then we obtain

$$f(x_1,\ldots,x_n)=x_1^d(c_2^{e_2^1}\cdots c_n^{e_n^1}+\cdots+c_2^{e_2^k}\cdots c_n^{e_n^k})+h(x_1,\ldots,x_n) \tag{3.6}$$

for some $h \in \mathbb{F}_q[x_1, \ldots, x_n]$. By the argument in the proof of Lemma 2.2, there exist $c_2, \ldots, c_n \in \mathbb{F}_q$ such that $c_2^{e_2^1} \cdots c_n^{e_n^1} + \cdots + c_2^{e_2^k} \cdots c_n^{e_n^k} \neq 0$, which proves our claim. Note that $\deg_{x_1}(h) < d$. As a result, for any $\alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the polynomial $g(x) = f_1(x, \alpha_2, \ldots, \alpha_n)$ is of degree d, and hence by Hermite's criterion [3, Theorem 7.4], it is not a permutation polynomial. Then Theorem 3.4 shows that any other component f_i has to be non-linear. $\square$

Remark 3.7. One can immediately obtain from the proof of Theorem 3.6 that if $F = (f_1, \ldots, f_n) \in \mathcal{F}$, $\deg(F) = d > 1$ and $d | q - 1$, then F is not a vectorial local permutation.

Remark 3.8. In fact, one can prove a more general result in a similar way. Let $F = (f_1, \ldots, f_n) \in \mathcal{F}$ and $\deg(F) \geq 2$. Suppose that there exist j, $i_1, \ldots, i_k \in \{1, \ldots, n\}$ such that

$$\deg_{x_{i_1}} f_j(x_1, \ldots, x_n) + \cdots + deg_{x_{i_k}} f_j(x_1, \ldots, x_n) = d$$

where $q > d^2$ and $d | q - 1$. Then f_i cannot be a linear polynomial for any $i = 1, \ldots, n$.

Acknowledgement

The authors would like to thank Arne Winterhof for pointing out the problem and helpful discussions. N.A. is supported by the Austrian Science Fund (FWF): Project F5505–N26 and Project F5511–N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". Parts of this paper was written while C. K. visited Johannes Kepler University and RICAM, and N.A. visited Sabancı University. Authors gratefully acknowledge the hospitality and financial support provided by all three institutions.

References

[1] W. S. Diestelkamp, S.G. Hartke, R.H. Kenney, *On the degree of local permutation polynomials*, J. Combin. Math. Combin. Comput. 50 (2004), 129–140.

[2] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts inMathematics No. 52.

[3] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd edn. Encyclopedia Math. Appl., vol. 20. Cambridge University Press, Cambridge (1997).

[4] G. L. Mullen, *Local permutation polynomials over* $\mathbb{Z}_p$, Fibonacci Quart. 18 (1980), 104–108.

[5] G. L. Mullen, *Local permutation polynomials in three variables over* $\mathbb{Z}_p$, Fibonacci Quart. 18 (1980), 208–214.

[6] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), 1001–1005.

[7] H. Niederreiter, *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. 28 (1971), 415 – 422.

[8] H. Niederreiter and C.P. Xing, *Algebraic geometry in coding theory and cryptography*, Princeton UniversityPress, Princeton, NJ (2009).

[9] H. Stichtenoth, *Algebraic function fields and codes*, 2^{nd} Edition, Graduate Texts in Mathematics 254, Springer Verlag, 2009.

[10] D. Wan, *A p-adic lifting lemma and its applications to permutation polynomials*, Proceedings of the International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing, Lecture Notes in Pure and Appl. Math., Marcel Dekker, New York, 141 (1992), 209–216.