Bull. Malays. Math. Sci. Soc. (2025) 48:40
https://doi.org/10.1007/s40840-025-01825-5

BULLETIN of the
MALAYSIAN MATHEMATICAL
SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

Local Permutation Polynomials of Maximum Degree Over Prime Finite Fields

Jaime Gutierrez[1] · Jorge Jiménez Urroz[2]

Received: 19 February 2024 / Revised: 12 November 2024 / Accepted: 6 January 2025 /
Published online: 13 January 2025

Abstract

Let q be a power of a prime p, $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_q[x_1, \ldots, x_n]$ be the ring of polynomials in n variables over $\mathbb{F}_q$. The construction and study of local permutation polynomials of $\mathbb{F}_q[x_1, \ldots, x_n]$ is recently increasing interest among the experts. In this work, we study local permutation polynomials of maximum degree $n(q-2)$ defined over the prime finite field $\mathbb{F}_p$. In particular, we explicitly construct families of such polynomials when $p \geq 5$ and $n \leq p-1$; and for any q of the form $q = p^{pr}$ when $r \geq 1$ and $p \geq 3$.

Keywords Permutation polynomials · Local permutation polynomials · Finite Fields · Multivariate polynomials ring

Mathematics Subject Classification 11T06 · 11T22

1 Introduction

Let q be a power of prime p, $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^n$ denote the cartesian product of n copies of $\mathbb{F}_q$, for any integer $n \geq 1$. Also let us use the notation $\overline{x} = (x_1, \ldots, x_n)$ and $\overline{x}_i = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots x_n)$. The ring of polynomials in n variables over $\mathbb{F}_q$ will be denoted by $\mathbb{F}_q[\overline{x}]$. It is well known that any map from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ can be uniquely represented as $f \in \mathbb{F}_q[\overline{x}]$ such that $\deg_{x_i}(f) < q$ for all

Communicated by Rosihan M. Ali.

Jorge Jiménez Urroz contributed equally to this work.

✉ Jaime Gutierrez
jaime.gutierrez@unican.es

Jorge Jiménez Urroz
jorge.urroz@upm.es

[1] Departamento de Matemática Aplicada y Ciencias de la Computación, Universidad de Cantabria, Santander, Spain

[2] Departamento de Matemáticas, Universidad Politécnica de Madrid, Madrid, Spain

$i = 1, \dots, n$, where $\deg_{x_i}(f)$ is the degree of f as a polynomial in the variable x_i with coefficients in the polynomial ring $\mathbb{F}_q[\overline{x}_i]$, see [7]. Throughout this paper, we identify all functions $\mathbb{F}_q^n \to \mathbb{F}_q$ with such polynomials, and every polynomial, will be of degree $\deg_{x_i}(f) < q$, unless otherwise specified. As a consequence, any polynomial $f(x_1, \dots, x_n)$ has degree at most $n(q-1)$.

A polynomial $f \in \mathbb{F}_q[\overline{x}]$ is called a *local permutation polynomial* (or LPP) if for each i, $1 \leq i \leq n$, the polynomial $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$ is a permutation polynomial in $\mathbb{F}_q[x_i]$, for all choices of $\overline{a}_i \in \mathbb{F}_q^{n-1}$.

Mullen [9, 10] gave necessary and sufficient conditions for polynomials in two and three variables to be local permutations polynomials over a prime field $\mathbb{F}_p$. These conditions are expressed in terms of the coefficients of the polynomial.

On the other hand, any LPP has degrees at most $n(q-2)$, see Proposition 1 in [3]. Diestelkamp, Hartke and Kenney [2] proved that this bound is sharp for $n = 2$ variables, see also [3] for a short proof of this fact. Recent results about degree bounds for n local permutation polynomials defining a permutation of $\mathbb{F}_q^n$ are presented in [1, 4] which proved the existence of LPP of maximum degree over $\mathbb{F}_q[x_1 \dots, x_n]$ for any $q > 3$ and any $n \geq 1$. However, it is still an open problem to know whether there are LPP of maximum degree on $\mathbb{F}_q[x_1, \dots, x_n]$ defined over the prime field $\mathbb{F}_p$. Giving others families of LPP of maximum degree and providing applications to Latin hypercubes is an interesting problem, see [2, 6, 8] for the relation between Latin Squares and LPP of maximum degree $2(q-2)$.

The main contribution in this paper is to show general constructions of local permutation polynomials of maximum degree for all n defined over $\mathbb{F}_p$. We can get the result for a large proportion of cases, but not all. Concretely, two of the main results are the following.

Theorem 1 *Let $p \geq 5$ be a prime number and $n < p - 1$ a positive integer. There exists an LPP in $\mathbb{F}_q[x_1, \dots, x_n]$ defined over $\mathbb{F}_p$ of maximum degree for every $q = p^r$. Moreover if $r \geq 2$, then the result is also true for $n = p - 1$.*

Theorem 2 *Let $q = p^{p^r} > 3$ for $p \geq 3$ prime and $r \geq 1$ integer. There exists an LPP $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ of maximum degree $n(q-2)$ defined over $\mathbb{F}_p$.*

2 Proof of the Theorem 1

We need the following result proved in [3, 4].

Theorem 3 *Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$ be a non constant polynomial.*

1. *If $f = g(x_1, \dots, x_m) + h(x_{m+1}, \dots, x_n)$, $\quad 1 \leq m < n$, then f is LPP $\iff$ g and h are local permutation polynomials.*
2. *Let $g(z) \in \mathbb{F}_q[z]$ be permutation polynomial. Then f is a (local) permutation polynomial $\iff$ $g(f(x_1, \dots, x_n)$ is a (local) permutation polynomial.*
3. *Let $h_1(x_1), \dots, h_n(x_n)$ be permutation polynomials. Then f is (local) permutation polynomial $\iff$ $f(h_1(x_1), \dots, h_n(x_n))$ is (local) permutation polynomial.*
4. *The univariate permutation polynomial $t(x) = x + \sum_{k=0}^{q-2} x^k \in \mathbb{F}_q[x]$ permutes 1 and 0, and leave fixed any other element in $\mathbb{F}_q$.*

5. *If f is PP then f is linear if $q = 2$ and has degree at most $n(q-1)$ otherwise.*
6. *If f is a LPP then f is linear if $q = 2$ or $q = 3$, and has degree at most $n(q-2)$ otherwise.*

Proof of Theorem 1 *Let $S(x_1, \dots, x_n) = x_1 + \cdots + x_n$, then the polynomial $F = t(x) \circ S(x_1^{q-2}, \dots, x_n^{q-2})$ is an LPP by Theorem 3. Also, if $k \le q-2$ and $x^{k(q-2)} \equiv x^{q-2} \pmod{x^q - x}$, then $x^{k(q-2)} \equiv x^{q-2} \pmod{x^{q-1} - 1}$, but*

$$x^{k(q-2)} = x^{(k-1)(q-1)+q-1-k} \equiv x^{q-1-k} \pmod{x^{q-1} - 1},$$

so

$$x^{k(q-2)} \equiv x^{q-1-k} \pmod{x^q - x}, \tag{1}$$

and $x^{k(q-2)} \equiv x^{q-2} \pmod{x^q - x}$ can happen if and only if $k = 1$. We note that F will have maximum degree $n(q-2)$ if and only if $t(x) \circ S(x_1, \cdots, x_n)$ has the monomial $x_1 \cdots x_n$ with nonzero coefficient. Now, for any $0 \le k \le q-2$, S^k is a form of degree k, so all the terms are of the form $x_1^{a_1} \cdots x_n^{a_n}$ with $a_1 + \cdots + a_n = k$ and this contains the term $a_1 = a_2 = \cdots = a_n = 1$ if and only if $k = n$. Then, in this case, $S^n = n! x_1 \cdots x_n +$ terms in less variables, so

$$F = n! x_1^{q-2} \cdots x_n^{q-2} + \text{ terms in less variables},$$

which proves the first part of the theorem.

Finally, note that in the case $r \ge 2$, we can include the case $n = p-1$, but for $r = 1$ the sum in the definition of t only reaches to $p-2$, so the case $n = p-1$ is not included. □

3 Proof of the Theorem 2

We first include the following result on how permutation polynomials behave under addition. It is the core of the idea behind the proof of Theorem 2, included below.

Let $s(x) = \sum_{k=0}^{q-2} x^k$. As it is shown in [4], $s(x) = t(x) - x$, where $t(x)$ is as in Theorem 3.

Theorem 4 *Let $l(x) \in \mathbb{F}_q[x]$ be any permutation polynomial such that $l(0) = 0$ and $l(1) = 1$. Then, the polynomial $h(x) = l(x) + s(x)$ is a PP.*

Proof *For any $x \ne 0, 1$ we have $s(x) = 0$ and hence $h(x) = l(x)$ permutes the elements of $\mathbb{F}_q / \{0, 1\}$. On the other hand $h(0) = l(0) + s(0) = 1$, while $h(1) = l(1) - 1 = 0$.* □

Remark 1 Note that whenever $l(x)$ has degree smaller than $q-2$, then $h(x)$ has degree exactly $q-2$. Also in the case when degree of $l(x)$ is $q-2$ but with leading coefficient not -1.

With this in mind we prove Theorem 2 as follows. Applying the Lagrange interpolation formula in one variable, we write the polynomial $f(x) \in \mathbb{F}_q[x]$ as the linear combination

$$f(x)=\sum_{i=0}^{q-1}\alpha_i g_i(x),$$

where $\{a_0,\ldots,a_{q-1}\}=\mathbb{F}_q$, $f(a_i)=\alpha_i$, and $g_i=g_i(x)=1-(x-a_i)^{q-1}$, for $i=0,\ldots,q-1$. The following lemma follows directly from the definition of $g_0,\ldots,g_{q-1}$.

Lemma 1 *With the notation as above, the polynomial $f(x)$ has degree $q-2$ if and only if $\sum_{i=0}^{q-1}\alpha_i=0$ and $\sum_{i=0}^{q-1}a_i\alpha_i\neq 0$.*

Now let $q=p^{pr}$, for any $r\geq 1$ and ζ be a root of the polynomial given by $z(x)=x^p-x-1=\prod_{c\in\mathbb{F}_p}(x-c)-1$. It is well known that this polynomial is irreducible over $\mathbb{F}_p$, see [5]. Also, note that its p roots are $\zeta+i$ for $i=0,\ldots,p-1$. Hence we have constructed the algebraic extension

$$\mathbb{F}_p[x]/z(x)\simeq\mathbb{F}_p(\zeta)\simeq\mathbb{F}_{p^p}\subset\mathbb{F}_q. \tag{2}$$

Now, consider the polynomial given by

$$g(x)=\sum_{i=0}^{p-1}g_i(x)\in\mathbb{F}_q[x], \tag{3}$$

corresponding to $a_i=\frac{1}{\zeta+i}$, and $\alpha_i=1$, for $i=0,\ldots,p-1$ and $\alpha_i=0$ for any other $\alpha_i\in\mathbb{F}_q$. Then, $\sum_{i=0}^{q-1}\alpha_i=0$. On the other hand, a_i are the roots of the reciprocal polynomial $R(x)=x^pz(1/x)=1-x^{p-1}-x^p$, and the sum of its roots is nothing but the second biggest coefficient with negative sign, hence

$$\sum_{i=0}^{q-1}a_i\alpha_i=\sum_{i=0}^{p-1}\frac{1}{\zeta+i}=-1\neq 0.$$

So, $\deg(g(x))=q-2$ by Lemma 1. We show now that $g(x)\in\mathbb{F}_p[x]$. In fact, we can give the following explicit expression for $g(x)$.

Lemma 2 *Let $q=p^{pr}$ and $g(x)$ the polynomial defined in (3). Then,*

$$g(x)=\frac{x^q-x}{x^p+x^{p-1}-1}x^{p-2}. \tag{4}$$

In particular $g(x)\in\mathbb{F}_p[x]$.

Proof *First note that since $z(x)$ is irreducible over $\mathbb{F}_p$, we have that its reciprocal polynomial $R(x)=x^pz(1/x)=x^p+x^{p-1}-1$ is also irreducible over $\mathbb{F}_p$. So, by*

Lemma 2.13 of [7] $R(x) | x^q - x$, so the right hand side is indeed a polynomial in $\mathbb{F}_p[x]$. Now, for any $\alpha \in \mathbb{F}_q$ we have

$$x^q - x = (x-\alpha)^q - (x-\alpha), \tag{5}$$

since translation permutes the elements in $\mathbb{F}_q$. Now, consider $p(x) = \frac{x^q - x}{x-\alpha}$. Recall that α is a root of $x^q - x$ and hence $(x-\alpha) \mid (x^q - x)$, then $p(x) \in \mathbb{F}_q[x]$. By (5) we have

$$p(x) = (x-\alpha)^{q-1} - 1,$$

and hence $p(\alpha) = -1$. On the other hand, for any root α of $R(x)$ we have

$$\begin{aligned} x^p + x^{p-1} - 1 &= (x-\alpha)^p + \alpha^p + x^{p-1} - \alpha^{p-1} + \alpha^{p-1} - 1 \\ &= (x-\alpha)^p + x^{p-1} - \alpha^{p-1} \\ &= (x-\alpha)\left((x-\alpha)^{p-1} + \sum_{i=0}^{p-2} x^i \alpha^{p-2-i}\right). \end{aligned}$$

Taking $P(x) = \frac{x^p + x^{p-1} - 1}{x-\alpha}$, we get $P(\alpha) = -\alpha^{p-2}$. Then

$$\left.\frac{x^q - x}{x^p + x^{p-1} - 1} x^{p-2}\right|_{\alpha} = \left. x^{p-2} \frac{p(x)}{P(x)}\right|_{\alpha} = 1.$$

But

$$\left.\frac{x^q - x}{x^p + x^{p-1} - 1} x^{p-2}\right|_{\beta} = 0,$$

for any $\beta \in \mathbb{F}_q$ not a root of $R(x)$, since it is a root of the numerator, but not of the denominator. Hence, both polynomials $g(x)$ and $\frac{x^q - x}{x^p + x^{p-1} - 1} x^{p-2}$ have the same values for every $a \in \mathbb{F}_q$ and have the same degree, less than q, so they must be equal. □

Remark 2 It is worth to note that simply by looking at the values that $g(x)$ get on $\mathbb{F}_q$ it is straightforward to get the congruence

$$g(x) \equiv (1 - R(x))(1 - R(x)^{q-1}) \pmod{x^q - x},$$

since if $R(x) = 0$ the values on the left hand side is 1 and if $R(x) \neq 0$ the value is 0, as in $g(x)$.

Now consider the polynomial

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{n} g(x_i) + \sum_{i=1}^{n} x_i^{q-2}.$$

We clearly have $\deg(f(x)) = n(q-2)$, so it remains to prove that it is an LPP over $\mathbb{F}_q[x_1, \dots, x_n]$. Note that, since it is symmetric we only need to prove that for any $(c_2, \dots, c_n)$ the polynomial

$$F(x) = f(x, c_2, \dots, c_n),$$

is a permutation polynomial in $\mathbb{F}_q$. For convenience, denote $Z = \{a_0, \dots, a_{p-1}\}$. Now, if $c_i \notin Z$ for some $2 \le i \le n$, then $g(c_i) = 0$ and $F(x) = x^{q-2} + C$, which is a permutation polynomial over $\mathbb{F}_q$. Otherwise, if $c_i \in Z$ for all $2 \le i \le n$, then $F(x) = g(x) + x^{q-2} + C$. If $x \notin Z$, then $F(x) = x^{q-2} + C$, if $x \in Z$, then $F(x) = x^{q-2} + C + 1$. Now, if we take two distinct elements x, y in $\mathbb{F}_q \setminus Z$, then clearly $F(x) \neq F(y)$, and the same happens if $\{x, y\} \subset Z$. So, suppose $x \in Z$ and $y \in \mathbb{F}_q \setminus Z$, then $F(x) = x^{q-2} + C + 1$, while $F(y) = y^{q-2} + C$ but then if $F(y) = F(\frac{1}{\zeta+i})$ for $i = 0, 1, \dots, p-1$, we have that $y^{q-2} = \left(\frac{1}{\zeta+i}\right)^{q-2} + 1 = \zeta + i + 1$, which is impossible since then $y = \frac{1}{\zeta+i+1} \in Z$, and concluding the proof for extensions of $\mathbb{F}_{p^p}$.

Recall that our objective is to find LPP over $\mathbb{F}_q$ defined over the prime field. In this sense, it is important to note that this result is complementary to what we got in [4]. There, the following result was obtained.

Theorem 5 *Let q be such that $(b, q-1) = 1$ for some $1 < b < p-1$. Then, for any $n \ge 1$ there is an LPP over $\mathbb{F}_q[x_1, \dots, x_n]$ of maximum degree $n(q-2)$ and defined over $\mathbb{F}_p$.*

As was noted in [4], Theorem 5 does not cover every q, in particular for any $q = p^r$ where r is a multiple of $\varphi(p-2)!$, since in this case by Euler's Theorem we have $p^{\varphi(p-2)!} \equiv 1 \pmod{(p-2)!}$, and there is no b verifying the condition. On the other hand, the above theorem covers many cases. For example if $p \equiv 2 \pmod 3$, any extension of degree odd is included with $b = 3$, since $p^{2m+1} \equiv 2 \pmod 3$. In fact, we see that for any p there are infinitely many $q = p^r$ for which there is $1 < b < p-1$ such that $(b, q-1) = 1$. This is the content of the following result.

Lemma 3 *For any prime number p, and integer b coprime with $p-1$, there exist infinitely many $r \ge 1$ such that $(b, p^r - 1) = 1$.*

Proof *Let $b = p^a l$ with $p \nmid l$. For any $m \in \mathbb{N}$, take $r_m = m\varphi(l)$. Then $(b, p^{r_m+1} - 1) = (l, p^{r_m+1} - 1)$. Now, we will show that $(p^{r_m+1} - 1, l) = 1$. Note that $p^{r_m} \equiv 1 \pmod l$ and $(b, p-1) = 1$ by hypothesis and we have $l \mid (p^{r_m} - 1)$ and $(p(p-1), l) = 1$. Moreover, we have*

$$p^{r_m+1} - 1 = \left(p^{r_m+1} - p^{r_m}\right) + \left(p^{r_m} - 1\right) = p^{r_m}(p-1) + \left(p^{r_m} - 1\right).$$

Consequently,

$$\left(p^{r_m+1} - 1, l\right) = \left((p^{r_m+1} - 1) - (p^{r_m} - 1), l\right) = \left(p^{r_m}(p-1), l\right) = 1,$$

which is the desired result. □

The examples given by Lemma 3 give extensions of $\mathbb{F}_p$ of degree $m\varphi(l) + 1$ for any integer $m \geq 1$. Since this condition is not included in Theorem 2, we note that it complements Theorem 5, and get more examples of extensions with LPP's of maximum degree defined over the prime field. But the combination of Theorems 5 and 2 still does not encompass all cases. Observe that $\varphi(p-2)!$ is a multiple of $\varphi(l)$ for any $l < p-1$, so this case is still open.

Once we have gotten an LPP over $\mathbb{F}_q[x_1, \ldots, x_n]$, we would be tempted to use this same polynomial for subextension of $\mathbb{F}_q$, so we could get the result in every extension of $\mathbb{F}_p$. We do have the following.

Lemma 4 *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ an LPP with coefficients in $\mathbb{F}_{q_0}$ for some q_0 such that $\mathbb{F}_{q_0} \subset \mathbb{F}_q$. Then, $f \in \mathbb{F}_{q_0}[x_1, \ldots, x_n]$ is an LPP.*

Proof *The result follows since the polynomial sends elements in $\mathbb{F}_{q_0}$ to $\mathbb{F}_{q_0}$.* □

However, the main obstruction would be to keep the maximal degree. In the case of Theorem 2 the degree of the polynomial drops dramatically, when considering subextensions.

Lemma 5 *Let $q = p^{pr}$ for some integer $r \geq 1$ and $g(x)$ be the polynomial defined in (4). Let $g_0(x) \equiv g(x) \pmod{(x^{q_0} - x)}$ of degree smaller that q_0, for $q_0 \mid q$. Then $g_0(x) = 0$, for any $q_0 = p^l$ with $l|r$ not a multiple of p.*

Proof *Observe that since $\mathbb{F}_{q_0} \subset \mathbb{F}_q$, $(x^{q_0} - x) \mid (x^q - x)$ and since $p \nmid l$ we have* $\gcd(x^{q_0} - x, x^p + x^{p-1} - 1) = 1$. *In particular*

$$g(x) = (x^{q_0} - x)H(x),$$

and hence $g_0(x) = 0$. Note that it is clear from the definition of $g(x)$ since the polynomial vanishes at any point in $\mathbb{F}_q$, except the root of $R(x)$, which are not in $\mathbb{F}_{q_0}$ since $p \nmid l$. In particular, it vanishes at any element of $\mathbb{F}_{q_0}$. □

4 On the Degree of LPP

In paper [4] we tried another strategy to build local permutation polynomials of maximum degree, by composing with the transposition $t(x)$ defined in Theorem 3. The advantage is that those polynomials would be defined over the prime field $\mathbb{F}_p$ by definition. However, composition becomes really complicated very quickly, and we could only prove it for polynomials in 4 variables, and made the following conjecture in general

conjecture 1 *Let $t(x) \in \mathbb{F}_q[x]$ be the transposition defined as in Theorem 1, and consider the polynomials*

$$\begin{aligned} f_1 &= x_1 \\ f_i &= f_i(x_1, \ldots, x_i) = t(f_{i-1}(x_1, \ldots, x_{i-1})^{q-2} + x_i^{q-2}) = t(f_{i-1}^{q-2} + x_i^{q-2}). \end{aligned} \tag{6}$$

Then $f_n(x_1,\dots,x_n)$ is an LPP of degree $n(q-2)$ when $q=p^r>3$ and $p\neq 2$.

We should clarify that in the paper [4] we already proved that the polynomials f_i, for $i=1,\dots,n$, are LPP defined over $\mathbb{F}_p[x_1,\dots,x_n]$, so the claim of the conjecture is only about the fact that these polynomials have maximal degree.

As we have already shown, (see [4]), the degree might vary completely even in the easiest cases, and this section is to show how subtle could be the previous conjecture. First, we need the following technical result.

Lemma 6 *Let a,b integers and $S_b(x_1,\dots,x_a)=(x_1+\cdots+x_a)^b$. Then*

$$S_b(x_1,\dots,x_a)=\sum_{\alpha_1+\cdots+\alpha_a=b} c_{\alpha_1,\dots,\alpha_n}\prod_{i=1}^{a} x_i^{\alpha_i},$$

where $c_{\alpha_1,\dots,\alpha_n}=\frac{b!}{\prod_{i=1}^{a}\alpha_i!}$.

Proof *It is straightforward.* □

For any $x\in\mathbb{R}$ we denote $[x]$ the integer part of x, i.e. the highest integer smaller than or equal to x.

Proposition 6 *Let q be a prime power of p. Any monomial of the form $\prod_{i=1}^{a}x_i^{\alpha_i}$ with $\{(\alpha_1,\dots,\alpha_a):\alpha_1+\cdots+\alpha_a=b\}$ does not appear in the sum $S_b(x_1,\dots,x_a)\in\mathbb{F}_q[x_1,\dots,x_a]$, if $[\log_p b]>M$, where $M=\max\{[\log_p\alpha_i]:i=1,\dots,a\}$.*

The proof is a direct consequence of the following lemma.

Lemma 7 *For any integer n and real numbers $x_1,\dots,x_n$, we have*

$$\sum_{i=1}^{n}[x_i]\le[\sum_{i=1}^{n}x_i].$$

Proof *Suppose $x_i=[x_i]+\varepsilon_i$. Then, $\sum x_i=\sum[x_i]+\sum\varepsilon_i$. There exist $k\geq 0$ such that $k\le\sum\varepsilon_i<k+1$, then*

$$\sum[x_i]+k\le\sum x_i<\sum[x_i]+k+1,$$

so $\sum[x_i]\le\sum[x_i]+k=[\sum x_i]$.

Now we can prove Proposition 6 in the following way. Since the number of times that a prime p divides $m!$ is $\sum_{n\le[\log_p m]}\left[\frac{m}{p^n}\right]$, the number of times that p divides $c_{\alpha_1,\dots,\alpha_n}$ is exactly

$$N=\sum_{n\le[\log_p b]}\left[\frac{b}{p^n}\right]-\sum_{i=1}^{a}\sum_{n\le[\log_p\alpha_i]}\left[\frac{\alpha_i}{p^n}\right],$$

and by Lemma 7 we get

$$\begin{aligned} N &= \sum_{n\le[\log_p b]}\left[\frac{b}{p^n}\right] - \sum_{n\le M}\sum_{i=1}^{a}\left[\frac{\alpha_i}{p^n}\right] \\ &\ge \sum_{n\le[\log_p b]}\left[\frac{b}{p^n}\right] - \sum_{n\le M}\left[\frac{\sum_{i=1}^{a}\alpha_i}{p^n}\right] \\ &= \sum_{n\le[\log_p b]}\left[\frac{b}{p^n}\right] - \sum_{n\le M}\left[\frac{b}{p^n}\right] > 0. \end{aligned}$$

□

Corollary 1 *With the above notation, for any $b < q-1$ we have that deg$(S_b(x_1^{q-2}, \dots, x_a^{q-2})) < a(q-2)$ if $b \ne a$ or $b = a$ and $a \ge p$. And deg$(S_b(x_1^{q-2}, \dots, x_a^{q-2})) = a(q-2)$ if $b = a$ and $a < p$.*

Proof *We know from (1) that for any integer $k \le q-2$, we have the congruence $x^{k(q-2)} \equiv x^{q-k-1} \pmod{x^q - x}$ if $k \ne 0$. Now suppose that the monomial $\prod_{i=1}^{a} x_i^{\alpha_i}$ has r non zero exponents. Then $\sum_{i=1}^{a}\alpha_i = \sum_{i=1}^{r}\alpha_i = b$, and we see that $r \le \min\{a, b\}$. Now,*

$$\prod_{i=1}^{a} x_i^{\alpha_i(q-2)} \equiv \prod_{i=1}^{r} x_i^{q-\alpha_i-1} \pmod{\prod_{i=1}^{a} x_i^q - x_i},$$

and hence

$$deg\left(\prod_{i=1}^{a} x_i^{\alpha_i(q-2)} \pmod{x^q - x}\right) = r(q-1) - \sum_{i=1}^{r}\alpha_i = r(q-1) - b.$$

If $b < a$, then $r(q-1) - b \le b(q-2) < a(q-2)$. On the other hand, if $a < b$, then $r(q-1) - b \le a(q-1) - b < a(q-2)$. Finally, if $a = b$, then $r(q-1) - b < a(q-2)$ unless $r = a$, and in this case $\alpha_i = 1$ for all $i = 1, \dots, a$, and hence $c(1, \dots, 1) = a!$, which is 0 unless $a \le p-1$. □

The previous result has a direct consequence.

Corollary 2 *For any integer $n > q-2$, we have* $\deg(t(x_1^{q-2} + \cdots + x_n^{q-2})) < n(q-2)$.

So, we can see how composition of $t(x)$ with S_b does not preserve maximal degree. It should be noted that the previous Corollary shows the subtle character of Conjecture 1 since in fact the structure of the polynomial $t(S_b)$ is very similar to the construction in Conjecture 1 trying to preserve the degree by separating the variables, and controlling the degree of the composition, while being defined over the prime field.

Acknowledgements The authors would like to thank the anonymous referees for their helpful comments and suggestions, which have greatly improved the presentation and quality of this paper.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Declarations

Conflict of interest All authors declare that they have no Conflict of interest.

References

1. Anbar, N., Kasikci, C., Topuzoglu, A.: On components of vectorial permutations of $\mathbb{F}_q^n$. Finite Fields Appl. **58**, 124–132 (2019)
2. Diestelkamp, W.S., Hartke, S.G., Kenney, R.H.: On the degree of local permutation polynomials. J. Comb. Math. Comb. Comput. **50**, 129–140 (2004)
3. Gutierrez, J., Urroz, J.J.: Local permutation polynomials and the action of e-Klenian groups. Finite Fields Appl. (2023). https://doi.org/10.1016/j.ffa.2023.102261
4. Gutierrez, J., Urroz, J.J.: Permutation and local permutation polynomials of maximum degree, arXiv:2308.01258v2 (2023)
5. Hammarhjelm, G.: Construction of irreducible polynomials over finite fields, Upsala University Project Report 17 (2014)
6. Keedwell, A.D., Dénes, J.: Latin Squares and their Applications. Elsevier, Amsterdam (2015)
7. Lidl, R., Niederreiter, H.: Finite fields. Encyclopedia of Mathematics ans its Applications, Cambridge University Press, Cambridge (1997)
8. Laywine, C., Mullen, G.: Discrete Mathematics Using Latin Squares. John Wiley and Sons Inc, New York (1998)
9. Mullen, G.L.: Local permutation polynomials over $\mathbb{Z}_p$. Fibonacci Q. **18**, 104–108 (1980)
10. Mullen, G.L.: Local permutation polynomials in three variables over $\mathbb{Z}_p$. Fibonacci Q. **18**, 208–214 (1980)
11. Niederreiter, H.: Permutation polynomials in several variables over finite fields. Proc. Jpn. Acad. **46**, 1001–1005 (1970)
12. Niederreiter, H.: Orthogonal systems of polynomials in finite fields. Proc. Am. Math. Soc. **28**, 415–422 (1971)
13. Shparlinski, I.: Finite fields: theory and computation. Kluwer Academic Publishers, Dordrecht (1999)