Enumerating permutation polynomials

Theodoulos Garefalakis[a,1], Giorgos Kapetanakis[a,2,*]

[a] *Department of Mathematics and Applied Mathematics, University of Crete, 70013 Heraklion, Greece*

Abstract

We consider the problem of enumerating polynomials over $\mathbb{F}_q$, that have certain coefficients prescribed to given values and permute certain substructures of $\mathbb{F}_q$. In particular, we are interested in the group of N-th roots of unity and in the submodules of $\mathbb{F}_q$. We employ the techniques of Konyagin and Pappalardi to obtain results that are similar to their results in [*Finite Fields and their Applications*, 12(1):26–37, 2006]. As a consequence, we prove conditions that ensure the existence of low-degree permutation polynomials of the mentioned substructures of $\mathbb{F}_q$.

Keywords: finite fields, permutation polynomials
2010 MSC: 11T06, 11T23

1. Introduction

Let $q = p^t$, where p is a prime and t is a positive integer. A polynomial over the finite field $\mathbb{F}_q$ is called a *permutation polynomial* if it induces a permutation on $\mathbb{F}_q$. The study of permutation polynomials goes back to the work of Hermite [6], Dickson [5], and subsequently Carlitz [3] and others. Recently, interest in permutation polynomials has been renewed due to applications they have found in coding theory, cryptography and combinatorics. We refer to Chapter 7 of [10] for background on permutation polynomials, as well as an extensive discussion on the history of the subject.

In a recent work, Coulter, Henderson and Matthews [4] present a new construction of permutation polynomials. Their method requires a polynomial that permutes the group of N-th roots of unity, μ_N, where $N \mid q-1$, and an auxiliary function T which contracts $\mathbb{F}_q$ to $\mu_N \cup \{0\}$ and has some additional linearity property. This idea was generalized by Akbary, Ghioca and Wang [2].

*Corresponding author

Email addresses: `tgaref@uoc.gr` (Theodoulos Garefalakis), `gnkapet@gmail.com` (Giorgos Kapetanakis)

[1] Tel.: +30 2810 393845, Fax: +30 2810 393881

[2] Tel.: +30 2810 393724, Fax: +30 2810 393881

In different line of work, Konyagin and Pappalardi [7, 8] count the permutation polynomials that have given coefficients equal to zero. Given a permutation $\sigma \in S(\mathbb{F}_q)$, there exists a unique polynomial in $f_\sigma \in \mathbb{F}_q[X]$ of degree at most $q-2$ such that $f_\sigma(c) = \sigma(c)$ for all $c \in \mathbb{F}_q$. For any $0 < k_1 < \cdots < k_d < q-1$, they define $N_q(k_1, \ldots, k_d)$ to be the number of permutations σ such that the corresponding polynomial f_σ has the coefficients of X^{k_i}, $1 \le i \le d$, equal to zero and prove the following main result.

Theorem 1.1 ([8], Theorem 1).

$$\left| N_q(k_1, \ldots, k_d) - \frac{q!}{q^d} \right| \le \left(1 + \frac{1}{\sqrt{e}}\right)^q ((q - k_1 - 1)q)^{q/2}.$$

In particular, this implies that there exist such permutations, given that $q!/q^d > (1 + e^{-1/2})^q((q - k_1 - 1)q)^{q/2}$.

Akbary, Ghioca and Wang [1] sharpened this result by enumerating permutation polynomials of prescribed shape, that is, with a given set of non-zero monomials.

In the present work, we consider the problem of enumerating polynomials over $\mathbb{F}_q$, that have certain coefficients fixed to given values, and permute certain substructures of $\mathbb{F}_q$, namely the group of N-th roots of unity and submodules of $\mathbb{F}_q$ and prove the following theorems.

Theorem 1.2. *If $N!/\mathfrak{q}^d \ge [(\mathfrak{q} - 1)(N - k_1)]^{N/2}(1 + e^{-1/2})^N$, then there exists a polynomial of $\mathbb{F}_q[X]$ of degree at most $N - 1$, that permutes μ_N, the N-th roots of unity, with the coefficients of X^{k_i} equal to $a_i \in \mathbb{F}_q$, for $i = 1, \ldots, d$ and $0 < k_1 < \cdots < k_d < N$, where $N \mid q - 1$ and $\mathfrak{q}$ is the minimum divisor of q with $N \mid \mathfrak{q} - 1$.*

Theorem 1.3. *Let $\mathbb{F}_r$ be a proper subfield of $\mathbb{F}_q$. Suppose $\mathfrak{r}!/\mathfrak{q}^d \ge \mathfrak{q}^{\mathfrak{r}/2}(\mathfrak{r} - k_1 - 1)^{\mathfrak{r}/2}(1 + e^{-1/2})^{\mathfrak{r}}$, then there exists a polynomial of $\mathbb{F}_q[X]$ that permutes $\mathcal{F}$, an $\mathbb{F}_r[X]$-submodule of $\mathbb{F}_q$, with its coefficients of X^{k_i} equal to $a_i \in \mathbb{F}_q$, for $i = 1, \ldots, d$ and $0 < k_1 < \cdots < k_d < N$, where $\mathfrak{r} = r^n = |\mathcal{F}|$, $\mathfrak{q} = r^\rho$ and ρ is the order and n is the degree of the Order of $\mathcal{F}$.*

We employ the techniques of Konyagin and Pappalardi to obtain results that are similar to those in [8]. In particular, Theorems 1.2 and 1.3 can be viewed as the analoges of Theorem 1.1 for roots of unity and submodules respectively, while they also imply the existence of low-degree polynomials that permute these substructures of $\mathbb{F}_q$, see Corollaries 2.1 and 3.1.

2. Enumeration of polynomials that permute roots of unity

Let $N \mid q-1$ and $\sigma \in S(\mu_N)$ be a permutation of μ_N. We define the polynomial

$$f_\sigma(X) = \frac{1}{N} \sum_{c \in \mu_N} \sigma(c) g_c(X), \tag{1}$$

where $g_c(X) = \sum_{j=0}^{N-1} c^{-j}X^j$, for $c \in \mu_N$. It is clear that $g_c(c) = N$ and $g_c(x) = 0$ for all $x \in \mu_N \setminus \{c\}$, hence $f_\sigma(\omega) = \sigma(\omega)$, for every $\omega \in \mu_N$.

Given d integers $0 < k_1 < \cdots < k_d < N$, we denote

$$N_q(\mathbf{k}, \mathbf{a}) = \left|\left\{\sigma \in S(\mu_N) \mid \text{ the coefficient of } X^{k_i} \text{ of } f_\sigma \text{ is } a_i, \forall\, 1 \le i \le d\right\}\right|,$$

where $\mathbf{k} = (k_1, \ldots, k_d)$ and $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{F}_q^d$. From (1), we see that the j-th coefficient of f_σ is equal to some $a \in \mathbb{F}_q$ if and only if

$$\sum_{c \in \mu_N} c^{-j}\sigma(c) = Na,$$

so we have

$$N_q(\mathbf{k}, \mathbf{a}) = \left|\left\{\sigma \in S(\mu_N) \mid \sum_{c \in \mu_N} c^{-k_i}\sigma(c) = Na_i, \forall\, 1 \le i \le d\right\}\right|.$$

For any $S \subseteq \mu_N$, define the sets

$$A_S = \left\{f : \mu_N \to S \mid \sum_{c \in \mu_N} c^{-k_i} f(c) = Na_i, \forall\, 1 \le i \le d\right\},$$
$$B_S = \left\{f : \mu_N \to S \mid f \text{ is surjective}, \sum_{c \in \mu_N} c^{-k_i} f(c) = Na_i, \forall\, 1 \le i \le d\right\}.$$

Also, define $A(S) = |A_S|$ and $B(S) = |B_S|$. It is not hard to see that since $A(M) = \sum_{T \subseteq M} B(T)$, for every $M \subseteq \mu_N$, we have that

$$B(M) = \sum_{T \subseteq M} (-1)^{|M|-|T|} A(T). \tag{2}$$

For $M = \mu_N$, the above implies

$$N_q(\mathbf{k}, \mathbf{a}) = \sum_{S \subseteq \mu_N} (-1)^{N-|S|} A(S). \tag{3}$$

Recall that $q = p^t$. Set $e_p(u) := e^{2\pi i u/p}$ and $\mathrm{Tr}(x)$ the absolute trace of $x \in \mathbb{F}_q$, i.e. $\mathrm{Tr}(x) := x + x^p + \cdots + x^{p^{t-1}}$ for $x \in \mathbb{F}_q$. Further, let $\mathfrak{q}$ be the smallest power of p such that $N \mid \mathfrak{q} - 1$, i.e. $\mathbb{F}_\mathfrak{q}$ is the smallest subfield of $\mathbb{F}_q$ containing μ_N. If

$S \subseteq \mu_N$, then

$$\begin{aligned}
A(S) &= \frac{1}{\mathfrak{q}^d} \sum_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_\mathfrak{q}^d} \sum_{f:\mu_N\to S} e_p\left(\mathrm{Tr}\left(\sum_{i=1}^d \alpha_i\left(-Na_i + \sum_{c\in\mu_N} c^{-k_i} f(c)\right)\right)\right)\\
&= \frac{1}{\mathfrak{q}^d} \sum_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_\mathfrak{q}^d} \sum_{f:\mu_N\to S} \frac{e_p\left(\sum_{c\in\mu_N}\mathrm{Tr}\left(f(c)\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)}{e_p\left(\mathrm{Tr}\left(N\sum_{i=1}^d \alpha_i a_i\right)\right)}\\
&= \frac{1}{\mathfrak{q}^d} \sum_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_\mathfrak{q}^d} \frac{\prod_{c\in\mu_N}\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)}{e_p\left(\mathrm{Tr}\left(N\sum_{i=1}^d \alpha_i a_i\right)\right)}\\
&= \frac{|S|^N}{\mathfrak{q}^d} + R_S, \qquad (4)
\end{aligned}$$

where

$$\begin{aligned}
|R_S| &\le \frac{\mathfrak{q}^d-1}{\mathfrak{q}^d} \max_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_\mathfrak{q}^d\setminus\{0\}} \frac{\prod_{c\in\mu_N}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)\right|}{\left|e_p\left(\mathrm{Tr}\left(N\sum_{i=1}^d \alpha_i a_i\right)\right)\right|}\\
&= \frac{\mathfrak{q}^d-1}{\mathfrak{q}^d} \max_{(\alpha_1,\ldots,\alpha_d)\in\mathbb{F}_\mathfrak{q}^d\setminus\{0\}} \prod_{c\in\mu_N}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)\right|.
\end{aligned}$$

Moreover, the AM-GM inequality implies

$$\begin{aligned}
\prod_{c\in\mu_N}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)\right| &\le \left(\frac{1}{N}\sum_{c\in\mu_N}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)\right|^2\right)^{\frac{N}{2}}\\
&\le \left(\frac{1}{N}\sum_{c\in\mathbb{F}_\mathfrak{q}^*}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{N-k_i}\right)\right)\right|^2\right)^{N/2}\\
&\le \left(\frac{1}{N}\sum_{u\in\mathbb{F}_\mathfrak{q}^*}(N-k_1)\left|\sum_{t\in S} e_p(\mathrm{Tr}(tu))\right|^2\right)^{N/2}.
\end{aligned}$$

With the help of the well-known identity, see [9, Chapter 3],

$$\sum_{u\in\mathbb{F}_\mathfrak{q}}\left|\sum_{t\in S} e_p(\mathrm{Tr}(tu))\right|^2 = \mathfrak{q}|S|, \qquad (5)$$

we eventually get that

$$\prod_{c\in\mu_N}\left|\sum_{t\in S} e_p\left(\mathrm{Tr}\left(t\sum_{i=1}^d \alpha_i c^{-k_i}\right)\right)\right| \le \left(\frac{(\mathfrak{q}-1)(N-k_1)|S|}{N}\right)^{N/2},$$

which implies

$$|R_S| \le \frac{\mathfrak{q}^d - 1}{\mathfrak{q}^d} \left(\frac{(\mathfrak{q}-1)(N-k_1)|S|}{N} \right)^{N/2} < \left(\frac{(\mathfrak{q}-1)(N-k_1)|S|}{N} \right)^{N/2}. \quad (6)$$

By working similarly as in Eq. (2), but by considering the mappings $\mu_N \to \mu_N$, we conclude that

$$\sum_{S \subseteq \mu_N} (-1)^{N-|S|} |S|^N = N!,$$

that combined with Equations (3), (4) and (6) and the fact that $j \le N e^{j/N-1}$, since $1 + x \le e^x$ for all x, we get

$$\begin{aligned}
\left| N_q(\mathbf{k}, \mathbf{a}) - \frac{N!}{\mathfrak{q}^d} \right| &< \left(\frac{(\mathfrak{q}-1)(N-k_1)}{N} \right)^{N/2} \sum_{j=0}^{N} \binom{N}{j} j^{N/2} \\
&\le \left(\frac{(\mathfrak{q}-1)(N-k_1)}{N} \right)^{N/2} \sum_{j=0}^{N} \binom{N}{j} (N e^{j/N-1})^{N/2} \\
&= [(\mathfrak{q}-1)(N-k_1)]^{N/2} \sum_{j=0}^{N} \binom{N}{j} (e^{-1/2})^{N-j} \\
&= [(\mathfrak{q}-1)(N-k_1)]^{N/2} (1 + e^{-1/2})^N.
\end{aligned}$$

Summing up, we have proved that

$$N_q(\mathbf{k}, \mathbf{a}) > \frac{N!}{\mathfrak{q}^d} - [(\mathfrak{q}-1)(N-k_1)]^{N/2} (1 + e^{-1/2})^N,$$

which implies the Theorem 1.2.

If we apply this result in the case $k_b = N-1, k_{b-1} = N-1-1, \dots, k_1 = N-b$ and $a_i = 0$ for all i, then we end up with the following interesting consequence.

Corollary 2.1. *With the same assumptions as in Theorem 1.2, if*

$$\sqrt[N]{N!/\mathfrak{q}^b} \ge \sqrt{b(\mathfrak{q}-1)}(1 + e^{-1/2}),$$

then there exists a polynomial of $\mathbb{F}_q$ *of degree less than* $N-b$ *that permutes* μ_N*.*

3. Enumeration of polynomials that permute additive submodules

Throughout this section, we see $\mathbb{F}_q$ as a $\mathbb{F}_r[X]$-module, where $\mathbb{F}_r$ is a proper subfield of $\mathbb{F}_q$, under the action $f \circ x = \sum_{i=0}^{k} f_i x^{q^i}$ for $f = \sum_{i=0}^{k} f_i X^i \in \mathbb{F}_r[X]$ and $x \in \mathbb{F}_q$. Furthermore, it follows directly from the Normal Basis Theorem, see [10, Theorem 2.35], that $\mathbb{F}_q$ is a cyclic $\mathbb{F}_r[X]$-module.

Let $\mathcal{F}$ be an $\mathbb{F}_r[X]$-submodule of $\mathbb{F}_q$, where $\mathfrak{r} := |\mathcal{F}| = r^n \le q$. Since $\mathbb{F}_r[X]$ is a principal ideal domain and $\mathcal{F}$ is a $\mathbb{F}_r[X]$-submodule of $\mathbb{F}_q$, which is cyclic, it follows that $\mathcal{F}$ will be cyclic as well, see [11, Theorem 6.3]. As a consequence, there exists some monic $f \in \mathbb{F}_r[X]$, of degree n, with $f \mid X^m - 1$, such that

$$\mathcal{F} = \{x \in \mathbb{F}_q \mid f \circ x = 0\},$$

which is known as the *Order* of $\mathcal{F}$. Also, for every $x \in \mathcal{F}$ we have that

$$\sum_{i=0}^{n} f_i x^{r^i - 1} = \begin{cases} 0, & \text{if } x \neq 0, \\ f_0, & \text{if } x = 0, \end{cases}$$

while $f_0 \neq 0$, since $f \mid X^m - 1$. Now, for $\sigma \in S(\mathcal{F})$ a permutation of $\mathcal{F}$, we define

$$f_\sigma(X) = \frac{1}{f_0} \sum_{c \in \mathcal{F}} \sigma(c) \sum_{i=0}^{n} f_i (X - c)^{r^i - 1} \tag{7}$$

and it is clear that $f_\sigma(\omega) = \sigma(\omega)$ for every $\omega \in \mathcal{F}$.

Given d integers $0 < k_1 < \cdots < k_d < \mathfrak{r}$ and $(a_1, \ldots, a_d) \in \mathbb{F}_q^d$, we denote

$$N_q(\mathbf{k}, \mathbf{a}) = \left|\left\{\sigma \in S(\mathcal{F}) \mid \text{ the coefficient of } X^{k_i} \text{ of } f_\sigma \text{ is } a_i, \forall\, 1 \leq i \leq d\right\}\right|.$$

From (7), we deduce that the j-th coefficient of f_σ is a if and only if

$$\sum_{c \in \mathcal{F}} \sum_{i=0}^{n} \binom{r^i - 1}{j} f_i (-c)^{r^i - 1 - j} \sigma(c) = f_0 a,$$

hence

$$N_q(\mathbf{k}, \mathbf{a}) = \\ \left|\left\{\sigma \in S(\mathcal{F}) \mid \sum_{c \in \mathcal{F}} \sum_{i=0}^{n} \binom{r^i - 1}{k_j} f_i c^{r^i - 1 - k_j} \sigma(c) = f_0 a_j, \forall\, 1 \leq j \leq d\right\}\right|.$$

For any $S \subseteq \mathcal{F}$, define the sets

$$A_S = \left\{g : \mathcal{F} \to S \mid \sum_{c \in \mathcal{F}} \sum_{i=0}^{n} F_{ij} c^{r^i - 1 - k_j} g(c) = f_0 a_j, \forall\, 1 \leq j \leq d\right\},$$
$$B_S = \{g \in A_S \mid g \text{ is surjective}\},$$

where F_{ij} stands for $\binom{r^i - 1}{k_j} f_i$. Define $A(S) = |A_S|$ and $B(S) = |B_S|$. As with Eq. (2), we can show that $A(M) = \sum_{T \subseteq M} B(T)$, for every $M \subseteq \mathcal{F}$, hence

$$N_q(\mathbf{k}, \mathbf{a}) = \sum_{S \subseteq \mathcal{F}} (-1)^{\mathfrak{r} - |S|} A(S). \tag{8}$$

Furthermore, let ρ be the *order* of f, i.e. ρ is minimal such that $f \mid X^\rho - 1$ and let $\mathfrak{q} := r^\rho$. It follows that $\mathbb{F}_\mathfrak{q}$ is the smallest subfield of $\mathbb{F}_q$ containing $\mathcal{F}$. For

$S \subseteq \mathcal{F}$, as in the case of Equation (4), we have

$$\begin{aligned}
A(S) &= \frac{1}{\mathfrak{q}^d} \sum_{(\alpha_1,\dots,\alpha_d)\in\mathbb{F}_{\mathfrak{q}}^d} \sum_{g:\mathcal{F}\to S} \frac{e_p\left(\sum_{c\in\mathcal{F}} \operatorname{Tr}\left(g(c)\sum_{j=1}^d \alpha_j \sum_{i=0}^n F_{ij} c^{r^i-1-k_j}\right)\right)}{e_p\left(\operatorname{Tr}\left(\sum_{j=1}^d f_0\alpha_j a_j\right)\right)} \\
&= \frac{1}{\mathfrak{q}^d} \sum_{(\alpha_1,\dots,\alpha_d)\in\mathbb{F}_{\mathfrak{q}}^d} \frac{\prod_{c\in\mathcal{F}} \sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)}{e_p\left(\operatorname{Tr}\left(\sum_{j=1}^d f_0\alpha_j a_j\right)\right)} \\
&= \frac{|S|^{\mathfrak{r}}}{\mathfrak{q}^d} + R_S, \qquad (9)
\end{aligned}$$

where

$$\begin{aligned}
|R_S| \leq& \frac{\mathfrak{q}^d-1}{\mathfrak{q}^d} \max_{(\alpha_1,\dots,\alpha_d)\in\mathbb{F}_{\mathfrak{q}}^d\setminus\{0\}} \frac{\prod_{c\in\mathcal{F}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right|}{\left|e_p\left(\operatorname{Tr}\left(\sum_{j=1}^d f_0\alpha_j a_j\right)\right)\right|} \\
=& \frac{\mathfrak{q}^d-1}{\mathfrak{q}^d} \max_{(\alpha_1,\dots,\alpha_d)\in\mathbb{F}_{\mathfrak{q}}^d\setminus\{0\}} \prod_{c\in\mathcal{F}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right|.
\end{aligned}$$

Also, the AM-GM inequality yields

$$\begin{aligned}
&\prod_{c\in\mathcal{F}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right| \\
&\leq \left(\frac{1}{\mathfrak{r}} \sum_{c\in\mathcal{F}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right|^2\right)^{\mathfrak{r}/2} \\
&\leq \left(\frac{1}{\mathfrak{r}} \sum_{c\in\mathbb{F}_{\mathfrak{q}}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right|^2\right)^{\mathfrak{r}/2} \\
&\leq \left(\frac{1}{\mathfrak{r}} \sum_{u\in\mathbb{F}_{\mathfrak{q}}} (\mathfrak{r}-1-k_1) \left|\sum_{t\in S} e_p(\operatorname{Tr}(tu))\right|^2\right)^{\mathfrak{r}/2}.
\end{aligned}$$

With the help of (5), we show that

$$\prod_{c\in\mathcal{F}} \left|\sum_{t\in S} e_p\left(\operatorname{Tr}\left(t\sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r^i-1-k_j}\right)\right)\right| \leq \left(\mathfrak{q}\left(1-\frac{k_1+1}{\mathfrak{r}}\right)|S|\right)^{\mathfrak{r}/2},$$

that, in turn, yields

$$|R_S| \leq \frac{\mathfrak{q}^d-1}{\mathfrak{q}^d}\left(\mathfrak{q}\left(1-\frac{k_1+1}{\mathfrak{r}}\right)|S|\right)^{\mathfrak{r}/2} < \left(\mathfrak{q}\left(1-\frac{k_1+1}{\mathfrak{r}}\right)|S|\right)^{\mathfrak{r}/2}. \qquad (10)$$

Now, as in the case of the roots of unity, it is clear that

$$\sum_{S\subseteq\mathcal{F}}(-1)^{\mathfrak{r}-|S|}|S|^{\mathfrak{r}}=\mathfrak{r}!,$$

which combined with Equations (8), (9) and (10) and the fact that $j \le \mathfrak{r}e^{j/\mathfrak{r}-1}$, gives

$$\begin{aligned}\left|N_q(\mathbf{k},\mathbf{a})-\frac{\mathfrak{r}!}{\mathfrak{q}^d}\right| &< \mathfrak{q}^{\mathfrak{r}/2}\left(1-\frac{k_1+1}{\mathfrak{r}}\right)^{\mathfrak{r}/2}\sum_{j=0}^{\mathfrak{r}}\binom{\mathfrak{r}}{j}j^{\mathfrak{r}/2}\\ &\le \mathfrak{q}^{\mathfrak{r}/2}\left(1-\frac{k_1+1}{\mathfrak{r}}\right)^{\mathfrak{r}/2}\sum_{j=0}^{\mathfrak{r}}\binom{\mathfrak{r}}{j}\left(\mathfrak{r}e^{j/\mathfrak{r}-1}\right)^{\mathfrak{r}/2}\\ &= \mathfrak{q}^{\mathfrak{r}/2}(\mathfrak{r}-k_1-1)^{\mathfrak{r}/2}(1+e^{-1/2})^{\mathfrak{r}}.\end{aligned}$$

To sum up, in this section we proved that

$$N_q(\mathbf{k},\mathbf{a})>\frac{\mathfrak{r}!}{\mathfrak{q}^d}-\mathfrak{q}^{\mathfrak{r}/2}(\mathfrak{r}-k_1-1)^{\mathfrak{r}/2}(1+e^{-1/2})^{\mathfrak{r}}$$

which implies Theorem 1.3.

By applying this for $k_b=\mathfrak{r}-1, k_{b-1}=\mathfrak{r}-1-1,\dots,k_1=\mathfrak{r}-b$ and $a_i=0$ for all i, we end up with the following.

Corollary 3.1. *With the same assumptions as in Theorem 1.3, if*

$$\sqrt[\mathfrak{r}]{\frac{\mathfrak{r}!}{\mathfrak{q}^d}}\ge\sqrt{\mathfrak{q}(b-1)}(1+e^{-1/2}),$$

then there exists a polynomial of $\mathbb{F}_q$ of degree less than $\mathfrak{r}-b$ that permutes $\mathcal{F}$.

Aknowledgments

The authors would like the reviewer for his/her suggestions and corrections.

References

[1] A. Akbary, D. Ghioca and Q. Wang. On permutation polynomials with prescribed shape. *Finite Fields Appl.*, 15:195–206, 2009.

[2] A. Akbary, D. Ghioca and Q. Wang. On constructing permutations of finite fields. *Finite Fields Appl.*, 17:51–67, 2011.

[3] L. Carlitz. Permutations in a finite field. *Proc. Amer. Math. Soc.*, 4:538, 1953.

[4] R. Coulter, M. Henderson and R. Matthews. A note on constructing permutation polynomials. *Finite Fields Appl.*, 15:553–557, 2009.

[5] L. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11:65–120, 161–183, 1897.

[6] C. Hermite. Sur les fonctions de sept lettres. *C.R. Acad. Sci. Paris*, 57:750–757, 1863.

[7] S. Konyagin and F. Pappalardi. Enumerating permutation polynomials over finite fields by degree. *Finite Fields Appl.*, 8(4):548–553, 2002.

[8] S. Konyagin and F. Pappalardi. Enumerating permutation polynomials over finite fields by degree II. *Finite Fields Appl.*, 12(1):26–37, 2006.

[9] S. Konyagin and I. Shparlinski. *Character Sums with Exponential Functions and their Applications.* Cambridge University Press, Cambridge, 2004.

[10] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, Reading, Mass., 1983.

[11] S. Roman. *Advanced Linear Algebra.* Springer-Verlag, New York, 2008.