Enumerating permutation polynomials

Theodoulos Garefalakis\textsuperscript{a,1}, Giorgos Kapetanakis\textsuperscript{a,2,*}

\textsuperscript{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 \cite{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 \cite{6}, Dickson \cite{5}, and subsequently Carlitz \cite{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 \cite{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 \cite{4} present a new construction of permutation polynomials. Their method requires a polynomial that permutes the group of $N$-th roots of unity, $\mu_N$, 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 \cite{2}.
In different line of work, Konyagin and Pappalardi \cite{7,8} count the permutation polynomials that have given coefficients equal to zero. Given a permutation \( \sigma \in S(F_q) \), there exists a unique polynomial in \( f_\sigma \in F_q[X] \) of degree at most \( q-2 \) such that \( f_\sigma(c) = \sigma(c) \) for all \( c \in F_q \). 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 \( \sigma \) such that the corresponding polynomial \( f_\sigma \) has the coefficients of \( X^{k_i}, 1 \leq i \leq d \), equal to zero and prove the following main result.

**Theorem 1.1** \cite{8}, Theorem 1.

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

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

Akbary, Ghioca and Wang \cite{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 \( F_q \), that have certain coefficients fixed to given values, and permute certain substructures of \( F_q \), namely the group of \( N \)-th roots of unity and submodules of \( F_q \) and prove the following theorems.

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

**Theorem 1.3.** Let \( \mathcal{F} \) be a proper subfield of \( F_q \). Suppose \( \frac{r!}{q^d} \geq \frac{r^N}{r^{k_1-1}}(1 + e^{-1/2})^{r} \), then there exists a polynomial of \( F_q[X] \) that permutes \( \mathcal{F} \), an \( F_q[X] \)-submodule of \( F_q \), with its coefficients of \( X^{k_i} \) equal to \( a_i \in F_q \), for \( i = 1, \ldots, d \) and \( 0 < k_1 < \cdots < k_d < N \), where \( r = r^n = |\mathcal{F}| \), \( q = r^\rho \) and \( \rho \) 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 \cite{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 \( F_q \), 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 \( \mu_N \). We define the polynomial

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

(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

\[
N_q(\mathbf{k}, \mathbf{a}) = \left| \left\{ \sigma \in S(\mu_N) \mid \sum_{c \in \mu_N} c^{-k_i} \sigma(c) = a_i, \forall 1 \leq i \leq d \right\} \right|,
\]

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 \( f_\sigma \) 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

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

For any \( S \subseteq \mu_N \), define the sets

\[
A_S = \left\{ f : \mu_N \to S \mid \sum_{c \in \mu_N} c^{-k_i} f(c) = Na_i, \forall 1 \leq i \leq d \right\},
\]

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

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

\[
B(M) = \sum_{T \subseteq M} (-1)^{|M|-|T|} A(T).
\]

For \( M = \mu_N \), the above implies

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

Recall that \( q = p^t \). Set \( e_p(u) := e^{2\pi i u/p} \) and \( \text{Tr}(x) \) the absolute trace of \( x \in \mathbb{F}_q \), i.e. \( \text{Tr}(x) := x + x^p + \cdots + x^{p^{t-1}} \) for \( x \in \mathbb{F}_q \). Further, let \( q \) be the smallest power of \( p \) such that \( N \mid q - 1 \), i.e. \( \mathbb{F}_q \) is the smallest subfield of \( \mathbb{F}_q \) containing \( \mu_N \). If
$S \subseteq \mu_N$, then
\[
A(S) = \frac{1}{q^d} \sum_{(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d} \sum_{f: \mu_N \to S} e_p \left( \frac{\text{Tr} \left( \sum_{i=1}^d \alpha_i \left( -Na_i + \sum_{c \in \mu_N} c^{-k_i} f(c) \right) \right)}{1} \right)
\]
\[
= \frac{1}{q^d} \sum_{(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d} \sum_{f: \mu_N \to S} e_p \left( \frac{\text{Tr} \left( f(c) \sum_{i=1}^d \alpha_i c^{-k_i} \right)}{1} \right)
\]
\[
= \frac{1}{q^d} \sum_{(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d} \prod_{c \in \mu_N} \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right)
\]
\[
= \frac{|S|^N}{q^d} + R_S,
\]
where
\[
|R_S| \leq \frac{q^d - 1}{q^d} \max_{(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d \setminus \{0\}} \left| \prod_{c \in \mu_N} \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right) \right|
\]
\[
= \frac{q^d - 1}{q^d} \max_{(\alpha_1, \ldots, \alpha_d) \in \mathbb{F}_q^d \setminus \{0\}} \prod_{c \in \mu_N} \left| \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right) \right|.
\]
Moreover, the AM-GM inequality implies
\[
\prod_{c \in \mu_N} \left| \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right) \right| \leq \left( \frac{1}{N} \sum_{c \in \mu_N} \left| \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right) \right| \right)^{2/N}
\]
\[
\leq \left( \frac{1}{N} \sum_{c \in \mathbb{F}_q^d} \left| \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{N-k_i} \right) \right) \right| \right)^{2/N}
\]
\[
\leq \left( \frac{1}{N} \sum_{u \in \mathbb{F}_q} (N - k_1) \left| \sum_{t \in S} e_p(\text{Tr}(tu)) \right| \right)^{2/N}.
\]
With the help of the well-known identity, see [9, Chapter 3],
\[
\sum_{u \in \mathbb{F}_q} \left| \sum_{t \in S} e_p(\text{Tr}(tu)) \right|^2 = q|S|,
\]
we eventually get that
\[
\prod_{c \in \mu_N} \left| \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{i=1}^d \alpha_i c^{-k_i} \right) \right) \right| \leq \left( \frac{(q-1)(N-k_1)|S|}{N} \right)^{N/2},
\]
which implies
\[
|R_S| \leq \frac{q^d - 1}{q^d} \left( \frac{(q-1)(N-k_1)|S|}{N} \right)^{N/2} < \left( \frac{(q-1)(N-k_1)|S|}{N} \right)^{N/2}. \quad (6)
\]

By working similarly as in Eq. (2), but by considering the mappings \( \mu_N \rightarrow \mu_N \), 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 \( j \leq N e^{j/N - 1} \), since \( 1 + x \leq e^x \) for all \( x \), we get
\[
N_q(k, a) - \frac{N!}{q^d} < \left( \frac{(q-1)(N-k_1)}{N} \right)^{N/2} \sum_{j=0}^{N} \binom{N}{j} j^{N/2} \leq \left( \frac{(q-1)(N-k_1)}{N} \right)^{N/2} \sum_{j=0}^{N} \binom{N}{j} (N e^{j/N - 1})^{N/2} = [(q-1)(N-k_1)]^{N/2} \sum_{j=0}^{N} \binom{N}{j} (e^{-1/2})^{N-j} = [(q-1)(N-k_1)]^{N/2}(1 + e^{-1/2})^N.
\]

Summing up, we have proved that
\[
N_q(k, a) > \frac{N!}{q^d} - [(q-1)(N-k_1)]^{N/2}(1 + e^{-1/2})^N,
\]
which implies the Theorem 1.2.

If we apply this result in the case \( k_b = N - 1, k_b-1 = N - 1 - 1, \ldots, k_1 = N - b \) 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**
\[
\sqrt[N!/q^d]{b(q-1)(1 + e^{-1/2})},
\]
**then there exists a polynomial of \( \mathbb{F}_q \) of degree less than \( N - b \) that permutes \( \mu_N \).**

### 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 \( r := |\mathcal{F}| = r^m \leq q \). 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 $f \in \mathbb{F}_q[X]$, of degree $n$, with $f | X^m - 1$, 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 $f | X^m - 1$. Now, for $\sigma \in S(\mathcal{F})$ a permutation of $\mathcal{F}$, we define

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

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

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

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

From (7), we deduce that the $j$-th coefficient of $f_\sigma$ 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

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

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

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

$$B_S = \{ g \in A_S \mid g \text{ is surjective} \},$$

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

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

(8)

Furthermore, let $\rho$ be the order of $f$, i.e. $\rho$ is minimal such that $f | X^\rho - 1$ and let $q := r^\rho$. It follows that $\mathbb{F}_q$ is the smallest subfield of $\mathbb{F}_q$ containing $\mathcal{F}$.
that, in turn, yields

\[ \sum_{c \in F} \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r-1} - k_i \right) \right) \]

Also, the AM-GM inequality yields

\[ \prod_{c \in F} \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r-1} - k_i \right) \right) \]

where

\[ |R_S| \leq \frac{q^d - 1}{q^d} \prod_{(a_1, \ldots, a_d) \in F^d \setminus \{0\}} \sum_{t \in S} e_p \left( \text{Tr} \left( t \sum_{j=1}^d \sum_{i=0}^n \alpha_j F_{ij} c^{r-1} - k_i \right) \right) \]

That, in turn, yields

\[ |R_S| \leq \frac{q^d - 1}{q^d} \left( q \left( 1 - \frac{k_1 + 1}{r} \right) |S| \right)^{\tau/2} \leq \left( q \left( 1 - \frac{k_1 + 1}{r} \right) |S| \right)^{\tau/2} \]
Now, as in the case of the roots of unity, it is clear that

\[ \sum_{S \subseteq F} (-1)^{|S|} r^{|S|} = r!, \]

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

\[ \left| N_q(k, a) - \frac{r!}{q^d} \right| < q^{r/2} \left( 1 - \frac{k_1 + 1}{r} \right)^{r/2} \sum_{j=0}^{r} \binom{r}{j} j^{r/2} \]
\[ \leq q^{r/2} \left( 1 - \frac{k_1 + 1}{r} \right)^{r/2} \sum_{j=0}^{r} \binom{r}{j} \left( r e^{j/r - 1} \right)^{r/2} \]
\[ = q^{r/2} (r - k_1 - 1)^{r/2} (1 + e^{-1/2})^{r}. \]

To sum up, in this section we proved that

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

which implies Theorem 1.3.

By applying this for \( k_b = r - 1, k_{b-1} = r - 1 - 1, \ldots, k_1 = r - b \) 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

\[ \sqrt{q^{r/2}} \geq \sqrt{q(b-1)}(1 + e^{-1/2}), \]

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

**Aknowledgments**

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

**References**


