Finite Fields and Their Applications 47 (2017) 85–93

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Enumerating permutation polynomials

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

Department of Mathematics and Applied Mathematics, University of Crete, 70013 Heraklion, Greece

ARTICLE INFO

Article history:
Received 12 February 2016
Received in revised form 9 December 2016
Accepted 3 June 2017
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
11T06
11T23

Keywords:
Finite fields
Permutation polynomials

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 Konyagin and Pappalardi (2006) [8]. As a consequence, we prove conditions that ensure the existence of low-degree permutation polynomials of the mentioned substructures of $\mathbb{F}_q$.

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

* Corresponding author.
E-mail addresses: tgaref@uoc.gr (T. Garefalakis), gnkapet@gmail.com (G. Kapetanakis).
[1] Fax: +30 2810 393881.

http://dx.doi.org/10.1016/j.ffa.2017.06.007
1071-5797/

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].

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 analogies 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.