Finite Fields and Their Applications 34 (2015) 139–152

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On coefficient constraints and evaluation restrictions for linearized polynomials

Giacomo Micheli [1]

Institut für Mathematik Universität Zürich, Switzerland

ARTICLE INFO

Article history:
Received 30 April 2014
Accepted 2 February 2015
Available online 20 February 2015
Communicated by S. Gao

MSC:
11T06
15A03

Keywords:
Linearized polynomials
Module theory
Linear algebra

ABSTRACT

We provide an elementary approach to compute the monoid structure of q-linearized subfield preserving polynomials having coefficients in a subfield $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$. Additionally, we derive generalizations for some classical results by Brawley, Carlitz and Vaughan, of which we provide simpler proofs.

1. Introduction

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^m}$ be an extension of degree m. We say that $f \in \mathbb{F}_{q^m}[x]/(x^{q^m} - x)$ is a *permutation polynomial* if the induced application from $\mathbb{F}_{q^m}$ to itself is a bijection. As is well known (see for example [6]) the set of all permutation polynomials over $\mathbb{F}_{q^m}$ endowed with *composition of maps* as operation is isomorphic to the symmetric group S_{q^m}, since to every permutation of the elements of the field cor-

E-mail address: giacomo.micheli@math.uzh.ch.

[1] The author was supported in part by Swiss National Science Foundation grant number 149716 and *Armasuisse*.

http://dx.doi.org/10.1016/j.ffa.2015.02.001

responds (due to Lagrange interpolation) exactly one polynomial in $\mathbb{F}_{q^m}[x]/(x^{q^m} - x)$. In [3], Carlitz and Hayes asked which is the structure of the group consisting of all permutations of $\mathbb{F}_{q^m}$ such that their corresponding polynomials have coefficients over $\mathbb{F}_q$. This is indeed a subgroup of the monoid $\big(\mathbb{F}_q[x]/(x^{q^m} - x), \circ\big)$ that is canonically embedded in $\big(\mathbb{F}_{q^m}[x]/(x^{q^m} - x), \circ\big)$. We now observe that, if f is a permutation polynomial having coefficients over a subfield $\mathbb{F}_q$, then it *splits* all the intermediate extensions between $\mathbb{F}_q$ and the whole field $\mathbb{F}_{q^m}$ in the following sense:

$$\forall i, j | m \quad f(\mathbb{F}_{q^i} \setminus \mathbb{F}_{q^j}) = \mathbb{F}_{q^i} \setminus \mathbb{F}_{q^j}$$

and

$$f(\mathbb{F}_q) = \mathbb{F}_q.$$

If we now drop the equality condition and ask for all the $f \in \mathbb{F}_q[x]/(x^{q^m} - x)$ (not necessarily bijective) such that

$$\forall i, j | m \quad f(\mathbb{F}_{q^i} \setminus \mathbb{F}_{q^j}) \subseteq \mathbb{F}_{q^i} \setminus \mathbb{F}_{q^j}$$

($f(\mathbb{F}_q) \subseteq \mathbb{F}_q$ becomes obvious) we obtain the monoid of *canonical subfield preserving polynomials* (with parameters q and m) that has already been studied in [7] (although in the present paper no results form [7] are needed). A nice property of this new setting is that the subgroup of invertible elements of the monoid of canonical subfield preserving polynomials consists exactly of the permutation polynomials having coefficients over the subfield $\mathbb{F}_q$. As a corollary, once we know the monoid structure of this set [7], we get the results presented in [3] very easily, by working in the general context of subfield preserving polynomials.

The study of linear maps over finite fields is of great interest in cryptography (see e.g. [8,1]) and coding theory (see e.g. [5,4]). The group structure of q-linear permutation polynomials of $\mathbb{F}_{q^m}$ having coefficients over the subfield $\mathbb{F}_{q^d}$ is provided in [2]. It is then natural to ask which is the monoid structure of q-linear canonical (of parameters (q^d, m)) subfield preserving polynomials. In the present paper, in order to establish this monoid structure, we will use techniques from group and semigroup theory, linear algebra, commutative and noncommutative ring theory and module theory. Indeed, our purpose is not only to get new results, but also to show that classical finite field theoretic propositions can be easily obtained by using more general frameworks (as it happens for example in the case of Theorem 13, in comparison with the same result in [9, Theorem 3.8] and [9, Theorem 3.1]).

It follows a brief outline of the paper. In Section 2 definitions and notations are given. In Section 3 we prove some preliminary linear algebra propositions. In Section 4 some monoid and group structures relative to restrictions of coefficients to some intermediate extensions between $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ are provided.