Finite Fields and Their Applications 34 (2015) 36–44

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Roots and coefficients of multivariate polynomials over finite fields

Olav Geil

Department of Mathematical Sciences, Aalborg University, Denmark

ARTICLE INFO

Article history:
Received 7 October 2014
Received in revised form 3 January 2015
Accepted 10 January 2015
Available online 28 January 2015
Communicated by Rudolf Lidl

MSC:
11T06

Keywords:
Coefficient
Finite field
Multivariate polynomial
Root

ABSTRACT

Kopparty and Wang studied in [3] the relation between the roots of a univariate polynomial over $\mathbb{F}_q$ and the zero–nonzero pattern of its coefficients. We generalize their results to polynomials in more variables.

1. Introduction

In [3] Kopparty and Wang considered the zero–nonzero pattern of a univariate polynomial $P(X)$ over $\mathbb{F}_q$ and its relation to the number of roots in $\mathbb{F}_q^*$. Their main theorem [3, Theorem 1] states that a polynomial with many zeros cannot have long sequences of consecutive coefficients all being equal to zero. Then in [3, Theorem 2] they gave necessary and sufficient conditions for a product of pairwise different linear factors to

E-mail address: olav@math.aau.dk.

http://dx.doi.org/10.1016/j.ffa.2015.01.001
1071-5797/

have sequences of zero coefficients of maximal possible length for any polynomial with prescribed number of roots. In this note we generalize the above mentioned results to polynomials in more variables.

In Section 2 we start by recalling the results by Kopparty and Wang. In Section 3 we then present and prove the generalizations.[1]

2. Univariate polynomials

The main theorem in [3] is their Theorem 1 which we present in a slightly stronger version.

Theorem 1. *Let $P(X) \in \mathbb{F}_q[X]$ be a nonzero polynomial of degree at most $q-2$, say $P(X) = \sum_{i=0}^{q-2} b_i X^i$. Let m be the number of $x \in \mathbb{F}_q^*$ with $P(x) \neq 0$. Then there does not exist any $k \in \{0, \ldots, q-2\}$ where all the m coefficients b_k, $b_{k+1 \text{ rem}(q-1)}, \ldots, b_{k+m-1 \text{ rem}(q-1)}$ are zero.*

The modification made in Theorem 1 is that we consider $k \in \{0, \ldots, q-2\}$ rather than just $k \in \{0, \ldots, q-1-m\}$. The proof in [3] is easily modified to cover this more general situation. Alternatively, one can deduce it by writing $P(X) = X^s Q(X)$ with s maximal and then applying [3, Theorem 1] to $Q(X)$.

Obviously, if we consider a product of $q-1-m$ pairwise different linear factors $X-x$ with $x \neq 0$, this polynomial has exactly m non-roots in $\mathbb{F}_q^*$ and we have $b_{q-m} = \cdots = b_{q-2} = 0$ which is a sequence of $m-1$ consecutive zero coefficients modulo $q-1$. The below theorem, corresponding to [3, Theorem 2], gives sufficient and necessary conditions for a sub-sequence of $m-1$ consecutive zeros among $b_0, \ldots, b_{q-m-2}$ to exist.

Theorem 2. *Let S be a subset of $\mathbb{F}_q^*$ of size $q-1-m$, where $m \geq 2$ and consider*

$$P(X) = \prod_{a \in S} (X-a) = \sum_{i=0}^{q-1-m} b_i X^i. \tag{1}$$

There exists a $k \in \{1, \ldots, q-2m\}$ such that $b_k = \cdots = b_{k+m-2} = 0$ if and only if $\mathbb{F}_q^* \backslash S$ is contained in γH for some $\gamma \in \mathbb{F}_q^*$ and for some proper multiplicative subgroup H of $\mathbb{F}_q^*$.

Inspecting the proof in [3] one sees that for polynomials of the form (1) the existence of one sub-sequence of $m-1$ consecutive zero coefficients in $b_0, \ldots, b_{|S|-1}$ is equivalent to the existence of $(q-1)/|H|$ such disjoint sequences.

[1] Throughout this note we shall use the notation $F(\vec{X}) \text{ rem}(G_1(\vec{X}), \ldots, G_w(\vec{X}))$ for the remainder of the polynomial $F(\vec{X})$ after division with the ordered set of polynomials $(G_1(\vec{X}), \ldots, G_w(\vec{X}))$. The remainder in general depends on the monomial ordering under consideration. For the cases that we consider, however, the choice of monomial ordering is of no significance.