Roots and coefficients of polynomials over finite fields\textsuperscript{\dag}

Swastik Kopparty\textsuperscript{a}, Qiang Wang\textsuperscript{b,}\textsuperscript{*}

\textsuperscript{a}Department of Mathematics & Department of Computer Science, Rutgers University.
\textsuperscript{b}School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada

Abstract

In this note, we give a short proof of a result of Muratović-Ribić and Wang on the relation between the the coefficients of a polynomial over a finite field $\mathbb{F}_q$ and the number of fixed points of the mapping on $\mathbb{F}_q$ induced by that polynomial.

Keywords: finite fields, polynomials, coefficients

MSC: 11T06

Our main theorem relates the roots of a univariate polynomial over $\mathbb{F}_q$ and zero-nonzero pattern of its coefficients. We give a short proof of this theorem using an idea from [1] (see Lemma 3.10 there, which talks about the zero-nonzero patterns of the coefficients of subspace polynomials). The main theorem then easily implies Theorem 1 of [2].

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

Proof. Suppose that for some $k \in \{0,1,\ldots,q-1-m\}$ we have

$$b_k = b_{k+1} = \ldots = b_{k+m-1} = 0.$$ 

Consider the polynomial

$$Q(X) = X^{q-1-(m+k)} \cdot P(X) \mod (X^{q-1} - 1),$$

Observe that the number of roots of $Q(X)$ in $\mathbb{F}_q^*$ equals the number of roots of $P(X)$ in $\mathbb{F}_q^*$, which equals $q - 1 - m$.

\textsuperscript{\dag}Swastik Kopparty’s research is partially supported by a Sloan Fellowship and NSF CCF-1253886. Qiang Wang’s research is partially supported by NSERC of Canada. We would like to thank RICAM, in particular, Arne Winterhof and Annette Weihs, for the warm hospitality and help.

\textsuperscript{*}Corresponding author.

Email addresses: swastik.kopparty@rutgers.edu (Swastik Kopparty), wang@math.carleton.ca (Qiang Wang)
On the other hand, observe that the coefficient vector of \( Q \) is obtained by a cyclic rotation of the coefficient vector of \( P \). In fact, this cyclic rotation moves the interval of zero coefficients of \( P \) to the highest degree monomials: \( X^{q-1-m}, X^{q-m}, \ldots, X^{q-1} \). Therefore \( Q(X) \) is a nonzero polynomial of degree at most \( q - 2 - m \).

But \( Q(X) \) has exactly \( q - 1 - m \) roots in \( \mathbb{F}_q^* \). This is a contradiction, and the theorem follows.

**Corollary 1 ([2]).** Let \( F(X) = \sum_{i=0}^{q-1} a_i X^i \) be a polynomial over \( \mathbb{F}_q \) of degree \( \leq q - 1 \). Let \( T = \{ x \in \mathbb{F}_q^* \mid F(x) \neq x \} \) be the set of nonzero moved elements. Suppose \( |T| = m \). Then for every \( k \), \( 1 \leq k \leq q - 2 - m \), at least one of the \( m \) consecutive coefficients \( a_{k+1}, a_{k+2}, \ldots, a_{k+m} \) is nonzero.

Moreover, if \( F(0) = 0 \) then it is also true for \( k = 0 \) and \( k = q - 1 - m \).

**Proof.** If \( F(X) = X \mod (X^{q-1} - 1) \), then the result is trivial, and so we assume that this is not the case.

Let \( P(X) = (F(X) - X) \mod (X^{q-1} - 1) \) (thus \( P(X) \) is a nonzero polynomial of degree \( < q - 1 \)). Note that for \( x \in \mathbb{F}_q^* \), we have \( P(x) \neq 0 \) if and only if \( F(x) \neq x \). Thus \( T = \{ x \in \mathbb{F}_q^* \mid P(x) \neq 0 \} \).

If we write \( P(X) = \sum_{i=0}^{q-2} b_i X^i \), then we have \( b_0 = a_{q-1} + a_0, b_1 = a_1 - 1, \) and \( b_i = a_i \) for each \( i \in \{2, 3, \ldots, q - 2\} \).

By Theorem 1, for every \( k \) with \( 1 \leq k \leq q - 1 - m \), we have that one of the coefficients \( b_k, b_{k+1}, \ldots, b_{k+m-1} \) is nonzero. This implies that for every \( k, 1 \leq k \leq q - 2 - m \), at least one of the \( m \) consecutive coefficients \( a_{k+1}, a_{k+2}, \ldots, a_{k+m} \) is nonzero.

Moreover, if \( F(0) = 0 \) then \( F(X) = XF'(X) \) where \( F'(X) = \sum_{i=1}^{q-1} a_i X^{i-1} \) is a nonzero polynomial of degree at most \( q - 2 \). Let \( P'(X) = F'(X) - 1 \). Then the number of nonzero \( X \in \mathbb{F}_q^* \) such that \( P'(X) \neq 0 \) is equal to \( m = |T| \). By Theorem 1, for every \( k \in \{1, \ldots, q - m\} \), one of the \( m \) coefficients \( a_k, \ldots, a_{k+m-1} \) is nonzero. In particular, at least one of \( m \) coefficients \( a_1, \ldots, a_m \) is nonzero, as well as one of \( m \) coefficients \( a_{q-m}, a_{q-m+1}, \ldots, a_{q-1} \).

We remark that Corollary 1 is stated in terms of the number of nonzero moved elements, which is equivalent to Theorem 1 in [2] that was first stated in terms of number of moved elements.

We now point out a variation of the argument of Theorem 1 which shows that the zero-nonzero pattern of the coefficients of splitting polynomials is sensitive to the presence of multiplicative subgroups in \( \mathbb{F}_q^* \). This is analogous to Lemma 3.10 of [1], which shows that the zero-nonzero pattern of the coefficients of subspace polynomials is sensitive to the presence of subfields of \( \mathbb{F}_{p^n}^* \).

Theorem 1 states that polynomials with \( q - 1 - m \) roots in \( \mathbb{F}_q^* \) cannot have \( m \) consecutive 0 coefficients. Theorem 2 states that a polynomial of degree \( q - 1 - m \) with \( q - 1 - m \) roots in \( \mathbb{F}_q^* \) cannot have \( m - 1 \) consecutive 0 coefficients unless the set of roots has a special property (it should contain the complement of some coset of a multiplicative subgroup).
Theorem 2. Let $S$ be a subset of $\mathbb{F}_q^*$ with size $q - 1 - m$ with $m \geq 2$ and

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

Then $P(X)$ has an interval of at least $m - 1$ consecutive zero coefficients (i.e., exists $1 \leq k \leq q - 2m$ such that $b_k = \cdots = b_{k+m-2} = 0$) if and only if $\mathbb{F}_q^* \setminus S$ is contained in $\gamma H$, for some $\gamma \in \mathbb{F}_q^*$ and some proper multiplicative subgroup $H$ of $\mathbb{F}_q^*$.

Proof. Suppose there exists an interval of $m - 1$ successive zero coefficients $b_k = \cdots = b_{k+m-2} = 0$. Define $Q(X) = X^{q-k-m} \cdot P(X) \mod (X^{q-1} - 1)$. Using our hypothesis, it is easy to see that $Q(X)$ is a nonzero polynomial of degree at most $q - 1 - m$.

Observe that $\{x \in \mathbb{F}_q^* \mid Q(x) = 0\} = \{x \in \mathbb{F}_q^* \mid P(x) = 0\} = S$, which has size $q - 1 - m$. Thus the degree of $Q(X)$ must exactly equal $q - 1 - m$, and so $Q(X) = \alpha \cdot \prod_{a \in S} (X - a) = \alpha \cdot P(X)$ for some $\alpha \in \mathbb{F}_q^*$.

This implies that $\alpha \cdot P(X) = Q(X)$. Going back to the definitions, this means that $P(X) \cdot (X^{q-k-m} - \alpha) = 0 \mod (X^{q-1} - 1)$.

We know that $P(X)$ vanishes only on the set $S$; thus every element of $\mathbb{F}_q^* \setminus S$ is a root of $(X^{q-k-m} - \alpha)$. Let $\gamma \in \mathbb{F}_q^* \setminus S$. Let $H$ equal the subgroup $\{x \in \mathbb{F}_q^* \mid x^{q-k-m} = 1\}$, and note that it is a proper subset of $\mathbb{F}_q^*$ (since $q - k - m < q - 1$). Then $\mathbb{F}_q^* \setminus S$ is contained in $\gamma H$, as required.

For the reverse direction, suppose $|H| = d$. Then $d \mid (q - 1)$ and $\gamma H = \{x \in \mathbb{F}_q^* \mid x^d = \gamma^d\}$.

We first consider the case $S = \mathbb{F}_q^* \setminus \gamma H$. Then we have $\prod_{a \in S} (X - a) = \frac{X^{q-1} - 1}{X^d - \gamma^d}$, which is of the form $\sum_{j=1}^{(q-1)/d} b_j X^{(q-1) - jd}$. This proves the result for $S = \mathbb{F}_q^* \setminus \gamma H$.

For general $S \supseteq \mathbb{F}_q^* \setminus \gamma H$, write $S = (\mathbb{F}_q^* \setminus \gamma H) \cup T$. In this case, $d = m + |T|$. Then we have

$$\prod_{a \in S} (X - a) = \prod_{a \in \mathbb{F}_q^* \setminus \gamma H} (X - a) \cdot \prod_{a \in T} (X - a)$$

$$= \left(\sum_{j=1}^{(q-1)/d} b_j X^{(q-1) - jd}\right) \cdot U(X),$$

where $U(X)$ is a polynomial of degree $|T|$. This implies the result for general $S \supseteq \mathbb{F}_q^* \setminus \gamma H$. 

We note that the nonzero coefficients of $P(x)$ satisfying Theorem 2 must meet the condition $b_{i+q-k-m} \mod (q-1) = \alpha b_i$ for some $\alpha \in \mathbb{F}_q^*$.

\footnote{Note that by Theorem 1, $P(X)$ has an interval of at least $m - 1$ consecutive zero coefficients if and only if it has an interval of exactly $m - 1$ consecutive zero coefficients.}
References
