On coefficients of polynomials over finite fields[☆]

Amela Muratović-Ribić[a], Qiang Wang[b,*]

[a] *University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina*
[b] *School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada*

Abstract

In this paper we study the relation between coefficients of a polynomial over finite field $\mathbb{F}_q$ and the moved elements by the mapping that induces the polynomial. The relation is established by a special system of linear equations. Using this relation we give the lower bound on the number of nonzero coefficients of polynomial that depends on the number m of moved elements. Moreover we show that there exist permutation polynomials of special form that achieve this bound when $m \mid q-1$. In the other direction, we show that if the number of moved elements is small then there is an recurrence relation among these coefficients. Using these recurrence relations, we improve the lower bound of nonzero coefficients when $m \nmid q-1$ and $m \leq \frac{q-1}{2}$. As a byproduct, we show that the moved elements must satisfy certain polynomial equations if the mapping induces a polynomial such that there are only two nonzero coefficients out of $2m$ consecutive coefficients. Finally we provide an algorithm to compute the coefficients of the polynomial induced by a given mapping with $\mathcal{O}(q^{3/2})$ operations.

Keywords: finite fields, polynomials, coefficients, algorithm
MSC: 11T06; 12Y05

1. Introduction

Let p be a prime, n be a positive integer, and $q = p^n$. Let $\mathbb{F}_q$ denotes a finite field of order q. Computing coefficients of a polynomial over finite field $\mathbb{F}_q$ efficiently is an important question in practice. It is for the purpose of computational efficiency that one would prefer polynomials with small number of nonzero coefficients in applications in cryptography or coding theory. In [15], G. L. Mullen posed the problem of computing the coefficients of the inverse polynomial of a permutation polynomial efficiently (Problem 10). This motivated Muratović-Ribić [17] to characterize all the coefficients of the inverse polynomial of a permutation polynomial of the form $x^r f(x^s)^{(q-1)/s}$. Later on, the result was extended to arbitrary permutation polynomial by Wang [21]. Both results give formulas of coefficients of the inverse polynomials in terms of the images of the original permutation polynomials. On the other hand, for a permutation polynomial $f(x)$ itself, Mullen and Vioreanu [16] gave a formula to compute coefficients of $f(x)$ in terms of elements s of finite fields which are moved by the permutation polynomial $f(x)$ as a bijective mapping (i.e., $f(s) \neq s$), see also in [23], where the application of this formula in exploring the connection between the cycle structure of a permutation of $\mathbb{F}_q$ and the degree of the polynomial representing it is established.

[☆] Research of Qiang Wang was partially supported by NSERC of Canada
[*] Corresponding author
Email addresses: amela@pmf.unsa.ba (Amela Muratović-Ribić), wang@math.carleton.ca (Qiang Wang)

Some recent work in this direction can be found in [10] where an asymptotic formula is given for the number of permutations for which the associated permutation polynomial has d coefficients in specified fixed positions equal to 0. Other than permutation polynomials, coefficients of other special types of polynomials (e.g., irreducible polynomials, primitive polynomials, primitive normal polynomials) are also studied extensively recently. In this area, the goal is to study the distribution of these polynomials with prescribed coefficients (including the existence results and enumeration results on these polynomials). There are numerous papers on these topics, hence we can not include all the relevant references. Instead, we refer the readers to a small list to start, for example, [3], [4], [5], [6], [7], [13], [14], [18], [20], [24], [25]. In this paper we take a different direction. We study coefficients of arbitrary polynomials and characterize those polynomials with small number of nonzero coefficients over $\mathbb{F}_q$. We also provide an algorithm for calculating the coefficients of any polynomial with complexity $\mathcal{O}(q^{3/2})$ as a consequence of our results. We compare our algorithm with several other interpolation algorithms and it seems that our algorithm is simple and quite useful for small q's.

Let us consider any polynomial of degree at most $q-1$, not necessarily a permutation polynomial. Further in this paper we will assume that $\theta : \mathbb{F}_q \to \mathbb{F}_q$ is any given mapping (not necessarily bijective) such that $T = \{s \mid s \in \mathbb{F}_q, \theta(s) \neq s\} = \{s_1, s_2, \dots s_m\} \subseteq \mathbb{F}_q$. We will say that element $s \in \mathbb{F}_q$ is *moved* by θ if $\theta(s) \neq s$ and s is *fixed* otherwise. Because any mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be interpolated by a polynomial of degree at most $q-1$, we let $f(x)$ be the polynomial in $\mathbb{F}_q[x]$ of degree $\leq q-1$ induced by θ. In Section 2 we will give a formula for the coefficients a_k of x^k in $f(x)$ by using only the elements in the set T, namely,

$$\begin{cases} a_k = \displaystyle\sum_{s\in T} s^{q-1-k}(s-\theta(s)) + \delta_1^k, & k = 1, \dots, q-2, \\ a_0 + a_{q-1} = \displaystyle\sum_{s\in T} s^{q-1}(s-\theta(s)), \end{cases} \tag{1}$$

where δ_i^j is the Kronecker delta such that δ_i^j equals 1 if $i = j$ and 0 otherwise. This generalizes the result of Mullen and Vioreanu [16] who considered the case of permutation polynomials. Indeed, if $f(x)$ is a permutation polynomial of $\mathbb{F}_q$, then $a_{q-1} = 0$ and thus $a_k = \displaystyle\sum_{s\in T} s^{q-1-k}(s-\theta(s)) + \delta_1^k$ for $k = 0, 1, \dots q-2$.

Throughout the paper, we denote

$$a'_k = a_k, \quad 2 \leq k \leq q-2, a'_1 = a_1 - 1, \quad a'_{q-1} = a_0 + a_{q-1}.$$

Then a'_k's are coefficients of $f^*(x) = f(x) - x$ when $1 \leq k \leq q-2$. In particular, if $f(0) = 0$ (i.e., $0 \notin T$), then $a_0 = 0$ and $a'_{q-1} = a_{q-1}$. Therefore we have the following system of linear equations ($s - \theta(s)$ as variables):

$$\sum_{s\in T} s^{q-1-k}(s-\theta(s)) = a'_k, \ k = q-1, q-2, \dots, 1. \tag{2}$$

If $m \leq q-1$, we let $q-1 = mv + r$, where $0 \leq r < m$. We partition the coefficients a'_k into $v+1$ blocks as follows:

$$a'_{q-1}, a'_{q-2}, \dots, a'_{q-m};$$
$$a'_{q-m-1}, a'_{q-m-2}, \dots, a'_{q-2m};$$
$$\vdots$$

$$a'_{q-(v-1)m-1}, a'_{q-(v-1)m-2}, \ldots, a'_{q-vm};$$
$$a'_{q-vm-1}, \ldots, a'_1;$$

In each block of the first v blocks, there are m successive coefficients whose subscripts are in descending order. Further in the paper we will call these blocks *m-blocks*. The *first m-block* refers to the first row above and *second m-block* refers to the second row above, etc.

If $m < q-1$, then we can obtain a recurrence relation on these coefficient a'_k's by studying the consistent system. That is,

$$a'_{q-1-m-t} = r^{(t)}_{m-1}a'_{q-m} + \ldots + r^{(t)}_1 a'_{q-2} + r^{(t)}_0 a'_{q-1}$$

for $t = 0, 1, \ldots, q-1-m$, where $r^{(t)}_j$ are coefficients of x^j in the expansion of the polynomial $r^{(t)}(x) = x^{m+t} \pmod{P(x)}$ and $P(x) = \prod_{z=1}^{m}(x - s_z)$. We also show that these $r^{(t)}_j$ for different t's can be obtained recursively from $r^{(0)}_j, \ldots, r^{(0)}_{j-t}$ (note that $r^{(0)}_{j-t} = 0$ if $j < t$). These preliminary results and notations are given in Section 2.

On the other hand, without assumption of $f(0) = 0$ or $m \leq q-1$, by studying the general relation (1) we prove Theorem 1 in Section 3, which gives lower bounds of nonzero coefficients of a polynomial over $\mathbb{F}_q$.

Theorem 1. *Let $f(x)$ be the polynomial over $\mathbb{F}_q$ of degree $\leq q-1$ representing the mapping $\theta : \mathbb{F}_q \to \mathbb{F}_q$ which moves $m > 1$ elements of $\mathbb{F}_q$, i.e., $\mid T \mid = m$.*

(a) If 0 is a fixed point of θ, then there is no k, $1 \leq k \leq q-1-m$ such that the successive m coefficients $a_{k+1}, a_{k+2}, \ldots, a_{k+m}$ of the induced polynomial $f(x)$ are all equal to the zero. Moreover, there are at least $\frac{q-1}{m} - 1$ nonzero coefficients in $f(x)$ if $m \mid q-1$ and at least $\frac{q-1}{m}$ nonzero coefficients in $f(x)$ if $m \nmid q-1$.

(b) If 0 is not a fixed point of θ, then there is no k, $1 \leq k \leq q-1-m$ such that the successive $m-1$ coefficients $a_{k+1}, a_{k+2}, \ldots, a_{k+m-1}$ of the induced polynomial $f(x)$ are all equal to the zero. Moreover, there are least $\frac{q-1}{m-1} - 1$ nonzero coefficients a_k of $f(x)$ if $(m-1) \mid (q-1)$ and are least $\frac{q-1}{m-1}$ nonzero coefficients a_k of $f(x)$ if $m-1 \nmid q-1$.

In fact, the lower bound in Theorem 1 (a) can be achieved when $m \mid q-1$.

Theorem 2. *Let $m \mid q-1$ and let ψ be a primitive root of $x^m - 1 = 0$.*
(a) The polynomial $f(x)$ which moves m elements has $\frac{q-1}{m} - 1$ nonzero coefficients if and only if $f(x)$ is induced by a mapping θ which moves an m-subset $T = \{s, s\psi, s\psi^2, \ldots, s\psi^{m-1}\}$ $(s \neq 0)$ of $\mathbb{F}_q$ and defined by

$$\theta(s\psi^j) = (1 + m^{-1})s\psi^j, \quad j = 0, 1, \ldots, m-1.$$

(b) The polynomial $f(x)$ induced by mapping θ defined by $\theta(s\psi^j) = s\psi^{j+i}$ for some i on the set $T = \{s, s\psi, s\psi^2, \ldots, s\psi^{m-1}\}$ is a permutation polynomial with $\frac{q-1}{m}$ nonzero coefficients if $1 + m^{-1} \neq \psi^i$ and with $\frac{q-1}{m} - 1$ nonzero coefficients for $1 + m^{-1} = \psi^i$.

The proof of Theorem 2 and some lower bounds for the number of the special permutation polynomials of the degree $q - m$ where $m \mid q-1$ are given in Section 4. In Section 5 we provide an algorithm to compute the coefficients of the polynomial induced by a given mapping with $\mathcal{O}(q^{3/2})$ operations.

In the case $m \nmid q-1$ the lower bound for the number of coefficients in the Theorem 1 (a) can be improved :

Theorem 3. *Assume that* 0 *is fixed point of* θ *and* $m \nmid q-1$. *If there exist positive integers* d *and* k *such that* $m = kd$, $(k+1)d \mid q-1$, *and the moved elements by* θ *are solutions of the equation* $\frac{x^{(k+1)d}-(-b)^{k+1}}{x^d+b} = 0$ *for some* $b \in \mathbb{F}_q^*$, *then the number of the nonzero coefficients of* $f(x)$ *is at least*

$$2\frac{q-1}{(k+1)d} - 1.$$

Otherwise, the number of the nonzero coefficients in $f(x)$ *is at least* $\lfloor \frac{3}{2} \lfloor \frac{q-1}{m} \rfloor \rfloor$.

Note that in some cases $2\frac{q-1}{(k+1)d} - 1 < \lfloor \frac{3}{2} \lfloor \frac{q-1}{kd} \rfloor \rfloor$, for example for $k = 2$.

It requires that we study polynomials which has only two nonzero coefficients in consecutive two m-blocks (Lemmas 7, 8). These two lemmas and Theorem 3 are proved in Section 6. We remark that Lemma 4 (for $m \mid q-1$) and Lemmas 7, 8 (for $m \nmid q-1$) together give the results on coefficients of polynomials which has only two nonzero coefficients in consecutive two m-blocks. Namely, if the set of moved elements by the polynomial $f(x) = \sum_{k=0}^{q-1} a_k x^k$ with $f(0) = 0$ has size m and the coefficients a'_k of the polynomial $f(x) - x = \sum_{k=1}^{q-1} a'_k x^k$ satisfy that there is only one nonzero coefficient among the m coefficients $a'_{q-um-1}, \ldots, a'_{q-(u+1)m}$ and one nonzero coefficient among the second m coefficients $a'_{q-(u+1)m-1}, \ldots, a'_{q-(u+2)m}$, then these moved elements satisfy certain polynomial equations in Lemma 4 or Lemma 7 and therefore lower bounds of the number of coefficients a'_k can be obtained. These results are interesting by themselves and may have other potential applications.

2. Preliminary results

A polynomial $f(x)$ induced by θ is given by

$$f(x) = x - \left(\sum_{s \in T} (s - \theta(s)) \frac{x^q - x}{x - s} \right). \tag{3}$$

Indeed, if $x \notin T = \{s \mid s \in \mathbb{F}_q, \theta(s) \neq s\}$, then $\theta(x) = x$ and $f(x) = x_0 - \left(\sum_{s \in T} (s - \theta(s)) \frac{x^q - x}{x - s} \right) = x = \theta(x)$. Otherwise, $x = s_0$ for some $s_0 \in T$. Then $f(s_0) = s_0 - \left(\sum_{s \in T} (s - \theta(s)) \frac{s_0^q - s_0}{s_0 - s} \right) = s_0 - \left(\sum_{s \in T, s \neq s_0} (s - \theta(s)) \frac{s_0^q - s_0}{s_0 - s} \right) - (s_0 - \theta(s_0)) = \theta(s_0)$. However, we can obtain a formula to compute coefficients a_k of $f(x)$ in terms of moved elements by θ only.

Lemma 1. *Let* $f(x)$ *be the polynomial over* $\mathbb{F}_q$ *of degree* $\leq q-1$ *representing the mapping* $\theta : \mathbb{F}_q \to \mathbb{F}_q$ *which moves* $m \geq 1$ *elements of* $\mathbb{F}_q$, *i.e.,* $\mid T \mid = m$, *where* $T = \{s \mid s \in \mathbb{F}_q, \theta(s) \neq s\}$. *Then coefficients of the polynomial* $f(x)$ *are given by*

$$\begin{cases} a_k = \sum_{s \in T} s^{q-1-k}(s - \theta(s)) + \delta_1^k, & k = 1, \ldots, q-2, \\ a_0 + a_{q-1} = \sum_{s \in T} s^{q-1}(s - \theta(s)), \end{cases}$$

where δ_i^j *is the Kronecker delta satisfying that* $\delta_i^j = 1$ *if* $i = j$ *and* 0 *otherwise. Trivially, if* $T = \emptyset$ *then* $f(x) = x$.

Proof. Let $f(x) = \sum_{k=0}^{q-1} a_k x^k$. Then it is well known that $a_j = -\sum_{s\in\mathbb{F}_q} s^{q-1-j}\theta(s)$ for $1 \le j \le q-2$ and $a_0 + a_{q-1} = -\sum_{s\in\mathbb{F}_q} s^{q-1}\theta(s)$ (e.g., [16]). By [11, Lemma 7.3], we have $\delta_t^{q-1} + \sum_{s\in\mathbb{F}_q} s^t = 0$. Hence the coefficients of $f(x)$ are given by

$$\begin{aligned} a_k &= -\sum_{s\in\mathbb{F}_q} s^{q-1-k}\theta(s) = \delta_{q-k}^{q-1} + \sum_{s\in\mathbb{F}_q} s^{q-k} - \sum_{s\in\mathbb{F}_q} s^{q-1-k}\theta(s) \\ &= \delta_1^k + \sum_{s\in T} s^{q-1-k}(s-\theta(s)) \qquad k = 1, 2, \ldots, q-2. \end{aligned}$$

Similarly, $a_0 + a_{q-1} = \sum_{s\in T} s^{q-1}(s-\theta(s))$. □

We remark that if $f(x)$ is a permutation polynomial, then $a_{q-1} = 0$ and thus $a_k = \sum_{s\in T} s^{q-1-k}(s - \theta(s)) + \delta_1^k$ for $k = 0, 1, \ldots q-2$. As an immediate consequence of Lemma 1 we have

Corollary 1. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}_q[x]$ induced by permutations α and β, respectively, which move disjoint sets of elements. Then the composition $\alpha\beta = \beta\alpha$ induce the polynomial $f(x)+g(x)-x$.*

Corollary 2. *If a mapping θ moves only elements of the subfield K of $\mathbb{F}$ to itself, i.e., $T \subseteq K$ and $\theta(T) \subseteq K$, then $f(x) \in K[x]$.*

In the following sections, we study these coefficients a_k's of $f(x) = \sum_{k=0}^{q-1} a_k x^k$. If we let

$$\begin{aligned} a'_k &= a_k, \quad 2 \le k \le q-2, \\ a'_1 &= a_1 - 1, \quad a'_{q-1} = a_0 + a_{q-1}. \end{aligned}$$

then it is enough to study a'_k's which are coefficients of $f^*(x) = f(x) - x$ for $1 \le k \le q-2$. In particular, if $f(0) = 0$ (i.e., $0 \notin T$), then $a_0 = 0$ and $a'_{q-1} = a_{q-1}$. Hence Equation (1) can be rewritten as

$$\sum_{s\in T} s^{q-1-k}(s-\theta(s)) = a'_k, \ k = q-1, q-2, \ldots, 1. \tag{4}$$

We note that Equation (4) gives a system of $q-1$ linear equations of m variables $\{s - \theta(s), s \in T\}$. Because $f(x)$ is induced by a given mapping θ, the system is consistent. Then we can obtain a recurrence relation on these coefficient a'_k's when $m < q-1$ using the following result on the system of linear equations such that the coefficients matrix is of Vandermonde type.

Lemma 2. *Let $s_1, s_2, \ldots, s_m$ be distinct elements of finite field $\mathbb{F}_q$, $P(x) = \prod_{z=1}^{m}(x - s_z)$, and $r_j^{(t)}$ be the coefficient of x^j in the expansion of the polynomial $r^{(t)}(x) = x^{m+t} \pmod{P(x)}$. Let $m < w$ and the system of linear equations $Vx = c$ be*

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_1 & s_2 & \ldots & s_m \\ s_1^2 & s_2^2 & \ldots & s_m^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^{w-1} & s_2^{w-1} & \ldots & s_m^{w-1} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{w-1} \end{bmatrix}.$$

If the system $Vx = c$ has a solution then
(a) $c_{m+t} = r_{m-1}^{(t)} c_{m-1} + \ldots + r_1^{(t)} c_1 + r_0^{(t)} c_0$ *for* $t = 0, 1, \ldots, w-m$*;*
(b) $c_{v+m+t} = r_{m-1}^{(t)} c_{v+m-1} + \ldots + r_0^{(t)} c_v$ *for all non-negative* $0 \le t \le m-1$ *and* $0 \le v \le w-m-t$*.*

Proof. (a) Because the coefficient matrix of the first m equations is a Vandermonde matrix and $s_1, \ldots, s_m$ are distinct, the first m equations together produce a unique solution. To analyze the whole system we need to find linear relation between first m rows of V and other rows of V because there are more equations than the number of variables.

Let $P(x) = \prod_{z=1}^{m}(x - s_z)$. The Euclidean algorithm implies that there are unique polynomials $q^{(t)}(x)$ and $r^{(t)}(x)$ for $(t \ge 0)$ such that $x^{m+t} = q^{(t)}(x)P(x) + r^{(t)}(x)$ where $\deg(r^{(t)}(x)) < m$.

As $s_i^{m+t} = q^{(t)}(s_i)P(s_i) + r^{(t)}(s_i) = r^{(t)}(s_i) = r_{m-1}^{(t)} s_i^{m-1} + \ldots + r_1^{(t)} s_i + r_0^{(t)}$, for $i = 1, 2, \ldots, m$, it follows that $(m+t)$-th row of V is a linear combination of first m rows with coefficients $r_j^{(t)}$, $j = 0, 1, \ldots, m-1$. Because the system $Vx = c$ is consistent, the constant terms must satisfy $c_{m+t} = r_{m-1}^{(t)} c_{m-1} + \ldots + r_1^{(t)} c_1 + r_0^{(t)} c_0$ for $t = 0, 1, \ldots w-m$ and thus (a) is proved.

(b) If $w \ge 2m$, then the linear dependence of the first $2m$ rows of the matrix V is given by

$$\begin{bmatrix} r_0^{(0)} & \cdots & r_{m-1}^{(0)} \\ \vdots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{m-1}^{(m-1)} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ s_1 & s_2 & \cdots & s_m \\ s_1^2 & s_2^2 & \cdots & s_m^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^{m-1} & s_2^{m-1} & \cdots & s_m^{m-1} \end{bmatrix} = \begin{bmatrix} s_1^m & \cdots & s_m^m \\ s_1^{m+1} & \cdots & s_m^{m+1} \\ \vdots & \vdots & \vdots \\ s_1^{2m-1} & \cdots & s_m^{2m-1} \end{bmatrix}.$$

Multiplying the above matrix equation from the righthand side by

$$\begin{bmatrix} s_1^v & 0 & 0 & \cdots & 0 \\ 0 & s_2^v & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & s_m^v \end{bmatrix},$$

where $0 \le v \le w-m$, the linear dependence of the successive rows remains the same, i.e.,

$$\begin{bmatrix} r_0^{(0)} & \cdots & r_{m-1}^{(0)} \\ \vdots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{m-1}^{(m-1)} \end{bmatrix} \begin{bmatrix} s_1^v & s_2^v & \cdots & s_m^v \\ s_1^{v+1} & s_2^{v+1} & \cdots & s_m^{v+1} \\ \vdots & \vdots & \vdots & \vdots \\ s_1^{m+v-1} & s_2^{m+v-1} & \cdots & s_m^{m+v-1} \end{bmatrix} = \begin{bmatrix} s_1^{m+v} & \cdots & s_m^{m+v} \\ s_1^{m+v+1} & \cdots & s_m^{m+v+1} \\ \vdots & \vdots & \vdots \\ s_1^{2m+v-1} & \cdots & s_m^{2m+v-1} \end{bmatrix}.$$

Because the system is consistent, the constant terms c_j must satisfy $c_{v+m+t} = r_{m-1}^{(t)} c_{v+m-1} + \cdots + r_0^{(t)} c_v$ for $0 \le t \le m-1$. If $w < 2m$, then the proof can be done similarly. □

So, if we let $w = q-1$ and $c_0 = a'_{q-1}, c_1 = a'_{q-2}, \ldots, c_{q-2} = a'_1$, where a'_k's are defined in the paragraph above Equation (2), then by Lemma 2 we have

$$a'_{q-1-m-t} = r_{m-1}^{(t)} a'_{q-m} + \ldots + r_1^{(t)} a'_{q-2} + r_0^{(t)} a'_{q-1} \tag{5}$$

for $t = 0, 1, \ldots q-1-m$, where $r_j^{(t)}$ are coefficients of the polynomial $r^{(t)}(x) = x^{m+t} \pmod{P(x)}$. Next we show that $r_j^{(t)}$ for different t's can be obtained recursively from $r_j^{(0)}, \ldots, r_{j-t}^{(0)}$ where $r_{j-t}^{(0)} = 0$ if $j < t$.

Lemma 3. *Let $s_1, s_2, \ldots, s_m$ be distinct elements of finite field $\mathbb{F}_q$, $P(x) = \prod_{z=1}^{m}(x - s_z)$, and $r_j^{(t)}$ be the coefficient of x^j in the expansion of the polynomial $r^{(t)}(x) = x^{m+t} \pmod{P(x)}$ for $t \geq 0$. Then*

(a) The coefficient $r_j^{(t)}$ satisfies the following recurrence relation

$$r_j^{(t+1)} = r_j^{(0)} r_{m-1}^{(t)} + r_{j-1}^{(t)}, \quad j = 0, 1, \ldots, m-1, \tag{6}$$

where $r_j^{(t)} = 0$ for $j < 0$.

(b) The coefficient $r_j^{(t)}$ also satisfies the following recurrence relation

$$r_j^{(t)} = r_j^{(0)} A_t + r_{j-1}^{(0)} A_{t-1} + \ldots + r_{j-t}^{(0)} A_0, \quad j = 0, 1, \ldots, k-1, \tag{7}$$

where the coefficients $A_t, \ldots, A_0$ are given by

$$A_0 = 1, \quad A_1 = r_{m-1}^{(0)}, \quad A_t = A_{t-1} r_{m-1}^{(0)} + A_{t-2} r_{m-2}^{(0)} + \ldots + A_{t-i} r_{m-i}^{(0)} + \ldots + A_0 r_{m-t}^{(0)}. \tag{8}$$

Proof. (a) Let $P(x) = \prod_{z=1}^{m}(x - s_z)$. The Euclidean algorithm implies that there are unique polynomials $q^{(t)}(x)$ and $r^{(t)}(x)$ for $(t \geq 0)$ such that $x^{m+t} = q^{(t)}(x)P(x) + r^{(t)}(x)$ where $\deg(r^{(t)}(x)) < m$. As $P(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ where $b_j = (-1)^{m-j}\sigma_{m-j}$ and σ_j's are elementary symmetric polynomials in $s_1, s_2, \ldots, s_m$, the coefficients of polynomial $r^{(0)}(x) = x^m - q^{(0)}(x)P(x) = x^m - P(x)$ are known. Let

$$r^{(t)}(x) = r_{m-1}^{(t)} x^{m-1} + r_{m-2}^{(t)} x^{m-2} + \ldots + r_1^{(t)} x + r_0^{(t)}.$$

Because

$$x^{m+t+1} = x x^{m+t} = x\left(q^{(t)}(x)P(x) + r^{(t)}(x)\right)$$

$$= x q^{(t)}(x)P(x) + (r_{m-1}^{(t)} x^m + r_{m-2}^{(t)} x^{m-1} + \ldots + r_0^{(t)} x)$$

$$= x q^{(t)}(x)P(x) + r_{m-1}^{(t)}\left(q^{(0)}(x)P(x) + r^{(0)}(x)\right) + r_{m-2}^{(t)} x^{m-1} + \ldots + r_0^{(t)} x =$$

$$\left(x q^{(t)}(x) + r_{m-1}^{(t)} q^{(0)}(x)\right) P(x) + r_{m-1}^{(t)}(r_{m-1}^{(0)} x^{m-1} + \ldots + r_0^{(0)}) + (r_{m-2}^{(t)} x^{m-1} + \ldots + r_0^{(t)} x),$$

the recurrence relation (6) is proved by comparing the remainders of $x^{m+t+1} = q^{(t+1)}(x)P(x) + r^{(t+1)}(x)$.

(b) We prove it inductively on t. For $t = 1$, we obtain $r_j^{(1)} = r_j^{(0)} r_{m-1}^{(0)} + r_{j-1}^{(0)}$ from (a). Hence the result is true for $t = 1$ as $A_0 = 1$ and $A_1 = r_{m-1}^{(0)}$. Assume that Equation (7) holds for t. Then using Equations (6) and (8) we have

$$r_j^{(t+1)} = r_j^{(0)} r_{m-1}^{(t)} + r_{j-1}^{(t)} =$$

$$r_j^{(0)}\left(r_{m-1}^{(0)} A_t + r_{m-2}^{(0)} A_{t-1} + \ldots + r_{m-t-1}^{(0)} A_0\right) + r_{j-1}^{(0)} A_t + r_{j-2}^{(0)} A_{t-1} + \ldots + r_{j-t-1}^{(0)} A_0.$$

Because A_t is given by Equation (8), we obtain

$$A_{t+1} = r_{m-1}^{(0)} A_t + r_{m-2}^{(0)} A_{t-1} + \ldots + r_{m-t-1}^{(0)} A_0.$$

Therefore,

$$r_j^{(t+1)} = r_j^{(0)} A_{t+1} + r_{j-1}^{(0)} A_t + r_{j-2}^{(0)} A_{t-1} + \ldots + r_{j-t-1}^{(0)} A_0.$$

Hence the result holds for all $t \geq 0$. □

3. Proof of Theorem 1

In this section, we study the minimum number of nonzero coefficients of $f(x)$ which is induced by a given mapping θ that moves $m > 1$ elements.

Proof of Theorem 1. *(a)* If 0 is a fixed point of θ, then $a_0 = 0$ and thus $a'_{q-1} = a_{q-1}$. In this case, a'_{q-1} is also the coefficient of x^{q-1} in $f^*(x)$. Assume that there is a k such that $0 \le k \le q-1-m$ and

$$a'_{k+i} = 0$$

for $i = m, m-1, m-2, \ldots, 1$. By Lemma 1, this can be written as

$$\sum_{s \in T} s^{m-i}(s^{q-1-k-m}\big(s - \theta(s)\big)) = 0, \quad i = m, m-1, \ldots, 1.$$

If we consider elements $s^{q-1-k-m}(s-\theta(s))$ as unknown variables and s^{m-i} as coefficients, the only solution of this system is zero as the coefficient matrix is a regular Vandermonde matrix. This gives a contradiction as $\theta(s) \neq s$ for each $s \in T$. Hence such k does not exist. This implies that there are no m successive a'_k all equal to the zero. Because $0 \notin T$, we have $m \le q-1$. Let $q-1 = mv + r$, where $0 \le r < m$. In each block of m successive coefficients among

$$a'_{q-1}, a'_{q-2}, \ldots a'_{q-m};$$

$$a'_{q-m-1}, a'_{q-m-2}, \ldots a'_{q-2m};$$

$$\vdots$$

$$a'_{q-(v-1)m-1}, a'_{q-(v-1)m-2}, \ldots, a'_{q-vm};$$

there is at least one non-zero coefficient. Hence there are at least v nonzero a'_k's. If $r = 0$, then a'_1 could be -1 and thus $a_1 = 0$. Hence there are at least $v-1$ nonzero coefficients a_k of $f(x)$. If $r > 0$, then there are least v nonzero coefficients a_k of $f(x)$.
(b) If 0 is not a fixed point of θ, then $0 \in T$ and $a_0 \neq 0$. Assume that there is a k such that $0 \le k \le q-1-m$ and

$$a'_{k+i} = 0$$

for $i = m-1, m-2, \ldots, 1$ ($m-1$ successive a'_k's are zeroes). Again, since $0 \in T$, by Lemma 1, this can be written as

$$\sum_{s \in S \setminus \{0\}} s^{m-i}(s^{q-1-k-m}\big(s - \theta(s)\big)) = 0, \quad i = m-1, \ldots, 1.$$

For the similar reason as above, the only solution of this system is zero, which is a contradiction. Hence such k does not exist. This implies that there is no $m-1$ successive a'_k all equal to zero.

Although $a'_{q-1} \neq 0$ does not always imply $a_{q-1} = 0$, we note that if $a'_{q-1} = a_0 + a_{q-1} = a_0$ then $a_{q-1} = 0$. Hence there are at least $\frac{q-1}{m-1} - 1$ nonzero coefficients a_k of $f(x)$ if $m-1 \mid q-1$ and there are least $\frac{q-1}{m-1}$ nonzero coefficients a_k of $f(x)$ if $m-1 \nmid q-1$. □

4. Polynomials achieving the lower bound with $m \mid q-1$

In this section we describe polynomials that have the minimum number of nonzero coefficients when $m \mid q-1$. They turn out to be a special type of permutation polynomials. First of all, we prove the following lemma which deals with the case when all the moved elements satisfying the equation $x^m = z$ for some $z \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Lemma 4. *Let $f(0) = 0$ and $T = \{s \mid s \in \mathbb{F}_q, f(s) \neq s\} = \{s_1, \ldots, s_m\}$. If two successive m-blocks have all coefficients equal to the 0 except one nonzero coefficient in the same position in each block, then elements of T are solutions of the equation $x^m = z$ for some $z \in \mathbb{F}_q^*$ and thus $m \mid q-1$. Conversely, if all the elements of T are solutions of the equation $x^m = z$ for some $z \in \mathbb{F}_q^*$ where $m \mid q-1$, then $a'_{q-1-j} = a'_{q-1-j-m} z$ for every j such that $m \leq j \leq q-2$.*

Proof. Let $q-1 = mv + r$ where $0 \leq r < m$. Let $0 \leq i < v-1$ (v is number of m-blocks). Assume that $(i+1)$-th and $(i+2)$-th m-blocks both contain all zeros except at j-th position, i.e.,

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_1 & s_2 & \ldots & s_m \\ \vdots & \vdots & \ddots & \vdots \\ s_1^{m-1} & s_2^{m-1} & \ldots & s_m^{m-1} \end{bmatrix} \begin{bmatrix} s_1^{im}(s_1 - \theta(s_1)) \\ s_2^{im}(s_2 - \theta(s_2)) \\ \vdots \\ s_m^{im}(s_m - \theta(s_m)) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a'_{q-1-im-j} \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_1 & s_2 & \ldots & s_m \\ \vdots & \vdots & \ddots & \vdots \\ s_1^{m-1} & s_2^{m-1} & \ldots & s_m^{m-1} \end{bmatrix} \begin{bmatrix} s_1^{(i+1)m}\big(s_1 - \theta(s_1)\big) \\ s_2^{(i+1)m}\big(s_2 - \theta(s_2)\big) \\ \vdots \\ s_m^{(i+1)m}\big(s_m - \theta(s_m)\big) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a'_{q-1-(i+1)m-j} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $\vec{y} = y\vec{e}_j$, $y \in \mathbb{F}_q$, where $\vec{e}_j = (0, \ldots, 0, 1, 0, \ldots 0)^T$ and 1 is at j-th position. Denote by

$$V := \begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_1 & s_2 & \ldots & s_m \\ \vdots & \vdots & \ddots & \vdots \\ s_1^{m-1} & s_2^{m-1} & \ldots & s_m^{m-1} \end{bmatrix}.$$

Then solutions of the system $V\vec{x} = \vec{y}$, where y varies over $\mathbb{F}_q$, form a vector subspace of the $\mathbb{F}_q^m$ over $\mathbb{F}_q$. As there are q different vectors $\vec{y}$ and V is a regular matrix, this subspace has q elements with a basis of one vector and all its elements are linearly dependent. Namely, if matrix equations above are satisfied then vectors $(s_1^{im}(s_1 - \theta(s_1)), \ldots, s_m^{im}(s_m - \theta(s_m)))^T$ and $(s_1^{(i+1)m}(s_1 - \theta(s_1)), \ldots, s_m^{(i+1)m}(s_m - \theta(s_m)))^T$ are linearly dependent. Hence $z s_k^{im}(s_k - \theta(s_k)) = s_k^{(i+1)m}(s_k - \theta(s_k))$ for some $z \in \mathbb{F}_q^*$. As $0 \notin T$ it follows

that $s_k^m = z$ for all $k = 1, 2, \ldots, m$ and some $z \in \mathbb{F}_q^*$. As s_k are distinct, equation $x^m - z = 0$ has all solutions in $\mathbb{F}_q$ and thus $m \mid q-1$.

The converse follows directly from Equation (2). □

Lemma 5. *Let $m \mid q-1$ and ψ be primitive m-th root of unity in $\mathbb{F}_q$. Let $f(x)$ be the polynomial induced by the cycle of the form*

$$(s, s\psi^i, s\psi^{2i}, s\psi^{3i}, \ldots, s\psi^{(m-1)i})$$

for some $s \in \mathbb{F}_q^*$ and positive integer i. Then $f(x) - x$ has $(q-1)/m$ possible nonzero coefficients a'_{q-um} where $u = 1, 2, \ldots, \frac{q-1}{m}$ and all other coefficients are equal to the zero.

Proof. By Lemma 1 (or the main theorem in [16]), the coefficients a_i of induced polynomial $f(x)$ are given by

$$\begin{aligned} a'_{q-1-t} &= \sum_{j=0}^{m-1} (s\psi^j)^t (s\psi^j - s\psi^{j+i}) \\ &= (1-\psi^i) s^{t+1} \sum_{j=0}^{m-1} \psi^{j(t+1)}. \end{aligned}$$

If $\gcd(t+1, m) \neq m$ then $\sum_{j=0}^{m-1} \psi^{j(t+1)} = 0$ and thus $a'_{q-1-t} = 0$. If $\gcd(t+1, m) = m$ then we have $t = um - 1$ and $\sum_{j=0}^{m-1} \psi^{j(t+1)} = m$. Therefore

$$a_{q-um} = s^{t+1}(1-\psi^i)m + \delta_1^{q-um},$$

where $u = 1, 2, \ldots, \frac{q-1}{m}$. Thus $a'_{q-um} = a_{q-um} - \delta_1^{q-um}$ can have at most $\frac{q-1}{m}$ possible non-zeros. □

We note that $a_1 = 0$ (i.e., $a'_1 = -1$) if and only if $m(1-\psi^i) = -1$. More generally, we can prove Theorem 2.

Proof of Theorem 2. (a) We first prove that any mapping θ moving an m-set $T = \{s, s\psi, \ldots, s\psi^{m-1}\}$ ($s \neq 0$) defined by $\theta(s\psi^j) = (1 + m^{-1})s\psi^j$ induces a polynomial with $(q-1)/m - 1$ nonzero coefficients. By Lemma 1, we obtain

$$\begin{aligned} a'_k &= \sum_{j=0}^{m-1} (s\psi^j)^{q-1-k} (s\psi^j - \theta(s\psi^j)) \\ &= \sum_{j=0}^{m-1} (s\psi^j)^{q-1-k} (s\psi^j - (1+m^{-1})s\psi^j)) \\ &= -\sum_{j=0}^{m-1} (s\psi^j)^{q-k} m^{-1}. \end{aligned}$$

Similar to the proof of Lemma 5, we know that $a'_k = 0$ if and only if $\gcd(q-k, m) \neq m$. If $\gcd(q-k, m) = m$ then $a'_{q-um} = -s^{um}$ for $1 \leq u \leq (q-1)/m$. Hence $a_{q-um} \neq 0$ for $1 \leq u \leq (q-1)/m - 1$. However, $a'_1 = -s^{q-1} = -1$ implies that $a_1 = -a'_1 + 1 = 0$. Hence there are exactly $(q-1)/m - 1$ nonzero coefficients in $f(x)$.

Conversely, we need to prove that if a polynomial $f(x)$ moves m elements and contains the least number of possible nonzero coefficients, then it must be defined by $\theta(s\psi^j) = (1+m^{-1})s\psi^j$ on the set T. By the proof of Theorem 1, the least number of the nonzero coefficients is $(q-1)/m-1$. In this case, $q-1 = vm$ and in particular, each m-block contains at most 1 nonzero coefficient at the last position, i.e., $a'_{q-im} \neq 0$ $i = 1, 2, \ldots, v-1$ and $a_1 = 0$. By Lemma 4, all moved elements are roots of $x^m - s^m = 0$ for some $s \neq 0$. Moreover, $a'_{q-1-j} = a'_{q-1-j-m}s^m$ and $a'_1 = -1$. Thus $j = um$ where $u < v$. Consider

$$V = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ s & s\psi & \ldots & s\psi^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ s^{m-1} & (s\psi)^{m-1} & \ldots & (s\psi^{m-1})^{m-1} \end{bmatrix}.$$

By the proof of Lemma 4, we obtain that all solutions of the system $Vx = b\vec{e}_m$ are linearly dependent when b varies in $\mathbb{F}_q$. Because $s((1-\psi), \psi(1-\psi), \psi^2(1-\psi), \ldots, \psi^{m-1}(1-\psi))$ is a solution to $Vx = s^m(1-\psi)m\vec{e}_m$ and $(s-\theta(s), s\psi-\theta(s\psi), \ldots, s\psi^{m-1}-\theta(s\psi^{m-1}))$ is a solution to $Vx = a'_{q-1-m}\vec{e}_m$ by the proof of Lemma 4, there exists $a \in \mathbb{F}_q$ such that

$$s\psi^j - \theta(s\psi^j) = a(s\psi^j - s\psi^{j+1}).$$

This implies that

$$\theta(s\psi^j) = (1-a)s\psi^j + as\psi^{j+1} = s\psi^j(1-a+a\psi), \quad j = 0, 1, \ldots, m-1.$$

Now $a'_1 = -1$ and Lemma 1 implies $1 - a + a\psi = 1 + m^{-1}$.
(b) Similar to the proof of Lemma 5, the induced permutation polynomial from θ has $\frac{q-1}{m}$ possible nonzero coefficients. Moreover, by Lemma 1, we know

$$a_1 = 1 + \sum_{j=0}^{m} s_j^{q-2}(s_j - \theta(s_j)) = 1 + \sum_{j=1}^{m} s_j^{q-2}(s_j - \psi^i s_j) = 1 + (1-\psi^i)m.$$

Hence $a_1 = 0$ if and only if $\psi^i = 1+m^{-1}$. Therefore f has $\frac{q-1}{m}-1$ nonzero coefficients if $\psi^i = 1+m^{-1}$. □

For the polynomial which moves m elements, the following general result regarding its degree holds.

Theorem 4. *Let $f(x)$ be a polynomial over $\mathbb{F}_q$ with degree at most $q-1$. If f has exactly $k < q$ fixed elements of $\mathbb{F}_q$, then the degree of f is at least k. This lower bound is achieved for $\binom{q}{k}(q-1)$ polynomials.*

Proof. Let T be the subset of $\mathbb{F}_q$ which contains all the elements in $\mathbb{F}_q$ not fixed by f. Since the polynomial $f(x)$ fixes elements of the set $\mathbb{F}_q \setminus T$ then it can be written as

$$f(x) = x + h(x) \prod_{s \in \mathbb{F}_q \setminus T} (x - s)$$

where $h(x)$ is some polynomial with no zeros in T. Indeed, for every $s \in \mathbb{F}_q \setminus T$, $f(s) - s = 0$ implies $(x-s) \mid f(x) - x$ and so $\prod_{s \in \mathbb{F}_q \setminus T}(x-s) \mid f(x) - x$. Now if $h(x)$ has a zero $a \in T$ then a would be a fixed element of $f(x)$, a contradiction. Therefore, $deg(f) \geq k = deg(\prod_{s \in \mathbb{F}_q \setminus T}(x-s))$. Further $\deg(f(x)) = k$ if and only if $h(x) = c$ where $c \in \mathbb{F}_q \setminus \{0\}$ and so there are $q-1$ polynomials of the least degree with this property for the fixed set T of moved elements and in total there are $\binom{q}{k}(q-1)$ polynomials of degree k with k fixed elements. □

Now we derive some lower bounds for the number of permutation polynomials with the given degree at most $q-m$ where $m \mid q-1$ and at most $\frac{q-1}{m}$ nonzero coefficients.

Proposition 1. *Let $m \mid q-1$. Then*
(a) There are at least $(m-1)\frac{q-1}{m}$ permutation polynomials, each moves m elements, has the degree $q-m$, and has at most $\frac{q-1}{m}$ nonzero coefficients. In particular, if ψ is m-th root of unity and $1+m^{-1}=\psi^i$ for some i then there are exactly $\frac{q-1}{m}$ permutation polynomials of degree $q-m$, each moves m elements and has exactly $\frac{q-1}{m}-1$ nonzero coefficients.
(b) There are at least $m^{\frac{q-1}{m}}-1$ permutation polynomials with the degree at most $q-m$ and at most $\frac{q-1}{m}$ nonzero coefficients.
(c) The number of permutation polynomials of degree at most $q-m$ is at least $q^2(m^{\frac{q-1}{m}}-1)$.
(d) The number of permutation polynomials of the degree $q-m$ which induce full m-cycles is at least $q\frac{q-1}{m}\varphi(m)$.
(e) The number of the permutation polynomials of the degree $q-m$ which moves m elements is at least $q\frac{q-1}{m}(m-1)$.

Proof. (a) Let ξ be a generator of $\mathbb{F}_q^*$. Let $m \mid q-1$. Let $\psi=\xi^{\frac{q-1}{m}}$ and let $w=\xi^k$, $k \in \{0,1,\ldots,\frac{q-1}{m}-1\}$. By Theorem 2, permutation polynomials induced by $\theta_{i,k} : w\psi^j \to w\psi^{j+i}$, where $i \in \{1,2,\ldots,m-1\}$ are permutation polynomials which moves the m elements and has at most $\frac{q-1}{m}$ non-zero coefficients (these are a_{q-um}'s where $u=1,\ldots,(q-1)/m-1$). For different choices of i and k we have distinct permutations with this property. Therefore there are at least $(m-1)\frac{q-1}{m}$ permutation polynomials of degree $q-m$ which move m elements and have at most $\frac{q-1}{m}$ nonzero coefficients. The rest of proof of (a) follows from Theorem 2 (b). where $j=0,1,2,\ldots,\frac{q-1}{m}-1$ are permutation polynomials of degree $q-m$, each moves m elements,and has exactly $\frac{q-1}{m}-1$ nonzero coefficients.

(b) If $k \neq k'$, then permutations $\theta_{i,k}$ and $\theta_{i,k'}$ are disjoint. By Corollary 1, composition of distinct permutations $\theta_{i,k}$ has also at most $\frac{q-1}{m}$ nonzero coefficients because the positions of $\frac{q-1}{m}-1$ nonzero coefficients of $\theta_{i,k}$ are determined by q and m only and 1 extra nonzero coefficient comes from the coefficient of x. Thus we can obtain

$$\binom{\frac{q-1}{m}}{1}(m-1)+\binom{\frac{q-1}{m}}{2}(m-1)^2+\ldots+\binom{\frac{q-1}{m}}{\frac{q-1}{m}}(m-1)^{\frac{q-1}{m}}=m^{\frac{q-1}{m}}-1,$$

such permutations by varying the number of k's from 1 to $\frac{q-1}{m}$. Thus the lower bound for the number of permutation polynomials of the degree at most $q-m$ and at most $\frac{q-1}{m}$ nonzero coefficients is

$$m^{\frac{q-1}{m}}-1.$$

(c) For any permutation polynomial in the proof of (b), composition with the linear polynomial $x+b$ from the right side and the linear polynomial $x+c$ from the left side results in a permutation polynomial of the same degree. Hence there are $q^2(m^{\frac{q-1}{m}}-1)$ such polynomials. We now show that these polynomials are all distinct. Indeed, if the permutation $\theta_{i,k}$ is composed by $x+b$ from right and $x+c$ from the left then we have mapping $\theta_{i,k}(x+b)+c$ which sends elements $\xi^k\psi^j-b$ to $\xi^k\psi^{j+i}+c$ and sends x to $x+b+c$ otherwise. Obviously, for different choices of b,c,i,k we have different mappings.

(d) If we want to estimate the lower bound for the number of permutation polynomials of the degree $q-m$ we should note that conjugation with a linear polynomial does not change the degree. To obtain the

number of m-cycles with a given property we can take the set $T = \{1, \psi, \psi^2, \ldots, \psi^{m-1}\}$ and the mapping $\theta_i : \psi^j \to \psi^{j+i}$. If $\gcd(i, m) = 1$ then θ_i is full cycle on T. Then mappings $(ax + b) \circ \theta_i \circ (ax + b)^{-1} : aT + b \to aT + b$ are full cycles on the set $aT + b$ where $a = \xi^t$, for $t = 0, 1, \ldots, \frac{q-1}{m} - 1$. Thus there are at least

$$q\frac{q-1}{m}\varphi(m)$$

permutation polynomials of the degree $q - m$ which induce full m-cycles. This bound was obtained in [12, Theorem 1.1].

(e) From the previous case it immediately follows that the number of permutation that moves the m elements of the set $aT + b$, not necessarily full cycles, of the degree $q - m$ is at least

$$q\frac{q-1}{m}(m-1)$$

as we don't necessarily have $\gcd(m, k) = 1$. □

We remark that the lower bound in (b) can be improved. In fact, in the proof of (b) we considered permutations $\theta_{i,k}$ which moves m elements and have at most $\frac{q-1}{m}$ nonzero coefficients a'_{q-um}, $u = 1, 2, \ldots, \frac{q-1}{m} - 1$, by Theorem 2. Similarly, we can consider permutation polynomials (denote corresponding mapping by $\theta^d_{i,k}$) which moves dm elements and have at most $\frac{q-1}{dm}$ nonzero coefficients $a'_{q-s(dm)}$, $s = 1, 2, \ldots, \frac{q-1}{dm}$. By Corollary 1, composition of disjoint permutations $\theta_{i,k}$ and $\theta^d_{i,k}$ induces a permutation polynomial with degree $q - m$ and at most $\frac{q-1}{m}$ nonzero coefficients. We omit the details since the expressions are more complicated.

5. An algorithm for computing the coefficients of polynomials

It is usual to use Lagrange interpolation formula or variations of it such as $f(x) = \sum_{s\in\mathbb{F}_q} \theta(s)(1-(x-s)^{q-1})$ (see [11])) or Equation (3) for calculating coefficients of a polynomial induced by a mapping θ over a finite field. The classical Lagrange interpolation formula needs $\mathcal{O}(q^2)$ operations. In general we cannot expect any algorithm with performance better than $\mathcal{O}(q)$ because there are q coefficient to determine. Here we will give algorithm for computing the polynomial induced by given mapping $\theta : \mathbb{F}_q \to \mathbb{F}_q$ of complexity $\mathcal{O}(q^{3/2})$. Let $\theta' : \mathbb{F}_q \to \mathbb{F}_q$ be a given mapping. Let $\theta(x) = \theta'(x) - \theta'(0)$, i.e., $\theta(0) = 0$. We want to find a polynomial $f(x)$ such that $f(x)$ and $f(x) - f(0)$ induce mapping θ and θ' respectively.

Let $1 < m$ be a factor of $q-1$ of moderate size (it is desirable to choose $m \approx \sqrt{q-1}$ if one can and it will be justified in Equation (9)). Let $D < \mathbb{F}_q^*$ be a cyclic subgroup of order m, i.e., $D = \{d_1, d_2, \ldots, d_m\} = \{x \mid x \in \mathbb{F}_q, x^m = 1\}$ and s_i, $i = 1, 2, \ldots, \frac{q-1}{m}$ are distinct representatives of the equivalence classes s_iD. For each equivalence class s_iD, let $f_i(x)$ be a polynomial induced by the mapping ϕ_i such that $\phi_i \mid_{s_iD} = \theta \mid_{s_iD}$ and ϕ_i fixes all other elements of $\mathbb{F}_q$. So $f_i(x)$ moves at most m elements (say $m_i \le m$ elements) and all the moved elements in s_iD are roots of the equation $x^m = s_i^m$. Hence coefficients $b^{(i)}_{q-1-j}$ of $f_i(x) - x$ can be computed directly by using Lemma 1 for $j = 0, \ldots, m-1$. For $j = m, \ldots, q-2$, for the purpose of computational efficiency, we apply Lemma 4 to obtain $b^i_{q-1-j} = b^i_{q-1-j-m}s_i^m$. Finally we apply the following result to find coefficients of $f(x)$.

Lemma 6. *Let T_i for $i = 1, \ldots, h$ be pairwise disjoint subsets of $\mathbb{F}_q$ and $0 \notin \bigcup_{i=1}^h T_i$. Let ϕ_i, $i = 1, 2, \ldots h$, be mappings such that ϕ_i moves elements of set T_i and let the polynomial induced by ϕ_i be*

$f_i(x) = \sum_{j=0}^{q-1} a_j^{(i)} x^j$. *Define the mapping*

$$\theta(x) = \begin{cases} \phi_i(x), & x \in T_i, \quad i = 1, 2, \ldots h; \\ x, & x \in \mathbb{F}_q \setminus (\bigcup_{i=1}^{h} T_i). \end{cases}$$

Then the polynomial induced by θ *is* $f(x) = \sum_{i=1}^{h} f_i(x) - (h-1)x$. *In particular, the coefficient* c_1' *of* $f(x) - x$ *is* $c_1' = \sum_{i=1}^{h} a_1^{(i)} - h$.

Proof. By Lemma 1 and $0 \notin \bigcup_{i=1}^{h} T_i$, the coefficients of the polynomial induced by θ are given by

$$\begin{cases} c_k = \sum\limits_{s \in \cup_{i=1}^{h} T_i} s^{q-1-k}(s - \theta(s)) + \delta_1^k, & k = 1, \ldots q-2, \\ c_{q-1} = \sum\limits_{s \in \cup_{i=1}^{h} T_i} s^{q-1}(s - \theta(s)), \\ c_0 = 0, \end{cases}$$

Then for $k = 2, 3, \ldots, q-2$ we have

$$c_k = \sum_{i=1}^{h} \sum_{s \in T_i} s^{q-1-k}(s - \phi_i(s)) = \sum_{i=1}^{h} a_k^{(i)}.$$

Further

$$c_{q-1} = \sum_{i=1}^{h} \sum_{s \in T_i} s^{q-1}(s - \phi_i(s)) = \sum_{i=1}^{h} a_{q-1}^{(i)},$$

and

$$c_1' = \sum_{i=1}^{h} \sum_{s \in T_i} s^{q-1-1}(s - \phi_i(s)) = \sum_{i=1}^{h} a_1^{(i)\prime} = \sum_{i=1}^{h} (a_1^{(i)} - 1) = \sum_{i=1}^{h} a_1^{(i)} - h.$$

Hence $c_1 = \sum_{i=1}^{h} a_1^{(i)} - (h-1)$ and $f(x) = \sum_{i=1}^{h} f_i(x) - (h-1)x$. □

Now we present the following algorithm to compute the coefficients of a polynomials induced by a given mapping.

Input: a given mapping θ with $\theta(0) = 0$ over $\mathbb{F}_q$, $1 < m \mid q-1$, a cyclic subgroup $D = \{d_1, d_2, \ldots, d_m\}$, and distinct coset representatives $s_i, i = 1, \ldots, \frac{q-1}{m}$.

Output: coefficients a_i of the polynomial induced by θ.

Algorithm:

Set $a_1 = -\frac{q-1}{m} + 1$ and $a_j = 0$ for $j = 0, 2, 3, \ldots, q-1$.

FOR $i = 1, 2, \ldots, \frac{q-1}{m}$

{

Set $b_j = 0$, for $j = 1, 2 \ldots q-1$;

(1) FOR $z = 1, 2, \ldots, m$

$a \leftarrow s_i d_z$

$Q_z = a - \theta(a)$

FOR $t = 0, 1, \ldots, m-2$

$b_{q-1-t} \leftarrow b_{q-1-t} + Q_z$;
$Q_z \leftarrow Q_z \cdot a$
$b_{q-1-(m-1)} \leftarrow b_{q-1-(m-1)} + Q_z$;
(2) FOR $u = 1, 2, \ldots, \frac{q-1}{m} - 1$
$W \leftarrow s_i^{um}$;
FOR $t = 0, 1, \ldots, m-1$
$b_{q-1-um-t} \leftarrow W \cdot b_{q-1-t}$
(3) FOR $j = 1, 2, \ldots, q-1$
$a_j \leftarrow a_j + b_j$.

}

To evaluate b_j where $j = q-1, \ldots, q-m$ in Step (1) we need m^2+m additions and m^2 multiplications. Suppose we need 1 multiplication for each $(s_i^m)^u$ (if elements s_i^m are represented as ψ^j where ψ is a primitive element of $\mathbb{F}_q^*$). So there are totally $(m+1)(\frac{q-1}{m} - 1)$ multiplications in Step (2) to compute b_j, $j = q-m-1, \ldots, 1$. To correct coefficients of $f(x)$ in Step (3) we need $q-1$ additions. Therefore for $i = 1, 2, \ldots, \frac{q-1}{m}$ there are $m^2 + (m+1)(\frac{q-1}{m} - 1)$ multiplications and $m + m^2 + (q-1)$ additions or $2m^2 + 2(q-1) - 1 + \frac{q-1}{m}$ operations. Thus in total there are

$$h(m) = \frac{q-1}{m}(2m^2 + 2(q-1) - 1 + \frac{q-1}{m}) = 2(q-1)m + \frac{2(q-1)^2 - (q-1)}{m} + \frac{(q-1)^2}{m^2}$$

operations. Note that the above expression is quite complicated to find the minimal value of $h(m)$ by computing its derivative. Instead, we choose $m = \sqrt{q-1}$ directly. Then we have

$$h(\sqrt{q-1}) = 4(q-1)^{3/2} + (q-1) - \sqrt{q-1} = \mathcal{O}(q^{3/2}). \tag{9}$$

If the number of operations for calculating each $(s_i^u)^m$ is $m-1$ in Step (2) (the worst possible case), then the above algorithm still has complexity $\mathcal{O}(q^{3/2})$ in a similar way.

We should also note that it is not always possible to find $m \mid q-1$ such that $m \approx \sqrt{q-1}$. If $q = p^{2n}$ then we should choose $m = p^n + 1$. In any case for $1 < m < q-1$ where $m \approx (q-1)^{1/k}$ $k \geq 2$ this algorithm is better than $\mathcal{O}(q^2)$.

There exists a fast version of Lagrange interpolation algorithm which is a divide-and conquer algorithm and it is based on polynomial multiplication over finite fields. It is known from [19] that FFT based algorithm are superior to the classical algorithms for polynomials of degree 25 modulo 100-bit prime. Here the fast interpolation algorithm needs $\mathcal{O}(q(\log q)^2 \log\log q)$ operations (see [8]). Asymptotically this fast Lagrange interpolation algorithm has better performance than ours. However, our algorithm is simple and can be used for computations by hand when q is small. Moreover, we have the exact counts for the number of operations for any q.

We note that the above algorithm is also suitable for parallel computing because coefficients for the distinct equivalent classes can be calculated simultaneously by distinct processors.

In the case when the number m_θ of moved elements by the mapping θ is small, i.e., $m_\theta \leq 2\sqrt{q-1} - 1$ we should apply an algorithm which directly follows from the Lemma 1:

Input: a given mapping θ over $\mathbb{F}_q$ and set $t = \{s_1, s_2, \ldots, s_{m_\theta}\}$ of the moved elements by θ.

Output: coefficients a_i of the polynomial induced by θ.

Algorithm:

Set $a_1 = 1$, $a_0 = \theta(0)$ and $a_j = 0$ for $j = 2, 3, \ldots, q-1$.

FOR $i = 1, 2, \ldots, m_\theta$

{ $Q = s_i - \theta(s_i)$
FOR $t = 0, 1, \ldots, q-2$
$\{a_{q-1-t} \leftarrow a_{q-1-t} + Q;$
$Q \leftarrow Q \cdot s_i$ $\}$
}
$a_{q-1} \leftarrow a_{q-1} - a_0$.

This algorithm has $qm_\theta + 1$ additions and $(q-1)m_\theta$ multiplications, i.e., totally $(2q-1)m_\theta + 1$ operations, which has better performance than the previous algorithm.

6. Proof of Theorem 3

In this section, we study the minimum number of nonzero coefficients of $f(x)$ which is induced by a given mapping θ that moves $m > 1$ elements such that $m \nmid q-1$. In order to complete the proof of Theorem 3 we need the following lemmas.

Lemma 7. *Let $m < \frac{q-1}{2}$. Let $T = \{s_1, s_2, \ldots, s_m\}$ be the set of all elements of $\mathbb{F}_q$ moved by $f(x)$. Assume $m \nmid (q-1)$ and $0 \notin T$. If two successive m-blocks, i-th and $(i+1)$-th block, have one nonzero coefficient in each m-block, respectively, then $s_1, s_2, \ldots, s_m$ are roots of the polynomial*

$$P(x) = x^{kd} - bx^{(k-1)d} + b^2x^{(k-2)d} - \ldots + (-1)^k b^k = \frac{x^{(k+1)d} - (-b)^{k+1}}{x^d + b},$$

where $m = kd$ and $(k+1)d \mid q-1$ and $-b = v^d$ for some $v \in \mathbb{F}_q^*$.

Lemma 8. *If there exists an integer d such that $m = kd$, $(k+1)d \mid q-1$, and the moved elements by θ are roots of the polynomial $P(x) = \frac{x^{(k+1)d} - (-b)^{k+1}}{x^d + b}$ for some $-b = v^d \in \mathbb{F}_q^*$, then the number of the nonzero coefficients of $f(x)$ is at least $2\frac{q-1}{(k+1)d} - 1$.*

Let us first prove Theorem 3.

Proof of Theorem 3. First we show that if $m > \frac{q-1}{2}$ then any of these two lower bounds is 1. Obviously, if $m > \frac{q-1}{2}$ then $\lfloor \frac{3}{2} \lfloor \frac{q-1}{m} \rfloor \rfloor = 1$. Also, if $m = kd > \frac{q-1}{2}$, then $(k+1)d \mid q-1$ implies $(k+1)d = q-1$ and so $2\frac{q-1}{(k+1)d} - 1 = 1$ as well. Therefore we have a trivial lower bound when $m > \frac{q-1}{2}$.

Assume now $m < \frac{q-1}{2}$. If there is exactly one non-zero coefficient in each of two successive m-blocks then, by Lemma 7, $s_1, s_2, \ldots, s_m$ are solutions of the equation

$$\frac{x^{(k+1)d} - (-b)^{k+1}}{x^d + b} = 0.$$

On the other hand by Lemma 8, $2\frac{q-1}{(k+1)d} - 1$ is the least number of nonzero coefficients in the polynomial with given set of moved elements.

Otherwise, the nonzero coefficients in the successive m-blocks in the best case have a pattern of $1, 2, 1, 2, \ldots$, (or $2, 1, 2, 1, \ldots$). Let $q - 1 = vm + r$. If v is even, the least number of nonzero coefficients is $\frac{3}{2}v = \frac{3}{2}\lfloor \frac{q-1}{m} \rfloor$. If v is odd, the least number of nonzero coefficients is either $\frac{3}{2}(v-1) + 1 = \frac{3}{2}\lfloor \frac{q-1}{m} \rfloor - \frac{1}{2}$ or $\frac{3}{2}(v-1) + 2 = \frac{3}{2}\lfloor \frac{q-1}{m} \rfloor + \frac{1}{2}$. Both are greater than or equal to $\lfloor \frac{3}{2} \lfloor \frac{q-1}{m} \rfloor \rfloor$. □

We demonstrate now a few examples which meet the lower bounds in the theorem.

First, we consider $\mathbb{F}_{11}$, $T = \{1, -1, 2, -2\}$ and $f(x) = 4x^7 + 9x^5 + 7x^3$. Indeed, in this case, $m = 4$. As $\frac{3m}{2} \nmid q-1$, the lower bound for the number of nonzero coefficients is $\lfloor \frac{3}{2} \lfloor \frac{q-1}{m} \rfloor \rfloor = 3$. This set of moved elements is not the solution set of the equation of $\frac{x^{(k+1)d} - (-b)^{k+1}}{x^d + b} = 0$.

Secondly, let $\mathbb{F}_q = \mathbb{F}_{2^6}$, $d = 3$, $m = 2d = 6 \nmid q - 1 = 63$ and $3d = 9 \mid 63$. The polynomial $f(x) = x + \frac{x^{64} - x}{x^6 + x^3 + 1} = x^4 - x^{10} + x^{13} - x^{19} + x^{22} - x^{28} + x^{31} - x^{37} + x^{40} - x^{46} + x^{49} - x^{55} + x^{58}$ moves 6 elements which are solutions of $x^6 + x^3 + 1 = \frac{x^9 + 1}{x^3 + 1} = 0$ and it has $2\frac{q-1}{3d} - 1 = 13$ nonzero coefficients. Further $\lfloor \frac{3}{2} \lfloor \frac{63}{6} \rfloor \rfloor = 15 > 2\frac{q-1}{3d} - 1$.

Finally, an example of monomial which satisfies the trivial bound is $f(x) = x^2$ over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$ with $\alpha^2 = \alpha + 1$.

We end this section with the proofs of Lemma 7 and Lemma 8.

Proof of Lemma 7. Let $f(x) = \sum_{k=0}^{q-1} a_k x^k$ be any polynomial moving m elements such that $a_0 = 0$, i.e., $0 \notin T$. Let a'_k be defined as in Section 2. Let $q - 1 = ms + r$ where $1 \le r \le m - 1$.

For $t \ge 0$ by Equation (5), we have the following recurrence relation

$$a'_{q-1-m-t} = \sum_{j=0}^{m-1} r_j^{(t)} a'_{q-1-j}.$$

Assume that in the first m-block all coefficients are zeros except a'_{q-1-j_0} where $0 \le j_0 \le m-1$. This means that, for $q - 1 - m \ge t \ge 0$,

$$a'_{q-1-m-t} = \sum_{i=0}^{m-1} r_i^{(t)} a'_{q-1-i} = r_{j_0}^{(t)} a'_{q-1-j_0}.$$

Thus

$$a'_{q-1-m-t} = 0 \quad \text{if and only if} \quad r_{j_0}^{(t)} = 0. \tag{10}$$

Assume that the coefficients in the second block satisfies $a'_{q-1-m} = a'_{q-1-m-1} = \ldots = a'_{q-1-m-(h-1)} = a'_{q-1-m-(h+1)} = \ldots = a'_{q-2m} = 0$ and $a'_{q-1-m-h} \neq 0$. As a consequence of Theorem 1, we must have $0 \le h \le j_0$. Moreover, by Equation (10), we have

$$r_{j_0}^{(t)} = 0 \ for\ t = 0, \ldots, h-1, h+1, \ldots, m-1, \ and\ r_{j_0}^{(h)} \neq 0$$

Hence we now divide our discussions into two cases:

CASE I: Assume that $a'_{q-1-m} = 0$, i.e, $h > 0$.

Using the fact that

$$r_{j_0}^{(t)} = 0 \ for\ t = 0, \ldots, h-1, \ and\ r_{j_0}^{(h)} \neq 0,$$

and the recurrence relation (7), i.e.,

$$r_{j_0}^{(t)} = r_{j_0}^{(0)} A_t + r_{j_0-1}^{(0)} A_{t-1} + \ldots + r_{j_0-t}^{(0)} A_0,$$

we can show that $r_{j_0}^{(t)} = r_{j_0-t}^{(0)} = 0$ for $t = 1, 2, \ldots h-1$. Indeed, for $t = 1$,

$$0 = r_{j_0}^{(1)} = r_{j_0}^{(0)} A_1 + r_{j_0-1}^{(0)} A_0 = r_{j_0-1}^{(0)},$$

and more generally

$$0 = r_{j_0}^{(t)} = r_{j_0}^{(0)} A_t + r_{j_0-1}^{(0)} A_{t-1} + \ldots + r_{j_0-t}^{(0)} A_0 = 0 + r_{j_0-t}^{(0)} A_0 = r_{j_0-t}^{(0)}.$$

On the other hand, we have

$$0 \neq r_{j_0}^{(h)} = r_{j_0}^{(0)} A_h + r_{j_0-1}^{(0)} A_{h-1} + \ldots + r_{j_0-h}^{(0)} A_0 = r_{j_0-h}^{(0)}.$$

Since $r_{j_0}^{(0)} = \cdots = r_{j_0-h+1}^{(0)} = 0$, by Equations (7) and (8), we have for $t > h$ that

$$r_{j_0}^{(t)} = r_{j_0}^{(0)} A_t + r_{j_0-1}^{(0)} A_{t-1} + \ldots + r_{j_0-t}^{(0)} A_0 = A_{t-h} r_{j_0-h}^{(0)} + A_{t-h-1} r_{j_0-h-1}^{(0)} + \ldots + A_0 r_{j_0-t}^{(0)}$$

$$= (A_{t-h-1} r_{m-1}^{(0)} + A_{t-h-2} r_{m-2}^{(0)} + \ldots + A_0 r_{m-(t-h)}^{(0)}) r_{j_0-h}^{(0)} + A_{t-h-1} r_{j_0-h-1}^{(0)} + \ldots + A_0 r_{j-t}^{(0)}$$

$$= A_{t-h-1}(r_{m-1}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-h-1}^{(0)}) + A_{t-h-2}(r_{m-2}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-h-2}^{(0)}) + \ldots +$$

$$+ A_0(r_{m-(t-h)}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-t}^{(0)}).$$

Using the fact that $r_{j_0}^{(t)} = 0$ for $t = h+1$, we obtain

$$r_{j_0}^{(h+1)} = A_0(r_{m-1}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-h-1}^{(0)}) = 0$$

and thus $(r_{m-1}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-h-1}^{(0)}) = 0$. More generally, for any $h \leq t \leq m-1$, we have $r_{j_0}^{(t)} = A_0(r_{m-(t-h)}^{(0)} r_{j_0-h}^{(0)} + r_{j_0-t}^{(0)}) = 0$, i.e.,

$$r_{j_0-h}^{(0)} r_{m-(t-h)}^{(0)} + r_{j_0-t}^{(0)} = 0, \quad t = h+1, h+2, \ldots m-1.$$

As in Lemma 3, $r_i^{(0)} = 0$ for $i < 0$. Hence for $t = j_0 + 1, \ldots, m-1$, we obtain $r_{j_0-t}^{(0)} = 0$ and thus $r_{m-(j_0-h)-1}^{(0)} = \ldots = r_{h+1}^{(0)} = 0$ because $r_{j_0-h}^{(0)} \neq 0$.

In summary, our assumption of having the nonzero coefficients at $(q-1-j_0)$-th and $(q-1-m-h)$-th positions in the first two m-blocks of coefficients lead us to the following relations on coefficients $r_k^{(0)}$:
(a) $r_{j_0-t}^{(0)} = 0$ for $t = 1, 2, \ldots h-1$,
(b) $r_{j_0-h}^{(0)} \neq 0$,
(c) $r_{m-(j_0-h)-1}^{(0)} = \ldots = r_{h+1}^{(0)} = 0$, and
(d) $r_{j_0-h}^{(0)} r_{m-(t-h)}^{(0)} + r_{j_0-t}^{(0)} = 0, \quad t > h$.

We remark that conditions (b)-(d) still hold even for $h = 0$, which will be considered in case II.

We continue our discussion with the following three sub-cases:

(1) Assume that $j_0 - h < m - (j_0 - h) < j_0$. Then it follows from (a) that $r_{m-(j_0-h)}^{(0)} = 0$ and then from (d) that $r_0^{(0)} = 0$ because $j_0 > h$ (as a result of Theorem 1). However, we know that 0 is fixed element of $f(x)$ and thus $s_i \neq 0$. Hence by definition $r_0^{(0)} = s_1 \cdots s_m \neq 0$, a contradiction.

(2) Assume that $m - (j_0 - h) \geq j_0 > j_0 - h$. Then from (a) and (c) we obtain $r_{m-(j_0-h)-1}^{(0)} = \ldots = r_u^{(0)} = 0$ where $u = \min\{h+1, j_0 - h + 1\}$.

If $h < j_0 - h$ then $r^{(0)}_{j_0-h} = 0$, a contradiction to (b). Therefore $u = j_0 - h + 1$. Using $x^m = P(x) + r^{(0)}(x)$ together with relation (d) we obtain

$$\prod_{i=1}^{m}(x - s_i) = x^m - r^{(0)}_{m-1}x^{m-1} - \ldots - r^{(0)}_{m-(j_0-h)}x^{m-(j_0-h)} - r^{(0)}_{j_0-h}x^{j_0-h} - \ldots - r^{(0)}_0 =$$

$$(x^{m-(j_0-h)} - r^{(0)}_{j_0-h})(x^{j_0-h} - r^{(0)}_{m-1}x^{j_0-h-1} - \ldots - r^{(0)}_{m-(j_0-h)}) = (x^{m-(j_0-h)} - r^{(0)}_{j_0-h})R(x).$$

Because $x^{m-(j_0-h)} - r^{(0)}_{j_0-h} \mid P(x)$, $P(x) \mid x^{q-1} - 1$ and $r^{(0)}_{j_0-h} \neq 0$, we obtain that $m - (j_0 - h) \mid q - 1$. Because $m \nmid q - 1$, $j_0 - h \neq 0$, i.e., $\deg(R(x)) > 1$. Denote $d = m - (j_0 - h)$ and $r^{(0)}_{j_0-h} = b$. Then we have $d < m$.

Let us arrange the elements of T in a way such that the solutions of the $x^d - b = 0$ are at the beginning of list (i.e., $s_1, \ldots, s_d$ are solutions to $x^d - b = 0$) and other elements at the end $(s_{d+1}, \ldots, s_m)$. If we look at the system of equations for the coefficients of the induced polynomial in the first block

$$\begin{bmatrix} 1 & \ldots & 1 & 1 & \ldots & 1 \\ s_1 & \ldots & s_d & s_{d+1} & \ldots & s_m \\ \vdots & \ddots & & & \ddots & \vdots \\ b & \ldots & b & s^d_{d+1} & \ldots & s^d_m \\ \vdots & \ddots & & & \ddots & \vdots \\ bs_1^{j_0-h-1} & \ldots & bs_d^{j_0-h-1} & s^{m-1}_{d+1} & \ldots & s^{m-1}_m \end{bmatrix} \begin{bmatrix} s_1 - \theta(s_1) \\ \vdots \\ s_m - \theta(s_m) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a_{q-1-j_0} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Under our assumption, $d = m - j_0 + h > j_0 - h$. Subtracting the first $j_0 - h$ rows multiplied by b from the last $j_0 - h$ rows in the augmented matrix of the above system, the last $j_0 - h$ rows of the matrix become

$$\left[\begin{array}{ccccccc} 0 & \ldots & 0 & s^d_{d+1} - b & \ldots & s^d_m - b & |0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & |\vdots \\ 0 & \ldots & 0 & s^{d+(j_0-h)-1}_{d+1} - bs^{(j_0-h)-1}_{d+1} & \vdots & s^{d+(j_0-h)-1}_m - bs^{(j_0-h)-1}_m & |0 \end{array}\right],$$

which generates a homogeneous system of the equations of $m - d$ unknown variables

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_{d+1} & s_{d+2} & \ldots & s_m \\ \vdots & & \ddots & \\ s^{(j_0-h)-1}_{d+1} & s^{(j_0-h)-1}_{d+2} & \ldots & s^{(j_0-h)-1}_m \end{bmatrix} \begin{bmatrix} s^d_{d+1} - b & 0 & \ldots & 0 \\ 0 & s^d_{d+2} - b & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & \ldots & s^d_m - b \end{bmatrix} \begin{bmatrix} s_{d+1} - \theta(s_{d+1}) \\ \vdots \\ s_m - \theta(s_m) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix},$$

i.e.,

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ s_{d+1} & s_{d+2} & \ldots & s_m \\ \vdots & & \ddots & \\ s^{(j_0-h)-1}_{d+1} & s^{(j_0-h)-1}_{d+2} & \ldots & s^{(j_0-h)-1}_m \end{bmatrix} \begin{bmatrix} (s^d_{d+1} - b)(s_{d+1} - \theta(s_{d+1})) \\ \vdots \\ (s^d_m - b)(s_m - \theta(s_m)) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Because the above coefficient matrix is regular and $s^d_j \neq b$ for $j = d + 1, \ldots m$ from the assumption, we must have $\theta(s_j) = s_j$ for $j = d + 1, \ldots m$, a contradiction.

(3) Assume that $j_0 > (j_0 - h) \geq m - (j_0 - h)$. Because of (a) and $r^{(0)}_{j_0} = 0$, there exists $e \geq j_0$ such that $r^{(0)}_e = r^{(0)}_{e-1} = \ldots = r^{(0)}_{j_0} = \ldots = r^{(0)}_{(j_0-h)+1} = 0$.

But relation (d)

$$r^{(0)}_{j_0-h} r^{(0)}_{m-(t-h)} + r^{(0)}_{j_0-t} = 0, \quad t > h$$

implies that for any y such that $j_0 - h + 1 \leq y \leq e$ and $t = m + h - y > h$ we have $m - (t - h) = y$ and

$$0 = r^{(0)}_y = r^{(0)}_{j_0-(m+h-y)} = r^{(0)}_{y-(m-(j_0-h))}.$$

Using now this result in (d) with $t = 2m+2h-y-j_0$ (indeed, $t > h$ because $t-h = 2m+h-y-j_0 = (m - (j_0 - h)) + (m - y) > 0$), we obtain $m - (t - h) = j_0 - (m + h - y)$ and $r^{(0)}_{y-2(m-(j_0-h))} = r^{(0)}_{j_0-(2m+2h-y-j_0)} = r^{(0)}_{2j_0-2m-2h+y} = 0$. More generally, we have

$$r^{(0)}_e = r^{(0)}_{e-(m-(j_0-h))} = r^{(0)}_{e-2(m-(j_0-h))} = \ldots = 0,$$

$$r^{(0)}_{e-1} = r^{(0)}_{e-1-(m-(j_0-h))} = r^{(0)}_{e-1-2(m-(j_0-h))} = \ldots = 0,$$

$$\vdots$$

$$r^{(0)}_{(j_0-h)+1} = r^{(0)}_{(j_0-h)+1-(m-(j_0-h))} = r^{(0)}_{(j_0-h)+1-2(m-(j_0-h))} = \ldots = 0,$$

where indices are well defined.

Thus polynomial $P(x)$ has blocks of the coefficients of the length $d = m - (j_0 - h)$ with say l successive zeros and g successive possibly nonzero elements where $l + g = d$. Block of coefficients $r^{(0)}_e = r^{(0)}_{e-1} = \ldots = r^{(0)}_{j_0} = \ldots = r^{(0)}_{(j_0-h)+1} = 0$ is block of l zero coefficients and block $r^{(0)}_{(j_0-h)}, r^{(0)}_{(j_0-h)-1}, \ldots, r^{(0)}_{(j_0-h)-g+1}$ is block of possibly nonzero coefficients.

In relation (d), we have $r^{(0)}_{j_0-h} r^{(0)}_{m-(t-h)} + r^{(0)}_{j_0-t} = 0$ for $t > h$. Put $t = h+1$, $t = h+2$, $\ldots$, $t = h+g-1$ to obtain

$$\begin{gathered} r^{(0)}_{j_0-h} r^{(0)}_{m-1} + r^{(0)}_{j_0-h-1} = 0, \\ r^{(0)}_{j_0-h} r^{(0)}_{m-2} + r^{(0)}_{j_0-h-2} = 0, \\ \vdots \\ r^{(0)}_{j_0-h} r^{(0)}_{m-g+1} + r^{(0)}_{j_0-h-g+1} = 0, \end{gathered}$$

Similarly putting in (d) $t = j_0 - (g-1), j_0 - (g-2), \ldots, j_0$ (note that $j_0 - (g-1) > d - (g-1) > l = e - (j_0 - h) \geq j_0 - (j_0 - h) = h$), we obtain

$$\begin{gathered} r^{(0)}_{j_0-h} r^{(0)}_{m-(j_0-h)+(g-1)} + r^{(0)}_{g-1} = 0, . \\ r^{(0)}_{j_0-h} r^{(0)}_{m-(j_0-h)+(g-2)} + r^{(0)}_{g-2} = 0, \\ \vdots \\ r^{(0)}_{j_0-h} r^{(0)}_{m-(j_0-h)} + r^{(0)}_0 = 0. \end{gathered}$$

Also as $r_0^{(0)} \neq 0$ and $r_{m-(j_0-h)}^{(0)} r_{j_0-h}^{(0)} + r_0^{(0)} = 0$ it implies that $r_{m-(j_0-h)}^{(0)} \neq 0$ so that $m-(j_0-h) \neq y \pm k(m-(j_0-h))$ for any $j_0-h+1 \leq y \leq e$ and $k = 0, 1, 2, \ldots$. Thus the coefficients of the polynomial $P(x)$ at the beginning and at the end are possible non-zeros.

In particular, we show that there are exactly g nonzero coefficients at the end. Indeed, $r_{m-j_0-h}^{(0)} \neq 0$, $r_0^{(0)} \neq 0$, and $d = m-(j_0-h) = l+g$ imply that there exists one block of zero coefficients among the last $d+1$ coefficients of $P(x)$. Moreover, $r_{m-(j_0-h)-1}^{(0)} = \ldots = r_{h+1}^{(0)} = 0$ must be the block of l zero coefficients. Suppose not, this implies that $m-(j_0-h)-1-h = m-j_0-1 < l = m-(j_0-h)-g$ and thus $h > g-1$. Also this block of zero coefficients must be embedded into a block of nonzero coefficients. Hence $m-j_0-1 < g$ and $r_h^{(0)} \neq 0$. Note that $r_0^{(0)} \neq 0$, there are $h-1$ coefficients from $r_{h-1}^{(0)}$ to $r_1^{(0)}$. However, $l > h$, there are not enough coefficients which could form a block of l zero coefficients, a contradiction.

Because there are $m+1$ coefficients in $P(x)$, this implies that $m+1 = k(m-(j_0-h))+g$ for some k. Hence $m = k(m-(j_0-h))+g-1$. Note $m-(m-(j_0-h)) = j_0-h$, then we can write

$$
\begin{aligned}
\prod_{i=1}^{m}(x-s_i) \quad = \quad & x^m - r_{m-1}^{(0)}x^{m-1} - \ldots r_{m-g+1}^{(0)}x^{m-g+1} + 0 + \ldots + 0 \\
& - r_{j_0-h}^{(0)}x^{j_0-h} - r_{j_0-h-1}^{(0)}x^{j_0-h-1} - \ldots - r_{j_0-h-g+1}^{(0)}x^{j_0-h-g+1} + 0 + \ldots + 0 \\
& - r_{(j_0-h)-(m-(j_0-h))}^{(0)}x^{(j_0-h)-(m-(j_0-h))} - \ldots \\
& - r_{(j_0-h)-(g-1)-(m-(j_0-h))}^{(0)}x^{(j_0-h)-(g-1)-(m-(j_0-h))} + 0 + \ldots + 0 \\
& - r_{(j_0-h)-2(m-(j_0-h))}^{(0)}x^{(j_0-h)-2(m-(j_0-h))} - \ldots \\
& - r_{(j_0-h)-(g-1)-2(m-(j_0-h))}^{(0)}x^{(j_0-h)-(g-1)-2(m-(j_0-h))} + 0 + \ldots + 0 \\
& - \ldots \\
& - r_{(j_0-h)-(k-2)(m-(j_0-h))}^{(0)}x^{(j_0-h)-(k-2)(m-(j_0-h))} - \ldots \\
& - r_{(j_0-h)-(g-1)-(k-2)(m-(j_0-h))}^{(0)}x^{(j_0-h)-(g-1)-(k-2)(m-(j_0-h))} + 0 + \ldots + 0 \\
& - r_{g-1}^{(0)}x^{g-1} - r_{g-2}^{(0)}x^{g-2} - \ldots - r_0^{(0)}.
\end{aligned}
$$

Using again the relation (d) to the nonzero coefficients we have that $r_{j_0-h}^{(0)} r_{m-u}^{(0)} = -r_{m-u-(m-(j_0-h))}^{(0)} = -r_{j_0-h-u}^{(0)}$ for $0 \leq u \leq g-1$. Hence $r_{m-u}^{(0)} = -(r_{j_0-h}^{(0)})^{-1} r_{j_0-h)}^{(0)} = (r_{j_0-h}^{(0)})^{-2} r_{j_0-h-(m-(j_0-h))}^{(0)} = -(r_{j_0-h}^{(0)})^{-3} r_{j_0-h-2(m-(j_0-h))}^{(0)} = \ldots$.

Let $b = r_{j_0-h}^{(0)}$, finally we have

$$
\begin{aligned}
& \prod_{i=1}^{m}(x-s_i) \\
& = (x^{k(m-(j_0-h))} - bx^{(k-1)(m-(j_0-h))} + \ldots + (-b)^k)(x^{g-1} - r_{m-1}^{(0)}x^{g-2} - \ldots - r_{m-g+1}^{(0)}) \\
& := Q(x)R(x).
\end{aligned}
$$

Assume $R(x) \neq 1$, again as in the previous case if we put zeros of the $Q(x)$ first, then we can reduce the augmented matrix using rows $i, m-(j_0-h)+i, 2(m-(j_0-h))+i, \ldots, k(m-(j_0-h))+i$ for

$i = 0, 1, \ldots, g-1$ so that the last g rows (note that $j_0 > g$) have a form

$$\begin{bmatrix} 0 & \ldots & 0 & Q(s_{m-(g-1)})s_{m-(g-1)}^{m-(g-1)} & \ldots & Q(s_m)s_m^{m-(g-1)} & |0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & |\vdots \\ 0 & \ldots & 0 & Q(s_{m-(g-1)})s_{m-(g-1)}^{m} & \vdots & Q(s_m)s_m^{m} & |0 \end{bmatrix},$$

which implies that $Q(s_i) = 0$ for $i = m-(g-1), \ldots, m$, a contradiction.

Hence $R(x) = 1$. Then

$$\prod_{i=1}^{m}(x - s_i) = x^{k(m-(j_0-h))} - bx^{(k-1)(m-(j_0-h))} + \ldots + (-1)^k b^k$$

$$= x^{kd} - bx^{(k-1)d} + b^2x^{(k-2)d} - \ldots + (-1)^k b^k,$$

where $d = m - (j_0 - h)$ and $kd = m$.

CASE II: Assume $a'_{q-m-1} \neq 0$ and this is the only nonzero coefficient in the second m-block. Then the relations (b)-(d) still hold for $h = 0$. That is,

(b') $r_{j_0}^{(0)} \neq 0$,

(c') $r_{m-j_0-1}^{(0)} = \ldots = r_1^{(0)} = 0$, and

(d') $r_{j_0}^{(0)} r_{m-t}^{(0)} + r_{j_0-t}^{(0)} = 0, \quad t > 0.$

We start from the block of zeros $r_1^{(0)} = r_2^{(0)} = \ldots = r_{m-j_0-1}^{(0)} = 0$ given in relation (c'). Suppose $j_0 = 0$. Then we have $a'_{q-1} = a'_{q-1-m} = 0$. By Lemma 4, we must have $m \mid q-1$, a contradiction.

Hence $j_0 > 0$. Because $r_{j_0}^{(0)} \neq 0$, we must have $j_0 > m - j_0 - 1$ by relation (c') and thus $2j_0 - m + 1 > 0$. Taking now $t = j_0 - 1, j_0 - 2 \ldots, 2j_0 - m + 1$ (that is, $j_0 - t = 1, 2, \ldots, m - j_0 - 1$) in relation (d') we obtain the following block of zeros $r_{m-j_0+1}^{(0)} = r_{m-j_0+2}^{(0)} = \ldots = r_{2m-2j_0-1}^{(0)} = 0$. If $j_0 \neq m - j_0$, then $j_0 > 2m - 2j_0 - 1$ because $r_{j_0}^{(0)} \neq 0$. Continuing this process we can see that in the polynomial $P(x)$ we have blocks of the length $m - j_0$ with a first nonzero element and all other zeros in each block up to the leading coefficient. Note that this process must be stop after a finite number of times. In summary, we have blocks of zeros of the length $m - j_0 - 1$ and nonzero elements between them, i.e., coefficients $r_{s(m-j_0)}^{(0)}$ for $s = 1, \ldots$ are nonzero. Also $r_{j_0}^{(0)}$ is nonzero so $j_0 = s(m - j_0)$ for some $s > 0$. In (d') we take $t = 1, 2, \ldots, m - j_0 - 1$ and it follows that we have block of zeros with the length $m - j_0 - 1$ in the beginning. So coefficients $r_0^{(0)}, \ldots, r_{m-1}^{(0)}$ have blocks of the length $m - j_0$ with same distribution of the zero and nonzero elements and therefore $(m - j_0) \mid m$. Thus the polynomial $P(x)$ is of the form

$$P(x) = x^m - bx^{j_0} + b^2x^{j_0-(m-j_0)} - \ldots + (-b)^{\frac{m}{m-j_0}},$$

for some $b \in \mathbb{F}_q$. Taking $d = m - j_0$ and $m = kd$ we can write this as

$$P(x) = x^{kd} - bx^{(k-1)d} + b^2x^{(k-2)d} - \ldots + (-1)^k b^k.$$

Summarizing both cases I and II, we conclude that if there is exactly one nonzero coefficient in both first and second m-block then polynomial $P(x)$ is of the form

$$P(x) = x^{kd} - bx^{(k-1)d} + b^2x^{(k-2)d} - \ldots + (-1)^k b^k,$$

for some $b \in \mathbb{F}_q$ and $m = kd$. Finally we want to show that $(k+1)d \mid q-1$. If $k = 1$ then $P(x) = x^d - b^d$. As all solutions of $P(x) = 0$ are in $\mathbb{F}_q$ it implies that $m = d \mid q-1$, a contradiction and thus $k > 1$. In particular,

$$(x^{kd} - bx^{(k-1)d} + b^2x^{(k-2)d} - \ldots + (-1)^k b^k)(x^d - (-b)) = x^{(k+1)d} - (-b)^{k+1}.$$

Hence

$$P(x) = \frac{x^{(k+1)d} - (-b)^{k+1}}{x^d - (-b)}.$$

This means that there are at least kd distinct solutions in $\mathbb{F}_q$ for the equation $x^{(k+1)d} - (-b)^{k+1} = 0$ because these are solutions of $P(x) = 0$. In particular, this implies $b \neq 0$. Let ψ be a generator of multiplicative group $\mathbb{F}_q \setminus \{0\}$. Then $-b = \psi^u$ for some $0 \leq u < q-1$. Equation $x^{(k+1)d} = \psi^{u(k+1)}$ has solution in $\mathbb{F}_q$ of the form $x = \psi^v$ where v and l are solutions of the Diophantine equation $v(k+1)d = u(k+1) + l(q-1)$. Let $h = \gcd((k+1)d, q-1)$. Then $h \mid u(k+1)$. So we have a Diophantine equation $v\frac{(k+1)d}{h} = l\frac{q-1}{h} + \frac{u(k+1)}{h}$. If v_0 is the least nonnegative integer which satisfies the given Diophantine equation then all other solutions are of the form $v = v_0 + w\frac{q-1}{h}$ where w is integer and $v_0 < \frac{q-1}{h}$. But there are at least kd solutions of this equation in the range $0 \leq v < q-1$ for $w = 0, 1, \ldots, h-1$. This implies that $h - 1 \geq kd$. However, for $k > 1$ we have $h > kd \geq \frac{(k+1)d}{2}$ and $h \mid (k+1)d$. Hence this implies $h = (k+1)d$ and thus $(k+1)d \mid q-1$. Also $-b = \psi^u = \psi^{u_1 d} = v^d$.

Hence we proved the result with the assumption that two nonzero coefficients are in the first two m-blocks. But Lemma 2 implies that the same results holds for any two successive m-blocks. □

Proof of Lemma 8. As in Theorem 4, any polynomial which moves T and has degree $\leq q-1$ can be represented by

$$f(x) = x + h(x) \prod_{s \in \mathbb{F}_q \setminus T} (x - s) = x + h(x)(x^d + b)\frac{x^q - x}{x^{(k+1)d} - (-b)^{k+1}}$$

where $h(x)$ is polynomial with $\deg(h(x)) \leq q - 1 - |\mathbb{F}_q \setminus T| = kd - 1$ and with no zeros in T. Let $h(x) = h_0 + h_1x + \ldots + h_{kd-1}x^{kd-1}$. Define $h_j = 0$ for $j = kd, kd+1, \ldots, (k+1)d-1$. Then $\frac{x^q - x}{x^{(k+1)d} - (-b)^{k+1}} = x(x^{(k+1)d(\frac{q-1}{d(k+1)} - 1)} + \ldots + (-b)^{u(k+1)}x^{(k+1)d(\frac{q-1}{d(k+1)} - 1 - u)} + \ldots + (-b)^{(k+1)(\frac{q-1}{d(k+1)} - 1)})$ and thus

$$\begin{aligned}
h(x)\frac{x^q - x}{x^{(k+1)d} - (-b)^{k+1}} &= \sum_{i=0}^{(k+1)d-1} h_i x^i \sum_{u=0}^{\frac{q-1}{(k+1)d} - 1} (-b)^{(k+1)(\frac{q-1}{d(k+1)} - 1 - u)} x^{(k+1)du+1} \\
&= \sum_{u=0}^{\frac{q-1}{(k+1)d} - 1} \sum_{i=0}^{(k+1)d-1} h_i (-b)^{(k+1)(\frac{q-1}{d(k+1)} - 1 - u)} x^{(k+1)du+1+i} \\
&= \sum_{j=1}^{q-2} d_j x^j,
\end{aligned}$$

where we write $j - 1 = ud(k+1) + i$ with $i < d(k+1)$ and $d_j = h_i(-b)^{(\frac{q-1}{d(k+1)} - 1 - u)(k+1)}$. Finally, multiplying by $x^d + b$ gives the polynomial $f(x) - x = \sum_{j=1}^{q-1} a'_j x^j$ with coefficients $a'_j = bd_j + d_{j-d}$ where $d_j = 0$ if $j \leq 0$. We consider the coefficients a'_j according to three different ranges of i's.

First, if $j-1 = ud(k+1)+i$ where $kd > i \geq d$ then $bd_j + d_{j-d} = 0$ if and only if $bh_i + h_{i-d} = 0$.

Secondly, if $i < d$ then $j - d = ud(k+1) + i - d = (u-1)d(k+1) + dk + i$ and thus $d_{j-d} = h_{dk+i}(-b)^{(\frac{q-1}{d(k+1)}-u))(k+1)} = 0$ by the definition of h_{dk+i}. Therefore $a'_j = bd_j = 0$ if and only if $h_i = 0$.

Thirdly, if $kd \leq i < (k+1)d$ then we have that $h_i = 0$ and thus $d_j = 0$. This implies $a'_j = d_{j-d} = 0$ if and only if $h_{i-d} = 0$.

Now, using the fact that at least one of the coefficients h_i is nonzero, we show that in every block of successive coefficients $a'_{ud(k+1)+1}, \ldots, a'_{(u+1)d(k+1)}$ we have at least two nonzero coefficients. Indeed, assume $h_t \neq 0$. By the definition of $h(x)$, $0 \leq h_t \leq kd-1$. Let $j = ud(k+1)+t+1$. Note that $a'_j = bd_j + d_{j-d}$ and $a'_{j+d} = bd_{j+d} + d_j$. If both are nonzero then we have two nonzero coefficients in this block of successive coefficients.

Suppose $a'_j = 0$. Because $a'_j = bd_j + d_{j-d}$ and $d_j = h_t(-b)^{(\frac{q-1}{d(k+1)}-1-u)(k+1)} \neq 0$, we obtain that $h_{t-d} \neq 0$. If $a'_{j-d} \neq 0$, then we find one nonzero coefficient; otherwise, $a'_{j-d} = bd_{j-d} + d_{j-2d} = 0$ implies $h_{t-2d} \neq 0$. If $t-2d < d$, then this implies that $a'_{j-2d} \neq 0$. If $t-2d \geq d$, then we consider h_{t-3d} and continue this process until we find some $s_0 > 1$ such that $a'_{j-s_0 d} \neq 0$ and $t - s_0 d > 0$.

Similarly, $a'_{j+d} = 0$ implies $h_{t+d} \neq 0$. If $kd \leq t+2d$, then $a'_{j+2d} \neq 0$. Otherwise, $a'_{j+2d} = bd_{j+2d} + d_{j+d} = 0$ if and only if $bh_{t+2d} + d_{t+d} = 0$. If $a'_{j+2d} = 0$, then $h_{t+d} \neq 0$ implies that $h_{t+2d} \neq 0$. Thus we can find $s_1 > 1$ such that $a'_{j+s_1 d} \neq 0$ and $t + s_1 d < d(k+1)$ similarly.

Therefore there are at least two nonzero coefficient in every block of successive coefficients $a'_{ud(k+1)+1}$, $\ldots$, $a'_{(u+1)d(k+1)}$. In total, we have at least $2\frac{q-1}{(k+1)d}$ nonzero coefficients in $f(x)$. In particular, if $a'_1 = -1$ then in the best case we have $2\frac{q-1}{(k+1)d} - 1$ nonzero coefficients in $f(x)$. □

We remark that this best case can be achieved for $h(x) = \mu x^i((-b)^{z-1} + (-b)^{z-2}x^d + (-b)^{z-3}x^{2d} - \ldots + x^{(z-1)d})$ where $0 \leq i < d$ and $z \leq k$. Indeed, by expanding the expression of $f(x) - x$ as in the proof of Lemma 8, we can obtain that $a'_{ud(k+1)+i+1} = \mu(-b)^{k+1}(-b)^{(\frac{q-1}{d(k+1)}-u))(k+1)} \neq 0$, $a'_{ud(k+1)+sd+i+1} = 0$ for $s = 1, 2, \ldots, z-1$ and $a'_{ud(k+1)+zd+i+1} \neq 0$. In particular, if $i = 0$ then $a'_1 = \mu(-b)^{k+1+\frac{q-1}{d}}$. If $\mu(-b)^{k+1+\frac{q-1}{d}} = -1$ then we achieve this lower bound. As long as $h(x)$ does not have zeros in the set of moved elements T and thus $h(x)$ has no common roots with $P(x) = \frac{x^{(k+1)d} - (-b)^{k+1}}{x^d + b}$ which is the case that $\gcd(k+1, z) = 1$, the corresponding $f(x)$ has exactly $2\frac{q-1}{(k+1)d} - 1$ nonzero coefficients.

Next we prove that $h(x)$ does not have zeros in the set of moved elements T. Let $-b = v^d$. If $z > 1$ and $i = 0$ then

$$f(x) = x + \mu x(x^{dz} - v^{dz}) \sum_{u=0}^{\frac{q-1}{(k+1)d}-1} v^{u(k+1)d} x^{(\frac{q-1}{(k+1)d}-1-u)(k+1)d}.$$

If ψ is $(k+1)d$-th primitive root of unity in $\mathbb{F}_q$ then all moved elements are of the form $x = \psi^l v$ where $l = 1, 2 \ldots, (k+1)d$ and $(k+1) \nmid l$. However, $(\psi^l v)^{zd} = (-b)^z \psi^{lzd} \neq (-b)^z$ because $(k+1)d \nmid lzd$. Hence $h(x)$ does not have zeros in the set of moved elements T.

Since we have

$$\begin{aligned} & f(v\psi^l) \\ = \; & v\psi^l + \mu v\psi^l(v^{dz}\psi^{ldz} - v^{dz})v^{(\frac{q-1}{(k+1)d}-1)(k+1)d} \sum_{u=0}^{\frac{q-1}{(k+1)d}-1} \psi^{u(k+1)d} \\ = \; & v\psi^l + \mu v\psi^l(v^{dz}\psi^{ldz} - v^{dz})v^{(\frac{q-1}{(k+1)d}-1)(k+1)d} \frac{q-1}{(k+1)d} \\ = \; & v\psi^l + v\psi^l(\mu \frac{q-1}{(k+1)d} v^{q-1-(k+1)d+dz})\psi^{ldz} - v\psi^l(\mu \frac{q-1}{(k+1)d} v^{q-1-(k+1)d+dz}), \end{aligned}$$

we can choose μ such that $\mu \frac{q-1}{(k+1)d} v^{q-1-(k+1)d+dz} = 1$. Then we have

$$f(v\psi^l) = c\psi^l + v\psi^{l(dz+1)} - v\psi^l = v\psi^{l(dz+1)}.$$

This mapping induces a permutation if $\gcd(k+1, dz+1) = 1$. Hence in this case we have permutation polynomials with minimal number of nonzero coefficients. The similar results hold for $z = 1$.

Finally we note that polynomials in Theorem 2 are of the form $f(x) = x + \mu \frac{x^q - x}{x^m - z^m}$.

Conclusions

In many applications we want to have polynomials with small number of nonzero coefficients (sparse polynomials). For examples, sparse irreducible polynomials are important in efficient hardware implementation of feedback shift registers and finite field arithmetic ([1], [9], [22]). In this paper we show how to obtain such polynomials for a given set of moved elements. In particular, some classes of polynomials with small number of nonzero coefficients are studied. Moreover, using Lemma 6 and Corollary 1 we can combine these mappings to construct polynomials with bigger sets of moved elements and similar property.

References

[1] E. R. Berlekamp, Bit-serial Reed-Solomon encoders, *IEEE Trans. Info. Theory* **28** (1982), 869-874.

[2] C.-Y. Chao, Polynomials over finite fields which commute with a permutation polynomial, *J. Algebra* **163** (1994), 295-311.

[3] S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields Appl.* **11** (2005), no. 3, 337357.

[4] S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.* **12** (2006), no. 3, 425491.

[5] S. D Cohen and M. Preern, The Hansen-Mullen primitive conjecture: completion of proof, *Number theory and polynomials*, 89120, London Math. Soc. Lecture Note Ser., 352, Cambridge Univ. Press, Cambridge, 2008.

[6] S. Fan, W. Han, and K. Feng, Primitive normal polynomials with multiple coefficients prescribed:An asymptotic result, *Finite Fields Appl.* 13 (2007), 1029-1044.

[7] T. Garefalakis, Irreducible polynomials with consecutive zero coefficients, *Finite Fields Appl.* **14** (2008), no. 1, 201208.

[8] J. von zur Gathen and J. Gerhard, Modern computer algebra, Cambridge University Press, New York, 1999. xiv+753 pp.

[9] S. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.

[10] S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree II, *Finite Fields Appl.* **12** (2006), 26-37.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[12] C. Malvenuto and F. Pappalardi, Enumerating permutation polynomials II: k-cycles with minimal degree, *Finite Field Appl.* **10** (2004), 72-96.

[13] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Artith*, **132** (2008), 329-350.

[14] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields and Their Applications*, **14** (2008), 798-815.

[15] G. L. Mullen, *Permutation polynomials over finite fields*, in: Finite fields, Coding Theory, and Advances in Communication and Computing, Las Vegas, NY, 1991, pp. 131-151.

[16] G. L. Mullen and B. G. Vioreanu, Explicit Formulas for Permutation Polynomials over Finite Fields, *Bulletin of the Institute of Combinatorics and its Applications* **57** (2009), 99-106.

[17] A. Muratović-Ribić, A note on the coefficients of inverse polynomials, *Finite Fields Appl.* **13** (2007), no. 4, 977-980.

[18] B. Omidi Koma, D. Panario, and Q. Wang, The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms, *Discrete Math.* **310** (2010), no. 8, 12821292.

[19] V. Shoup, Factoring polynomials over finite fields: asymptotic complexity vs. reality, *Proc. IMACS Symp. on Symbolic Computation, New Trends and Developments*, Lille, France, 1993. 124-129.

[20] D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.*, **66** (1997), 1195-1212.

[21] Q. Wang, On inverse permutation polynomial, *Finite Fields Appl.* **15** (2009), no. 2, 207–213.

[22] M. Wang and I. F. Blake, Bit-serial multiplication in finite fields, *IEEE Trans. Comput.* **38** (1989), 1457-1460.

[23] C. Wells, The degree of permutation polynomials over finite fields, J. Combinatorial Theory **7** (1969), 49-55.

[24] J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields and Their Applications*, **12** (2006), 211-221.

[25] J. L. Yucas and G. L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, *Discrete Mathematics*, **274** (2004), 265-279.