FROBENIUS MATRICES AND A VARIANT OF
ZOLOTAREV’S THEOREM

HAI-LIANG WU AND LI-YUAN WANG

Abstract. In this paper, with the help of the theory of matrices and finite fields we generalize Zolotarev’s theorem to an arbitrary finite dimensional vector space over $\mathbb{F}_q$, where $\mathbb{F}_q$ denotes the finite field with $q$ elements.

1. Introduction

Investigating permutations over a finite set is a classical topic in number theory and combinatorics. In particular, the signs of permutations have been extensively investigated. Recall that a permutation $\sigma$ is called even (respectively odd) if it is a product of an even (respectively odd) number of transpositions. We define $\text{sign}(\sigma) = 1$ if $\sigma$ is even and $\text{sign}(\sigma) = -1$ if $\sigma$ is odd.

Let $p$ be an odd prime, and let $a$ be an integer with $p \nmid a$. Clearly the sequence

$$0 \mod p, a \times 1 \mod p, \cdots, a \times (p - 1) \mod p$$

is a permutation $\pi_p$ of the sequence

$$0 \mod p, 1 \mod p, \cdots, (p - 1) \mod p.$$

The well-known Zolotarev’s theorem [3] states that $\text{sign}(\pi_p)$ coincides with the Legendre symbol $(\frac{a}{p})$. Later many mathematicians investigated various variants of Zolotarev’s theorem. For example, Let $n$ be a positive odd integer, and let $b$ be an integer relatively prime to $n$. Then Frobenius (cf. [1]) proved that the Jacobi symbol $(\frac{b}{n})$ is the sign of the permutation of $\mathbb{Z}/n\mathbb{Z} = \{0 \mod n, \cdots, n - 1 \mod n\}$ induced by multiplication by $b \mod n$. Finally, Lerch [2] generalized the above results and he obtained the following theorem:

Theorem 1.1. (Lerch) Let $n$ be any positive integer, and let $c$ be an integer relatively prime to $n$. Let $\pi_c$ be a permutation of $\mathbb{Z}/n\mathbb{Z}$ induced by

\[\text{2020 Mathematics Subject Classification. Primary 05A05; Secondary 11C20, 15B33.}\]

\[\text{Keywords. Zolotarev’s lemma, permutations, finite fields.}\]

\[\text{Supported by the National Natural Science Foundation of China (Grant No. 11971222).}\]
multiplication by \( c \mod n \). Then we have

\[
\text{sign}(\pi_c) = \begin{cases} 
\left(\frac{c}{n}\right) 
& \text{if } n \text{ is odd}, \\
1 
& \text{if } n \equiv 2 \pmod{4}, \\
(-1)^{\frac{n-1}{2}} 
& \text{if } n \equiv 0 \pmod{4}.
\end{cases}
\]

Motivated by the above work, in this paper we shall study a new variant of Zolotarev’s theorem. We first introduce some notations. Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, and let \( n \) be a positive integer. Let \( \mathbb{F}_n^q := \{ x = (x_1, x_2, \cdots, x_n)^T : x_i \in \mathbb{F}_q \} \) be the \( n \)-dimensional vector space over \( \mathbb{F}_q \), where \( M^T \) denotes the transpose of the matrix \( M \). We also let \( \mathbb{M}_n(\mathbb{F}_q) \) be the set of all \( n \times n \) matrices with entries in \( \mathbb{F}_q \), and let \( \mathbb{M}_n(\mathbb{F}_q)^\times := \{ M \in \mathbb{M}_n(\mathbb{F}_q) : M \text{ is invertible} \} \).

Then given any \( A \in \mathbb{M}_n(\mathbb{F}_q)^\times \), the bijection: 

\[
x \rightarrow Ax
\]

induces a permutation \( \tau(A) \) of \( \mathbb{F}_n^q \). To show that this permutation is indeed an extension of the above permutations, we briefly study the following special case. Let \( p \) be an odd prime, and let \( a \) be an integer relatively prime to \( p \). Suppose that \( A \) is the scalar matrix:

\[
A = \begin{bmatrix} a & a & \cdots & a \\
               & a & \cdots & a \\
               &   & \ddots & \vdots \\
               &   &       & a 
\end{bmatrix}
\]

We shall later show that

\[
\text{sign}(\tau(A)) = \left(\frac{a}{p}\right)^n = \left(\frac{\det A}{p}\right).
\]

In view of the above, we see that the permutation induced by multiplication by \( A \) is a natural extension of the permutations investigated by Zolotarev, Frobenius and Lerch. We assume that the characteristic of \( \mathbb{F}_q \) is greater than 2. Let \( \widehat{\mathbb{F}}_q^\times \) denote the group of all multiplicity characters over \( \mathbb{F}_p^\times \), and let \( \chi \) be the quadratic character in \( \widehat{\mathbb{F}}_q^\times \). Now we state our main result.

**Theorem 1.2.** Suppose that the characteristic of \( \mathbb{F}_q \) is greater than 2. Then for any \( A \in \mathbb{M}_n(\mathbb{F}_q)^\times \) we have

\[
\text{sign}(\tau(A)) = \chi(\det A).
\]

To make the above result more accessible, we introduce the following example. When \( \mathbb{F}_q = \mathbb{F}_3 \) and \( n = 2 \), we let \( A = \begin{bmatrix} 1 & -1 \\
                             1 & 1 \end{bmatrix} \). Let the sequence

\[
x_1, x_2, \cdots, x_9 = \begin{bmatrix} -1 \\
                       -1 \end{bmatrix}, \begin{bmatrix} -1 \\
                       0 \end{bmatrix}, \begin{bmatrix} -1 \\
                       1 \end{bmatrix}, \begin{bmatrix} 0 \\
                       -1 \end{bmatrix}, \begin{bmatrix} 0 \\
                       0 \end{bmatrix}, \begin{bmatrix} 1 \\
                       -1 \end{bmatrix}, \begin{bmatrix} 1 \\
                       0 \end{bmatrix}, \begin{bmatrix} 1 \\
                       1 \end{bmatrix}.
\]

By computation we can verify that the sequence

\[
Ax_1, Ax_2, \cdots, Ax_9
\]
is equal to
\[ x_6, x_1, x_8, x_7, x_5, x_3, x_2, x_9, x_4. \]
Now it is easy to see that \( \text{sign}(\tau(A)) = \left( \frac{2}{3} \right) = -1 \). We will prove our main result in Section 2.

2. PROOF OF THE MAIN RESULT

Throughout this section, we assume that the characteristic of \( \mathbb{F}_q \) is greater than 2. Let \( \hat{\mathbb{F}}^\times_q \) denote the group of all multiplicity characters over \( \mathbb{F}_p^\times \), and let \( \chi \) be the quadratic character in \( \hat{\mathbb{F}}^\times_q \). We also let \( I_n \) denote the \( n \times n \) identity matrix.

We first consider diagonal matrices.

**Lemma 2.1.** Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and let \( n \) be a positive integer. Then for any invertible diagonal matrix \( D \in M_n(\mathbb{F}_q) \) we have
\[ \text{sign}(\tau(D)) = \chi(\det D). \]

**Proof.** We first consider the case
\[ D_a = \begin{bmatrix} a & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 1 \end{bmatrix}, \]
where \( a \in \mathbb{F}_q^\times \). Given any \( (x_2, x_3, \ldots, x_n)^T \in \mathbb{F}_q^{n-1} \), we set
\[ C_{x_2,x_3,\ldots,x_n} := \{(x, x_2, x_3, \ldots, x_n)^T : x \in \mathbb{F}_q\}. \]
It is easy to see that \( \tau(D_a) \) can be factored into permutations on each \( C_{x_2,x_3,\ldots,x_n} \). Similar to Zolotarev’s theorem, it is easy to see that
\[ \text{sign}(\tau(D_a) |_{C_{x_2,x_3,\ldots,x_n}}) = \chi(a). \]
Hence
\[ \text{sign}(\tau(D_a)) = \prod_{C_{x_2,x_3,\ldots,x_n}} \text{sign}(\tau(D_a) |_{C_{x_2,x_3,\ldots,x_n}}) = \chi(a)^{n-1} = \chi(a). \quad (2.1) \]

Now for any diagonal matrix \( D \in M_n(\mathbb{F}_q) \) of the form
\[ \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix} = \begin{bmatrix} \lambda_1 & 1 & & \\ 1 & 1 & & \\ & \ddots & \ddots & \\ & & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ & \ddots \\ & & \lambda_n \end{bmatrix}, \]
it is easy to see that
\[ \text{sign}(\tau(D)) = \chi(\lambda_1) \cdots \chi(\lambda_n) = \chi(\det D). \]
This completes the proof. \( \square \)

We also need the following result.
Lemma 2.2. For any \(1 \leq i < j \leq n\), let \(I_{ij}\) be the elementary matrix obtained from the identity matrix \(I_n\) by switching \(i\)-th row and \(j\)-th row. Then we have
\[
\text{sign}(\tau(I_{ij})) = \chi(-1).
\]

Proof. For any \(1 \leq i < j \leq n\), we set
\[
C_{ij} := \{(x_1, \ldots, x_n)^T \in \mathbb{F}_q^n : x_i = x_j\},
\]
and
\[
D_{ij} := \{(x_1, \ldots, x_n)^T \in \mathbb{F}_q^n : x_i \neq x_j\}.
\]
Clearly \(\tau(I_{ij})|_{C_{ij}}\) is identity and \(\tau(I_{ij})|_{D_{ij}}\) is a product of \((q^n - q^{n-1})/2\) transpositions. Hence we have
\[
\text{sign}(I_{ij}) = (-1)^{\frac{q^n - q^{n-1}}{2}} = \chi(-1).
\]
This completes the proof. \(\square\)

Let \(g(t) = t^m + a_1 t^{m-1} + \cdots + a_m \in \mathbb{F}_q[t]\). Then the Frobenius matrix \(N_g\) with respect to \(g(t)\) is an \(m \times m\) matrix defined by
\[
N_g := \begin{bmatrix}
0 & 0 & \cdots & 0 & -a_m \\
1 & 0 & \cdots & 0 & -a_{m-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -a_1
\end{bmatrix}.
\]

We need the following result concerning the rational canonical form of a matrix.

Lemma 2.3. Let \(M \in M_n(\mathbb{F}_q)\), and let \(f_\chi(t)\) be the characteristic polynomial of \(M\). Suppose that \(f_\chi(t) = p_1(t)^{e_1} \cdots p_r(t)^{e_r}\) with \(e_1, \ldots, e_r\) positive integers and \(p_1, \ldots, p_r\) distinct monic irreducible polynomials over \(\mathbb{F}_q\). Then there exists a matrix \(T \in M_n(\mathbb{F}_q)^*\) such that
\[
TMT^{-1} = \begin{bmatrix}
L_1 & & \\
& L_2 & \\
& & \ddots \\
& & & L_r
\end{bmatrix},
\]
where
\[
L_i = \begin{bmatrix}
N_{p_1} & & \\
& N_{p_1} & \\
& & \ddots \\
& & & N_{p_1}
\end{bmatrix}.
\]
We also call this form the rational canonical form of \(A\).

We now consider the Frobenius matrices.

Lemma 2.4. Let \(g(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{F}_q[t]\) with \(a_n \neq 0\), and let \(N(g)\) be the Frobenius matrix with respect to \(g\). Then we have
\[
\text{sign}(\tau(N_g)) = \chi(\det N_g).
\]
Proof. One can verify that
\[ \tau(N_g) = \tau(A_3) \circ \tau(A_2) \circ \tau(A_1), \]
where
\[
A_1 = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ -a_{n-1} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & 0 & \cdots & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} a_n \\ 1 \\ \vdots \\ \vdots \end{bmatrix}.
\]
By Lemma 2.1 we have \( \text{sign}(\tau(A_3)) = \chi(a_n) = \chi(\det A_3) \). Noting that
\[ A_1 = I_{12}I_{13} \cdots I_{1n}, \]
by Lemma 2.2 we obtain
\[ \text{sign}(\tau(A_1)) = \chi(-1)^n = \chi(\det A_1). \]
Note that the dimension of subspace \( V = \{ x \in \mathbb{F}_q^n : A_2x = x \} \) is \( n - 1 \) and \( A_2^2 = I \). Hence \( \tau(A_2) \) is a product of \( (q^n - q^{n-1})/2 \) transpositions. Hence \( \text{sign}(\tau(A_2)) = (-1)^{\frac{q^n-q^{n-1}}{2}} = \chi(-1) = \chi(\det A_2) \). Then our desired result follows from \( \det N_g = \det A_1 \cdot \det A_2 \cdot \det A_3 \).

We are now in a position to prove our main result.

**Proof of Theorem 1.2.** We first consider case
\[
P = \begin{bmatrix} L & I \\ \vdots & \vdots \\ & \vdots \\ & & I \end{bmatrix},
\]
where
\[
L = \begin{bmatrix} N_g & I \\ \vdots & \vdots \end{bmatrix},
\]
and \( N_g \) is the Frobenius matrix with respect to the monic polynomial \( g(t) \). By Lemma 2.4 it is easy to see that \( \text{sign}(\tau(P)) = \chi(\det N_g) \). Now by Lemma 2.3 we see that there is an invertible matrix \( T \) such that \( TAT^{-1} \) is of the rational canonical form. In view of the above, one can verify that
\[ \text{sign}(\tau(A)) = \chi(\det A). \]
This completes the proof.
References

[1] A. Brunyate, P.L. Clark, Extending the Zolotarev-Frobenius approach to quadratic reciprocity, Ramamujan J. 37 (2015) 25–50.
[2] M. Lerch, Sur un théorème de Zolotarev, Bull. Intern. de l’Acad. François Joseph 3 (1896), 34–37.
[3] G. Zolotarev, Nouvelle déonstration de la loi de réciprocité de Legendre, Nouvelles Ann. Math. 11 (1872), 354–362.

(Hai-Liang Wu) School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, People’s Republic of China
Email address: whl.math@smail.nju.edu.cn

(Li-Yuan Wang) School of Physical and Mathematical Sciences, Nanjing Tech University, Nanjing 211816, People’s Republic of China
Email address: wly@smail.nju.edu.cn