Bull. Aust. Math. Soc. (First published online 2024), page 1 of 7*
doi:10.1017/S0004972724000765
*Provisional—final page numbers to be inserted when paper edition is published

A CONJECTURE OF ZHI-WEI SUN ON MATRICES CONCERNING MULTIPLICATIVE SUBGROUPS OF FINITE FIELDS

JIE LI and HAI-LIANG WU✉

(Received 15 May 2024; accepted 13 July 2024)

Abstract

Motivated by the recent work of Zhi-Wei Sun ['Problems and results on determinants involving Legendre symbols', Preprint, arXiv:2405.03626], we study some matrices concerning subgroups of finite fields. For example, let $q \equiv 3 \pmod 4$ be an odd prime power and let ϕ be the unique quadratic multiplicative character of the finite field $\mathbb{F}_q$. If the set $\{s_1, \ldots, s_{(q-1)/2}\} = \{x^2 : x \in \mathbb{F}_q \setminus \{0\}\}$, then we prove that

$$\det[t + \phi(s_i + s_j) + \phi(s_i - s_j)]_{1 \le i,j \le (q-1)/2} = \left(\frac{q-1}{2}t - 1\right)q^{(q-3)/4}.$$

This confirms a conjecture of Zhi-Wei Sun.

2020 *Mathematics subject classification*: primary 11T24; secondary 11R18, 12E20, 15A15.

Keywords and phrases: Legendre symbols, finite fields, cyclotomic matrices, determinants.

1. Introduction

Let p be an odd prime. Research on determinants involving the Legendre symbol $(\frac{\cdot}{p})$ can be traced back to Lehmer [4], Carlitz [1] and Chapman [2]. For example, Carlitz [1, Theorem 4] studied the determinant

$$\det C(t) := \det\left[t + \left(\frac{i-j}{p}\right)\right]_{1 \le i,j \le p-1}$$

and showed that

$$\det C(t) = (-1)^{(p-1)/2} p^{(p-3)/2}((p-1)t + (-1)^{(p-1)/2}).$$

Chapman [2] investigated some variants of $\det C(t)$. For instance, Chapman considered

$$\det C_1(t) := \det\left[t + \left(\frac{i+j-1}{p}\right)\right]_{1 \le i,j \le (p-1)/2}.$$

This work was supported by the Natural Science Foundation of China (Grant No. 12101321).
© The Author(s), 2024. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

If we let $\varepsilon_p > 1$ and h_p be the fundamental unit and the class number of $\mathbb{Q}(\sqrt{p})$, respectively, then Chapman [2] proved that

$$\det C_1(t) = \begin{cases} (-1)^{(p-1)/4} 2^{(p-1)/2}(-a_p t + b_p) & \text{if } p \equiv 1 \pmod 4, \\ -2^{(p-1)/2} t & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $a_p, b_p \in \mathbb{Q}$ are defined by the equality

$$\varepsilon_p^{h_p} = a_p + b_p\sqrt{p}.$$

In 2019, Sun [5] initiated the study of determinants involving the Legendre symbol and binary quadratic forms. For example, Sun considered the determinant

$$\det S_p := \det\left[\left(\frac{i^2+j^2}{p}\right)\right]_{1\le i,j\le (p-1)/2}.$$

Sun [5, Theorem 1.2] showed that $-\det S_p$ is always a quadratic residue modulo p. See also [3, 7] for recent work on this topic.

Recently, Sun [6] posed many interesting conjectures on determinants related to the Legendre symbol. We give one example.

CONJECTURE 1.1 (Sun; [6, Conjecture 1.1]). Let $p \equiv 3 \pmod 4$ be a prime. Then,

$$\det\left[t + \left(\frac{i^2+j^2}{p}\right) + \left(\frac{i^2-j^2}{p}\right)\right]_{1\le i,j\le (p-1)/2} = \left(\frac{p-1}{2}t - 1\right)p^{(p-3)/4}.$$

Motivated by these results, we will study some determinants involving the quadratic multiplicative character of a finite field. We first introduce some notation.

Let $q = p^s$ be an odd prime power with p prime and $s \in \mathbb{Z}^+$ and let $\mathbb{F}_q$ be the finite field of q elements. Let $\mathbb{F}_q^\times$ be the cyclic group of all nonzero elements of $\mathbb{F}_q$. For any positive integer k which divides $q-1$, let

$$D_k := \{a_1, a_2, \ldots, a_{(q-1)/k}\} = \{x^k : \ x \in \mathbb{F}_q^\times\}$$

be the subgroup of all nonzero kth powers in $\mathbb{F}_q$.

Let $\widehat{\mathbb{F}_q^\times}$ be the cyclic group of all multiplicative characters of $\mathbb{F}_q$. Throughout this paper, for any $\psi \in \widehat{\mathbb{F}_q^\times}$, we extend ψ to $\mathbb{F}_q$ by setting $\psi(0) = 0$. Also, if $2 \nmid q$, we use the symbol ϕ to denote the unique quadratic multiplicative character of $\mathbb{F}_q$, that is,

$$\phi(x) = \begin{cases} 1 & \text{if } x \in D_2, \\ 0 & \text{if } x = 0, \\ -1 & \text{otherwise.} \end{cases}$$

Inspired by the above results, we define the matrix $A_k(t)$ by

$$A_k(t) := [t + \phi(a_i + a_j) + \phi(a_i - a_j)]_{1\le i,j\le (q-1)/k}.$$

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

The integers c_k and d_k, which are related to the number of $\mathbb{F}_q$-rational points of certain hyperelliptic curves over $\mathbb{F}_q$, are defined by

$$|\{\infty\} \cup \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : \ y^2 = x^k + 1\}| = q + 1 - c_k \tag{1.1}$$

and

$$|\{\infty\} \cup \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : \ y^2 = x^k - 1\}| = q + 1 - d_k. \tag{1.2}$$

Now we state the main results of this paper.

THEOREM 1.2. *Let $q = p^s$ be an odd prime power with p prime and $s \in \mathbb{Z}^+$. Then, for any positive integer k which divides $q-1$, the following results hold.*

(i) *Suppose $q \equiv 1 \pmod{2k}$. Then $\det A_k(t) = 0$. In particular, if $q \equiv 1 \pmod 4$, then $\det A_2(t) = 0$.*

(ii) *If $q \equiv 3 \pmod 4$, then*

$$\det A_2(t) = \left(\frac{q-1}{2}t - 1\right)q^{(q-3)/4}.$$

(iii) *Suppose $q \equiv 1 \pmod 4$ and $q \not\equiv 1 \pmod{2k}$. Then there is an integer u_k such that*

$$\det A_k(t) = \left(\frac{q-1}{k}t - \frac{1}{k}(c_k + d_k + 2)\right) \cdot u_k^2.$$

REMARK 1.3. (i) Theorem 1.2(i) generalises [6, Theorem 1.1] to an arbitrary finite field with odd characteristic. In the case where $q = p$ is an odd prime, Theorem 1.2(ii) confirms Conjecture 1.1 posed by Zhi-Wei Sun.

(ii) For any k with $3 \le k < q-1$, $k \mid q-1$ and $q - 1 \not\equiv 0 \pmod{2k}$, we can also obtain the explicit value of $\det A_k(t)$. However, finding a simple expression for $\det A_k(t)$ seems very difficult.

We will prove our main results in Section 2.

2. Proof of Theorem 1.2

Throughout this section, we let χ be a generator of $\widehat{\mathbb{F}_q^\times}$. Also, for any $\chi^i, \chi^j \in \widehat{\mathbb{F}_q^\times}$, the Jacobi sum of χ^i and χ^j is defined by

$$J(\chi^i, \chi^j) = \sum_{x \in \mathbb{F}_q} \chi^i(x)\chi^j(1-x).$$

We begin with a known result in linear algebra.

LEMMA 2.1. *Let n be a positive integer and let M be an $n \times n$ complex matrix. Let $\lambda_1, \dots, \lambda_n \in \mathbb{C}$, and let $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{C}^n$ be column vectors. Suppose that*

$$M\mathbf{v}_i = \lambda_i \mathbf{v}_i$$

for $1 \le i \le n$ and that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent over $\mathbb{C}$. Then $\lambda_1, \dots, \lambda_n$ are exactly all the eigenvalues of M (counting multiplicity).

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

Before the proof of our main results, we first introduce the definition of circulant matrices. Let R be a commutative ring and let $b_0, b_1, \ldots, b_{n-1} \in R$. Then the circulant matrix of the tuple $(b_0, b_1, \ldots, b_{n-1})$ is defined by

$$C(b_0, b_1, \ldots, b_{n-1}) := [b_{i-j}]_{0\le i,j\le n-1},$$

where the indices are cyclic modulo n.

The second author [7, Lemma 3.4] proved the following result.

LEMMA 2.2. *Let $n \ge 1$ be an odd integer. Let R be a commutative ring and let $b_0, \ldots, b_{n-1} \in R$ such that $b_i = b_{n-i}$ for $1 \le i \le n-1$. Then there is an element $u \in R$ such that*

$$\det C(b_0, b_1, \ldots, b_{n-1}) = \Big(\sum_{i=0}^{n-1} b_i\Big)u^2.$$

Now we are in a position to prove our main results. For simplicity, we set $n = (q-1)/k$.

PROOF OF THEOREM 1.2. (i) Suppose $q - 1 \equiv 0 \pmod{2k}$. Let $\xi_{2k} \in \mathbb{F}_q$ be a primitive $2k$th root of unity. Then $-1 = \xi_{2k}^k \in D_k$. Thus, for any j with $1 \le j \le n$, there exists an integer j' with $1 \le j' \le n$ such that $a_{j'} = -a_j$ and $j \ne j'$. This implies that the jth column of $A_k(t)$ is the same as the j'th column of $A_k(t)$ and hence $\det A_k(t) = 0$.

(ii) Suppose now $q - 1 \not\equiv 0 \pmod{2k}$. Then, clearly k is even. For any integers m, n with $0 \le m \le n-1$ and $1 \le i \le n$,

$$\begin{aligned}\sum_{1\le j\le n} (\phi(a_i + a_j) + \phi(a_i - a_j))\chi^m(a_j) &= \sum_{1\le j\le n} \Big(\phi\Big(1 + \frac{a_j}{a_i}\Big) + \phi\Big(1 - \frac{a_j}{a_i}\Big)\Big)\chi^m\Big(\frac{a_j}{a_i}\Big)\chi^m(a_i)\\ &= \sum_{1\le j\le n} (\phi(1 + a_j) + \phi(1 - a_j))\chi^m(a_j)\chi^m(a_i).\end{aligned}$$

Let

$$\mathbf{v}_m = (\chi^m(a_1), \chi^m(a_2), \ldots, \chi^m(a_n))^T \quad \text{and} \quad \lambda_m = \sum_{1\le j\le n} (\phi(1 + a_j) + \phi(1 - a_j))\chi^m(a_j).$$

By the above results,

$$A_k(0)\mathbf{v}_m = \lambda_m \mathbf{v}_m \quad \text{for } 0 \le m \le n-1.$$

Since

$$\det[\chi^i(a_j)]_{0\le i\le n-1, 1\le j\le n} = \prod_{1\le i<j\le n} (\chi(a_j) - \chi(a_i)) \ne 0,$$

the vectors $\mathbf{v}_0, \ldots, \mathbf{v}_{n-1}$ are linearly independent over $\mathbb{C}$ and hence by Lemma 2.1, the complex numbers $\lambda_0, \ldots, \lambda_{n-1}$ are exactly all the eigenvalues of $A_k(0)$.

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

Now let $k = 2$. Then clearly $q \equiv 3 \pmod 4$ and n is odd in this case. We first evaluate $\det A_2(0)$. By the above,

$$\det A_2(0) = \lambda_0 \prod_{1\le m\le n-1} \lambda_m = \lambda_0 \prod_{1\le m\le (n-1)/2} |\lambda_{2m}|^2. \tag{2.1}$$

The last equality follows from $\overline{\lambda_m} = \lambda_{n-m}$ for $1 \le m \le n-1$. For λ_0,

$$\lambda_0 = \sum_{1\le j\le n} (\phi(1+a_j) + \phi(1-a_j)) = \frac{1}{2}\sum_{x\in\mathbb{F}_q^\times} \phi(1+x^2) - \frac{1}{2}\sum_{x\in\mathbb{F}_q^\times} \phi(x^2-1) = -1. \tag{2.2}$$

The last equality follows from

$$\sum_{x\in\mathbb{F}_q} \phi(x^2 \pm 1) = -1.$$

For λ_{2m} with $1 \le m \le (n-1)/2$, one can verify that

$$\begin{aligned}
\lambda_{2m} &= \sum_{1\le j\le n} (\phi(1+a_j) + \phi(1-a_j))\chi^{2m}(a_j) \\
&= \frac{1}{2}\sum_{x\in\mathbb{F}_q} \phi(1+x^2)\chi^{2m}(x^2) + \frac{1}{2}\sum_{x\in\mathbb{F}_q} \phi(1-x^2)\chi^{2m}(-x^2) \\
&= \sum_{x\in\mathbb{F}_q} \phi(1+x)\chi^{2m}(x) \\
&= \sum_{x\in\mathbb{F}_q} \phi(1+x)\chi^{2m}(-x) = J(\phi,\chi^{2m}).
\end{aligned} \tag{2.3}$$

Combining (2.2) and (2.3) with (2.1),

$$\det A_2(0) = -\prod_{1\le m\le (n-1)/2} |J(\phi,\chi^{2m})|^2 = -q^{(q-3)/4}.$$

Now we turn to $\det A_2(t)$. By (2.2) for $1 \le j \le n$,

$$\begin{aligned}
\sum_{1\le i\le n} (t + \phi(a_i+a_j) + \phi(a_i-a_j)) &= nt + \sum_{1\le i\le n} (\phi(1+a_j/a_i) + \phi(1-a_j/a_i)) \\
&= nt + \sum_{1\le i\le n} (\phi(1+a_i) + \phi(1-a_i)) \\
&= nt - 1.
\end{aligned}$$

This implies that $(nt-1) \mid \det A_2(t)$. Noting that $\det A_2(t) \in \mathbb{Z}[t]$ with degree ≤ 1,

$$\det A_2(t) = -\det A_2(0)\cdot(nt-1) = q^{(q-3)/4}\Big(\frac{q-1}{2}t - 1\Big).$$

(iii) Suppose $q \equiv 1 \pmod 4$ and $q \not\equiv 1 \pmod{2k}$. Clearly, $k \equiv 0 \pmod 2$ in this case. Let $g \in \mathbb{F}_q$ be a generator of the cyclic group $\mathbb{F}_q^\times$. Then one can verify that

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

$$\begin{aligned}\det A_k(t) &= \det[t+\phi(a_i+a_j)+\phi(a_i-a_j)]_{1\le i,j\le n}\\ &= \det[t+\phi(g^{k(i-j)}+1)+\phi(g^{k(i-j)}-1)]_{0\le i,j\le n-1}.\end{aligned}$$

For $0 \le i \le n-1$, let

$$b_i = t+\phi(g^{ki}+1)+\phi(g^{ki}-1).$$

Then one can easily verify that

$$\det A_k(t) = \det C(b_0, b_1, \dots, b_{n-1})$$

and that $b_i = b_{n-i}$ for $1 \le i \le n-1$. Now applying Lemma 2.2, we see that there is an element $u_k \in \mathbb{Z}[t]$ such that

$$\det A_k(t) = \Big(\sum_{i=0}^{n-1} b_i\Big)\cdot u_k^2.$$

One can verify that

$$\begin{aligned}\sum_{i=0}^{n-1} b_i &= nt + \sum_{1\le j\le n}(\phi(a_i+1)+\phi(a_i-1))\\ &= nt + \frac{1}{k}\sum_{x\in\mathbb{F}_q^\times}(\phi(x^k+1)+\phi(x^k-1))\\ &= nt - \frac{1}{k}(c_k+d_k+2),\end{aligned}$$

where c_k and d_k are defined by (1.1) and (1.2), and the last equality follows from

$$\sum_{x\in\mathbb{F}_q^\times}\phi(x^k+1) = -c_k-1 \quad\text{and}\quad \sum_{x\in\mathbb{F}_q^\times}\phi(x^k-1) = -d_k-1.$$

As $\det A_k(t) \in \mathbb{Z}[t]$ with degree ≤ 1, by the above, we see that $u_k \in \mathbb{Z}$. Hence,

$$\det A_k(t) = \Big(\frac{q-1}{k}t - \frac{1}{k}(c_k+d_k+2)\Big)\cdot u_k^2.$$

In view of the above, we have completed the proof of Theorem 1.2. □

Acknowledgement

The authors would like to thank the referee for helpful comments.

References

[1] L. Carlitz, 'Some cyclotomic matrices', *Acta Arith.* **5** (1959), 293–308.
[2] R. Chapman, 'Determinants of Legendre symbol matrices', *Acta Arith.* **115** (2004), 231–244.
[3] D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, 'On some determinants involving Jacobi symbols', *Finite Fields Appl.* **64** (2020), Article no. 101672.
[4] D. H. Lehmer, 'On certain character matrices', *Pacific J. Math.* **6** (1956), 491–499.

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press

[5] Z.-W. Sun, 'On some determinants with Legendre symbols entries', *Finite Fields Appl.* **56** (2019), 285–307.
[6] Z.-W. Sun, 'Problems and results on determinants involving Legendre symbols', Preprint, 2024, arXiv:2405.03626.
[7] H.-L. Wu, 'Elliptic curves over F_p and determinants of Legendre matrices', *Finite Fields Appl.* **76** (2021), Article no. 101929.

JIE LI, School of Science,
Nanjing University of Posts and Telecommunications,
Nanjing 210023, PR China
e-mail: lijiemath@163.com

HAI-LIANG WU, School of Science,
Nanjing University of Posts and Telecommunications,
Nanjing 210023, PR China
e-mail: whl.math@smail.nju.edu.cn

https://doi.org/10.1017/S0004972724000765 Published online by Cambridge University Press