Submitted to *Mathematics*. Pages 1 - 5.

OPEN ACCESS

Article

On Matrices Arising in the Finite Field Analogue of Euler's Integral Transform

Michael Griffin [1], **and Larry Rolen** [1]

[1] Dept. of Math & CS, Emory University, 400 Dowman Dr., W401 Atlanta, GA, USA 30322

* Authors to whom correspondence should be addressed; mjgrif3@emory.edu, larryrolen@gmail.com

Version January 15, 2013 submitted to Mathematics. *Typeset by LaTeX using class file mdpi.cls*

Abstract: In his 1984 Ph.D. thesis, J. Greene defined an analogue of the Euler integral transform for finite field hypergeometric series. Here we consider a special family of matrices which arise naturally in the study of this transform and prove a conjecture of Ono about the decomposition of certain finite field hypergeometric functions into functions of lower dimension.

Keywords: hypergeometric series; finite fields; Euler integral transform

1. Introduction and Statement of Results In his 1984 Ph.D. thesis [1], Greene initiated the study of hypergeometric functions over finite fields which are in many ways similar to the classical hypergeometric functions of Gauss. To define these functions, first let A and B be two multiplicative, complex-valued characters of $\mathbb{F}_q^\times$ extended to $\mathbb{F}_q$ by $A(0) = B(0) = 0$ and let $\binom{A}{B}$ be the normalized Jacobi sum

$$\binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}) = \frac{B(-1)}{q} \sum_{x \in \mathbb{F}_q} A(x)\overline{B}(1-x). \tag{1}$$

Here $\overline{B}$ denotes the complex conjugate of B. Greene defined the *Gaussian hypergeometric function* ${}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x\right)_p$ by

$$ {}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n \end{matrix} \middle| x\right)_p := \frac{q}{q-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x). $$

Here $\sum_\chi$ denotes the sum over all characters of $\mathbb{F}_q$. These functions have deep connections to certain combinatorial congruences of modular forms, as well as traces of Hecke operators and counting points on certain modular varieties [2]. For example, if we let ${}_2E_1(\lambda)\ :\quad y^2 = x(x-1)(x-\lambda)$ be the Legendre form elliptic curve ($\lambda \neq 0, 1$), we have the following result whenever $p \geq 5$ is a prime and $\lambda \in \mathbb{Q} - \{0, 1\}$ satisfies $\operatorname{ord}_p(\lambda(\lambda-1)) = 0$ [3]:

$${}_2F_1\left(\begin{matrix}\phi_p, & \phi_p \\ & \epsilon\end{matrix}\middle|\ \lambda\right)_p = -\frac{\phi_p(-1)\cdot\ {}_2a_1(p;\lambda)}{p}.$$

Here ϕ_p is the Legendre symbol modulo p, ϵ is the trivial character, and ${}_2a_1(p;\lambda)$ is the trace of Frobenius of ${}_2E_1(\lambda)$ at p. In analogy with the Euler integral transform for classical hypergeometric functions, it turns out that these Gaussian hypergeometric functions are traces of Gaussian hypergeometric functions of lower degree. More precisely, Greene proved the following fact:

$$\begin{aligned}&{}_{n+1}F_n\left(\begin{matrix}A_0, & A_1, & \dots, & A_n \\ & B_1, & \dots, & B_n\end{matrix}\middle|\ x\right)_p \\ &\quad = \frac{A_nB_n(-1)}{p}\sum_{y=0}^{p-1} {}_nF_{n-1}\left(\begin{matrix}A_0, & A_1, & \dots, & A_{n-1} \\ & B_1, & \dots, & B_{n-1}\end{matrix}\middle|\ x\right)_p \cdot A_n(y)\overline{A}_nB_n(1-y).\end{aligned} \tag{2}$$

This transform is related to the modularity of other varieties as well. For example, Ahlgren and Ono relate special values of ${}_4F_3$ hypergeometric functions to the coefficients of modular forms using the modularity of a certain Calabi-Yau threefold [4]. Thus, it is natural to consider the following matrix which plays the role of Euler's integral transform in an important special case.

Definition. Let p be an odd prime. Let $q = p^n \geq 5$ and M_q be the $(q-2)\times(q-2)$ matrix (a_{ij}) indexed by $i, j \in \mathbb{F}_q - \{0, 1\}$ where

$$a_{ij} = \phi_q(1-ij)\phi_q(ij).$$

Here ϕ_q denotes the quadratic character in $\mathbb{F}_q$. Based on numerical data, Ono made the following conjecture.

Conjecture (Ono). *Let f_q be the characteristic polynomial of M_q. Then*

$$f_q(x) = \begin{cases}(x+1)(x-1)(x+2)(x^2-q)^{(q-5)/2} & \textit{if } \phi_q(-1) = 1 \\ x(x^2-3)(x^2-q)^{(q-5)/2} & \textit{if } \phi_q(-1) = -1.\end{cases}$$

Our main result is the following.

Theorem 1.1. *Ono's conjecture is true.*

Remark For the eigenvalues $0, \pm1, -2$, we give explicit formulas for the eigenvectors (cf. Proposition 2.1).

The paper is organized as follows. In §2 we establish the claimed formulas for the eigenvalues $\lambda \in \{0, \pm1, -2\}$ using Jacobi sums. In §3 we complete the proof of the main theorem be proving that $(x^2 - q)^{\frac{q-5}{2}}$ divides the characteristic polynomial of M_q and that $x^2 - 3$ divides the characteristic polynomial when $\phi_q(-1) = -1$.

2. Eigenvectors for $\lambda \in \{0, \pm 1, -2\}$ The claimed formulas for the eigenvectors can be deduced using the following well-known lemma which we prove for completion.

Lemma 1. *If $a_0, a_1, a_2 \in \mathbb{F}_q$ and $a_2 \neq 0$, then*

$$\sum_{x \in \mathbb{F}_q} \phi_q(a_0 + a_1 x + a_2 x^2) = \begin{cases} -\phi_q(a_2) & \text{if } a_1^2 \neq 4a_0a_2 \\ \phi_q(a_2)(q-1) & \text{if } a_1^2 = 4a_0a_2. \end{cases}$$

Proof. Factor out a_2 and complete the square to get

$$\sum_{x \in \mathbb{F}_q} \phi_q(a_0 + a_1 x + a_2 x^2) = \phi_q(a_2) \sum_{x \in \mathbb{F}_q} \phi_q((x-a)^2 - b) = \phi_q(a_2) \sum_{x \in \mathbb{F}_q} \phi_q(x^2 - b),$$

where $a = -\frac{a_1}{2a_2}$ and $b = \frac{a_1^2 - 4a_0a_2}{4a_2}$. Then $b = 0$ if and only if the discriminant is 0, in which case the sum is clearly $\phi_q(a_2)(q-1)$. If $b \neq 0$, then the change of variables $y = x^2 - b$ gives

$$\sum_{x \in \mathbb{F}_q} \phi_q(x^2 - b) = \sum_{y} \phi_q(y)(\phi_q(y+b) + 1) = \sum_{y} \phi_q(y)\phi_q(y+b).$$

Now replacing y by $\frac{b}{2}(y-1)$ and making the change of variables $z = 1 - y^2$ shows that

$$\sum_{y} \phi_q(y^2 + by) = \sum_{y} \phi_q(y^2 - 1) = \phi_q(-1) \sum_{z} \phi_q(z)(\phi_q(1-z) + 1) = \phi_q(-1) J(\phi, \phi) = -1.$$

This follows from the classical evaluation of $J(\phi, \phi)$ (for example, see [5]). □

We are in position to prove the first case of Theorem 1.1 when $\lambda \in \{0, \pm 1, -2\}$.

Proposition 2.1. *If $\phi_q(-1) = 1$, then $\lambda \in \{\pm 1, -2\}$ are eigenvalues for the matrices M_q. If $\phi_q(-1) = -1$, then $\lambda = 0$ is an eigenvalue for M_q. These eigenvalues have the following corresponding eigenvectors $v = (v_k)_{k \in \mathbb{F}_q - \{0,1\}}$:*

$$\begin{aligned} \lambda &= -1, & v_k &= -\phi_q(k) + 1, \\ \lambda &= +1, & v_k &= 2(\phi_q(k^2 - k) - \phi_q(k) - 1), \\ \lambda &= -2, & v_k &= \phi_q(k^2 - k) + \phi_q(k) + 1, \\ \lambda &= 0, & v_k &= -\phi_q(k^2 - k) + \phi_q(k) + 1. \end{aligned}$$

Proof. We will give the full calculation for the eigenvalue $\lambda = -1$ when $\phi_q(-1) = 1$. The other three cases follow similarly.

When $\lambda = -1$, we must check the formula

$$-v_k = \sum_{s \neq 0,1} \phi_q(1 - ks)\phi_q(ks) v_s.$$

Using the lemma, we have

$$\begin{aligned} \sum_{s \neq 0,1} -\phi_q(1-ks)\phi_q(k) + \sum_{s \neq 0,1} \phi_q(1-ks)\phi_q(ks) &= \phi_q(k) + \phi_q(1-k)\phi_q(k) - 1 - \phi_q(1-k)\phi_q(k) \\ &= \phi_q(k) - 1. \end{aligned}$$

□

3. Determining the $\pm\sqrt{3}$ and $\pm\sqrt{q}$ Eigenspaces Here we complete the proof of Theorem 1.1 by computing the remaining eigenvalues. We begin with the $\pm\sqrt{3}$-eigenvalues when $\phi_q(-1) = -1$.

Proposition 3.1. *If $\phi_q(-1) = -1$, then the characteristic polynomial of M_q is divisible by $(x^2 - 3)$.*

Proof. We consider the matrix M_q^2 with entries $b_{i,j}$. Using the lemma, we find $b_{i,j} = -(1 + \phi_q(ij) + \phi_q(i - i^2)\phi_q(j - j^2))$ if $i \neq j$, and $b_{i,i} = q - 3$. By a similar calculation as in the proof of Proposition 2.1, we find that $v = (v_k), v' = (v'_k)$ are eigenvectors with eigenvalue 3 for M_q^2, where

$$v_k := 1 + \phi_q(k), \qquad v'_k := 1 + \phi_q(k^2 + k).$$

This follows by verifying

$$3v_k = (q - 3)(1 + \phi_q(k)) - \sum_{s \in \mathbb{F}_q \setminus \{0,1,k\}} (1 + \phi_q(s))(1 + \phi_q(ks) + \phi_q(k - k^2)\phi_q(s - s^2)),$$

and

$$3v'_k = (q - 3)(1 + \phi_q(k^2 + k)) - \sum_{s \in \mathbb{F}_q \setminus \{0,1,k\}} (1 + \phi_q(s^2 + s))(1 + \phi_q(ks) + \phi_q(k - k^2)\phi_q(s - s^2))$$

for the vectors v and v' respectively. As the characteristic polynomial of M_q is in $\mathbb{Z}[x]$, we find that $x^2 - 3$ divides the characteristic polynomial of M_q. □

We now finish the proof of Theorem 1.1.

Proposition 3.2. *The characteristic polynomial of M_q is divisible by $(x^2 - q)^{\frac{q-5}{2}}$.*

Proof. We begin by defining the following matrix related to M_q. Let p, q be as above. Let $\widetilde{M_q} = (\phi_q(1 - ij))_{i,j \in \mathbb{F}_q}$ be a $q \times q$ matrix indexed by values of $\mathbb{F}_q$. Then M_q is a the conjugate of a sub-matrix of $\widetilde{M_q}$. Suppose $\widetilde{M_q}$ has an eigenspace of dimension d. Then this eigenspace has a subspace of dimension $d - 2$ of eigenvectors (v_k) with $v_0 = v_1 = 0$. Thus it can be easily seen that M_q has an eigenspace of dimension $d - 2$ corresponding to the same eigenvalue. Using this fact, it suffices to prove that the characteristic polynomial of $\widetilde{M_q}$ is divisible by $(x^2 - q)^{\frac{q-1}{2}}$.

Consider the matrix $\widetilde{M_q}^2 = \left(\sum_{k \in \mathbb{F}_q} \phi_q(1 - ik)\phi_q(1 - jk)\right)_{i,j \in \mathbb{F}_q}$. For each $a \in \mathbb{F}_q - \{0, -1\}$, let $V_a = (v_i)_{i \in \mathbb{F}_q}$ be a vector indexed by elements of $\mathbb{F}_q$ such that $v_a = 1$, $v_{-1} = -\phi_q(-a)$, and $v_i = 0$ for all $i \in \mathbb{F}_q - \{-1, a\}$. Then if $(u_i) = \widetilde{M_q}^2 V_a$, we have

$$\begin{aligned} (u_i) &= \left(\sum_{j \in \mathbb{F}_q} v_j \sum_{k \in \mathbb{F}_q} \phi_q(1 - ik)\phi_q(1 - jk)\right) \\ &= \left(\sum_{k \in \mathbb{F}_q} \phi_q(1 - ik)\phi_q(1 - ak) - \phi_q(-a) \sum_{k \in \mathbb{F}_q} \phi_q(1 - ik)\phi_q(1 + k)\right). \end{aligned}$$

Since $a \neq 0, -1$, by Lemma 1 we find

$$\begin{aligned} u_0 &= 0, \\ u_a &= q - 1 + \phi_q(-a)^2 = q, \\ u_{-1} &= -\phi_q(-a) - \phi_q(-a)(q - 1) = -q\phi_q(-a). \end{aligned}$$

For all other i, we have $u_i = \phi_q(ia) - \phi_q(-a)\phi_q(-i) = 0$. Hence V_a is an eigenvector for $\widetilde{M}_q^2$ with eigenvalue q.

We may also define $V_0 = (v_i)$ so that $v_0 = 1$, and $v_i = 0$ for all other $i \in \mathbb{F}_q$. Then if $(u_i) = \widetilde{M_q}^2 V_0$, we have $u_0 = \sum_{k\in\mathbb{F}_q} \phi_q(1) = q$, and $u_i = \sum_{k\in\mathbb{F}_q} \phi_q(1-ik) = 0$ for $i \neq 0$. Hence V_0 is also an eigenvector for the eigenvalue q. This gives us a total of $q-1$ linearly independent eigenvectors corresponding to the eigenvalue q. Each eigenvalue (counting multiplicities) of $\widetilde{M}_q^2$ is the square of an eigenvalue of $\widetilde{M}_q$. Thus, $\widetilde{M}_q$ has eigenvalues $\pm\sqrt{q}$ of multiplicities that sum to $q-1$ and so M_q has eigenvalues $\pm\sqrt{q}$ of multiplicities summing to at least $q-5$. By Lemma 1, we have that $\mathrm{Trace}(M_q) = -1 - \phi_q(-1)$. But we already know that the sum of all other eigenvalues is $-1 - \phi_q(-1)$. Hence, the multiplicities of the $\pm\sqrt{q}$ eigenvalues must be equal. □

Acknowledgements The authors thank the National Science Foundation for its generous support, and their advisor Ken Ono for his guidance and for improving the quality of exposition of the article.

References

1. Greene, J.R. *Character Sum Analogues For Hypergeometric And Generalized Hypergeometric Functions Over Finite Fields*; ProQuest LLC, Ann Arbor, MI, 1984; p. 133. Thesis (Ph.D.)–University of Minnesota.
2. Ono, K. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*; Vol. 102, *CBMS Regional Conference Series in Mathematics*, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004; pp. viii+216.
3. Koike, M. Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields. *Hiroshima Math. J.* **1995**, *25*, 43–52.
4. Ahlgren, S.; Ono, K. A Gaussian hypergeometric series evaluation and Apéry number congruences. *J. Reine Angew. Math.* **2000**, *518*, 187–212.
5. Ireland, K.; Rosen, M. *A classical introduction to modern number theory*, second ed.; Vol. 84, *Graduate Texts in Mathematics*, Springer-Verlag: New York, 1990; pp. xiv+389.