CHARACTERIZATIONS OF THE *d*TH-POWER RESIDUE MATRICES OVER FINITE FIELDS

EVAN P. DUMMIT

ABSTRACT. In a recent paper of the author with D. Dummit and H. Kisilevsky, we constructed a collection of matrices defined by quadratic residue symbols, termed "quadratic residue matrices", associated to the splitting behavior of prime ideals in a composite of quadratic extensions of \mathbb{Q} , and proved a simple criterion characterizing such matrices. We then analyzed the analogous classes of matrices constructed from the cubic and quartic residue symbols for a set of prime ideals of $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(i)$, respectively. In this paper, the goal is to construct and study the finite-field analogues of these residue matrices, the "dth-power residue matrices", using the general dth-power residue symbol over a finite field.

1. The dTH-Power Residue Matrices

Our goal is to study the appropriate analogue of the residue matrices constructed in [1] in the finite-field setting.

Let q be a prime power and d be a positive integer with d dividing q-1, and let \mathbb{F}_q denote the finite field with q elements. We begin by recalling the standard definition and some basic properties of the dth-power residue symbol for polynomials in $\mathbb{F}_q[t]$.

Definition. If *P* is a monic irreducible polynomial over \mathbb{F}_q and $a \in \mathbb{F}_q[t]$ is relatively prime to *P*, the *d*th-power residue symbol $\left(\frac{a}{P}\right)_d$ is defined to be the unique *d*th root of unity in \mathbb{F}_q with

$$\left(\frac{a}{P}\right)_d \equiv a^{(|P|-1)/d} \pmod{P}$$

where |P| denotes the norm of P, defined as $q^{\deg(P)}$, the cardinality of $\mathbb{F}_q[t]/(P)$.

We remark here that the *d*th power residue map $\left(\frac{\cdot}{P}\right)_d$ is a surjective homomorphism from the multiplicative group of nonzero residue classes modulo *P* to the group of *d*th roots of unity in \mathbb{F}_q .

It will be convenient instead to consider the *d*th-power residue symbol as taking values in \mathbb{C} : to this end, choose a fixed isomorphism φ of the *d*th roots of unity in \mathbb{F}_q with the complex *d*th roots of unity.

Definition. If P is a monic irreducible polynomial over \mathbb{F}_q and $a \in \mathbb{F}_q[t]$, we define the modified dth-power residue symbol $\left[\frac{a}{P}\right]_d$ to be the complex root of unity with $\left[\frac{a}{P}\right]_d = \varphi\left(\left(\frac{a}{P}\right)_d\right)$.

We remark here (and will justify later) that the resulting class of matrices is independent of the isomorphism φ : any other isomorphism will produce the same class of matrices.

Definition. Let d be a positive integer. A "cyclotomic sign matrix of dth roots of unity" is an $n \times n$ matrix whose diagonal entries are all 0 and whose off-diagonal entries are all complex dth roots of unity.

With the correct class of matrices in hand, we can now define the dth-power residue matrices.

²⁰¹⁰ Mathematics Subject Classification. Primary 11A15; Secondary 11T06, 12E20, 05B20

Keywords: power residues, reciprocity laws, power residue matrices, residue symbols.

Definition. Let q be a prime power and d be an integer dividing q-1. The "dth-power residue" matrix associated to the monic irreducible polynomials P_1, P_2, \ldots, P_n in $\mathbb{F}_q[t]$ is the $n \times n$ matrix whose (i, j)-entry is the dth power residue symbol $\left[\frac{P_i}{P_i}\right]_{j}$.

Notice that the *d*th-power residue matrices are cyclotomic sign matrices of *d*th roots of unity. We would like to characterize, for a given *d* and *q*, which cyclotomic sign matrices of *d*th roots of unity actually arise as the *d*th-power residue matrix associated to some set of monic irreducible polynomials over \mathbb{F}_q . We should naturally expect *d*th-power reciprocity to impose some conditions.

Over $\mathbb{F}_q[t]$ the *d*th-power reciprocity law is as follows (cf. Theorem 3.3 of [3]): for any monic irreducible polynomials P and Q in $\mathbb{F}_q[t]$,

$$\left(\frac{P}{Q}\right)_d = (-1)^{(q-1)\deg(P)\deg(Q)/d} \left(\frac{Q}{P}\right)_d$$

and for the modified residue symbols the statement is the same [except with square brackets].

2. Characterizations of the dth-Power Residue Matrices

Observe that if (q-1)/d is even then the *d*th-power reciprocity law is symmetric, and thus all of the *d*th-power matrices are symmetric. The converse is also true:

Theorem 1. Let q be a prime power and d be an integer dividing q - 1 with (q - 1)/d even. If M is an $n \times n$ cyclotomic sign matrix of dth roots of unity, then the following are equivalent:

- (a) The matrix M is symmetric.
- (b) The matrix M is the dth-power residue matrix associated to distinct monic irreducible polynomials P_1, P_2, \ldots, P_n in $\mathbb{F}_q[t]$.

Proof. (a) implies (b): We inductively construct monic irreducible polynomials P_1, \ldots, P_n for which M is the dth-power residue matrix. For the base case, let P_1 be any monic irreducible polynomial of positive degree. For the inductive step, suppose that P_1, \ldots, P_k are monic irreducible polynomials such that $\left[\frac{P_i}{P_j}\right]_d = m_{i,j}$ for $1 \le i, j \le k$. For each $1 \le j \le k$, choose a nonzero residue class u_j modulo P_j such that $\left[\frac{u_j}{P_j}\right]_d = m_{k+1,j}$. By the Chinese Remainder Theorem and Kornblum's function-field analogue of Dirichlet's Theorem on primes in arithmetic progression (cf. Theorem 4.7 of [R]) we may choose a monic irreducible polynomial P_{k+1} satisfying the congruences $P_{k+1} \equiv u_j \pmod{P_j}$ for all $1 \le j \le k$. By construction, we have $\left[\frac{P_{k+1}}{P_j}\right]_d = m_{k+1,j}$ for all $1 \le j \le k$, and dth-power reciprocity along with the form of M ensures that also $\left[\frac{P_i}{P_{k+1}}\right]_d = m_{i,k+1}$ for all $1 \le i \le k$ is satisfied. Thus, M is the dth-power residue matrix associated to P_1, \ldots, P_n , as claimed.

(b) implies (a): This follows immediately from dth-power reciprocity, since

$$\left(\frac{P_i}{P_j}\right)_d = \left(\frac{P_j}{P_i}\right)_d$$

for all pairs (i, j) with $i \neq j$.

When (q-1)/d is odd, dth-power reciprocity takes a form quite similar to quadratic reciprocity over \mathbb{Q} , with polynomials of even and odd degree behaving like rational primes congruent to 1 and 3 (mod 4), respectively: if either P or Q has even degree, then $\left(\frac{P}{Q}\right)_d = \left(\frac{Q}{P}\right)_d$, and if both have odd degree then $\left(\frac{P}{Q}\right)_d = -\left(\frac{Q}{P}\right)_d$.

Observe that the property of whether a cyclotomic sign matrix is a *d*th-power residue matrix is invariant under conjugation by a permutation matrix (simply permute the underlying polynomials accordingly). If we reorder the polynomials so that the first *s* have odd degree and the remaining n - s have even degree, then by *d*th-power reciprocity the associated *d*th-power residue matrix *M* has the form

$$\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$$

where A is an $s \times s$ skew-symmetric cyclotomic sign matrix of dth roots of unity, S is an $(n-s) \times (n-s)$ symmetric cyclotomic sign matrix of dth roots of unity, and B is an $s \times (n-s)$ matrix all of whose entries are dth roots of unity. (Here B^t denotes the transpose of B.)

We now show that every matrix having the form above is a *d*th-power residue matrix when (q-1)/d is odd, and give an additional characterization:

Theorem 2. Let q be a prime power and d be an integer dividing q - 1 with (q - 1)/d odd. If M is an $n \times n$ cyclotomic sign matrix of dth roots of unity, then the following are equivalent:

(a) There exists an integer s with $1 \leq s \leq n$ such that the matrix M can be conjugated by a permutation matrix into a block matrix of the form

$$\begin{pmatrix} A & B \\ B^t & S \end{pmatrix}$$

where A is an $s \times s$ skew-symmetric cyclotomic sign matrix of dth roots of unity, S is an $(n-s) \times (n-s)$ symmetric cyclotomic sign matrix of dth roots of unity, and B is an $s \times (n-s)$ matrix all of whose entries are dth roots of unity. (Here B^t denotes the transpose of B.)

- (b) The matrix M is the dth-power residue matrix associated to a set of distinct monic irreducible polynomials P_1, P_2, \ldots, P_n in $\mathbb{F}_q[t]$.
- (c) If $M = (m_{j,k})$, then $m_{j,k} = \pm m_{k,j}$ for all j, k with $1 \le j, k \le n$, and there exists an integer s with $1 \le s \le n$ such that the diagonal entries of $M\overline{M}$ consist of s occurrences of n + 1 2s and n s occurrences of n 1.

Proof. (a) implies (b): Follows by the same proof as in Theorem 1, except we additionally impose the condition that the degree of the polynomial P_{k+1} is odd if $k \leq s$ or even if k > s, in order to obtain the correct entries below the diagonal.

(b) implies (c): Suppose that M is the dth-power residue matrix associated to the distinct monic irreducible polynomials P_1, \ldots, P_n . The first part of the criterion in (c) follows immediately from dth-power reciprocity.

For the second part, rearrange the polynomials, if necessary, so that the first s have odd degree and the remaining n - s have even degree. Note also that for any dth root of unity r in \mathbb{F}_q , $\varphi(r^{-1}) = \varphi(r)^{-1} = \overline{\varphi(r)}$.

For $1 \leq j \leq s$, the *j*th diagonal element of $M\overline{M}$ is

$$(M\overline{M})_{j,j} = \sum_{k=1}^{n} \left[\frac{P_j}{P_k}\right]_d \overline{\left[\frac{P_k}{P_j}\right]_d} = \sum_{k=1}^{n} \varphi\left(\left(\frac{P_j}{P_k}\right)_d \left(\frac{P_k}{P_j}\right)_d^{-1}\right) = n+1-2s$$

since by dth-power reciprocity the first s terms are -1 (except for the *j*th, which is 0), and the other n-s terms are +1.

For $s+1 \leq j \leq n$, the *j*th diagonal element of $M\overline{M}$ is

$$(M\overline{M})_{j,j} = \sum_{k=1}^{n} \left[\frac{P_j}{P_k}\right]_d \overline{\left[\frac{P_k}{P_j}\right]_d} = \sum_{k=1}^{n} \varphi\left(\left(\frac{P_j}{P_k}\right)_d \left(\frac{P_k}{P_j}\right)_d^{-1}\right) = n-1$$

since by dth-power reciprocity all terms are +1 (except for the *j*th, which is 0), proving (c).

(c) implies (a): Suppose that $m_{j,k} = \pm m_{k,j}$ for each pair (j,k), and that the diagonal entries of the matrix $M\overline{M}$ consist of s occurrences of n + 1 - 2s and n - s occurrences of n - 1.

Whenever $j \neq k$, by the assumptions that $m_{j,k} = \pm m_{k,j}$ and that the $m_{j,k}$ are dth roots of unity, we see that $m_{j,k}\overline{m_{k,j}}$ is either +1 (when $m_{j,k} = m_{k,j}$) or -1 (when $m_{j,k} = -m_{k,j}$).

By conjugating M by an appropriate permutation matrix we may place the s occurrences of n+1-2s in the first s rows of $M\overline{M}$. For $s < j \le n$, we have

$$(M\overline{M})_{j,j} = \sum_{k=1}^{n} m_{j,k}\overline{m_{k,j}} = n - 1,$$

but since there are only n-1 nonzero terms in the sum, we necessarily have $m_{j,k}\overline{m_{k,j}} = 1$ for each $j \neq k$, and hence $m_{j,k} = m_{k,j}$ for all $1 \leq k \leq n$ and $s < j \leq n$.

For $1 \leq j \leq s$, we have

$$(M\overline{M})_{j,j} = \sum_{k=1}^{n} m_{j,k} \overline{m_{k,j}} = n + 1 - 2 \cdot \# \{ 1 \le k \le s : m_{j,k} \overline{m_{k,j}} = -1 \}$$

since $m_{j,k}\overline{m_{k,j}} = +1$ whenever j > s and $m_{j,k}\overline{m_{k,j}}$ can only be 1 or -1. But now since there at most s terms in the count, and $(M\overline{M})_{j,j} = n + 1 - 2s$, we see that $m_{j,k}\overline{m_{k,j}} = -1$ and hence that $m_{j,k} = -m_{k,j}$ for $1 \le k \le s$. Thus M has the form in (a), completing the proof.

Remark. Observe that both condition (a) of Theorem 1, and conditions (a) and (c) of Theorem 2, are wholly independent of the choice of isomorphism φ between the *d*th roots of unity in \mathbb{F}_q and the complex *d*th roots of unity, and therefore we see that the classes of *d*th-power residue matrices are the same no matter which φ is used.

In a similar manner to the way the quadratic, cubic, and quartic residue matrices classify certain types of decomposition configurations over number fields (cf. [2]), the fact that not every $n \times n$ cyclotomic sign matrix of dth roots of unity arises as a dth-power residue matrix has implications for the possible decomposition configurations for primes in abelian extensions of $\mathbb{F}_q(t)$ with Galois group $(\mathbb{Z}/d\mathbb{Z})^n$.

Acknowledgements

The author would like to thank David Dummit for his many helpful comments during the preparation of this paper.

References

- David S. Dummit, Evan P. Dummit, and Hershy Kisilevsky. Characterizations of quadratic, cubic, and quartic residue matrices. Journal of Number Theory, 168:167–179, 2016.
- [2] David S. Dummit and Hershy Kisilevsky. Decomposition configuration types in minimally tamely ramified extensions of Q. arXiv preprint arXiv:1707.02493, 2017.
- [3] Michael Rosen. Number theory in function fields, volume 210. Springer Science & Business Media, 2013.

EVAN P. DUMMIT, ARIZONA STATE UNIVERSITY, SCHOOL OF MATHEMATICAL AND STATISTICAL SCIENCES, P.O. BOX 871804, TEMPE AZ 85287-1804

E-mail address: evan.dummit@asu.edu