ON THE MATRIX EQUATION $X^n = B$ OVER FINITE FIELDS

MARIA T. ACOSTA-DE-OROZCO and JAVIER GOMEZ-CALDERON

Department of Mathematics
Southwest Texas State University
San Marcos, Texas 78666-4603

Department of Mathematics
The Pennsylvania State University
New Kensington Campus
New Kensington, Pennsylvania 15068

(Received May 28, 1992 and in revised form April 19, 1993)

ABSTRACT. Let $GF(q)$ denote the finite field of order $q = p^e$ with $p$ odd and prime. Let $M_{m \times m}(q)$ denote the ring of $m \times m$ matrices with entries in $GF(q)$. In this paper, we consider the problem of determining the number $N(n,m,B)$ of the $n$-th roots in $M$ of a given matrix $B \in M$.

KEY WORDS AND PHRASES. Finite fields and matrix powers.

1991 AMS SUBJECT CLASSIFICATION CODE. 15A33.

1. INTRODUCTION.

Let $GF(q)$ denote the finite field of order $q = p^e$ with $p$ odd and prime. Let $M_{m \times m}(q)$ denote the ring of $m \times m$ matrices with entries in $GF(q)$. In this paper, we consider the problem of determining the number $N(n,m,B)$ of the $n$-th roots in $M$ of a given matrix $B \in M$; i.e., the number of solutions $X$ in $M$ of the equation

$$X^n = B \quad (1.1)$$

Our present work generalizes a recent paper of the authors [1] in which the case $N(n, 2, B)$ was considered. If $B$ denotes a scalar matrix, then equation (1.1) is called scalar equation, type of equations that has been already studied by Hodges in [3]. Also, if $B$ denotes the identity matrix and $n = 2$, then the solutions of (1.1) are called involutory matrices. Involutory matrices over either a finite field or a quotient ring of the rational integers have been extensively researched, with a detailed extension to all finite commutative rings given by McDonald in [5].

2. ESTIMATING $N(n,m,B)$.

Let $GF(q)$ denote the finite field of order $q = p^e$ with $p$ odd and prime. Let $M_{m \times m}(q)$ denote the ring of $m \times m$ matrices with entries in $GF(q)$ and let $GL(q,m)$ denote its group of units. We now make the following conventions:

(a) $n$ and $m$ will denote integers so that $1 < m$ and $1 < n < q$,
(b) $N(n,m,B)$ will denote the number of solutions $X$ in $M$ of the equation

$$X^n = B$$

(c) $g(m,d)$ will denote the cardinality of $GL(q^d,m)$. Thus

$$g(m,d) = \prod_{i=0}^{m-1} (q^m - q^d)$$

$$= q^{dm^2} \prod_{i=1}^{m} (1 - q^{-id})$$

We also define $g(0,d) = 1$.

Our first lemma is a result given by Hodges in ([3], Th. 2).
LEMMA 1. Suppose \( E(x) \) is a monic polynomial over \( GF(q) \) with factorization given by
\[
E(x) = F_1^{h_1} F_2^{h_2} \cdots F_s^{h_s},
\]
where the \( F_i \) are distinct monic irreducible polynomials, \( h_i \geq 1 \) and \( \deg F_i = d_i \) for \( i = 1, 2, \ldots, s \). Then the number of matrices \( B \) in \( M \) such that \( E(B) = 0 \) is given by
\[
g(m, 1) \sum_P \prod_{i=1}^s \prod_{j=1}^{h_i} g(K_{ij}, d_i)^{-1}
\]
where the summation is over all partitions \( P = P(m) \) defined by
\[
m = \sum_i s d_i \sum_{j=1}^{h_i} j k_{ij}, \quad k_{ij} \geq 0
\]
and \( a(P) = d, b_i(P) \) where \( b_i(P) \) is defined by
\[
b_i(P) = \sum_{u=1}^{h_i} k_{iu}^2 (u-1) + 2u k_{iu} \sum_{v=u+1}^{h_i} k_{iv}
\]

LEMMA 2. Let \( w \) denote a primitive element of \( GF(q) \). Let \( r \in GF(q)^* = GF(q) - \{0\} \) and write \( r = w^t \) for some \( t, 1 \leq t \leq q-1 \). Assume \( n \) divides \( q-1 \) but \( 4 \) is not factor of \( n \). Then
\[
\sum_P q^m(q-1)^m \leq N(n, m, r l) \leq \sum_P \frac{q^m}{(q-1)^m}
\]
where the summation is over all partitions \( P = P(m) \) defined by
\[
m = \frac{n}{(n, t)} \sum_{i=1}^n k_i, \quad k_i \geq 0
\]

PROOF. Let \( D \) denote the greatest common divisor of \( n \) and \( t \). Then
\[
x^n - w^t = \left(x^D\right)^{\frac{n}{D}} - \left(w^t\right)^{\frac{n}{D}}
\]
\[
= \prod_{i=0}^{D-1} \left(x^\frac{n}{D} - w^\frac{(q-1)i+t}{D}\right)
\]
\[
= \prod_{i=0}^{D-1} h_i(x).
\]
We also see that \( w^{\frac{(q-1)i+t}{D}} \) does not belong to the set of powers \( GF^S(q) = \{x^s : x \in GF(q)\} \) for all prime factors \( s \) of \( \frac{n}{D} \). Hence, by ([4], Ch. VIII, Th. 16), each factor \( h_i(x) \) is irreducible over \( GF(q)[x] \). Therefore, Lemma 1 with \( E(x) = x^n - w^t \) gives
\[
N(n, m, r l) = g(m, 1) \prod_{P} \prod_{i=1}^{D} g \left(k_i, \frac{n}{D} \right)^{-1}
\]
where the summation over all partition \( P = P(m) \) defined by
\[
m = \frac{n}{D} \sum_{i=1}^{D} k_i, \quad k_i \geq 0
\]
Hence,
\[
N(n, m, r l) = \sum_P \frac{q^m}{(q-1)^m} \prod_{i=1}^{D} \prod_{j=1}^{n} \left(1-q^{-\frac{n}{D}}\right)
\]
ON THE MATRIX EQUATION $X^n = b$ OVER FINITE FIELDS

$$\leq \sum_{P} \frac{q^{m^2}}{q^m} \left( \frac{q}{q-1} \right)^m$$

and

$$= \sum_{P} \frac{q^{m^2}}{(q-1)^m}$$

and

$$N(n, m, r_l) = \sum_{P} \frac{q^{m^2} \prod_{i=1}^{n} (1 - q^{-1})}{q^m \sum_{i=1}^{n} k_i^2} \prod_{i=1}^{n} \prod_{j=1}^{k_i} (1 - q^{-j})$$

$$\geq \sum_{P} \frac{q^{m^2} (1 - q^{-1})^m}{q^m \sum_{i=1}^{n} k_i^2}$$

$$\geq \sum_{P} q^n(q-1)^m$$

**REMARK 1.** If $r^m = w^m \not\in GF^n(q)$, then $n$ does not divide $tm$ and the number of partitions $P$ is zero. Thus, $N(n,m,rl) = 0$.

**REMARK 2.** If $r = w^{q-1} = 1$ and $1 < n < q$, including 4 as a possible factor of $n$, then one can obtain

$$\sum_{P} q^{m^2} \leq N(n,m,l) \leq \sum_{P} \frac{q^{m^2}}{(q-1)^m}$$

**LEMMA 3.**

$$\sum_{P} (q-1)^m \leq N(n,m,0) \leq \sum_{P} \frac{q^{m^2}}{(q-1)^m}$$

where $P$ denotes all partitions $P = P(m)$ defined by

$$m = \sum_{j=1}^{n} j k_j, \quad k_j \geq 0$$

**PROOF.** Applying Lemma 1, with $E(x) = x^n$, we obtain

$$N(n,m,0) = g(m,1) \sum_{P} q^{-b(P)} \prod_{j=1}^{n} g(k_j,1)^{-1}$$

where the summation is over all partitions $P = P(m)$ defined by

$$m = \sum_{j=1}^{n} j k_j, \quad k_j \geq 0$$

and $b(P) = \sum_{u=1}^{n} \left[ k_u^2 (u-1) + 2uk_u \sum_{v=u+1}^{n} k_v \right]$. Therefore,

$$(a) \quad N(n,m,0) = \sum_{P} \frac{q^{m^2} \prod_{i=1}^{n} (1 - q^{-i})}{q^{b(P)} \prod_{i=1}^{n} k_i^2 \prod_{j=1}^{k_i} (1 - q^{-j})}$$

where

$$b(P) + \sum_{i=1}^{n} k_i^2 = \sum_{u=1}^{n} \left[ k_u (u-1) + 2uk_u \sum_{v=u+1}^{n} k_v \right] + \sum_{i=1}^{n} k_i^2 \geq m.$$
542 M.T. ACOSTA-DE-OROZCO AND J. GOMEZ-CALDERON

\[
N(n,m,0) \leq \sum_{P} \frac{q^{m^2}}{q^m} \left( \frac{q}{q-1} \right)^m = \sum_{P} \frac{q^{m^2}}{q} (q-1)^m.
\]

(b) \[
N(n,m,o) = \sum_{P} \frac{q^{m^2} \prod_{i=1}^{n} (1-q^{-i})}{q^{b(P)} + \sum_{i=1}^{n} k_i^2} \geq \sum_{P} \frac{(q-1)^m}{q (q-1)^{b(P)+m}} = \sum_{P} \frac{(q-1)^m}{q (q-1)^{b(P)+m}} \geq \sum_{P} (q-1)^m.
\]

Now we will consider a nonscalar matrix B. We start with the following

**Lemma 4.** Let B denote a \( m \times m \) matrix over \( GF(q) \) with a minimal polynomial \( f_B(x) \). Let \( f_B(x) = f_1^b(x) f_2^b(x) \cdots f_r^b(x) \) with \( \text{deg}(f_i) = d_i \) denote the prime factorization of \( f_B(x) \). Assume that \( B \) is similar to a matrix of the form

\[
\text{diag}\left( C(f_1^b), \cdots, C(f_1^b), \cdots, C(f_r^b), \cdots, C(f_r^b) \right)
\]

where \( C(f_i^b) \) denotes the companion matrix of \( f_i^b \).

Let \( f_i(x^n) = \prod_{j=1}^{n} F_{i,j}(x) \) denote the prime factorization of \( f_i(x^n) \) for \( i = 1, 2, \cdots, r \). Let \( D_i \) denote the degree of \( F_{i,j}(x) \) for \( j = 1, 2, \cdots, a_i \). Then

\[
N(n,b,B) \leq \sum_{P} \frac{q^{m^2}}{q^{b(P)} + \sum_{i=1}^{a_i} k_i^2} \geq \sum_{P} (q-1)^m.
\]

**Proof.** If \( T^n = B \) then \( f_B(T^n) = 0 \). Thus the minimal polynomial of \( T \) divides \( f_B(x^n) \) and \( T \) is similar to a matrix of the form

\[
\text{diag}(E_1, E_2, \cdots, E_r)
\]

where

\[
E_i = \text{diag}(C(F_{1,i}^b), \cdots, C(F_{1,i}^b), \cdots, C(F_{i,a_i}^b)),
\]

with \( C(F_{i,j}^b) \) denoting the companion matrix of \( F_{i,j}^b \). So, we have a partition \( P = P(a_i, D_i, d_i, k_i) \) defined by

\[
D_i \sum_{j=1}^{a_i} R_{i,j} = d_i k_i, \quad R_{i,j} \geq 0
\]

for \( i = 1, 2, \cdots, r \).

**Proof.** If \( T^n = B \) then \( f_B(T^n) = 0 \). Thus the minimal polynomial of \( T \) divides \( f_B(x^n) \) and \( T \) is similar to a matrix of the form

\[
\text{diag}(E_1, E_2, \cdots, E_r)
\]

where

\[
E_i = \text{diag}(C(F_{1,i}^b), \cdots, C(F_{1,i}^b), \cdots, C(F_{i,a_i}^b)),
\]

with \( C(F_{i,j}^b) \) denoting the companion matrix of \( F_{i,j}^b \). So, we have a partition \( P = P(a_i, D_i, d_i, k_i) \) defined by

\[
D_i \sum_{j=1}^{a_i} R_{i,j} = d_i k_i
\]

for \( i = 1, 2, \cdots, r \). Therefore,

\[
N(n,m,B) \leq \sum_{P} \frac{|\text{com}(B)|}{|\text{com}(T)|}
\]

where \( \text{com}(H) = \{ X \in GL(q,m): XH = HX \} \) and the summation is over all partitions \( P \) defined
ON THE MATRIX EQUATION $X^n = B$ OVER FINITE FIELDS

by (2.4).

Now using the formula for $|\text{COM}(H)|$ given by L.E. Dickson in ([2], p. 235) we obtain

$$N(n, m, B) \leq \sum_{P} \prod_{i=1}^{a_i} g(k_i, d_i) \prod_{j=1}^{q} g(R_{ij}, D_i)$$

This completes the proof of the lemma.

REMARK. If $T$ is similar to a matrix of the form given in (2.3), then $T^n$ may have elementary divisors of the form $f_i^k(X)$ with $C_i < b_i$. This possibility is the main problem to get an equality at (2.2).

LEMMA 5. Let $B$ denote a $m \times m$ matrix over $GF(q)$ with minimal polynomial $f_B(x)$. Let $f_B(x) = f_1^{k_1}(x)f_2^{k_2}(x) \cdots f_r^{k_r}(x)$ with $d_i = \text{deg}(f_i)$ denote the prime factorization of $f_B(x)$. Assume $m = \sum_{i=1}^{r} b_i d_i$. Then

$$N(n, m, B) \leq n^r \leq n^m$$

Further, $N(n, m, B) = n^m$ if and only if $f_i(x) = x - a_i$ with $a_i \in GF^m(q)$ for $i = 1, 2, \ldots, r = m$.

PROOF. With notation as in Lemma 4, $m = \sum_{i=1}^{r} b_i d_i$ implies $k_i = k_2 = \cdots = k_r = 1$. Therefore, if $T^n = B$ then $D_i = d_i$ for all $i = 1, 2, \ldots, r$ and

$$N(n, m, B) \leq \sum_{P} 1$$

where the summation is over all partitions $P$ defined by

$$\sum_{j=1}^{a_i} R_{ij} = 1, \quad R_{ij} \geq 0$$

for $i = 1, 2, \ldots, r$. Thus,

$$N(n, m, B) \leq \prod_{i=1}^{r} a_i \geq n^r$$

Now if $N(n, m, B) = n^m$, then $r = m$. So, each polynomial $f_i^{k_i}(x)$ must be linear so that $f_i(x^n)$ splits as a product of $n$ distinct linear factors. Hence, $f_i(x) = x - a_i$ with $a_i \in GF^m(q)$ for $i = 1, 2, \ldots, r = m$. Conversely, if $f_i(x) = x - a_i$ with $a_i \in GF^m(q)$, then

$$Q^{-1} \text{diag} (e_1, e_2, \ldots, e_m) Q = B$$

for some matrix $Q$ in $GL(q, m)$ and for all $e_i$ in $GF(q)$ such that $e_i^n = a_i$ for $i = 1, 2, \ldots, r$. Therefore,

$$N(n, m, B) = n^m.$$ 

COROLLARY 6. If $B = \text{diag}(b_1, b_2, \ldots, b_m)$ with $b_i \neq b_j$ when $i \neq j$, then

$$N(n, m, B) = \begin{cases} n^m & \text{if } b_i \in GF^m(q) \text{ for } i = 1, 2, \ldots, m \\ 0, & \text{otherwise} \end{cases}$$

LEMMA 7. Let $B$ denote a $m \times m$ matrix over $GF(q)$. Assume that the minimal polynomial of $B$ is irreducible of degree $d < m$. Then, either $N(n, m, B) = 0$ or $N(n, m, B) \geq (q^d - 1)m/4$.

PROOF. Let $f_B(x)$ denote the minimal polynomial of a $m \times m$ matrix $B$ over $GF(q)$. Assume $f_B(x)$ is irreducible of degree $d < m$. Thus, $m = rd$ for some integer $r \geq 2$. Let $f_B(x^n) = F_1(x)F_2(x) \cdots F_a(x)$ denote the prime factorization of $f_B(x^n)$ and let $D$ denote the degree of each of the factors $F_i(x)$ for $i = 1, 2, \ldots, a$. Assume $N(n, m, B) > 0$. Then $T^n = B$ for some matrix $T$ that is similar to a matrix of the form

$$\text{diag} \left( \frac{C(F_1)}{R_1}, \cdots, \frac{C(F_a)}{R_a} \right)$$
where $C(F_i)$ denote the companion matrix of $F_i(x)$ for $i = 1, 2, \ldots, a$.

Therefore,

$$N(n, m, B) \geq \frac{|COM(B)|}{\prod_{i=1}^{a} (1 - q^{-D_i})}$$

$$\geq \frac{q^{d^2} \prod_{j=1}^{r} (1 - q^{-D_j})}{\sum_{i=1}^{a} R_i^2 \prod_{j=1}^{r} (1 - q^{-D_j})}$$

$$\geq \frac{q^{d^2}(1 - q^{-D})}{D} \sum_{i=1}^{a} R_i^2$$

$$\geq \begin{cases} q^{m(r-1)(q^d - 1)^r} & \text{if } m > d \\ q^{m(r-1)(q^d - 1)^r} & \text{if } m = D \\ \end{cases}$$

$$\geq (q^d - 1)^{m/d}.$$