BULL. AUSTRAL. MATH. SOC. 11T99, 16G10
VOL. 59 (1999) [59–64]

POLYNOMIAL EQUATIONS FOR MATRICES OVER FINITE FIELDS

JIUZHAO HUA

Let $E(x)$ be a monic polynomial over the finite field $\mathbf{F}_q$ of q elements. A formula for the number of $n \times n$ matrices θ over $\mathbf{F}_q$ satisfying $E(\theta) = 0$ is obtained by counting the representations of the algebra $\mathbb{F}_q[x]/(E(x))$ of degree n. This simplifies a formula of Hodges.

1. INTRODUCTION AND NOTATION

Let $\mathbb{F}_q$ denote the finite field of q elements, where q is a prime power. If $E = E(x)$ is a monic polynomial over $\mathbb{F}_q$, let $N(E, n)$ be the number of matrices θ of order n with entries in $\mathbb{F}_q$ such that $E(\theta) = 0$. In his paper [**2**], Hodges obtained a formula for $N(E, n)$, but this is not easy to handle in practice. The purpose of this note is to give a simplification of Hodges' formula. This was achieved by counting the representations of a finite dimensional algebra A; here $A = \mathbb{F}_q[x]/\big(E(x)\big)$.

A *matrix representation* of the algebra A of degree n is a homomorphism from A to the full matrix algebra $\mathcal{M}_n(\mathbb{F}_q)$, which consists of all $n \times n$ matrices over $\mathbb{F}_q$. Since A is generated by a single element x, every matrix representation of A is specified by a single matrix, that is, the image of x. It is clear that a square matrix θ over $\mathbb{F}_q$ satisfies the equation $E(\theta) = 0$ if and only if the map $x \mapsto \theta$ defines a matrix representation of A. Thus the number $N(E, n)$ is exactly the number of representations of A of degree n. In what follows, a representation always means a matrix representation.

Suppose that E can be factorised into the following form:

$$E = P_1^{h_1} P_2^{h_2} \dots P_s^{h_s}, \tag{1.1}$$

where the P_i are distinct monic irreducible polynomials over $\mathbb{F}_q$, $h_i \geqslant 1$ and $\deg P_i = d_i$ for $i = 1, \dots, s$. Thus, the Chinese Remainder Theorem for $\mathbb{F}_q[x]$ implies that

$$A \cong \mathbb{F}_q[x]/\Big(P_1^{h_1}\Big) \oplus \mathbb{F}_q[x]/\Big(P_2^{h_2}\Big) \oplus \dots \oplus \mathbb{F}_q[x]/\big(P_s^{h_s}\big). \tag{1.2}$$

So, the representations of A are determined by the representations of the algebra of the form $\mathbb{F}_q[x]/\Big(P(x)^h\Big)$ with $P(x)$ being monic irreducible over $\mathbb{F}_q$.

Received 25th May, 1998
I am indebted to Professor J. Brawley for bringing Hodges' work to my attention, and to my thesis advisor Peter Donovan for helpful comments.

2. Representations of $\mathbb{F}_q[x]/\left(P(x)^h\right)$

Let $P(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a monic irreducible polynomial of degree d over $\mathbb{F}_q$, and let h be a positive integer. Let $B = \mathbb{F}_q[x]/\left(P(x)^h\right)$.

Let $J(P)$ be the *companion matrix* of P, that is

$$J(P) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{d-1} \end{pmatrix}.$$

This has characteristic polynomial $P(\lambda)$. For any positive integer $m \geqslant 1$, let $J_m(P)$ denote the following block matrix:

$$J_m(P) = \begin{pmatrix} J(P) & I_d & 0 & \dots & 0 \\ 0 & J(P) & I_d & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & I_d \\ 0 & 0 & 0 & \dots & J(P) \end{pmatrix},$$

which has m blocks of $J(P)$ in the diagonal, where I_d denotes the identity matrix of order d.

The structure theorem for modules over principal ideal domains implies that every indecomposable representation of B is isomorphic to some $J_k(P)$ with $1 \leqslant k \leqslant h$. This is a modified Jordan canonical form theorem.

A *partition* $\lambda = (\lambda_1, \lambda_2, \dots)$ is a finite sequence $\lambda_1 \geqslant \lambda_2 \geqslant \cdots$ of non-negative integers. The λ_i's are called the *parts* of λ. The largest part of λ is denote by $l(\lambda)$, and the integer $|\lambda| = \lambda_1 + \lambda_2 + \cdots$ is called the *weight* of λ. Let $\mathcal{P}$ denote the set of all partitions including the unique partition of 0. Every partition λ can be written in the form $\left(1^{k_1}2^{k_2}3^{k_3}\cdots\right)$, which means that there are k_i parts equal to i in λ.

If $\mu = \left(1^{k_1}2^{k_2}\cdots r^{k_r}\right)$ is a partition, then we define

$$J_\mu(P) = \operatorname{diag}\big(\underbrace{J_1(P), \cdots, J_1(P)}_{k_1 \text{ copies}}, \underbrace{J_2(P), \cdots, J_2(P)}_{k_2 \text{ copies}}, \cdots\cdots, \underbrace{J_r(P), \cdots, J_r(P)}_{k_r \text{ copies}}\big).$$

Thus, $J_\mu(P)$ is a diagonal block matrix with k_i copies of $J_i(P)$ in the diagonal. It is clear that $J_\mu(P)$ has degree $|\mu| d$.

It follows from the Krull-Schmidt theorem that every representation of B is isomorphic to some $J_\mu(P)$ with some unique $\mu \in \mathcal{P}$ such that $l(\mu) \leqslant h$.

3. The number $N(E,n)$

The result in the last section and isomorphism (1.2) show that the isomorphism classes of representations of A of degree n are in one-to-one correspondence with the s-tuples $(\mu_1,\dots,\mu_s)\in\mathcal{P}^s$ such that $l(\mu_i)\leqslant h_i$ for $i=1,\dots,s$ and $\sum_{i=1}^{s}|\mu_i|d_i=n$; here $(\mu_1,\dots,\mu_s)$ corresponds to the matrix $J_{\mu_1}(P_1)\oplus J_{\mu_2}(P_2)\oplus\cdots\oplus J_{\mu_s}(P_s)$, where we use $M\oplus N$ to mean the diagonal block matrix $\operatorname{diag}(M,N)$.

If M is a representation of A of degree n, then the general linear group $GL(n,q)$, which consists of all non-singular $n\times n$ matrices over $\mathbb{F}_q$, acts transitively on the set of representations of A which are isomorphic to M. The stabiliser of M, which is denote by $\operatorname{Aut}(M)$, consists of all invertible matrices commuting with M. And so, the number of elements in this orbit is equal to $|GL(n,q)|/|\operatorname{Aut}(M)|$. As $J(P_i)$ and $J(P_j)$ have no common eigenvalues for all $i\neq j$, an easy exercise shows that

$$\operatorname{Aut}\big(J_{\mu_1}(P_1)\oplus\cdots\oplus J_{\mu_s}(P_s)\big)\cong\operatorname{Aut}\big(J_{\mu_1}(P_1)\big)\oplus\cdots\oplus\operatorname{Aut}\big(J_{\mu_s}(P_s)\big).\tag{3.1}$$

For $\lambda=(\lambda_1,\lambda_2,\cdots)\in\mathcal{P}$, we let $\lambda'=(\lambda'_1,\lambda'_2,\cdots)$ denote the partition conjugate to λ, that is, λ'_i is equal to the number of parts no less than i in λ, and we define $\langle\lambda,\lambda\rangle=\sum_{i\geqslant1}(\lambda'_i)^2$. For example if $\lambda=(3,2,2,1)$ then $\lambda'=(4,3,1)$ and $\langle\lambda,\lambda\rangle=4^2+3^2+1^2=26$. If $\lambda=(\lambda_1,\lambda_2,\cdots)\in\mathcal{P}$ with $\lambda_1\geqslant\lambda_2\geqslant\cdots$, following Macdonald [3] we define $n(\lambda)=\sum_{i\geqslant1}(i-1)\lambda_i$. It is a routine exercise to show that $\langle\lambda,\lambda\rangle=|\lambda|+2n(\lambda)$ for all $\lambda\in\mathcal{P}$. Again following Macdonald, for $\lambda=(1^{k_1}2^{k_2}\cdots)\in\mathcal{P}$ we define $b_\lambda(q)=\prod_{i\geqslant1}(1-q)(1-q^2)\cdots(1-q^{k_i})$.

Notice that for any $\mu\in\mathcal{P}$, $\operatorname{Aut}(J_\mu(P))$ is the centraliser of $J_\mu(P)$ in the group $GL(m,q)$, where $m=|\mu|\deg P$. Formula (2.6) of Macdonald [**3**, p.139] shows that $|\operatorname{Aut}(J_\mu(P))|=q^{d(|\mu|+2n(\mu))}b_\mu(q^{-d})$, where $d=\deg P$. Thus, with notations introduced as above, we have $|\operatorname{Aut}(J_\mu(P))|=q^{d\langle\mu,\mu\rangle}b_\mu(q^{-d})$. And so, the above isomorphism (3.1) implies that

$$|\operatorname{Aut}\big(J_{\mu_1}(P_1)\oplus\cdots\oplus J_{\mu_s}(P_s)\big)|=\prod_{i=1}^{s}q^{d_i\langle\mu_i,\mu_i\rangle}b_{\mu_i}(q^{-d_i}).$$

As $(\mu_1,\dots,\mu_s)$ runs through all s-tuples of partitions which satisfy $l(\mu_i)\leqslant h_i$ for $i=1,\dots,s$ and $\sum_{i=1}^{s}|\mu_i|d_i=n$, the matrix $J_{\mu_1}(P_1)\oplus J_{\mu_2}(P_2)\oplus\cdots\oplus J_{\mu_s}(P_s)$ runs through all isomorphism classes of representations of A of degree n. The number of representations of A which are isomorphic to a single representation $J_{\mu_1}(P_1)\oplus J_{\mu_2}(P_2)\oplus$

https://doi.org/10.1017/S0004972700032603 Published online by Cambridge University Press

$\cdots \oplus J_{\mu_s}(P_s)$ is found to be $|GL(n,q)|$ divided by $\prod_{i=1}^{s} q^{d_i\langle\mu_i,\mu_i\rangle} b_{\mu_i}(q^{-d_i})$. It is well-known that the group $GL(n,q)$ has order $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$. Thus we have proved the following theorem.

Theorem 3.1. *If $E=E(x)$ is a monic polynomial over $\mathbb{F}_q$ with factorisation given by (1.1), then the number of matrices θ of order n over $\mathbb{F}_q$ such that $E(\theta)=0$ is*

$$N(E,n)=\sum_{(\mu_1,\cdots,\mu_s)} \frac{\prod_{0\leqslant i\leqslant n-1}(q^n-q^i)}{\prod_{1\leqslant i\leqslant s} q^{d_i\langle\mu_i,\mu_i\rangle} b_{\mu_i}(q^{-d_i})}$$

where the summation is over all s-tuples of partitions $(\mu_1,\ldots,\mu_s)\in\mathcal{P}^s$ such that $l(\mu_i)\leqslant h_i$ for $i=1,2,\ldots,s$ and $\sum_{i=1}^{s}|\mu_i|d_i=n$.

4. The numbers $N(x^3-1,n)$ and $N(x^4-1,n)$

The numbers $N(x^2-1,n)$ and $N(x^3-1,n)$ were obtained by Hodges [1] and [2] respectively. Here we deduce $N(x^3-1,n)$ and $N(x^4-1,n)$ by using Theorem 3.1, and compare our results with those of Hodges.

For $k\geqslant 1$ we define $\psi_k(q)=(1-q^{-1})(1-q^{-2})\cdots(1-q^{-k})$, with the convention that $\psi_0(q)=1$. Then the order of $GL(n,q)$ can be written as $q^{n^2}\psi_n(q)$. If $\mu=(1^{k_1}2^{k_2}\cdots)\in\mathcal{P}$, then $b_\mu(q^{-1})=\prod_{i\geqslant 1}\psi_{k_i}(q)$.

Let us recall Hodges' results about $N(x^3-1,n)$. The factorisation of x^3-1 into irreducible polynomials over $\mathbb{F}_q$ depends on the residue of q modulo 3.

Case 1. $q\equiv 0 \mod 3$. Then $x^3-1=(x-1)^3$. Formula (6.1) of Hodges [2] implies that

$$N(x^3-1,n)=g_n\sum_{k_1+2k_2+3k_3=n} q^{-a(\pi)}(g_{k_1}g_{k_2}g_{k_3})^{-1}, \tag{4.1}$$

where $a(\pi)=2k_1(k_2+k_3)+k_2^2+4k_2k_3+2k_3^2$ and $g_k=g(k,1)$ with $g(k,d)=q^{dk^2}\prod_{i=1}^{k}(1-q^{-di})$. Note that if $\mu=(1^{k_1}2^{k_2}\cdots)$ then $\langle\mu,\mu\rangle=\sum_{i\geqslant 1}\Big(\sum_{j\geqslant i}k_j\Big)^2$. Now, Theorem 3.1 implies that

$$N(x^3-1,n)=\sum_{k_1+2k_2+3k_3=n}\frac{q^{n^2}\psi_n(q)}{q^{(k_1+k_2+k_3)^2+(k_2+k_3)^2+k_3^2}\psi_{k_1}(q)\psi_{k_2}(q)\psi_{k_3}(q)}. \tag{4.2}$$

Note that $g(k,d)=q^{dk^2}\psi_k(q^d)$ and thus $g_k=q^{k^2}\psi_k(q)$. A simple transformation shows that (4.1) and (4.2) are equivalent.

CASE 2. $q \equiv 1 \mod 3$. Then $x^3 - 1 = (x-1)(x-\alpha)(x-\beta)$ with $\alpha, \beta \in \mathbb{F}_q$ and $\alpha \neq \beta$, $\alpha \neq 1$, $\beta \neq 1$. Formula (6.2) of Hodges [2] shows that

$$N(x^3 - 1, n) = g_n \sum_{k_1+k_2+k_3=n} (g_{k_1} g_{k_2} g_{k_3})^{-1}. \tag{4.3}$$

Theorem 3.1 implies that

$$N(x^3 - 1, n) = \sum_{k_1+k_2+k_3=n} \frac{q^{n^2} \psi_n(q)}{q^{k_1^2+k_2^2+k_3^2} \psi_{k_1}(q) \psi_{k_2}(q) \psi_{k_3}(q)}. \tag{4.4}$$

It is easy to see that (4.3) and (4.4) are equivalent.

CASE 3. $q \equiv 2 \mod 3$. Then $x^3 - 1 = (x-1)(x^2+x+1)$ and x^2+x+1 is irreducible over $\mathbb{F}_q$. Formula (6.3) in Hodges [2] shows that

$$N(x^3 - 1, n) = g_n \sum_{k_1+2k_2=n} \left(g(k_1, 1) g(k_2, 2)\right)^{-1}.$$

The above Theorem 3.1 implies that

$$N(x^3 - 1, n) = \sum_{k_1+2k_2=n} \frac{q^{n^2} \psi_n(q)}{q^{k_1^2+2k_2^2} \psi_{k_1}(q) \psi_{k_2}(q^2)}.$$

It is clear that the above two formulae are equivalent.

The factorisation of $x^4 - 1$ into irreducible polynomials over $\mathbb{F}_q$ depends on the residue of q modulo 4. There are three cases to be considered.

CASE 1. $q \equiv 0$ *or* $2 \mod 4$. Then $\mathit{char}\, \mathbb{F}_q = 2$, and so $x^4 - 1 = (x-1)^4$. Thus Theorem 3.1 implies that

$$N(x^4 - 1, n) = \sum_{k_1+2k_2+3k_3+4k_4=n} \frac{q^{n^2} \psi_n(q)}{q^{t(k_1,k_2,k_3,k_4)} \psi_{k_1}(q) \psi_{k_2}(q) \psi_{k_3}(q) \psi_{k_4}(q)},$$

where $t(k_1, k_2, k_3, k_4) = (k_1+k_2+k_3+k_4)^2 + (k_2+k_3+k_4)^2 + (k_3+k_4)^2 + k_4^2$.

CASE 2. $q \equiv 1 \mod 4$. Then x^2+1 is reducible over $\mathbb{F}_q$, and $x^2+1 = (x-\alpha)(x-\beta)$ with $\alpha, \beta \in \mathbb{F}_q$ and $\alpha \neq \beta$, $\alpha \neq \pm 1$, $\beta \neq \pm 1$. Thus $x^4 - 1 = (x-1)(x+1)(x-\alpha)(x-\beta)$ in $\mathbb{F}_q[x]$, and hence Theorem 3.1 implies that

$$N(x^4 - 1, n) = \sum_{k_1+k_2+k_3+k_4=n} \frac{q^{n^2} \psi_n(q)}{q^{k_1^2+k_2^2+k_3^2+k_4^2} \psi_{k_1}(q) \psi_{k_2}(q) \psi_{k_3}(q) \psi_{k_4}(q)}.$$

CASE 3. $q \equiv 3 \bmod 4$. Then x^2+1 is irreducible over $\mathbb{F}_q$. Thus in $\mathbb{F}_q[x]$ we have $x^4-1=(x-1)(x+1)(x^2+1)$, and Theorem 3.1 implies that

$$N(x^4-1,n)=\sum_{k_1+k_2+2k_3=n}\frac{q^{n^2}\psi_n(q)}{q^{k_1^2+k_2^2+2k_3^2}\psi_{k_1}(q)\psi_{k_2}(q)\psi_{k_3}(q^2)}.$$

REFERENCES

[1] J. H. Hodges, 'The matrix equations $X^2-I=0$ over a finite field', *Amer. Math. Monthly* **65** (1958), 518–520.

[2] J.H. Hodges, 'Scalar polynomial equations for matrices over a finite field', *Duke Math. J.* **25** (1958), 291–296.

[3] I. G. Macdonald, *Symmetric functions and Hall polynomials* (Clarendon Press, Oxford, 1979).

School of Mathematics
University of New South Wales
Sydney NSW 2052
Australia
e-mail: hua@maths.unsw.edu.au