DISTRIBUTION OF MATRICES IN A FINITE FIELD

L. CARLITZ AND JOHN H. HODGES

1. Introduction and notation. This paper is mainly concerned with the distribution with respect to characteristic polynomial and factors of the characteristic polynomial, of square matrices with elements in a finite field $GF(q)$. The method employed is to investigate the properties of the polynomials in question, that is, the matric problems are reduced to problems concerning polynomials. In this connection see a recent paper by Walker [5] on Fermat's theorem for algebras; incidentally Walker's Theorem 3 had been proved earlier in [1; § 7].

The properties of matrices assumed here may be found in [4]. German capitals $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \cdots$ will denote square matrices with elements in $GF(q)$. Polynomials in an indeterminate x with coefficients in $GF(q)$ will be denoted by $F(x), M(x), \cdots$ in § 2 and simply by $F, M, \cdots$ elsewhere.

The number of partitions of the positive integer m into at most r parts will be denoted by $\pi_r(m)$, with $\pi_m(m)=\pi(m)$, the number of unrestricted partitions of m. The symbol $\pi'_r(m)$ will denote the *weighted* partition into at most r parts:

$$\pi'_r(m)=\sum_{k_1+2k_2+\cdots+rk_r=m} q^{k_1+k_2+\cdots+k_r}, \tag{1.1}$$

with $\pi'_m(m)=\pi'(m)$, the unrestricted weighted partition.

In Theorem 1 below the number of non-derogatory matrices of order m is given in terms of the Euler ϕ-function for $GF[q, x]$.

If $F=F(x)$ is a polynomial of degree m and $F=P_1^{r_1}\cdots P_s^{r_s}$, where the P_i are distinct irreducible polynomials, we find (Theorem 2) that the number of *classes* of similar matrices of order m with characteristic polynomial $F(x)$ is

$$C_m(F)=\pi(r_1)\cdots\pi(r_s)\ . \tag{1.2}$$

Theorem 3 determines the total number $N(m)$ of distinct classes of similar matrices of order m as

$$N(m)=\pi'(m)\ , \tag{1.3}$$

where $\pi'(m)$ is defined in (1.1) with $r=m$.

We also find (Theorem 4) the number of distinct classes of similar matrices of order m with minimum polynomial of degree r, where r is a fixed integer $\leq m$. Finally in § 4 we consider a polynomial problem

Received May 16, 1955.

which is suggested by the problem of determining the number of admissible minimum polynomials of fixed degree r for matrices of order m.

2. Non-derogatory matrices over $GF(q)$. Let A be a non-derogatory matrix of order m with elements in $GF(q)$, that is a matrix for which the characteristic and minimum polynomials are identical. Then it is well known that $\mathfrak{A}\mathfrak{S}=\mathfrak{S}\mathfrak{A}$ if and only if $\mathfrak{S}=F(\mathfrak{A})$, where $F(x)$ is a scalar polynomial of degree $\leq m-1$. Moreover if $M(x)$ denotes the characteristic polynomial of $\mathfrak{A}$, then $\mathfrak{S}$ is non-singular if and only if $(F(x), M(x))=1$. Clearly, corresponding to every such polynomial $F(x)$, there is a unique primary polynomial $G(x)$ of degree m such that $(F(x), M(x))=1$, if and only if $(G(x), M(x))=1$. Thus, the number of distinct non-singular matrices $\mathfrak{S}$ which commute with $\mathfrak{A}$ is the number of primary (sometimes called *monic*) polynomials $G(x)$ of degree m such that $(G(x), M(x))=1$. This number, which is the Euler function for $GF[q, x]$, the polynomial domain in x over $GF(q)$, is given in [2; 21] by the formula

$$\phi(M(x))=q^m \prod_{P(x)\mid M(x)}\left(1-\frac{1}{|P(x)|}\right), \tag{2.1}$$

where $P(x)$ runs through all primary prime divisors of $M(x)$ and $|P(x)|=q^e$, where $\deg P(x)=e$.

We recall that similar matrices have the same characteristic polynomial and that if two non-derogatory matrices have the same characteristic polynomial they are similar. Thus, as $\mathfrak{S}$ runs through all the non-singular matrices of order m, the form $\mathfrak{S}^{-1}\mathfrak{A}\mathfrak{S}$ runs through the set of all non-derogatory matrices of order m having characteristic polynomial $M(x)$, each one appearing as many times as $\mathfrak{A}$ appears, namely $\phi(M(x))$. If we let g_m denote the number of non-singular matrices of order m, we have

THEOREM 1. *The number of non-derogatory matrices of order m in $GF(q)$ is*

$$Y(m)=g_m \sum_{\deg M(x)=m} \frac{1}{\phi(M(x))}, \tag{2.2}$$

where the sum is over primary $M(x)$ only, $\phi(M(x))$ is the Euler function and $g_m=\prod_{r=0}^{m-1}(q^m-q^r)$ is the number of non-singular matrices of order m.

3. Distribution of classes of similar matrices in $GF(q)$. If $\mathfrak{A}$ and $\mathfrak{B}$ are matrices of order m with the elements in $GF(q)$, we will say that $\mathfrak{A}$ and $\mathfrak{B}$ are in the same *class* if and only if they are similar. If $F(x)$ is the characteristic polynomial of a matrix $\mathfrak{A}$ of order m, then

$$F=H_1H_2\cdots H_m\ , \tag{3.1}$$

where $H_{i+1}|H_i$, and the H_i are the invariant factors of $x\mathfrak{J}-\mathfrak{A}$. In particular we call H_1 the first invariant factor. (In the remainder of this paper a polynomial $F(x)$ will simply be denoted by the letter F.) If we put

$$H_i=E_iH_{i+1} \quad \text{and} \quad H_m=E_m\ , \tag{3.2}$$

then we also have

$$F=E_1E_2^2E_3^3\cdots E_m^m\ . \tag{3.3}$$

Let $C_m(F)$ denote the number of distinct classes of order m having characteristic polynomial F. Then it is clear that $C_m(F)$ is the number of distinct representations of F in the form of (3.3). If we also have

$$F=P_1^{r_1}P_2^{r_2}\cdots P_s^{r_s}\ , \tag{3.4}$$

where the P_i are distinct prime polynomials, it follows that

$$C_m(F)=C_m(P_1^{r_1})C_m(P_2^{r_2})\cdots C_m(P_s^{r_s})\ . \tag{3.5}$$

For any prime polynomial P and positive integer r, $C_m(P^r)$ is seen to be the number of unrestricted partitions of r, or $\pi(r)$. Thus in view of (3.5) we have proved the following.

THEOREM 2. *If F is a polynomial of order m with coefficients in $GF(q)$ and F has the factorization* (3.4), *then the number of distinct classes of order m having characteristic polynomial F is*

$$C_m(F)=\pi(r_1)\pi(r_2)\cdots\pi(r_s)\ . \tag{3.6}$$

Let $N(m)$ denote the number of distinct classes of matrices of order m. Then it is clear that

$$N(m)=\sum_{\deg F=m} C_m(F)\ ,$$

where the sum is over primary F only. In view of the definition of $C_m(F)$ and the factorization (3.3) we may write

$$\sum_F \frac{C_m(F)}{|F|^s}=\sum_{E_1}\frac{1}{|E_1|^s}\sum_{E_2}\frac{1}{|E_2|^{2s}}\cdots\sum_{E_m}\frac{1}{|E_m|^{ms}}\ , \tag{3.7}$$

where the sums are over all primary $F, E_1, \cdots, E_m$. Since we have

$$\zeta(s)=\sum_F\frac{1}{|F|^s}=\prod_P\left(1-\frac{1}{|P|^s}\right)^{-1}=\sum_{k=0}^{\infty}\frac{q^k}{q^{ks}}=(1-q^{1-s})^{-1}\ , \tag{3.8}$$

which converges absolutely for real $s>1$, (3.7) becomes

$$\sum_F \frac{C_m(F)}{|F|^s} = \sum_{k_1=0}^{\infty} \frac{q^{k_1}}{q^{k_1 s}} \sum_{k_2=0}^{\infty} \frac{q^{k_2}}{q^{2k_2 s}} \cdots \sum_{k_m=0}^{\infty} \frac{q^{k_m}}{q^{mk_m s}} . \tag{3.9}$$

It therefore follows that $N(m)$ is the coefficient of q^{-ms} in the right member of (3.9). Calculating this coefficient we get the following theorem.

THEOREM 3. *The number of distinct classes of similar matrices of order m in $GF(q)$ is*

$$N(m) = \sum_{k_1+2k_2+\cdots+mk_m=m} q^{k_1+k_2+\cdots+k_m} = \pi'(m) . \tag{3.10}$$

Let $N(m, r)$ denote the number of distinct classes of matrices of order m for which $\deg H_1 = r$, where H_1 is the first invariant factor as defined in (3.1). Then $N(m, r)$ will be the coefficient of $q^{-rs}q^{-mt}$ in the series

$$\sum_{H_{i+1}|H_i} \frac{1}{|H_1|^s |H_1 H_2 \cdots H_m|^t} , \tag{3.11}$$

where the H_i are all primary.

In view of the definition of the polynomials E_i, the series in (3.11) is equal to

$$\sum_{E_i} \frac{1}{|E_1 E_2 \cdots E_m|^s |E_1 E_2^2 \cdots E_m^m|^t} \sum_{E_1} \frac{1}{|E_1|^{s+t}} \cdots \sum_{E_m} \frac{1}{|E_m|^{s+mt}} .$$

Then with $s+t>1$, this product may be written as

$$\zeta(s+t)\zeta(s+2t)\cdots\zeta(s+mt) = \frac{1}{(1-q^{1-s-t})(1-q^{1-s-2t})\cdots(1-q^{1-s-mt})} . \tag{3.12}$$

In view of (3.8) it is clear that the coefficient of $q^{-rs}q^{-mt}$ in the right member of (3.12) is the same as in the product

$$\frac{1}{(1-q^{1-s-t})(1-q^{1-s-2t})\cdots(1-q^{1-s-mt})\cdots}$$

By means of a well-known identity [3; 278], this second product is equal to the series

$$\sum_{k=0}^{\infty} (q^{1-s-t})^k \frac{1}{(1-q^{-t})(1-q^{-2t})\cdots(1-q^{-kt})} . \tag{3.13}$$

By choosing $k=r$ in (3.13) the coefficient of q^{-rs-mt} may be easily obtained. We get the following theorem.

THEOREM 4. *The number of distinct classes of similar matrices of order m in $GF(q)$ for which* $\deg H_1 = r$, *where H_1 is the first invariant factor as defined in* (3.1), *is given by*

$$N(m, r) = q^r \sum_{i_1+2i_2+\cdots+ri_r=m-r} 1 = q^r \pi_r(m-r) .$$

4. Another problem. Let us consider the product

$$\prod \left\{1 + \frac{1}{|P|^s}\left(\frac{1}{|P|^t} + \frac{1}{|P|^{2t}} + \cdots\right) + \frac{1}{|P|^{2s}}\left(\frac{1}{|P|^{2t}} + \frac{1}{|P|^{3t}} + \cdots\right) + \cdots\right\} , \tag{4.1}$$

taken over all primary prime polynomials P in $GF(q)$. In order to determine an interval of convergence for this product, we consider the associated series

$$\sum_P \left\{\frac{1}{|P|^s}\left(\frac{1}{|P|^t} + \cdots\right) + \frac{1}{|P|^{2s}}\left(\frac{1}{|P|^{2t}} + \cdots\right) + \cdots\right\} . \tag{4.2}$$

The series may be written more simply as

$$\sum_P \frac{|P|^{-s-t}}{(1-|P|^{-t})(1-|P|^{-s-t})} . \tag{4.3}$$

For t real and positive, the denominators of the terms in (4.3) approach 1 as $\deg P$ grows large, so that we need only consider the numerators. Comparing with (3.8) we see that the series and consequently the product (4.1) converge absolutely for real s, t such that $t > 0$ and $s + t > 1$.

It is clear that the product (4.1) is equal to the series

$$\sum_{H|F} \frac{1}{|H|^s |F|^t} , \tag{4.4}$$

where the sum is over all pairs H, F of primary polynomials over $GF(q)$ such that $H|F$ and every distinct prime factor of F is a factor of H. Thus F and H may be thought of as characteristic and minimum polynomial, respectively, of some matrix. Letting $T(m, r)$ denote the number of such pairs for which $\deg F = m$ and $\deg H = r$, it is clear that $T(m, r)$ is the coefficient of q^{-rs-mt} in the series (4.4). Unfortunately, however, it does not seem possible to get a simple explicit formula for $T(m, r)$.[1]

If we take $s = 0$, then (4.1) and (4.4) converge for real $t > 1$, and denoting by $T(m)$ the coefficient of q^{-mt} in the series (4.4), we have

$$T(m) = \sum_{r=0}^{\infty} T(m, r) . \tag{4.5}$$

[1] We note that, were it not for possible repetions of H in (4.4), the number $T(m, r)$ would be the number of admissible minimum polynomials of degree $r = m$ for matrices of order m.

With $s=0$, (4.1) simplifies to

$$\prod_P \left\{1+\frac{|P|^{-t}}{1-|P|^{-t}}+\frac{|P|^{-2t}}{1-|P|^{-t}}+\cdots\right\}=\prod\frac{1-|P|^{-t}+|P|^{-2t}}{(1-|P|^{-t})^2} \tag{4.6}$$

$$=\prod\frac{(1+|P|^{-3t})(1-|P|^{-3t})}{(1-|P|^{-t})(1-|P|^{-2t})(1-|P|^{-3t})}\ .$$

Using (3.8) this is seen to be equal to

$$\frac{\zeta(t)\zeta(2t)\zeta(3t)}{\zeta(6t)}=(1-q^{1-6t})\sum_{k_1=0}^{\infty}\frac{q^{k_1}}{q^{k_1t}}\cdot\sum_{k_2=0}^{\infty}\frac{q^{k_2}}{q^{2k_2t}}\cdot\sum_{k_3=0}^{\infty}\frac{q^{k_3}}{q^{3k_3t}}\ . \tag{4.7}$$

Computing the coefficient of q^{-mt} in the product series on the right side of (4.7) gives the following theorem.

THEOREM 5. *If $T(m,r)$ is the number of pairs H, F of polynomials over $GF(q)$ such that $H|F$, every distinct prime factor of F is a factor of H,* $\deg F=m$ *and* $\deg H=r$, *then*

$$T(m)=\sum_{r=0}^{m}T(m,r)=\pi_3'(m)-q\pi_3'(m-6)\ , \tag{4.8}$$

where $\pi_r'(m)$ is the weighted partition defined by (1.1).

REFERENCES

1. L. Carlitz, *On polynomials in a Galois field*, Bull. Amer. Math. Soc., **38** (1932), 736-744.
2. R. Dedekind, *Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, J. Reine Angew. Math., **54** (1857), 1-26.
3. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, 1938.
4. C. C. MacDuffee, *The theory of matrices*, New York, 1946.
5. Gordon L. Walker, *Fermat's theorem for algebras*, Pacific J. Math., **4** (1954), 317-320.

DUKE UNIVERSITY