RESTRICTED PRODUCT OF THE CHARACTERISTIC POLYNOMIALS OF MATRICES OVER A FINITE FIELD

BY

L. CARLITZ[1]

1. Put $\Phi = GF(q)$, the finite field of order q and let Φ_m denote the set of $m \times m$ matrices M with elements in Φ. We separate Φ_m into similarity classes and let Φ_m^* denote a set of representatives of the similarity classes. Now put

$$U_m = \prod_{M \epsilon \Phi_m^*} f(M),$$

where the product is extended over the elements of Φ_m^* and

$$f(M) = \det(xI - M).$$

It is known [1] that

$$F_m = \prod_{\deg A = m} A(x),$$

the product of the monic polynomials of degree m in $GF[q, x]$, satisfies

$$F_m = \prod_{s=0}^{m-1} (x^{q^m} - x^{q^s}).$$

We shall show that

$$U_m = \prod_{t=1}^{m} F_t^{u_t(m)}, \tag{1}$$

where

$$u_t(m) = \sum_{s \geq 1} s\{\beta(m - st) - q\beta(m - s(t + 1))\} \tag{2}$$

and $\beta(m)$ is defined by

$$\beta(m) = \sum q^{c_1 + c_2 + \cdots + c_m}, \tag{3}$$

the summation extending over all nonnegative $c_1, \cdots, c_m$ such that

$$c_1 + 2c_2 + \cdots + mc_m = m.$$

It is known [2] that $\beta(m)$ is equal to the number of similarity classes of $m \times m$ matrices over Φ.

2. Let $A_1, A_2, \cdots, A_m$ denote the invariant factors of $xI - M$, so that the A_j are monic polynomials in $GF[q, x]$ that satisfy

$$A_j \mid A_{j+1} \qquad (j = 1, \cdots, m);$$

moreover

$$f(M) = \det(xI - M) = A_1 A_2 \cdots A_m$$

and

$$m = \deg A_1 + \deg A_2 + \cdots + \deg A_m.$$

Received December 16, 1965.

[1] Supported in part by a National Science Foundation grant.

If we put

$$A_1 = B_1, \quad A_j = A_{j-1}B_j = B_1B_2 \cdots B_j \qquad (j = 1, \cdots, m)$$

then

$$f(M) = B_1^m B_2^{m-1} \cdots B_m;$$

also if

$$b_j = \deg B_j \qquad (j = 1, \cdots, m) \tag{4}$$

then

$$m = mb_1 + (m-1)b_2 + \cdots + b_m. \tag{5}$$

Except for this condition the B_j are arbitrary monic polynomials. It therefore follows from the definition of U_m that

$$U_m = \prod B_1^m B_2^{m-1} \cdots B_m, \tag{6}$$

where the product extends over all monic polynomials $B_1, \cdots, B_m$ that satisfy (4) and (5). Making use of the definition of F_m it is clear that (6) reduces to

$$U_m \prod F_{b_1}^{mq^{b-b_1}} F_{b_2}^{(m-1)q^{b-b_2}} \cdots F_{b_m}^{q^{b-b_m}}, \tag{7}$$

where $b = b_1 + b_2 + \cdots + b_m$ and the product extends over all nonnegative integers $b_1, b_2, \cdots, b_m$ that satisfy (5).

It is convenient to change the notation slightly. If we put

$$c_j = b_{m-j+1} \qquad (j = 1, \cdots, m)$$

then (7) becomes

$$U_m = \prod F_{c_1}^{q^{c-c_1}} F_{c_2}^{2q^{c-c_2}} \cdots F_{c_m}^{mq^{c-c_m}}, \tag{8}$$

where $c = c_1 + c_2 + \cdots + c_m$ and the product now is over all non-negative $c_1, c_2, \cdots, c_m$ such that

$$c_1 + 2c_2 + \cdots + mc_m = m. \tag{9}$$

Clearly (8) implies

$$U_m = \prod_{t=1}^m F_t^{u_t(m)}, \tag{10}$$

where

$$u_t(m) = \sum_{\pi(m)} \sum_{k_j=t} jq^{k_1+\cdots+k_m-k_j}, \tag{11}$$

where the outer sum is over all partitions

$$m = k_1 + 2k_2 + 3k_3 + \cdots. \tag{12}$$

Then by (11) and (12)

$$\begin{aligned}\sum_{m=0}^\infty u_t(m)x^m &= \sum_{m=0}^\infty x^m \sum_{\pi(m)} \sum_{k_j=t} jq^{k_1+\cdots+k_m-k_j} \\ &= \sum_{k_1,k_2,\cdots=0}^\infty x^{k_1+2k_2+\cdots} \sum_{k_j=t} jq^{(k_1+k_2+\cdots)-k_j},\end{aligned}$$

so that

$$\begin{aligned}\sum_{t=1}^{m}\sum_{m=0}^{\infty} u_t(m)x^m y^t &= \sum_{k_1,k_2,\cdots=0}^{\infty} x^{k_1+2k_2+\cdots} q^{k_1+k_2+\cdots}\cdot\sum_{j=1;k_j>0}^{\infty} jq^{-k_j}y^{k_j}\\ &= \sum_{j=1}^{\infty} j\sum_{k_1,k_2,\cdots=0;k_j>0}^{\infty} x^{k_1+2k_2+\cdots}q^{k_1+k_2+\cdots}q^{-k_j}y^{k_j}\\ &= \prod_{n=1}^{\infty}(1-qx^n)^{-1}\cdot\sum_{j=1}^{\infty} jx^j y(1-qx^j)/(1-x^j y).\end{aligned}$$

Now

$$\begin{aligned}\sum_{m=0}^{\infty}\beta(m)x^m &= \sum_{m=0}^{\infty} x^m \sum_{c_1+2c_2+\cdots=m} q^{c_1+c_2+\cdots}\\ &= \prod_{n=1}^{\infty}(1-qx^n)^{-1}\end{aligned}$$

and

$$\sum_{j=1}^{\infty} jx^j y(1-qx^j)/(1-x^j y) = \sum_{j=1}^{\infty}\sum_{t=1}^{\infty} jx^{jt}y^t(1-qx^j),$$

so that

$$\sum_{t=1}^{m}\sum_{m=0}^{\infty} u_t(m)x^m y^t = \sum_{m=0}^{\infty}\beta(m)x^m\sum_{j=1}^{\infty} j\sum_{t=1}^{\infty} x^{jt}y^t(1-qx^j).$$

This implies

$$\sum_{m=0}^{\infty} u_t(m)x^m = \sum_{m=0}^{\infty}\beta(m)x^m\sum_{j=1}^{\infty} jx^{jt}(1-qx^j)$$

and therefore

$$u_t(m) = \sum_{j\geq 1} j\{\beta(m-jt) - q\beta(m-j(t+1))\}.$$

This completes the proof of (2).

In particular we have

$$\begin{aligned}u_m(m) &= \beta(0) = 1,\\ u_{m-1}(m) &= \beta(1) - q\beta(0) = 0 \qquad (\mathrm{m} > 2).\end{aligned}$$

Note that

$$\begin{aligned}u_{m-2}(m) &= \beta(2) - q\beta(1) = q \qquad (m > 4)\\ u_{m-3}(m) &= \beta(3) - q\beta(2) = q \qquad (m > 6)\\ u_{m-4}(m) &= \beta(4) - q\beta(3) = q^2 + q \qquad (m > 8).\end{aligned}$$

3. Comparing degrees on both sides of (1) and using the fact that the number of factors in the product (6) is $\beta(m)$, we get

$$m\beta(m) = \sum_{t=1}^{m} tq^t u_t(m). \tag{13}$$

This can be verified directly, thus affording a partial check of (1). It follows from

$$\sum_{m=0}^{\infty}\beta(m)x^m = \prod_{1}^{\infty}(1-qx^n)^{-1}$$

by differentiating with respect to x that

$$\sum_{0}^{\infty} m\beta(m)x^m = \prod_{1}^{\infty}(1-qx^n)^{-1}\cdot\sum_{1}^{\infty} nqx^n/(1-qx^n). \tag{14}$$

On the other hand

$$\begin{aligned}\sum_{m=1}^{\infty} x^m \sum_{t=1}^{m} tq^t u_t(m) &= \sum_{m=1}^{\infty} x^m \sum_{t=1}^{m} tq^t \sum_{s\geq 1} s\{\beta(m-st) - q\beta(m-s(t+1))\} \\ &= \sum_{s,t=1}^{\infty} stq^t x^{st} \sum_{m=0}^{\infty} \beta(m)x^m - q\sum_{s,t=1}^{\infty} stq^t x^{s(t+1)} \sum_{m=0}^{\infty} \beta(m)x^m \\ &= \sum_{m=0}^{\infty} \beta(m)x^m \{\sum_{s,t=1}^{\infty} stq^t x^{st} - \sum_{s,t=1}^{\infty} s(t-1)q^t x^{st}\} \\ &= \sum_{m=0}^{\infty} \beta(m)x^m \sum_{s,t=1}^{\infty} sq^t x^{st} \\ &= \sum_{m=0}^{\infty} \beta(m)x^m \sum_{s=1}^{\infty} sqx^s/(1-qx^s).\end{aligned}$$

Comparing this with (14) it is evident that we have proved (13).

Incidentally it follows from (14) that

$$m\beta(m) = \sum_{j=1}^{m} \sigma(j)\beta(m-j), \tag{15}$$

where

$$\sigma(n) = \sum_{st=n} sq^t.$$

Note that, for $q = 1$, $\beta(m)$ reduces to $p(m)$, the number of unrestricted partitions of m.

4. U_m can also be exhibited in the form

$$U_m = \prod_{k=1}^{m} (x^{q^k} - x)^{u_k'(m)}. \tag{16}$$

Indeed by (1)

$$\begin{aligned}U_m = \prod_{t=1}^{m} F_t^{u_t(m)} &= \prod_{t=1}^{m} \{\prod_{k=1}^{t} (x^{q^k} - x)^{q^{t-k}}\}^{u_t(m)} \\ &= \prod_{k=1}^{m} \prod_{t=k}^{m} (x^{q^k} - x)^{q^{t-k}u_t(m)} \\ &= \prod_{k=1}^{m} (x^{q^k} - x)^{\sum_{t=k}^{m} q^{t-k}u_t(m)},\end{aligned}$$

so that

$$\begin{aligned}u_k'(m) &= \sum_{t=k}^{m} q^{t-k}u_t(m) \\ &= \sum_{t=k}^{m} q^{t-k} \sum_{s\geq 1} s\{\beta(m-st) - q\cdot\beta(m-s(t+1))\} \\ &= \sum_{t=k;\, st\leq m}^{m} sq^{t-k}\beta(m-st) - \sum_{t=k+1;\, st\leq m}^{m} sq^{t-k}\beta(m-st) \\ &= \sum_{sk\leq m} s\beta(m-sk).\end{aligned}$$

Thus

$$u_k'(m) = \sum_{1\leq s\leq m/k} s\beta(m-sk). \tag{17}$$

Since $u_k'(m) - qu_{k+1}'(m) = u_k(m)$, it is evident that (17) and (2) are equivalent.

5. It would be of interest to evaluate

$$V_m = \prod_M \det(xI - M),$$

where now the product is over all Φ_m. We can show that

$$V_m = \prod_{t=1}^{m} F_t^{v_t(m)} \tag{18}$$

or equivalently

$$V_m = \prod_{t=1}^{m} (x^{q^t} - x)^{v_t'(m)}. \tag{19}$$

However it seems difficult to evaluate $v_t(m)$ or $v_t'(m)$.

To prove (18) let $xI - M$ have k_{ij} elementary divisors P_i^j, where $\deg P_i = d_i$. An exact formula for the number of nonsingular matrices that commute with M is known [3, pp. 229–236]. This number depends only on the elementary divisors but is very complicated. Let $e(k_{ij}, d_i)$ represent this number and let $g(m)$ be the total number of nonsingular $m \times m$ matrices. Then

$$N(k_{ij}, d_i) = g(m)/e(k_{ij}, d_i)$$

is the number of matrices similar to M. It follows that

$$V_m = \prod P_i^{jN(k_{ij}, d_i)} \tag{20}$$

the product extending over all irreducible P_i of degree d_i such that

$$m = \sum_{i,j} j\, d_i\, k_{ij}.$$

Since

$$\prod_{\deg P = d} P = \prod_{rs=d} (x^{q^r} - x)^{\mu(s)},$$

it is evident that (20) implies (19) which in turn implies (18). Unfortunately the value of $v_m(t)$ obtained in this way is very complicated.

To illustrate we compute V_2 by a direct method. Take

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

so that

$$xI - M = x^2 - (a + d)x + ad - bc.$$

Then

$$V_2 = \prod_{a,b,c,d} (x^2 - (a + d)x + ad - bc),$$

the product extending over all $a, b, c, d \in GF(q)$. Now

$$\begin{aligned} \prod_{bc} (y - bc) &= y^q \prod_{b \neq 0} \prod_c (y - bc) \\ &= y^q \prod_c (y - c)^{q-1} \\ &= y^q (y^q - y)^{q-1}. \end{aligned}$$

If we take $y = (x - a)(x - d)$ it is clear that

$$\begin{aligned} V_2 &= \prod_{a,d} (x - a)^q (x - d)^q \cdot \prod_{a,d} (x^{2q} - x^2 - (a + d)(x^q - x))^{q-1} \\ &= (x^q - x)^{2q^2} \cdot \prod_a (x^{2q} - x^2 - a\,(x^q - x))^{q(q-1)} \end{aligned}$$

$$= (x^q - x)^{2q^2}\{(x^{2q} - x^2)^q - (x^q - x)^{q-1}(x^{2q} - x^2)\}^{q(q-1)}$$
$$= (x^q - x)^{2q^2}(x^q - x)^{q^2}(q - 1)\{(x^q + x)^q - (x^q + x)\}^{q(q-1)}$$
$$= (x^q - x)^{q^3+q}(x^{q^2} - x)^{q(q-1)}.$$

Thus

$$V_2 = (x^q - x)^{q^3+q^2}(x^{q^2} - x)^{q^2-q} = F_1^{2q^2} F_2^{q^2-q}. \tag{21}$$

6. We can compute $v_m(m) = v_m'(m)$ in the following way. If $\det (xI - M) = P$, where P is an irreducible polynomial of degree m, then M is nonderogatory. Thus the matrices that commute with M are given by $f(M)$, where $f(x)$ is an arbitrary polynomial of degree $<m$. To get the nonsingular matrices that commute with M we take $f(x) \neq 0$. Thus the number of nonsingular matrices that commute with M is equal to $q^m - 1$. Therefore the number of matrices similar to M is $g(m)/(q^m - 1)$, where $g(m)$ is the number of nonsingular $m \times m$ matrices. It follows at once that

$$\begin{aligned} v_m(m) = v_m'(m) &= g(m)/(q^m - 1) \\ &= (q^m - q)(q^m - q^2) \cdots (q^m - q^{m-1}). \end{aligned} \tag{22}$$

It is also not difficult to compute $v_{m-1}'(m)$ for $m > 2$. Put $\det (xI - M) = (x + a)P$, where P is irreducible of degree $m - 1$. As before M is nonderogatory and we find that the number of nonsingular matrices that commute with M is equal to $(q - 1)(q^{m-1} - 1)$. Then the number of matrices similar to M is equal to

$$(q - 1)^{-1}(q^{m-1} - 1)^{-1}g(m).$$

It follows that

$$v_{m-1}'(m) = q(q - 1)^{-1}(q^{m-1} - 1)^{-1}g(m) \qquad (m > 2). \tag{23}$$

References

1. L. Carlitz, *On polynomials in a Galois field,* Bull. Amer. Math. Soc., vol. 38 (1932), pp. 736–744.
2. L. Carlitz and John H. Hodges, *Distribution of matrices in a finite field,* Pacific J. Math., vol. 6 (1965), pp. 225–230.
3. L. E. Dickson, *Linear groups*, New York, Dover, 1958.

Duke University
Durham, North Carolina