Commutators over finite fields

By LARRY S. JOHNSON (Durango, Col.), A. DUANE PORTER
and VERNE J. VARINEAU (Laramie, Wy.)

1. *Introduction.* The principal results of this paper are contained in Theorem 6 of Section 2 wherein formulas for the number of nonsingular $n \times n$ matrices over a finite field with a fixed trace are stated. A corollary result is a formula for the number of nonsingular commutators of order n. In Section 3 we evaluate a sum which is a variation of a formula of HODGES [4].

2. *The number of nonsingular commutators over a finite field.* We use the customary $GF(q)$ for a finite field of $q=p^r$ elements. All matrices mentioned in this paper are square unless otherwise specified. Recall that the trace of a matrix is the sum of its diagonal elements. The reader is also reminded of the meaning of commutator: A matrix B is a commutator if and only if there exists matrices X and Y such that $B=XY-YX$. A useful characterization of commutators is given by the following theorem [1, p. 2]:

Theorem 1. *A matrix over a field F is a commutator if and only if its trace is zero.*

Let us introduce the following notation: For any positive integer n and any $k \in GF(q)$ let $\varphi_k(n)$ denote the number of nonsingular matrices over $GF(q)$ of order n and trace k. Thus it is evident from Theorem 1 that $\varphi_0(n)$ is the number of commutators of order n over $GF(q)$. If we let $N(n)$ denote the number of nonsingular matrices of order n over $GF(q)$ we obtain the following:

Theorem 2. $\varphi_0(n)+(q-1)\varphi_k(n)=N(n)$ *for any* $k \neq 0$.

PROOF. We first show that if $h \neq 0$ and $k \neq 0$ then $\varphi_h(n)=\varphi_k(n)$. This follows by observing that the function $f(A)=kh^{-1}A$ is a one-one mapping of the set of nonsingular matrices of trace h onto the set of nonsingular matrices of trace k. Since there are $q-1$ choices for $k \neq 0$ the theorem follows immediately.

The following two theorems are special cases of a theorem of LANDSBERG [6], but we state them for use later in this paper.

Theorem 3. $N(n)=\prod_{j=0}^{n-1}(q^n-q^j)$.

Theorem 4. *If $Q(m, n)$ denotes the number of $m \times n$ matrices of rank m over $GF(q)$ then* $Q(m, n)=\prod_{j=0}^{m-1}(q^n-q^j)$.

By use of Theorems 2 and 3 we are able to derive explicit formulas for $\varphi_k(2)$ and for any $k \in GF(q)$.

Theorem 5. $\varphi_0(2)=q^2(q-1)$ *and* $\varphi_k(2)=q(q^2-q-1)$ *for any* $k\neq 0$.

PROOF. To determine $\varphi_0(2)$ we note that any 2×2 matrix A of trace 0 will have the form $A=\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$. We see that there are q^3 matrices of this form over GF(q). To determine the number of non-singular matrices of this form we shall subtract from q^3 the number of singular matrices of this form. But the number of singular matrices is given by the number of ways $\det(A)=-a^2-bc=0$.

Case I. Suppose $b\neq 0$. In this case b can be chosen in $q-1$ ways, a in q ways and c is fixed. Thus there are $q(q-1)$ matrices of the required form. *Case* II. Suppose $b=0$. Then $a=0$ and c can be any one of q choices. Hence in this case there is a total of q choices A. On combining cases I and II we see there are q^2 singular matrices of form A and the formula for $\varphi_0(2)$ follows.

On using this last result along with Theorems 2 and 3 we get

$$q^2(q-1)+(q-1)\varphi_k(2) = (q^2-1)(q^2-q).$$

On solving for $\varphi_k(2)$ we get the desired result.

We now prove three lemmas which ultimately lead to formulas for $\varphi_k(n)$ in Theorem 6.

Lemma 1. *If* $\alpha_k(n)$ *denotes the number of nonsingular matrices of order* n *and trace* k *having at least one non-zero element in the nth column above the* (n, n) *position then*

$$\varphi_k(n) = \alpha_k(n)+q^{n-1}[N(n-1)-\varphi_k(n-1)].$$

PROOF. We shall let $\beta_k(n)$ denote the number of nonsingular matrices T of trace k and order n having zero in every position in the nth column above the (n, n) position. Then, clearly, $\varphi_k(n)=\alpha_k(n)+\beta_k(n)$. We see that T has the form $T=\begin{bmatrix} A & 0 \\ B & t \end{bmatrix}$ where A is $(n-1)\times(n-1)$ B is $1\times n-1$ and t is a scalar. For T to be nonsingular A must be nonsingular and can be chosen in $N(n-1)$ ways. For each choice of A, t is fixed since the trace of T must be k. B can be chosen arbitrarily in q^{n-1} ways. Thus, at this stage, T can be chosen in $q^{n-1}N(n-1)$ ways. But not all of these choices are nonsingular. For if $\operatorname{tr}(A)=k$ then $t=0$ and T is singular. $\operatorname{tr}(A)=k$ for $\varphi_k(n-1)$ choices of A. Hence T is singular in $q^{n-1}\varphi_k(n-1)$ ways. It follows that $\beta_k(n)=q^{n-1}[N(n-1)-\varphi_k(n-1)]$ and the theorem results.

Lemma 2. $\alpha_k(n)=[Q(n-1, n)-N(n-1)](q^{n-1}-q^{n-2})$.

PROOF. Let V be any nonsingular nth order matrix of trace k with a non-zero element in some position in the nth column above the (n, n) position. Then V has the form $V=\begin{bmatrix} A & C \\ B & v \end{bmatrix}$ where A is square of order $n-1$, B is of dimensions $1\times n-1$, $C\neq 0$ is $n-1\times 1$ and v is scalar. Since V is nonsingular $[AC]$ must have rank $n-1$ so could be chosen in $Q(n-1, n)$ ways. However, some of these choices will be those with $C=0$ and these cannot be used as part of V. There are $N(n-1)$ such possibilities so that we may choose $[AC]$ in exactly $Q(n-1, n)-N(n-1)$ ways. Since the trace of V is fixed, after choosing its first $n-1$ rows, v is fixed. Then there are q^{n-1} choices for B. But not all of these choices of B yield a nonsingular V. We

must subtract from the q^{n-1} choices of B those choices such that $[Bv]$ is a linear combination of the top $n-1$ rows of V. From those $n-1$ rows select one such that the last element is not zero. In forming linear combinations of the top $n-1$ rows the scalar coefficients of the remaining $n-2$ rows may be chosen arbitrarily. But the scalar coefficient of the selected row with non-zero last element is then fixed so that the last element in the linear combination is v. There are q^{n-2} such combinations. Hence, there are $q^{n-1}-q^{n-2}$ choices of $[Bv]$ which are not linear combinations of the rows of $[AC]$. It follows that

$$\alpha_k(n)=[Q(n-1, n)-N(n-1)](q^{n-1}-q^{n-2}).$$

Lemma 3. $q\varphi_k(n)-N(n)=-q^{n-1}[q\varphi_k(n-1)-N(n-1)]$.

PROOF. On combining Lemmas 1 and 2 we get

$$\varphi_k(n)=[Q(n-1, n)-N(n-1)](q^{n-1}-q^{n-2})+q^{n-1}[N(n-1)-\varphi_k(n-1)].$$

On simplifying we obtain

$$\varphi_k(n)=(q^{n-1}-q^{n-2})Q(n-1, n)+q^{n-2}N(n-1)-q^{n-1}\varphi_k(n-1).$$

Hence, $q\varphi_k(n)=(q^n-q^{n-1})Q(n-1, n)+q^{n-1}[N(n-1)-q\varphi_k(n-1)]$. But, by Theorem 4, $Q(n-1, n)=\prod_{j=0}^{n-2}(q^n-q^j)$ so that $(q^n-q^{n-1})Q(n-1, n)=(q^n-q^{n-1})\prod_{j=0}^{n-2}(q^n-q^j)=$ $=\prod_{j=0}^{n-1}(q^n-q^j)$ which is $N(n)$ by Theorem 3. Therefore, the lemma follows.

The preceding lemmas culminate in the following theorem which gives a closed form expression for the number of nonsingular matrices of order n which have a given trace:

Theorem 6. $\varphi_0(n)=N(n)/q+(-1)^{n-2}q^{(n-2)(n+1)/2}(q-1)$ *and, for* $k\neq 0$,

$$\varphi_k(n)=N(n)/q+(-1)^{n-1}q^{(n-2)(n+1)/2}.$$

PROOF. By the use of Lemma 3 repeatedly we get

$$\begin{aligned}q\varphi_k(n)-N(n) &= -q^{n-1}[q\varphi_k(n-1)-N(n-1)]\\ &= q^{n-1}q^{n-2}[q\varphi_k(n-2)-N(n-2)]\\ &\cdots\\ &= (-1)^{n-2}q^{n-1}q^{n-2}\ldots q^2[q\varphi_k(2)-N(2)]\\ &= (-1)^{n-2}q^{(n-2)(n+1/2}[q\varphi_k(2)-N(2)].\end{aligned}$$

From Theorems 3 and 5 we get

$$q\varphi_0(n)-N(n)=(-1)^{n-2}q^{(n-2)(n+1)/2}[q\cdot q^2(q-1)-(q^2-1)(q^2-q)].$$

And, on simplifying,

$$\varphi_0(n)=N(n)/q+(-1)^{n-2}q^{(n-2)(n+1)/2}(q-1).$$

On using Theorems 3 and 5 for $k \neq 0$ we obtain

$$q\varphi_k(n) - N(n) = (-1)^{n-2} q^{(n-2)(n+1)/2}[q^2(q^2-q-1)-(q^2-1)(q^2-q)] =$$
$$= (-1)^{n-2} q^{(n-2)(n+1)/2}(-q).$$

Hence,

$$\varphi_k(n) = N(n)/q + (-1)^{n-1} q^{(n-2)(n+1)/2}.$$

Corollary. The number of nonsingular commutators of order n over $GF(q)$ is given by $N(n)/q + (-1)^{n-2} q^{(n-2)(n+1)/2}(q-1)$.

PROOF. This follows from Theorem 6, Theorem 1 and our notation.

3. *Evaluation of an exponential sum.* The problem of finding the number of matrices U and V, when U is $m \times n$ and V is $s \times t$, which satisfy the matrix equation $UAV = B$, with A and B arbitrary, but fixed, matrices of orders $n \times s$ and $m \times t$, respectively, has been solved by JOHN H. HODGES [4].

In connection with this problem, certain exponential sums were defined for rectangular matrices having elements in $GF(q)$. Analogous sums for symmetric, skew and hermitian matrices were also discussed by L. CARLITZ and HODGES [2], [3], [5]. The exponential sums in these papers have all been explicitly evaluated, but the results in some cases are very lengthy and detailed. By use of concepts related to this paper, we are able to obtain a short evaluation for a variation of the exponential sum discussed by Hodges in [4].

As in Hodges' paper, we define

$$e(\alpha) = \exp\left(2\pi i t(\alpha)/p\right)$$
$$t(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{f-1}},$$

where $\alpha \in GF(q)$, and $q = p^f$. It follows that

$$e(\alpha+\beta) = e(\alpha)e(\beta)$$

and

$$\sum_{\beta \in GF(q)} e(\alpha\beta) = \begin{cases} q & \text{if} \quad \alpha = 0 \\ 0 & \text{if} \quad \alpha \neq 0. \end{cases}$$

From this last equality it follows that if A is $n \times n$, then

$$\sum_{B(n,n)} e\{\sigma(AB)\} = \begin{cases} q^{n^2} & \text{if} \quad A = 0 \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where the sum is over all $n \times n$ matrices B. Here $\sigma(A)$ denotes the trace of A.

Now we define

$$H(B, n) = \sum_{C(n,n)} e\{-\sigma(BC)\}$$

where the summation is over all $n \times n$ matrices C with rank n. Hodges [4; p. 506] gives an explicit value of $H(B, n)$. We will also need the following theorem:

Theorem 7. *The only matrices which commute with a nonderogatory matrix A are the polynomial functions of A.* [7; p. 94].

Equation (1) is the basis for a technique of counting solutions of certain matrix equations. It is this technique and Theorem 7 which enable us to prove the following theorem.

Theorem 8. *Let A be a nonderogatory matrix whose minimum polynomial is irreducible over* GF(q). *If there is a solution of $AX-XA=C$, then there are q^n such solutions and furthermore*

$$\sum_{D(n,n)} e\{-\sigma(CD)\} = q^n,$$

where the sum is over all $n\times n$ matrices D which are polynomials in A.

PROOF. We assume that C is a matrix such that $AX-XA=C$ has a solution. Then every solution can be obtained from a sum of this C and a general solution of $AX-XA=0$. But by Theorem 7, there are exactly q^n solutions of $AX-XA=0$, namely the polynomials in A. Thus, there are precisely q^n solutions of $AX-XA=C$.

In view of (1) above, the number N of solutions of $AX-XA=C$ is given by

$$q^{-n^2} \sum_{X(n,n)} \sum_{D(n,n)} e\{\sigma[((AX-XA)-C)D]\},$$

where the sums are over all $n\times n$ matrices D, and all $n\times n$ matrices X. Thus, by using properties of trace and the exponential function, we have,

$$N = q^{-n^2} \sum_{D(n,n)} e\{\sigma(-CD)\} \sum_{X(n,n)} e\{\sigma[(AX-XA)D]\}.$$

But, since $\sigma(AB)=\sigma(BA)$, we have

$$\sigma[(AX-XA)D] = \sigma(AXD-XAD) = \sigma(AXD)-\sigma(XAD) = \sigma(DAX)-\sigma(AXD) =$$

$$= \sigma[(DA-AD)X].$$

Therefore,

$$N = q^{-n^2} \sum_{D(n,n)} e\{\sigma(-CD)\} \sum_{X(n,n)} e\{\sigma(DA-AD)X\}.$$

But again by (1) above

$$\sum_{X(n,n)} e\{\sigma(DA-AD)X\} = \begin{cases} q^{n^2} & \text{if} \quad DA-AD=0, \\ 0 & \text{if} \quad DA-AD\neq 0. \end{cases}$$

Therefore,

$$N = \sum_{D(n,n)} e\{\sigma(-CD)\}\cdot M,$$

where

$$M = \begin{cases} 1 & \text{if} \quad DA-AD=0, \\ 0 & \text{if} \quad DA-AD\neq 0. \end{cases}$$

But $DA-AD=0$ if and only if D is a polynomial in A. Therefore,

$$N = \sum_{D(n,n)} e\{\sigma(-CD)\} = q^n,$$

where the sum is over all $n\times n$ matrices D which are polynomials in A.

The above theorem shows in particular that if C is nonsingular and there is one solution of $AX-XA=C$, then there are exactly q^n matrices X such that $AX-XA=C$. We now give an example of an A and a nonsingular C such that $AX-XA=C$ has a solution. Let

$$A=\begin{bmatrix}0 & 1\\ 2 & 0\end{bmatrix}$$

and

$$C=\begin{bmatrix}2 & 0\\ 0 & -2\end{bmatrix}.$$

Then A is nonderogatory with minimum polynomial x^2-2 which is irreducible over 1/3.

ROTH [8; p. 465] has shown that the equation $AX-XA=C$ has a solution if and only if the matrices $A\times I-I\times A^T$ and $(A\times I-I\times A^T|C)$ have the same rank where the augmented matrix uses the columns of C in order. Recall that $A\times B$ is the direct product of A and B and that $(A|C)$ is the matrix obtained by augmenting the matrix A with the matrix C. But

$$A\times I-I\times A^T=\begin{bmatrix}0 & 1 & -2 & 0\\ 2 & 0 & 0 & -2\\ -1 & 0 & 0 & 1\\ 0 & -1 & 2 & 0\end{bmatrix}$$

has rank 2 and

$$(A\times I-I\times A^T|C)=\begin{bmatrix}0 & 1 & -2 & 0 & 2\\ 2 & 0 & 0 & -2 & 0\\ -1 & 0 & 0 & 1 & 0\\ 0 & -1 & 2 & 0 & -2\end{bmatrix}$$

has rank 2 also. Therefore $AX-XA=C$ has a solution by Roth's result. In this case, A is nonderogatory and C is nonsingular as desired.

References

[1] A. A. ALBERT and B. MUCKENHOUPT, On Matrices of Trace Zero, *Michigan Math. J.* **4** (1957), 1—3.
[2] L. CARLITZ, Representations by Quadratic Forms in a Finite Field, *Duke Math. Journal,* **21** (1954), 123—138.
[3] L. CARLITZ and JOHN H. HODGES, Representations by Hermitian Forms in a Finite Field, *Duke Math. Journal,* **22** (1955), 393—405.
[4] JOHN H. HODGES, Representations by Bilinear Forms in a Finite Field, *Duke Math. Jorunal,* **22** (1955), 497—510.
[5] JOHN H. HODGES, Exponential Sums for Symmetric Matrices in a Finite Field, *Math. Nachrichten,* **14** (1955), 331—339.
[6] G. LANDSBERG, Über eine Anzahlbestimmung und eine damit zusammenhangende Reihe, *J. Reine Angew. Math.* **111** (1893), 87—88.
[7] C. C. MACDUFFEE, The Theory of Matrices, *New York,* 1946.
[8] W. E. ROTH, On Direct Product Matrices, *Bull. Amer. Math. Soc.* **40** (1934), 461—468.

Fort Lewis College
University of Wyoming

(Received December 22, 1975.)