An exponential sum in a finite field

By A. DUANE PORTER (Laramie, Wyoming)

1. *Introduction and preliminaries.* Let $F=GF(q)$ be the finite field of $q=p^e$ elements, p odd. If $\alpha\in F$, we let

$$e(\alpha)=\exp 2\pi i t(\alpha)/p;\quad t(\alpha)=\alpha+\alpha^p+\cdots+\alpha^{p^{e-1}}, \tag{1.1}$$

where by its definition $t(\alpha)\in GF(p)$. It follows directly from (1.1) that

$$\begin{cases} e(\alpha+\beta)=e(\alpha)e(\beta), \text{ and} \\ \sum\limits_{\beta} e(\alpha\beta)=\begin{cases} q, & \alpha=0, \\ 0, & \alpha\neq 0, \end{cases} \end{cases} \tag{1.2}$$

where the sum is over all $\beta\in F$ and will be denoted by $R(\alpha)$. The well-known Gauss—Sum [1, π3] and its values for F will be denoted by

$$G(\alpha)=\sum_{\beta} e(\alpha\beta^2)=\begin{cases} q, & \alpha=0, \\ \psi(\alpha)G(1), & \alpha\neq 0, \end{cases} \tag{1.3}$$

where $\psi(\alpha)=0, 1, -1$ according as $\alpha=0$, $\alpha=$nonzero square of F, $\alpha=$nonsquare of F, and $G^2(1)=\psi(-1)q$. It is clear that $\psi(1/\alpha)=\psi(\alpha)$. Finally, the Cauchy—Gauss sum [2, π1] $G(\alpha,\beta)$ the following values

$$G(\alpha,\beta)=\sum_{\gamma} e\{\alpha\gamma+2\beta\gamma\}=\begin{cases} q, & \alpha=\beta=0, \\ 0, & \alpha=0,\ \beta\neq 0, \\ e(-\beta^2/\alpha)G(\alpha), & \alpha\neq 0. \end{cases} \tag{1.4}$$

These functions have been used in [3], [4], [5], [7], [11], and others, as an aid to counting the number of solutions of various polynomial and systems of polynomial equations. If $A=(a_{ij})$ is an $n\times n$ matrix, $a_{ij}\in F$, then we let $\sigma(A)=a_{11}+\cdots+a_{nn}$ be the trace of A. Using this definition, (1.2) may be generalized to matrices [10] as follows: Let $B=(b_{ij})$, $b_{ij}\in F$, be $n\times s$, then

$$\sum_{X} e\{\sigma(BX)\}=\begin{cases} q, & B=0, \\ 0, & B\neq 0, \end{cases} \tag{1.5}$$

where the sum is over all $s\times n$ matrices $X=(x_{ij})$, $x_{ij}\in F$. Exponential sums of the form (1.5), and other forms, in which various specific matrices have been used in the place of B and X (e.g. B skew, symmetric, or Hermitian, and X of a fixed rank)

have been discussed by CARLITZ and HODGES [6], [8], [9], [10]. Once again these formulas have proved useful in finding the number of solutions in F of certain matric equations, e.g. [12], [13].

In view of the generalization from (1. 2) to (1. 5), it seems natural to attempt a generalization of (1. 3) to matrices, and so consider

$$\sum_X e\{\sigma(CX^2)\}, \tag{1.6}$$

where $C=(c_{ij})$, $c_{ij}\in F$, is $n\times n$ and the sum is over all $n\times n$ matrices $X=(x_{ij})$, $x_{ij}\in F$. Just as the evaluation of (1. 3) is considerably more involved than that of (1. 2), we would expect the evaluation of (1. 6) to be more difficult than that of (1. 5). However, the degree of difficulty increases very rapidly when we realize the number of terms involved in squaring a matrix. As a result, we do not obtain an evaluation of (1. 6) for an arbitrary $n\times n$ matrix C. We are able to evaluate (1. 6) for an arbitrary 2×2 matrix C, and obtain fairly complete results for $n=3$. For $n>3$ we evaluate (1. 6) for a certain class of matrices. Even though our results are not complete, we feel this paper is a good start toward the evaluation of (1. 6). Since the other sums noted earlier have had much use, it is hoped that this sum will also.

2. *The case* $n=2$. We start our discussion with this case for two reasons: (1) we are able to obtain complete results in this case, (2) it displays many of the problems which can arise as we allow n to get larger.

Let $C=(c_{ij})$, $c_{ij}\in F$, be an arbitrary, but fixed, 2×2 matrix. We now prove

Theorem 1. *With C as defined above, the expression defined in* (1. 6) *in which the sum is taken over all 2×2 matrices $X=(x_{ij})$ has the following values:*

1. *if* $c_{11}=c_{22}=0$ *and*
   - a) $c_{12}=c_{21}=0$ (*so* $C=$*zero*), q^4,
   - b) c_{12} *or* $c_{21}\neq 0$, q^3,
2. *if* $c_{ii}=0$, $c_{jj}\neq 0$ $(i\neq j,\ 1\leqq i,j\leqq 2)$, *and*
   - a) $c_{ij}=c_{ji}=0$, $q^2\psi(c_{jj})G(1)$,
   - b) $c_{ij}\neq 0$ (or $c_{ji}\neq 0$) *and*
     - $c_{ji}=0$ (or $c_{ij}=0$), $q^2\psi(c_{jj})G(1)$,
     - $c_{ji}\neq 0$ (or $c_{ij}\neq 0$), $q^2\psi(c_{ij}c_{ji})$,
3. $c_{11}\neq 0$, $c_{22}\neq 0$, *and*
   - a) $c_{12}(c_{11}+c_{22})=0$, *with*
     - (1) $c_{11}+c_{22}=0$, $q^3\psi(-c_{11}c_{22})$,
     - (2) $c_{11}+c_{22}\neq 0$, $q^2\psi(-c_{11}c_{22})$,
   - b) $c_{12}(c_{11}+c_{22})\neq 0$, *with*
     - (1) $A=0$, $q^2G(1)\psi(c_{11}+c_{22})$,
     - (2) $A\neq 0$, $q^2\psi(-A)$,

where $\psi(a)$ *is defined in* $\pi 1$, $A=2c_{11}c_{22}-c_{12}c_{21}$, *and* $G(1)$ *is defined by* (1. 3).

PROOF. By matrix multiplication, we obtain

$$\text{(2. 1)} \qquad \begin{cases} \sigma(CX^2) = c_{11}(x_{11}^2 + x_{12}x_{21}) + c_{12}(x_{21}x_{11} + x_{22}x_{21}) + \\ \qquad + c_{21}(x_{11}x_{12} + x_{12}x_{22}) + c_{22}(x_{21}x_{12} + x_{22}^2). \end{cases}$$

By multiplying out the above expression, noting (1. 2) and recombining terms, we may write (1. 6) as

$$\text{(2. 2)} \qquad \begin{cases} \sum_X e\{\sigma(CX^2)\} = \sum_{x_{ij}} e\{c_{11}x_{11}^2 + 2(c_{12}x_{21} + c_{21}x_{12})x_{11}/2\} \cdot \\ \cdot e\{c_{22}x_{22}^2 + 2(c_{12}x_{21} + c_{21}x_{12})x_{22}/2\} e\{(c_{11} + c_{22})x_{21}x_{12}\}, \end{cases}$$

where the sum over x_{ij} indicates a sum in which each x_{ij}, $1 \leqq i, j \leqq 2$ takes on all values of F. We note that the constant 2 has been inserted so that (2. 2) will be in the form of (1. 4). By summing over x_{11} and x_{22} above in accordance with (1. 4), we obtain

$$\text{(2. 3)} \qquad \begin{cases} \sum_X e\{\sigma(CX^2)\} = \sum_{x_{12}, x_{21}} G(c_{11}, [c_{12}x_{21} + c_{21}x_{12}]/2) \cdot \\ \cdot G(c_{22}, [c_{12}x_{21} + c_{21}x_{12}]/2) \cdot e\{(c_{11} + c_{22})x_{21}x_{12}\}. \end{cases}$$

The value of the right side of (2. 3) depends upon whether the entries are zero or not zero. Hence, we must consider the various possibilities for the matrix C.

Case 1. $C_{11} = C_{22} = 0$. Then the right member of (2. 3) reduces to

$$\sum_{x_{12}, x_{21}} G(0, [c_{12}x_{21} + c_{21}x_{12}]/2) G(0, [c_{12}x_{21} + c_{21}x_{12}]/2).$$

(a) If $c_{12} = c_{21} = 0$ then $C =$ zero matrix and the above sum clearly has the values q^4.

(b) If $c_{21} \neq 0$, then the above sum is zero unless $c_{12}x_{12} + c_{21}x_{12} = 0$, so let $x_{12} = -c_{12}x_{21}/c_{21}$. Hence, x_{21} is arbitrary and the above sum has the value q^3. (Clearly, the same value will be obtained in (b) if we suppose $c_{12} \neq 0$).

Case 2. $c_{11} = 0$, $c_{22} \neq 0$. Then the right member of (2. 3) reduces to

$$\sum_{x_{12}, x_{21}} G(0, [c_{12}x_{21} + c_{21}x_{12}]/2) e\{-[c_{12}x_{21} + c_{21}x_{12}]^2/2^2 c_{22}\} G(c_{22}) e\{c_{22}x_{12}x_{21}\}.$$

Once again, the only nonzero contributions to the above sum are when $c_{12}x_{21} + c_{21}x_{12} = 0$.

(a) If $c_{12} = c_{21} = 0$, then in view of (1. 3) and (1. 4), we have

$$G(c_{22}) q \sum_{x_{12}, x_{21}} e\{c_{22}x_{12}x_{21}\} = q^2 \psi(c_{22}) G(1).$$

(b) If $c_{21} \neq 0$, let $x_{12} = -c_{12}x_{21}/c_{21}$ and obtain

$$G(c_{22}) q \sum_{x_{21}} e\{-(c_{22}c_{12}/c_{21})x_{21}^2\} = \begin{cases} q^2 \psi(c_{22}) G(1), & c_{12} = 0, \\ q^2 \psi(c_{12}c_{21}), & c_{12} \neq 0. \end{cases}$$

(We again note that the same values are obtained in (b) by interchanging the corresponding positions of c_{12} and c_{21}.)

Case 3. $c_{11}\neq 0$, $c_{22}=0$. The same argument as advanced in Case 2 is valid here if we simply replace c_{22} by c_{11}, and the values of the sum may be obtained in this way.

Case 4. $c_{11}\neq 0$, $c_{22}\neq 0$. In this situation the right member of (2. 3) may be written as

$$\begin{cases} G(c_{11})G(c_{22}) \sum\limits_{x_{12},x_{21}} e\{-(c_{12}x_{21}+c_{21}x_{12})^2/2^2c_{11}\}\cdot \\ \cdot e\{-(c_{12}x_{21}+c_{21}x_{12})^2/2^2c_{22}\}e\{(c_{11}+c_{22})x_{21}x_{12}\}. \end{cases} \tag{2.4}$$

We now square the numerators in the above expressions, recombine terms, note (1, 2), and after a lengthy, but straightforward, calculation write the sum over x_{12}, x_{21} as

(2, 5)

$$\begin{cases} \sum\limits_{x_{12},x_{21}} e\{[-c_{12}^2(c_{11}+c_{22})/2^2c_{11}c_{22}]x_{21}^2+2[(2c_{11}c_{22}-c_{12}c_{21})(c_{11}+c_{22})/2^2c_{11}c_{22}]\cdot \\ \cdot x_{12}x_{21}\}.e\{[-c_{21}^2(c_{11}+c_{22})/2^2c_{11}c_{22}]x_{12}^2\}. \end{cases}$$

We now have a sum of the form of (1. 4) in terms of summing over x_{21}. Hence, we consider the various cases necessary to evlluate it.

(a) $c_{12}(c_{11}+c_{22})=0$. In this situation the only nonzero contributions to (2. 5) come from terms such that $(2c_{11}c_{22}-c_{12}c_{21})(c_{11}+c_{22})x_{12}=0$.

(1) If $c_{11}+c_{22}=0$, then c_{12} and x_{12} may be arbitrary so that (2. 5) may be evaluated as

$$\sum_{x_{12}} G(0,0)e(0\,x_{12}^2)=q^2.$$

(1) If $c_{11}+c_{22}\neq 0$ then $c_{12}=0$ and $2c_{11}c_{22}-c_{12}c_{21}=c2_{11}c_{22}\neq 0$, so that x_{12} must be 0 and (2. 5) equals $qe(0)=q$.

(b) $c_{12}(c_{11}+c_{22})\neq 0$. Then by noting (1. 4), and after a great deal of computation, we write (2. 5) as

$$T=\sum_{x_{12}} e\{A(c_{11}+c_{22})x_{12}^2/c_{12}^2\}G(-c_{12}^2(c_{11}+c_{22})/2^2c_{11}c_{22}),$$

where $A=2(2c_{11}c_{22}-c_{12}c_{21})$. Since $c_{11}+c_{22}\neq 0$, the value of the above sums depend upon whether or not A is zero. In view of (1. 3), we obtain the following:

(1) If $A=0$, then $T=q\psi(c_{11}+c_{22})\psi(-c_{11}c_{22})G(1)$,
(2) If $A\neq 0$, then $T=q\psi(A)\psi(c_{11}c_{22})$.

The theorem now follows by substituting the values obtained for (2. 5) into (2. 4), noting that $G(c_{11})G(c_{22})=\psi(-c_{11}c_{22})q$ and simplifying the resulting expression.

3. *The case* $n=3$. In this situation the computations become very cumbersome (and the results very difficult to state) when we attempt to evaluate (1. 6) for an arbitrary matrix C. However, we can obtain an evaluation for a certain class of 3×3 matrices. We state these results in the following theorem.

Theorem 2. *Let $C=(c_{ij})$ be a 3×3 matrix with elements from F such that $c_{jj}=0$, $1\leqq j\leqq 3$. Then the expression defined in* (1. 6) *where the sum is over all 3×3 matrices $X=(x_{ij})$, $x_{ij}\in F$, has the following values:*

(1) q^9, $c_{ij}=0$, *all i and j,*

(2) $q^7[1-\psi^2(c_{12})]+q^6\psi^2(c_{12})$, $c_{21}\neq 0$, $c_{32}\neq 0$, $c_{13}=c_{31}=0$,

(3) $q^6[1-\psi^2(A_{11})]+q^4\psi(A_{11})G(1)$, $c_{21}\neq 0$, $c_{32}\neq 0$, c_{13} or $c_{31}\neq 0$,

where $\psi(2)$ is the Legendre function defined in $\pi 1$, $G(1)$ *is given in* (1. 3), *and* $A_{11}=$ $=c_{23}c_{12}c_{31}+c_{32}c_{21}c_{13}$.

We note that corresponding results can be obtained in (2) and (3) if we replace c_{21} and c_{23} by elements of any other row (or column) of the matrix C.

PROOF. We let $C=(c_{ij})$ and $X=(x_{ij})$ be 3×3 matrices with $c_{ij}, x_{ij}\in F$. If $C=$zero matrix, then (1) follows directly by the definition of trace and an application of (1. 2). If $C\neq$the zero matrix, we obtain

$$\sigma(CX^2)=\sum_{k=1}^{3}\sum_{i=1}^{3}\sum_{j=1}^{3}c_{ki}x_{ij}x_{jk}.$$

We multiply out the above expression, factor out x_{11}, x_{22}, x_{33}, sum over these variables in accordance with (1. 4), recall that $c_{ii}=0$, $1\leqq i\leqq 3$, and obtain

$$\sum_{x_{ij}}{}^{1}G(0, A/2)G(0, B/2)G(0, D/2)e(E+G+H), \tag{3. 1}$$

where

$$\begin{aligned}
A &= c_{12}x_{21}+c_{13}x_{31}+c_{21}x_{12}+c_{31}x_{13},\\
B &= c_{12}x_{21}+c_{21}x_{12}+c_{32}x_{23}+c_{23}x_{32},\\
D &= c_{13}x_{31}+c_{31}x_{13}+c_{23}x_{32}+c_{32}x_{23},\\
E &= c_{12}x_{23}x_{31}+c_{13}x_{32}x_{21},\\
G &= c_{21}x_{13}x_{32}+c_{23}x_{31}x_{12},\\
H &= c_{31}x_{12}x_{23}+c_{32}x_{21}x_{13},
\end{aligned}$$

and the sum over x_{ij} indicates a summation in which each x_{ij}, $i\neq j$, varies over all elements of F. The only nonzero contributions to the sum (3. 1) are from the terms in which $A=B=D=0$. If all $c_{ij}=0$, this condition would hold for all x_{ij} so the value of (3. 1) would be q^9.

Suppose $c_{21}\neq 0$, $c_{23}\neq 0$. (Similar results may be obtained corresponding to other elements being not 0.) Then setting $A=B=D=0$, we obtain

$$\begin{cases}
x_{12} = -(c_{12}x_{21}+c_{13}x_{31}+c_{31}x_{13})/c_{21},\\
x_{12} = -(c_{12}x_{21}+c_{32}x_{23}+c_{23}x_{32})/c_{21},\\
x_{32} = -(c_{13}x_{31}+c_{31}x_{13}+c_{32}x_{23})/c_{23}.
\end{cases} \tag{3. 2}$$

By equating the two expressions for x_{12} above and replacing x_{23} by its value from line 3 we are led to $c_{13}x_{31}+c_{31}x_{13}=0$. There are two ways in which this could happen:

1) $c_{13}=c_{31}=0$. By using this condition, substituting (3. 2) into (3. 1), noting (1. 4), and recombining terms, we obtain

$$q^3 \sum_{x_{ij}}{}^{11} e\{[c_{12}x_{31}-c_{21}c_{32}x_{13}/c_{23}]x_{23}\}e\{[c_{32}x_{13}-c_{23}c_{12}x_{31}/c_{21}]x_{21}\},$$

where the sum over x_{ij} is over x_{21}, x_{23}, x_{31}, x_{13}. If we now sum over x_{23} and x_{21} in accordance with (1. 2), we see that the only nonzero contributions come when $c_{12}x_{31}-c_{21}x_{32}x_{31}/c_{23} = 0 = x_{23}x_{13}-c_{23}x_{12}x_{31}/c_{21}$.

a) If $c_{12}=0$ the above sum is q^7.

b) If $c_{12}\neq 0$, then we obtain $x_{31}=c_{21}c_{32}x_{13}/c_{12}c_{23}$ from both expressions involving x_{31}. Hence, the choice of x_{13} is arbitrary so the above sum equals q^6.

2) $c_{13}\neq 0$. (Corresponding results will follow if $c_{31}\neq 0$.) Then since $c_{13}x_{31}+ +c_{31}x_{13} = 0$, we have $x_{31}=-c_{31}x_{13}/c_{13}$. By substituting (3. 2) into (3. 1), the above value for x_{31} into the resulting expression and after a lengthy simplification and recombining of terms as well as summing over x_{13} in accordance with (1. 4), we obtain

$$q^3 \sum_{x_{21},x_{23}} G(0, A_1/2)e\{-A_{11}x_{21}x_{23}/c_{23}c_{21}\},$$

where $A_1 = A_{11}x_{21}/c_{21}c_{13}-A_{11}x_{23}/c_{23}c_{13}$ with $A_{11} = c_{23}c_{12}c_{31}+c_{32}c_{21}c_{13}$. We note that the coefficients of ${x_{13}}^2$ cancel themselves in pairs resulting in the 0 which appears in $G(0, A_1/2)$. It is now apparent that the only nonzero contribution to the above sum and so also to (3. 1) in this case will come from those terms such that $A_1=0$. This can happen in two ways:

a) $A_{11}=0$. Then x_{21} and x_{31} are arbitrary and we obtain

$$q^3 \sum_{x_{21},x_{23}} qe\{0\, x_{21}x_{23}\} = q^6.$$

b) $A_{11}\neq 0$. We then let $x_{21}=c_{21}x_{23}/c_{23}$ so that $A=0$. By substituting this value into the inner exponential function above, and by noting (1. 3), we obtain

$$q^3 \sum_{x_{23}} qe\{A_{11}x_{23}^2/c_{23}^2\} = q^4\psi(A_{11}c_{23}^2)G(1) = q^4\psi(A_{11})G(1).$$

Hence, the theorem is verified.

If one wishes to see why we only discussed matrices C such that $c_{ii}=0$, $1\leqq i\leqq 3$, he may suppose this is not the case and then use (1. 4) to evaluate (3. 1). The resulting expression is very lengthy and difficult to handle (although it possibly could be evaluated).

In the hypothesis of Theorem 2, we only considered matrices C such that $c_{21}\neq 0$, $c_{23}\neq 0$. It is of some interest and also an aid in generalization to only assume $c_{21}\neq 0$. We do this in the next theorem. We state only one partial result in this direction. Results similar to all of Theorem 3 could be obtained in this situation, but we shall not state them.

Theorem 3. *Let $C=(c_{ij})$ be a 3×3 matrix such that $c_{21}\neq 0$, c_{12} is arbitrary and the remaining elements of C are zero. Then the sum defined by* (1. 6) *in which X is a 3×3 matrix is given by $q^5 f(c_{12})$ where $f(c_{12})=q^2$ or q according as $c_{12}=0$ or $c_{12}\neq 0$.*

PROOF. In this situation, by selecting $x_{12}=-c_{12}x_{21}/c_{21}$ (which are the only nonzero terms in (3. 2)), we write (3. 1) as

$$\sum_{x_{ij}}{}^{1} q^3 e\{c_{12}x_{23}x_{31}\}e\{c_{21}x_{13}x_{32}\}.$$

Hence, the value of x_{12} is fixed, but x_{21} may be chosen arbitrarily. If we now sum over x_{32} and x_{31} in accordance with (1. 2), we can see that to have nonzero contributions to the above sum, we must take $x_{13}=0$ (since $c_{21}\neq 0$). Also, if $c_{12}=0$ then x_{23} may be chosen arbitrarily; otherwise x_{23} must be taken to be 0. Hence, we obtain

$$q^3 \sum_{x_{21}} f(c_{12})\cdot q = q^5 f(c_{12}).$$

4. *The general case.* In this situation as in the case $n=3$, the computations are very cumbersome if we take C to be an arbitrary matrix. However, we obtain an evaluation of (1. 6) for a certain class of matrices. The proof of the theorem is slightly different in the two situations of n even or n odd. We prove the case n even. The odd case involves a different indexing procedure. We indicate a key step in the proof and omit the remainder of the proof.

Theorem 4. *Let $n\geqq 3$, $C=(c_{ij})$ be an $n\times n$ matrix such that $C=0$ or $c_{2t,\,2t-1}\neq 0$, $1\leqq t\leqq s$, $s=n/2$ or $(n-1)/2$ according as n is even or odd, and all other $c_{ij}=0$. Then*

$$\sum_{X} e\{\sigma(CX^2)\} = \begin{cases} q^{n^2}, & C=\text{zero}, \\ q^{3n^2/4}, & C\neq 0,\ n \text{ even}, \\ q^{(3n^2+1)/4}, & C\neq 0,\ n \text{ odd}, \end{cases}$$

where the sum over X is over all $n\times n$ matrices x_{ij}, with $x_{ij}\in F$.

PROOF. For $C=$zero the theorem follows directly from (1. 5), so we suppose $C\neq$zero. We carry out the beginning multiplications for an arbitrary matrix C so that some of the difficulties arising in the general evaluation can be seen. We note that

$$\sigma(CX^2) = \sum_{k=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ki}x_{ij}x_{jk}.$$

By substituting this value into (1. 6), collecting the terms of the resulting expression in the form of (1. 4), and summing over x_{ii}, $1\leqq i\leqq n$, we may write

$$\sum_{X} e\{\sigma(CX^2)\} = \sum_{x_{ij}}{}^{0} \prod_{r=1}^{n} G(c_{ii}, A_r/2)\, e\left\{\sum_{k=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}{}^{1} c_{ki}x_{ij}x_{jk}\right\}, \tag{4. 1}$$

where the sum over x_{ij} is over all x_{ij}, $i\neq j$, the prime in the sum over j indicates that for each choice of k, i, the sum over j is over all $j\neq k$, $j\neq i$, and

$$A_r = \sum_{i=1}^{n}{}^{r} c_{ri}x_{ir} + \sum_{k=1}^{n}{}^{r} c_{kr}x_{rk},$$

where the r on the summation symbols indicates that, respectively, $i\neq r$, $k\neq r$. If we now apply part of the hypothesis of the theorem and so take $c_{ii}=0$, $1\leqq i\leqq n$, we see that the only nonzero contributions to (4. 1) come from terms with $A_r=0$,

$1 \leqq r \leqq n$. We now take $n=2s$ and continue the proof. Each variable of the form $x_{2t-1,2t}$ appears in exactly two of the A_r, namely A_{2t-1} and A_{2t}. By setting $A_{2t-1}=$ $=0=A_{2t}$, recalling that $c_{2t,2t-1}\neq 0$, and solving for these variables, we obtain

$$(4.2)\quad \begin{cases} x_{2t-1,2t} = -\left(\sum_{i=1}^{n}{}^{(1)} c_{2t-1,i}x_{i,2t-1} + \sum_{k=1}^{n}{}^{(2)} c_{k,2t-1}x_{2t-1,k}\right)\Big/(c_{2t,2t-1}), \\ x_{2t-1,2t} = -\left(\sum_{i=1}^{n}{}^{(3)} c_{2t,i}x_{i,2t} + \sum_{k=1}^{n}{}^{(4)} c_{k,2t}x_{2t,k}\right)\Big/(c_{2t,2t-1}), \end{cases}$$

where the numbers in parentheses have the following meanings: (1) $i \neq 2t-1$, (2) $k \neq 2t-1, 2t$, (3) $i \neq 2t-1, 2t$, (4) $k \neq 2t$. By equating the above expressions we obtain

(4.3)

$$\sum_{i=1}^{n}{}^{(1)} c_{2t-1,i}x_{i,2t-1} + \sum_{k=1}^{n}{}^{(2)} c_{k,2t-1}x_{2t-1,k} = \sum_{i=1}^{n}{}^{(3)} c_{2t,i}x_{i,2t} + \sum_{k=1}^{n}{}^{(4)} c_{k,2t}x_{2t,k}.$$

If some of the remaining c_{ij} are not 0, then in view of (4.3), the sum in (4.1) becomes very cumbersome to evaluate. However, if we apply the hypothesis of the theorem regarding c_{ij}, then (4.3) is simply $0=0$, so by taking $x_{2t-1,2t}=0$, $1 \leqq t \leqq s$, we may write (4.1) as

$$(4.4)\qquad q^n \sum_{x_{ij}}{}^{12} e\left\{\sum_{t=1}^{s}\sum_{j=1}^{n}{}^{11} c_{2t,2t-1}x_{2t-1,j}x_{j,2t}\right\},$$

where the sum over x_{ij} indicates a sum over all x_{ij} except (1) x_{ii}, $1 \leqq i \leqq n$ and (2) $x_{2t-1,2t}$, $1 \leqq t \leqq s$, and the sum over j is over all $j \neq 2t-1, 2t$. It is clear that there are exactly $(n-2)s$ terms in the above expression.

By a careful examination of (4.4), we can see that for $n>3$ and $1 \leqq t, i \leqq s$, each x_{ij} of the form $x_{2t-1,2t}$. $i \neq t$, appears in exactly two terms in the following way: let $t=t_0$ and $i=i_0$ be fixed. Then, for this choice of t, we may take $j=2i_0$ and we obtain $x_{2t_0-1,2t_0}$. Also, we may take $t=i_0$ and $j=2t_0-1$ and so obtain the same $x_{2t_0-1,2t_0}$. These are the only two ways this x_{ij} may occur. But, since, $1 \leqq t$, $i \leqq s$ and $i \neq t$ in any one term, we have exactly $s(s-1)x_{ij}$ of the form $x_{2t-1,2t}$. But $s(s-1) = s(n-2)/2 =$ half of the number of terms in (4.4). Since each such x_{ij} appears twice, we see that one such x_{ij} is in every term of (4.4). By factoring out each $x_{2t-1,2i}$ from the two terms in which it appears and by using the properties of the exponential function noted in $\pi 1$, we may write (4.4) as

$$(4.5)\qquad q^n \sum_{x_{ij}}{}^{12} \prod_{t=1}^{s}\prod_{i=1}^{s}{}' e\{c_{2t,2t-1}x_{2i,2t} + c_{2i,2i-1}x_{2i-1,2t-1})x_{2t-1,2i}\},$$

where the sum over x_{ij} is as in (4.4) and the product over i is such that for a fixed choice of t we have $i \neq t$. From the representation of the subscripts on the x_{ij} inside the parentheses in (4.5), it is clear that the two x_{ij} in each factor are distinct from each other and also from $x_{2t-1,2i}$. Hence, we have $3s(n-2)/2$ distinct x_{ij} left in the exponential functions above. Since we have already summed over n x_{ij} in obtaining (4.1) and have fixed $s=n/2$ x_{ij} in obtaining (4.4) from (4.1), we can see that there are $n^2-(n+3s(n-2)/2+s)$ remaining x_{ij} of which the expression in (4.5) is

independent and which are included in the sum over x_{ij} in (4. 5). Since the functions in (4. 5) are independent of these x_{ij}, if we let each one vary over the elements of F and also interchange the order of sums and products in (4. 5), we obtain

$$(4.6)\quad q^{n^2-3s(n-2)/2-s}\prod_{t=1}^{s}\sum_{i=1}^{s}{}'\sum_{x_{it}} e\{(c_{2t,2t-1}x_{2i,2t}+c_{2i,2i-1}x_{2i-1,2t-1})x_{2t-1,2i})\},$$

where the sum over x_{it} indicates a sum over each $x_{2i,2t}$, $x_{2i-1,2t-1}$, $x_{2t-1,2i}$, and the product over i is as in (4. 5). In view of (1. 2), we can see that the only nonzero contributions to (4. 6) come from those terms such that $c_{2t,2t-1}x_{2i,2i}+$ $+c_{2i,2i-1}x_{2i-1,2t-1}=0$, for all $1\leqq t\neq i\leqq s$. Since each $c_{2t,2t-1}\neq 0$, we may fix $x_{2i,2t}=-c_{2i,2i-1}x_{2i-1,2t-1}/c_{2t,2t-1}$ and the above noted expression will be 0. Hence, $x_{2i-1,2t-1}$ may be chosen arbitrarily. If we now sum over $x_{2t-1,2i}$ in accordance with (1. 2), note (4. 1) through (4. 6), we get

$$\sum_{X} e\{\sigma(CX^2)\} = q^{n^2-s-3s(s-1)/2}\prod_{t=1}^{s}\prod_{i=1}^{s}{}' q^2 = q^{n^2-s^2} = q^{3n^2/4}.$$

Hence, the theorem is proven in the case n even. The theorem can be seen to be valid for $n=2$ by inspection even though (4. 5) is not valid.

For $n>3$ and odd, if we apply the hypothesis of the theorem regarding c_{ij} immediately, then the resulting expression for (4. 2) is just $x_{2t-1,2t}=0$. (If c_{ij} other than $c_{2t,2t-1}$ are not 0, then the statements preceding (4. 2) are not valid.) Then the key step is noting that in the forming of (4. 5) from (4. 4), the $x_{2t-1,2i}$ as described do not exhaust the terms of (4. 5) as they do in the even case. In particular, for n odd, (4. 5) is written as

$$(4.7)\qquad q^n\sum_{x_{ij}}{}^{12}\prod_{t=1}^{s} e\{c_{2t,2t-1}x_{2t-1,n}x_{n,2t}\}\prod_{t=1}^{s}{}' e\{k\},$$

where $k=(c_{2t,2t-1}x_{2i,2t}+c_{2i,2-i1}x_{2i-1,2t-1})x_{2t-1,2i}$. If we now note that the $x_{2t-1,n}$ $x_{n,2t}$ are all distinct, $1\leqq t\leqq s$, the proof proceeds along the same lines as the case n even and we obtain

$$\sum_{X} e\{CX^2\} = q^{(3n^2+1)/4}.$$

We also note that although the factorization of (4. 7) is not valid for $n=3$, the final formula does hold for $n=3$ as one can easily check by comparing with Theorem 3.

References

[1] L. Carlitz, The singular series for the sums of squares of polynomials, *Duke Math. J.* **14** (1947), 1105—1120.

[2] L. Carlitz, Weighted quadratic partitions in a finite field, *Canad. J. Math.* **5** (1953), 137—153.

[3] L. Carlitz, Representations by quadratic forms in a finite field, *Duke Math. J.* **21** (1954), 123—138.

[4] L. Carlitz, The number of solutions of some equations in a finite field, *J. Math. Soc. Japan*, **7** (1953), pp. 209—223.

[5] L. CARLITZ, The number of solutions of a particular equation in a finite field, *Publ. Math. (Debrecen)* **4** (1956), 117—121.
[6] L. CARLITZ and JOHN H. HODGES, Representations by hermitian forms in a finitie field, *Duke Math. J.* **22** (1955), 393—405.
[7] ECKFORD COHEN, The number of simultaneous solutions of a quadratic equation and a pair of linear equations over a galois field, *A. M. S. Notices, Feb. 1962, Abstract* 62t-41, p. 45.
[8] JOHN H. HODGES, Exponential sums for symmetric matrices in a finite field, *Math. Nachr.* **14** (1955) 331—339.
[9] JOHN H. HODGES, Exponential sums for skew matrices in a finite field, *Arch. Math.* **6** (1956), 116—121.
[10] JOHN H. HODGES, Representations by bilinear forms in a finite field, *Duke Math., J .2* (1956), 497—510.
[11] A. DUANE PORTER, Simultaneous equations in a finite field, *Publ. Math. (Debrecen)* **16** (1969), 99—110.
[12] A. DUANE PORTER, Some partitions of a skew matrix, *Annal. di Mathetmatica,* **72** (1969), 115—120.
[13] A. DUANE PORTER, Generalized bilinear forms in a finite field, *Duke Math., J.* **37** (1970), 55—60

(Received May 4, 1971.)