Simultaneous equations in a finite field

By A. DUANE PORTER (Laramie, Wyoming)

1. *Introduction.* Let $F=GF(q)$ be the finite field of $q=p^e$ elements, p odd. Exact formulas for the number of solutions in F of certain types of equations and pairs of equations have appeared in a number of recent papers [2], [3], [4], [5], [6]. In particular, Eckford Cohen [2; Th. I] determined the number of simultaneous solutions in F of a linear and a quadratic equation, and in [3] he considered a system of two linear and one quadratic equation.

In this paper, we would like to consider a system of the form

$$(1.1)\quad \sum_{j=1}^{n} a_j x_{j1}^{a_{j1}} \dots x_{jk}^{a_{jk}} = a; \quad \sum_{j=1}^{n} b_j x_{j1}^{b_{j1}} \dots x_{jk}^{b_{jk}} = b; \quad \sum_{j=1}^{n} c_j x_{j1}^{b_{j1}} \dots x_{jk}^{b_{jk}} = c,$$

with $a_j, b_j, c_j, a, b, c \in F$, and $a_{j1}, \dots, a_{jk}, b_{j1}, \dots, b_{jk}$ integers with $2=(a_{j1}, \dots, a_{jk})$, $1=(b_{j1}, \dots, b_{jk})$, all $1 \leqq j \leqq n$.

We remark that for $k=1$, $a_{j1}=2$, $b_{j1}=1$, $1 \leqq j \leqq n$, the above system reduces to the one considered by Cohen in [3]. As might be expected, the results of (1. 1) are somewhat more involved, and we are not able to obtain complete results for the case in which $a_{j1}, \dots, a_{jk}$, $1 \leqq j \leqq n$, are only subject to the above restriction. However, we do obtain satisfactory results with some restrictions placed upon $a_{j1}, \dots, a_{jk}$.

2. *Notation and preliminaries.* If F is as noted in Section 1 and $\alpha \in F$, we define

$$(2.1)\qquad e(\alpha) = \exp\left(2\pi i t(\alpha)/p\right); \quad t(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{r-1}},$$

so $t(\alpha) \in GF(p)$. Hence, it follows that

$$(2.2)\qquad e(\alpha+\beta) = e(\alpha)e(\beta); \quad \sum_{\beta} e(\alpha\beta) = \begin{cases} q, & \alpha=0, \\ 0, & \alpha \neq 0, \end{cases}$$

where the indicated sum is over all $\beta \in F$. If we let ψ denote the Legendre function for F, so $\psi(t)=0, 1, -1$, according as $t=0$, a non-zero square or a non-square of F, we define

$$(2.3)\qquad v(\alpha) = 1 - \psi^2(\alpha).$$

The well known Gauss sum $G(\alpha)$ is defined by

$$(2.4)\qquad G(\alpha) = \sum_{\beta \in F} e(\alpha\beta^2) = \begin{cases} q & \alpha=0, \\ \sum_{\beta} \psi(\beta) e(\alpha\beta) = \psi(\alpha) G(1), & \alpha \neq 0, \end{cases}$$

where

$$G^2(1) = \psi(-1)q. \tag{2. 5}$$

The Cauchy—Gauss sum will be denoted by $G(\alpha, \beta)$ and has [1; § 1] the values

$$\begin{cases} G(\alpha, \beta) = \sum\limits_{\gamma} e(\alpha\gamma^2 + 2\beta\gamma) = \begin{cases} q, & \alpha = 0,\ \beta = 0, \\ 0, & \alpha = 0,\ \beta \neq 0, \\ e(-\beta^2/\alpha)G(\alpha), & \alpha \neq 0, \end{cases} \\ G(\alpha, \beta) - \sum\limits_{j=1}^{t} e(\alpha\gamma_j^2 + 2\beta\gamma_j) = \sum\limits_{\gamma \neq \gamma_1, \dots, \gamma_t} e(\alpha\gamma^2 + 2\beta\gamma). \end{cases} \tag{2. 6}$$

We also find need for

$$\begin{cases} Q_t = q^{t-1} - (q-1)^{t-1} \\ R_t = (q-1)^{t-1} \end{cases} \tag{2. 7}$$

Finally, in view of (2. 2), (2. 3), it is clear that

$$\sum_{\beta \neq \beta_1, \dots, \beta_t} e(\alpha\beta) = v(\alpha)q - \sum_{j=1}^{t} e(\alpha\beta_t). \tag{2. 8}$$

3. *Some preliminary results.* It has been proven in [6; Lemma II] that

$$\sum_{x_1, \dots, x_n} x_1^{a_1} \dots x_n^{a_n} = \sum_{y_1, \dots, y_n} y_1 \dots y_n \tag{3. 1}$$

when $1 = (a_1, \dots, a_n)$ and the indicated sums are over all $x_1, \dots x_n$ and $y_1, \dots y_n$, respectively, in F. Also, it was noted in [6, 3. 5] that with $1 = (a_1, \dots, a_n)$

$$\sum_{x_1, \dots, x_n} e(x_1^{a_1} \dots x_n^{a_n}) = \sum_{y_1, \dots, y_n} e(y_1 \dots y_n) \tag{3. 2}$$

since, in the proof of (3. 1), it was shown that the product on both sides of the equality assumed every non-zero element of F exactly $(q-1)^{n-1}$ times.

For purposes of this paper we prove

Lemma 1. *If* $1 = (b_1, \dots, b_n)$ *and* $a_j = 2b_j$, $1 \leqq j \leqq n$, *then*

$$\sum_{x_1, \dots, x_n} x_1^{a_1} \dots x_n^{a_n} + x_1^{b_1} \dots x_n^{b_n} = \sum_{y_1, \dots, y_n} y_1^2 \dots y_n^2 + y_1 \dots y_n. \tag{3. 3}$$

Proof. Let $y_1, \dots, y_n$ be arbitrary, but fixed, with $y_1 \dots y_n \neq 0$ and $y_1^2 \dots y_n^2 + y_1 \dots y_n = f \in F$. By (3. 1) and (3. 2) there is some set $x_1, \dots, x_n$ such that $x_1^{b_1} \dots x_n^{b_n} = y_1 \dots y_n$. (And, as $x_1, \dots, x_n, y_1, \dots, y_n$ vary over all elements of F, this value is assumed exactly $(q-1)^{n-1}$ times by these products.). Then we have $x_1^{a_1} \dots x_n^{a_n} = (x_1^{b_1} \dots x_n^{b_n})^2 = (y_1 \dots y_n)^2 = y_1^2 \dots y_n^2$. Hence,

$$x_1^{a_1} \dots x_n^{a_n} + x_1^{b_1} \dots x_n^{b_1} = y_1^2 \dots y_n^2 + y_1 \dots y_n = f,$$

so that f is also assumed by the left side of (3. 3). Also, in view of the above discussion, f is assumed exactly the same number of times by $x_1^{a_1} + \dots + x_n^{a_n} + x_1^{b_1} + \dots + x_n^{b_n}$ and $y_1^2 + \dots + y_n^2 + y_1 + \dots + y_n$ as $x_1, \dots, x_n$ and $y_1, \dots, y_n$ vary over the elements of F. The above discussion could have also began with $x_1^{a_1} + \dots + x_n^{a_n} + x_1^{b_1} + \dots + x_n^{b_n} = f$. Hence both $x_1^{a_1} + \dots + x_n^{a_n} + x_1^{b_1} + \dots + x_n^{b_n}$ and $y_1^2 + \dots + y_n^2 + y_1 + \dots + y_n$ assume exactly the same field elements an equal number of times as $x_1, \dots, x_n$ and $y_1, \dots, y_n$ vary over F, so the lemma is established.

In view of the above discussion and (2. 2), we have immediately

Lemma 2. *If* $1=(b_1, \dots, b_n)$ *and* $a_j=2b_j$, $1 \leqq j \leqq n$, *then*

$$\sum_{x_1, \dots, x_n} e(x_1^{a_1} \dots x_n^{a_n}+x_1^{b_1} \dots x_n^{b_n}) = \sum_{y_1, \dots, y_n} e(y_1^2 \dots y_n^2+y_1 \dots y_n). \tag{3. 4}$$

Finally, we state

Lemma 3. When $2=(a_1, \dots, a_n)$ then

$$\sum_{x_1, \dots, x_n} e(x_1^{a_1} \dots x_n^{a_n}) = \sum_{y_1, \dots, y_n} e(y_1^2 \dots y_n^2).$$

The proof is similar to the proof of (3. 1), (3. 2), (3. 3), and (3. 4) so will not be repeated. The proof shows that as $x_1, \dots, x_n$ and $y_1, \dots, y_n$ vary over the elements of F, the product on both sides of the equation assumes every non-zero element of F exactly $2(q-1)^{n-1}$ times.

4. *The main theorem.* To simplify details of the proof, we only consider systems (1. 1) such that $a_j b_j c_j \neq 0$, $1 \leqq j \leqq n$. We then rearrange the coefficients in the following way: Let $s_1, \dots, s_t$ be non-zero integers such that $s_1+\dots+s_t=n$, and let $f_1, \dots, f_t$ be distinct non-zero elements of F such that

$$\begin{gathered} -c_j/b_j = f_r, \quad \text{for} \quad s_1+\dots+s_{r-1} < j \leqq s_1+\dots+s_r, \\ 2 \leqq r \leqq t, \quad \text{and} \quad s_{r-1}=0 \quad \text{for} \quad r=1. \end{gathered} \tag{4. 1}$$

Then we may prove

Theorem. *The number N of solutions in F of the system* (1. 1) *with* $1=(b_{j1}, \dots, b_{jk})$ *and* $a_{j1}=2b_{j1}, \dots, a_{jk}=2b_{jk}$, $1 \leqq j \leqq n$, *is given by*

$$\begin{aligned} N = {} & q^{kn-3}+q^{n-3} Q_k^n[v(b)q-1]+q^{n-2} Q_k^n[v(c)q-1]+ \\ & +\sum_{r=1}^{t} [v(c+bf_r)q-1][q^{n-(k-1)s_r-3} Q_k^{n-s_r}-q^{n-3} Q_k^n]+ \\ & +\sum_{i=0}^{n} Q_k^{n-i} R_k^i[\sigma_i B_i+D_i+E_i+F_i], \end{aligned}$$

where Q_k and R_k are defined by (2. 7); *$v(\alpha)$ by* (2. 3); *f_r and s_r by* (4. 1); *σ_i by* (4. 9); *B_i by* (4. 10) *and* (4. 11); *D_i by* (4. 23); *E_i by* (4. 30), *and F_i by* (4. 39).

PROOF. In view of (2. 2), it is clear that the number of solutions in F of (1. 1) is given by

$$\left\{ \begin{aligned} & N = q^{-3} S(1, n, x_{j1}, \dots, x_{jk}) \sum_{\alpha} e\left\{\left(\sum_{j=1}^{n} a_j x_{j1}^{a_{j1}} \dots x_{jk}^{a_{jk}}-a\right)\alpha\right\} \cdot \\ & \cdot \sum_{\beta} e\left\{\left(\sum_{j=1}^{n} 2b_j x_{j1}^{b_{j1}} \dots x_{jk}^{b_{jk}}-2b\right)\beta\right\} \sum_{\gamma} e\left\{\left(\sum_{j=1}^{n} 2c_j x_{j1}^{b_{j1}} \dots x_{jk}^{b_{jk}}-2c\right)\gamma\right\}, \end{aligned} \right. \tag{4. 2}$$

where $S(1, n, x_{j1}, \dots, x_{jk})$ indicates a summation in which each variable $x_{j1}, \dots, x_{jk}$,

$1 \leqq j \leqq n$, takes on all values of F independently, and the constants 2 have been inserted in the second two equations to facilitate later application of the sum defined in (2. 6). Clearly, since the characteristic of F is not 2, this does not change the number of solutions. If we note (2. 2), interchange the order of sums and products, and collect like terms, we obtain

$$N = q^{-3} \sum_{\alpha, \beta, \gamma} e(-a\alpha - 2b\beta - 2c\gamma) \prod_{j=1}^{n} S(j, j, x_{j1}, \ldots, x_{jk}) \cdot$$
$$\cdot e\{a_j x_{j1}^{a_{j1}} \ldots x_{jk}^{a_{jk}} + 2(b_j\beta + c_j\gamma) x_{j1}^{b_{j1}} \ldots x_{jk}^{b_{jk}}\}.$$

In view of (3. 4) and Lemma II, for each $1 \leqq j \leqq n$, we have

$$S(j, j, x_{j1}, \ldots, x_{jk}) e\{a_j x_{j1}^{a_{j1}} \ldots x_{jk}^{a_{jk}} + 2(b_j\beta + c_j\gamma) x_{j1}^{b_{j1}} \ldots x_{jk}^{b_{jk}}\} =$$
$$= S(j, j, y_{j1}, \ldots, y_{jk}) e\{a_j y_{j1}^2 \ldots y_{jk}^2 + 2(b_j\beta + c_j\gamma) y_{j1} \ldots y_{jk}\}.$$

If we substitute this value into (4. 2), and let an arbitrary one of the variables, say y_{j1}, take on all values of F in accordance with (2. 6), we obtain

$$(4.3) \qquad \begin{cases} N = q^{-3} \sum_{\alpha, \beta, \gamma} e(-a\alpha - 2b\beta - 2c\gamma) \prod_{j=1}^{n} S(j, j, y_{j2}, \ldots, y_{jk}) \cdot \\ \qquad \cdot G\big(a_j y_{j2}^2 \ldots y_{jk}^2, (b_j\beta + c_j\gamma) y_{j2} \ldots y_{jk}\big). \end{cases}$$

We now write (4. 3) as $\mathrm{N} = P + R$, where

$$(4.4) \qquad \begin{cases} P = \text{sum of terms of (4. 3) corresponding to } \alpha = 0, \\ R = \text{sum of terms of (4. 3) corresponding to } \alpha \neq 0. \end{cases}$$

For each of P and R, we consider three cases as follows: $\beta = 0$, $\gamma = 0$; $\beta \neq 0$, $\gamma = 0$; β arbitrary, $\gamma \neq 0$.

The contribution to P from the terms corresponding to $\alpha = 0$, $\beta = 0$, $\gamma = 0$ is clearly

$$(4.5) \qquad q^{kn-3}.$$

When $\beta \neq 0$, $\gamma = 0$, the contribution to P from (4. 3) may be written as

$$q^{-3} \sum_{\beta \neq 0} e(-2b\beta) \prod_{j=1}^{n} S(j, j, y_{j2}, \ldots, y_{jk}) G(0, b_j\beta y_{j2} \ldots y_{jk}).$$

In view of (2. 6) $G(0, b_j\beta y_{j2} \ldots y_{jk}) = 0$ unless $b_j\beta y_{j2} \ldots y_{jk} = 0$. Hence, the above line will be zero expect when $y_{j2} \ldots y_{jk} = 0$, all $1 \leqq j \leqq n$. Clearly, this product will be zero exactly $Q_k = q^{k-1} - (q-1)^{k-1}$ times as $y_{j2}, \ldots, y_{jk}$ vary over all elements of F. Hence, the sum in this case simplifies to

$$q^{-3} \sum_{\beta \neq 0} e(-2b\beta) \prod_{j=1}^{n} Q_k q,$$

which equals

$$(4.6) \qquad q^{n-3} Q_k^n [v(b) q - 1],$$

where $v(b)$ is defined by (2. 3).

When $\alpha = 0$, $\gamma \neq 0$, β is arbitrary then in view of (4. 1) $b_j\beta + c_j\gamma = 0$ if and only if $\beta = f_r\gamma$ for some $1 \leqq r \leqq t$. If in (4. 3), for arbitrary, but fixed $\gamma \neq 0$, we choose

$\beta = f_r\gamma$, then $y_{j2}, \ldots, y_{jk}$ may be arbitrary for $s_1 + \ldots + s_{r-1} < j \leqq s_1 + \ldots + s_r$, but $y_{j2} \ldots y_{jk} = 0$ for all other j or else $G(0, (b_j\beta + c_j\gamma)y_{j2} \ldots y_{jk}) = 0$. With β and $y_{j2}, \ldots, y_{jk}$ is defined above, the inner product in (4. 3) equals

$$Q_k^{n-s_r} q^{n+(k-1)s_r}, \tag{4. 7}$$

where Q_k us defined in (2. 7). Clearly, when $\beta \neq f_r\gamma$, all $1 \leqq r \leqq t$, the value of the inner product is

$$Q_k^n q^n. \tag{4. 7)'$$

Now, for $\alpha \neq 0$, $\gamma \neq 0$, we break the sum over β in (4. 3) into $\beta = f_r\gamma$ plus sum over $\beta \neq f_r\gamma$, $1 \leqq r \leqq t$, and for each case use (4. 7) or (4. 7)′ as the value of the corresponding inner product, and obtain

$$q^{-3} \sum_{\gamma \neq 0} \left[\sum_{r=1}^{t} Q_k^{n-s_r} q^{n+(k-1)s_r} e\{(-2bf_r - 2c)\gamma\} \right] + \\ + q^{-3} \sum_{\gamma \neq 0} e(-2c\gamma) \sum_{\beta \neq f_r\gamma,\, 1 \leqq r \leqq t} e(-2b\beta) Q_k^n q^n.$$

If we now make the substitution required by (2. 8), note (2. 2), (2. 3), and rearrange terms, the above expression may be written as

$$\sum_{r=1}^{t} [v(c+bf_r)q-1][q^{n+(k-1)s_r-3} Q_k^{n-s_r} - q^{n-3} Q_k^n] + q^{n-2} Q_k^n v(b)[v(c)q-1]. \tag{4. 8}$$

Hence, the value of P as defined in (4. 4) is given by the sum of lines (4. 5), (4. 6), (4. 8).

Moving to a consideration of the value of R, we first consider those terms corresponding to $\alpha \neq 0$, $\beta = 0$, $\gamma = 0$. Then, in view of (2. 6), the value of the inner product in (4. 3) depends upon whether $y_{j2} \ldots y_{jk} = 0$ or $y_{j2} \ldots y_{jk} \neq 0$. Clearly, this product is zero Q_k times and not zero R_k times, see (2. 7), as $y_{j2}, \ldots, y_{jk}$ vary over the elements of F. Hence, the sum of terms of (4. 3) corresponding to this case may be written as

$$q^{-3} \sum_{\alpha \neq 0} e(-a\alpha) \prod_{j=1}^{n} [Q_k q + R_k \psi(\alpha) G(1) \psi(a_j)],$$

where $\psi(c)$ is defined above (2. 3); $G(1)$ in (2. 4) and (2. 5). We let $T = R_k \psi(\alpha) G(1)$ so T is a complex number and the above line may be written as

$$q^{-3} \sum_{\alpha \neq 0} e(-a\alpha) T^n \prod_{j=1}^{n} [Q_k q T^{-1} + \psi(a_j)].$$

The inner product above will clearly yield a sum involving the elementary symmetric functions [7; pp. 77—81] of $\psi(a_1), \ldots, \psi(a_n)$. In particular, we define

$$\tag{4. 9} \begin{cases} \sigma_i = \sum\limits_{j_1, \ldots, j_i} \psi(a_{j_1} \ldots a_{j_i}), \\ \text{where the sum is over all } j_1, \ldots, j_i \text{ such that for} \\ 1 \leqq v \leqq i,\ v \leqq j_v \leqq n - i + v, \text{ and for each term} \\ \text{in the sum } j_1 < j_2 < \ldots < j_i. \text{ Also, we define} \\ \sigma_0 = 1, \end{cases}$$

so that we obtain

$$\sum_{i=0}^{n} Q_k^{n-i} R_k^i \sigma_i [q^{n-i-3} G^i(1) \sum_{\alpha \neq 0} \psi^i(\alpha) e(-a\alpha)].$$

In view of (2. 2), (2. 4), (2. 5), and the definition of ψ, the value inside the brackets in the above line depends upon whether i is even or odd.

For i even, the value is

$$\psi^{i/2}(-1)[v(a)q-1]q^{(2n-i-6)/2}, \tag{4. 10}$$

and for i odd, the value is

$$\psi^{(i+1)/2}(-1)\psi(a)q^{(2n-i-5)/2}. \tag{4. 11}$$

Hence, the total contribution to R from the terms of (4. 3) corresponding to $\alpha \neq 0$, $\beta = 0$, $\gamma = 0$ is

$$\sum_{i=0}^{n} Q_k^{n-i} R_k^i \sigma_i B_i, \quad \text{where} \tag{4. 12}$$

Q_k and R_k are defined by (2. 7), σ_i is defined by (4. 9), and B_i by (4. 10) and (4. 11).

We now find the sum of terms of R corresponding to $\alpha \neq 0$, $\beta \neq 0$, $\gamma = 0$. This case becomes more cumbersome to write down so we will omit a number of the details in the proof. First, we note that in view of (2. 4), (2. 6), (2. 7), we may write the sum of terms of (4. 3) corresponding to this case as

$$q^{-3} \sum_{\alpha \neq 0, \beta \neq 0} e(-a\alpha - 2b\beta) \prod_{j=1}^{n} [Q_k q + R_k \psi(\alpha) G(1) e(-b_j^2 \beta^2 / a_j \alpha) \psi(a_j)]. \tag{4. 13}$$

We define $\delta_i =$ i-th elementary symmetric function of $e(-b_1^2\beta^2/a_1\alpha)\psi(a_1), \ldots$ $\ldots, e(-b_n^2\beta^2/a_n\alpha)\psi(a_n)$ so that

$$\delta_i = \sum_{j_1, \ldots, j_i} e(-b_{j_1}^2 \beta^2 / a_{j_i}\alpha) \ldots e(-b_{j_i}^2 \beta^2 / a_{j_i}\alpha) \psi(a_{j_1} \ldots a_{j_i}),$$

where the sum over $j_1, \ldots, j_i$ is defined as in (4. 9). To simplify writing δ_i, we also define

$$\begin{cases} a_{ij} = a_{j_1} \ldots a_{j_i}, \\ b_{ij} = -[b_{j_1}^2/a_{j_1} + \ldots + b_{j_i}^2/a_{j_i}], \end{cases} \tag{4. 14}$$

so that, in view of (2. 2), we may write δ_i as

$$\delta_i = \sum_{j_1, \ldots, j_i} \psi(a_{ij}) e(b_{ij}\beta^2/\alpha), \tag{4. 15}$$

with the sum over $j_1, \ldots, j_i$ as defined in (4. 9). Hence, by defining $\delta_0 = 1$, we may write (4. 13) as

$$q^{-3} \sum_{\alpha \neq 0, \beta \neq 0} e(-a\alpha - 2b\beta) \sum_{i=0}^{n} Q_k^{n-i} q^{n-i} R_k^i G^i(1) \psi^i(\alpha) \delta_i.$$

If we note (4. 15), recombine terms and sum over $\beta \neq 0$ in accordance with (2. 6), we obtain

$$q^{-3} \sum_{\alpha \neq 0} e(-a\alpha) \sum_{i=0}^{n} Q_k^{n-i} q^{n-i} R_k^i G^i(1) \psi^i(\alpha) \sum_{j_1, \ldots, j_i} [G(b_{ij}/\alpha, -b) - 1] \psi(a_{ij}). \tag{4. 17}$$

We now divide the sum over $j_1, \ldots, j_i$ as

$$\tag{4.18} \left\{\begin{array}{l} \displaystyle\sum_{j_1, \ldots, j_i} = M(i, 1) + M(i, 2) \\ \text{where } M(i, 1) = \text{sum over all } j_1, \ldots, j_i \text{ such that } b_{ij} \neq 0, \\ \quad \text{and } M(i, 2) = \text{sum over all } j_1, \ldots, j_i \text{ such that } b_{ij} = 0. \end{array}\right.$$

To simplify writing the results, we consider separate cases for $b=0$ and $b \neq 0$. Then in each case find values for the terms of (4. 17) when i is even and i odd.

If $b=0$, (4. 17) may be written as

$$\sum_{i=0}^{n} Q_k^{n-i} R_k^i q^{n-i-3} G^i(1) \sum_{\alpha \neq 0} \psi^i(\alpha) e(-a\alpha) \big[M(i, 1) \psi(a_{ij}) [G(b_{ij}/\alpha) - 1] + \\ + M(i, 2) \psi(a_{ij}) [q - 1]\big),$$

so that the value of the above terms corresponding to i even is

$$\tag{4.19} \left\{\begin{array}{l} Q_k^{n-i} R_k^i q^{(2n-i-6)/2} \psi^{i/2}(-1) \big(M(i, 1) \psi(a_{ij}) [\psi(ab_{ij}) q - v(a) q + 1] + \\ \qquad + M(i, 2) \psi(a_{ij}) (q-1) [v(a) q - 1]\big), \end{array}\right.$$

and the value for terms corresponding to i odd is

$$\tag{4.20} \left\{\begin{array}{l} \qquad Q_k^{n-i} R_k^i q^{(2n-i-5)/2} \psi^{(i+1)/2}(-1) \big[M(i, 1) \psi(a_{ij}) \times \\ \times \big(\psi(b_{ij}) [v(a) q - 1] - \psi(-a)\big) + \big[M(i, 2) \psi(a_{ij}) \psi(-a) [q-1]\big], \end{array}\right.$$

where we have used (2. 2), (2. 3), (2. 4), (2. 5), and the definition of ψ in the evaluation of these terms.

If $b \neq 0$, (4. 17) may be written as

$$\sum_{i=0}^{n} Q_k^{n-i} R_k^i q^{n-i-3} G^i(1) \sum_{\alpha \neq 0} \psi^i(\alpha) e(-a\alpha) [M(i, 1) \psi(a_{ij}) \times \\ \times \{e(-b^2 \alpha/b_{ij}) G(b_{ij}/\alpha) - 1\} + M(i, 2) \psi(a_{ij}) (-1)],$$

so as before, we have for i even

$$\tag{4.21} \left\{\begin{array}{l} Q_k^{n-i} R_k^i \psi^{i/2}(-1) q^{(2n-i-6)/2} \big(M(i, 1) \psi(a_{ij}) \big[\psi(ab_{ij} + b^2) q - \\ \qquad - v(a) q + 1\big] - M(i, 2) \psi(a_{ij}) [v(a) q - 1\big], \end{array}\right.$$

and for i odd,

$$\tag{4.22} \left\{\begin{array}{l} Q_k^{n-i} R_k^i \psi^{(i+1)/2}(-1) q^{(2n-i-5)/2} \big(M(i, 1) \psi(a_{ij}) [\{v(a + b^2/b_{ij}) q - 1\} \times \\ \qquad \times \psi(b_{ij}) - \psi(-a)] - M(i, 2) \psi(-aa_{ij})\big). \end{array}\right.$$

Hence, if we combine (4. 19), (4. 20), (4. 21), (4. 22) we have that the value of

(4. 17) and hence the sum of terms of R corresponding to $\alpha\neq 0$, $\beta\neq 0$ is given by

$$(4.23)\quad \begin{cases} \displaystyle\sum_{i=0}^{n} Q_k^{n-i} R_k^i D_i, \\ \text{where for } i \text{ even} \\ D_i = q^{(2n-i-6)/2}\psi^{i/2}(-1)\big(M(i,1)\psi(a_{ij})[\psi(ab_{ij}+b^2)q+v(a)q+1]+ \\ \qquad +M(i,2)\psi(a_{ij})[v(a)q-1][v(b)q-1]\big), \\ \text{and for } i \text{ odd} \\ D_i = q^{(2n-i-5)/2}\psi^{(i+1)/2}(-1)\big(M(i,1)\psi(a_{ij})]\psi(b_{ij})\{v(a+b^2/b_{ij})q-1\} \\ \qquad -\psi(-a)]+M(i,2)\psi(-aa_{ij})[v(b)q-1]\big), \end{cases}$$

with $M(i, 1)$ and $M(i, 2)$ defined by (4. 18); a_{ij} and b_{ij} by (4. 14).

Finally, we consider the sum of terms of R corresponding to $\alpha\neq 0$, β arbitrary, $\gamma\neq 0$. We divide the sum over β in (4. 3) into $\beta=f_r\gamma$, $1\leqq r\leqq t$, plus sum ober $\beta\neq f_r\gamma$, where f_r is defined by (4. 1). If we make this substitution and note (2. 6), (2. 7), we obtain

$$(4.24)\quad \begin{cases} q^{-3}\displaystyle\sum_{\alpha\neq 0} e(-a\alpha)\sum_{r=1}^{t}\sum_{\gamma\neq 0}\{(-2bf_r-2c)\gamma\}\prod_{j=1}^{n}[Q_k q+R_k\psi(\alpha)G(1)h_{rj}]+ \\ +q^{-3}\displaystyle\sum_{\alpha\neq 0,\beta\neq 0} e(-a\alpha-2c\gamma)\sum_{\beta\neq f_r\gamma,\,1\leqq r\leqq t} e(-2b\beta)\prod_{j=1}^{n}[Q_k q+R_k\psi(\alpha)G(1)u_j], \end{cases}$$

where

$$h_{rj} = \psi(a_j), \quad \text{for} \quad s_1+\dots+s_{r-1}<j\leqq s_1+\dots+s_r,$$

$$h_{rj} = \psi(a_j)e\{-(b_j f_r+c_j)^2\gamma^2/a_j\alpha\}, \quad \text{otherwise}$$

$$u_j = \psi(a_j)e\{-(b_j\beta+c_j\gamma)^2/a_j\alpha\}, \quad \text{all} \quad 1\leqq j\leqq n.$$

We now define $\varepsilon_{ri}=i$-th elementary symmetric function of $h_{r1},\dots,h_{rn}$ and $\xi_i=i$-th elementary symmetric function of $u_1,\dots,u_n$ so that

$$(4.25)\quad \begin{cases} \varepsilon_{ri} = \displaystyle\sum_{j_1,\dots,j_i} h_{rj_1}\dots h_{rj_i}, \\ \zeta_i = \displaystyle\sum_{j_1,\dots,j_i} u_{j_1}\dots u_{j_i}, \end{cases}$$

with the above sums over $j_1,\dots,j_i$ defined as in (4. 9), and $\varepsilon_{r0}=1=\zeta_0$. We also find use for the following definition:

$$(4.26)\qquad b_{ijr} = -(b_{j_1}f_r+c_{j_1})^2/a_{j_1}+\dots+-(b_{j_i}f_r+c_{j_i})^2/a_{j_i})$$

where clearly

$$(b_{j_z}f_r+c_{j_z})^2 = 0 \quad \text{for} \quad s_1+\dots+s_{r-1}<j_z\leqq s_1+\dots+s_r.$$

Hence, in view of the definition of h_{rj}, (2. 2), (4. 14), and (4. 25) we may write

$$(4.27)\qquad \varepsilon_{ri} = \sum_{j_1,\dots,j_i}\psi(a_{ij})e(b_{ijr}\gamma^2/\alpha).$$

If we now use this value and multiply out the inner product in the top line of (4. 24), recombine terms, and sum over $\gamma \neq 0$ in accordance with (2. 6), this line may be written as

$$(4.\,28)\quad \sum_{i=0}^{n} \sum_{r=1}^{t} Q_k^{n-i} R_k^i q^{n-i-3} G^i(1) \sum_{\alpha \neq 0} \psi^i(\alpha) e(-a\alpha) \sum_{j_1, \dots, j_i} [G(b_{ijr}/\alpha,\, 2bf_r + 2c) - 1] \psi(a_{ij}).$$

We now divide the sum over $j_1, \dots, j_i$ as

$$(4.\,29)\quad \begin{cases} \displaystyle\sum_{j_1, \dots, j_i} = M_r(i, 1) + M_r(i, 2) \\ \text{where } M_r(i, 1) = \text{sum over all } j_1, \dots, j_i \text{ such that } b_{ijr} \neq 0, \\ \quad \text{and } M_r(i, 2) = \text{sum over all } j_1, \dots, j_i \text{ such that } b_{ijr} = 0. \end{cases}$$

We can note the similarity between lines (4. 28) and (4. 29) with (4. 17) and (4. 18). Hence, to evaluate (4. 28), we consider separately cases sorresponding to $bf_r + c = 0$ and $bf_r + c \neq 0$, and so obtain results corresponding to (4. 19) through (4. 22). If we carry out these details and combine the results, the sum of the terms corresponding to (4. 28) may be written as

$$(4.\,30)\quad \begin{cases} \displaystyle\sum_{i=0}^{n} Q_k^{n-i} R_k^i E_i, \\ \text{where for } i \text{ even} \\ \displaystyle E_i = \sum_{r=1}^{t} q^{(2n-i-6)/2} \psi^{i/2}(-1) \big(M_r(i, 1) \psi(a_{ij}) [\psi(ab_{ij} + [bf_r + c]^2) q - \\ \qquad - v(a) q + 1] + M_r(i, 2) \psi(a_{ij}) [v(a) q - 1] [v(bf_r + c) q - 1]\big), \\ \text{and for } i \text{ odd} \\ \displaystyle E_i = \sum_{r=1}^{t} q^{(2n-i-5)/2} \psi^{(i+1)/2}(-1) \big(M_r(i, 1) \psi(a_{ij}) [\psi(b_{ijr}) \times \\ \times \{v(a + [bf_r + c]^2\}/b_{ijr}) q - 1 - \psi(-a) + M_r(i, 2) \psi(-aa_{ij}) + \\ \qquad + [v(bf_r + c) q - 1]\big), \end{cases}$$

with $M_r(i, 1)$ and $M_r(i, 2)$ defined by (4. 29); b_{ijr} defined by (4. 26); f_r defined by (4. 1). Hence, we have the value of the sum of terms in the first line of (4. 24).

If we multiply out the product over j in the second line of (4. 24) as we did in (4. 25) through (4. 28), note (2. 2), (2. 6), and collect like terms, we obtain

$$(4.\,31)\quad \begin{cases} \displaystyle\sum_{\alpha \neq 0,\, \gamma \neq 0} e(-a\alpha + 2c\gamma) \sum_{i=0}^{n} Q_k^{n-i} q^{n-i-3} R_k^i \psi^i(\alpha) G^i(1) \times \\ \displaystyle\quad \times \sum_{j_1, \dots, j_i} \psi(a_{ij}) e(c_{ij} \gamma^2/\alpha) [G(b_{ij}/\alpha,\, d_{ij}\gamma/\alpha - b) - \\ \displaystyle\qquad - \sum_{r=1}^{t} e(b_{ij} f_r^2 \gamma^2/\alpha + 2[d_{ij}\gamma/\alpha - b] f_r)], \end{cases}$$

where

$$\begin{cases} c_{ij} = -[c^2_{j_1}/a_{j_1} + \ldots + c^2_{j_i}/a_{j_i}], \\ d_{ij} = -[b_{j_1}c_{j_1}/a_{j_1} + \ldots + b_{j_i}c_{j_i}/a_{j_i}]. \end{cases} \tag{4. 32}$$

We also need the following definitions in which the operation denotes integral multiple [7; pp. 36].

$$\begin{cases} x_{ijr} = -a + [bf_r + c]^2/(b_{ij}f_r + c_{ij} + 2d_{ij}), \\ y_{iu} = m_u \cdot [-a + c_{ij}b^2/d^2_{iju} - 2bc/d_{iju}], \\ z_{ij} = [d_{ij}b/b_{ij} - c]^2/[c_{ij} - d^2/b_{ij}] + [a + b^2/b_{ij}], \end{cases} \tag{4. 33}$$

where, for $0 \leqq i \leqq n$, d_{iju}, $1 \leqq u \leqq w$, is of multiplicity m_u with $d_{iju} \neq d_{ijv}$ for $1 \leqq u \neq \neq v \leqq w$, and this set of w elements denotes the distinct elements among the d_{ij}.

To evaluate (4. 31), we must divide the sum over $j_1, \ldots, j_i$ as indicated in (4. 18) as well as the divisions listed below.

$$\begin{cases} \text{We write } M(i, 1) = M(i, 1, 1) + M(i, 1, 2), \text{ where} \\ M(i, 1, 1) = \text{sum of terms of } M(i, 1) \text{ such that } b_{ij}c_{ij} - d_{ij} \neq 0, \\ M(i, 1, 2) = \text{sum of terms of } M(i, 1) \text{ such that } b_{ij}c_{ij} - d_{ij} = 0. \end{cases} \tag{4. 34}$$

$$\begin{cases} \text{We write } M(i, 2) = M(i, 2, 1) + M(i, 2, 2), \text{ where} \\ M(i, 2, 1) = \text{sum of terms of } M(i, 2) \text{ such that } d_{ij} \neq 0, \\ M(i, 2, 2) = \text{sum of terms of } M(i, 2) \text{ such that } d_{ij} = 0. \end{cases} \tag{4. 35}$$

$$\begin{cases} \text{We write } M(i, 2, 2) = M(i, 2, 2, 1) + M(i, 2, 2, 2), \text{ where} \\ M(i, 2, 2, 1) = \text{sum of terms of } M(i, 2, 2) \text{ such that } c_{ij} \neq 0. \\ M(i, 2, 2, 2) = \text{sum of terms of } M(i, 2, 2) \text{ such that } c_{ij} = 0. \end{cases} \tag{4. 36}$$

Finally, we write

$$\begin{cases} \sum\limits_{j_1, \ldots, j_i} = M(i, 0) + \sum\limits_{r=1}^{t} M(i, r), \\ M(i, 0) = \text{sum of terms such that } b_{ij}f_r + c_{ij} + 2d_{ij} \neq 0, \qquad 1 \leqq r \leqq t, \\ M(i, r) = \text{sum of terms such that } b_{ij}f_r + c_{ij} + 2d_{ij} = 0. \end{cases} \tag{4. 37}$$

If we now proced to evaluate (4. 31) by considering the cases outlined in (4. 34) through (4. 37), we obtain, after a very lengthy, but straightforward, calculation

$$\sum_{i=0}^{n} Q_k^{n-i} R_k^i F_i \tag{4. 38}$$

as the value of (4. 31), with F_i given by

$$\begin{cases} F_i = \psi(a_{ij})[M(i, 1, 1)\psi(b_{ij}c_{ij} - d^2_{ij})T_i + M(i, 1, 2)\overline{K}_i + \\ + M(i, 2, 1)\psi^2(b)K_i -- M(i, 2, 2)v(b)W_i + \\ + M(i, 2, 2, 1)v(b)\overline{H}_i + M(i, 2, 2, 2)v(b)[v(c)q - 1]H_i - \\ - \sum\limits_{r=1}^{t} \{M(i, 0)\psi(b_{ij}f_r + c_{ij} + 2d_{ij})\overline{V}_i + M(i, r)v(bf_r + c)V_i - \sum\limits_{j_1, \ldots, j_i} \overline{T}_i\} - \\ - M(i, 1)\overline{W}_i], \end{cases} \tag{4. 39}$$

where $\psi(a_{ij})$ must be distributed inside the sums to be defined, and

$$H_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)[v(a)q-1], & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+3)/2}(-1)\psi(a), & i \text{ odd}, \end{cases}$$

$$\overline{H}_i = \begin{cases} q^{(2n-i-2)/2}\psi^{i/2}(-1)\psi(c^2+ac_{ij}), & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+1)/2}(-1)\psi(c_{ij})[v(c^2/c_{ij}+a)q-1], & i \text{ odd}, \end{cases}$$

$$K_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)\sum_{u=1}^{w} v(y_{iu}q-1), & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+1)/2}(-1)\sum_{u=1}^{w} \psi(y_{iu}), & i \text{ odd}, \end{cases}$$

$$\overline{K}_i = \begin{cases} q^{(2n-i-2)/2}\psi^{i/2}(-1)\psi(ab_{ij}+b^2)v(d_{ij}b/b_{ij}-c), & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+1)/2}(-1)\psi(b_{ij})v(d_{ij}b/b_{ij}-c)\times & \\ \times[v(a+b^2/b_{ij})q-1], & i \text{ odd}, \end{cases}$$

$$T_i = \begin{cases} q^{(2n-i-4)/2}\psi^{(i+2)/2}(-1)v(z_{ij}q-1), & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+1)/2}(-1)\psi(z_{ij}), & i \text{ odd}, \end{cases}$$

$$\overline{T}_i = \begin{cases} q^{(2n-i-6)/2}\psi^{i/2}(-1)[v(a)q-1], & i \text{ even}, \\ q^{(2n-i-5)/2}\psi^{(i+3)/2}(-1)\psi(a), & i \text{ odd}, \end{cases}$$

$$W_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)[v(a)q-1], & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+3)/2}(-1)\psi(a), & i \text{ odd}, \end{cases}$$

$$\overline{W}_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)\psi(b_{ij}a+b^2), & i \text{ even}, \\ q^{(2n-i-5)/2}\psi(b_{ij})\psi^{(i+1)/2}(-1)v[(a+b^2/b_{ij})q-1], & i \text{ odd}, \end{cases}$$

$$V_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)[v(a)q-1], & i \text{ even}, \\ q^{(2n-i-3)/2}\psi^{(i+3)/2}(-1)\psi(a), & i \text{ odd}, \end{cases}$$

$$\overline{V}_i = \begin{cases} q^{(2n-i-4)/2}\psi^{i/2}(-1)\psi(x_{ijr}), & i \text{ even}, \\ q^{(2n-i-5)/2}\psi^{(i+1)/2}(-1)v(x_{ijr}q-1), & i \text{ odd}. \end{cases}$$

In the above $\psi(\alpha)$ and $v(\alpha)$ are defined by (2. 3); a_{ij} and b_{ij} by (4. 14), and x_{ijr}, y_{iu}, z_{ij} by (4. 33).

Hence, by combining (4. 4), (4. 5), (4. 6), (4. 8), (4. 12), (4. 23), (4. 30), and (4. 38) the theorem is established.

References

[1] L. Carlitz, Weighted quadratic partitions over a finite field, *Canad. J. Math.* **5** (1953), 317—323.

[2] Eckford Cohen, Simultaneous pairs of linear and quadratic equations in a Galois field, *Canad. J. Math.* **9** (1957), 74—78.

[3] 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* 62 T-41, p. 45.

[4] John H. Hodges, Simultaneous pairs of linear and quadratic matrix equations obver a finite field, *Math. Z.* **84** (1964), 38—44.

[5] John H. Hodges, A skew matrix equation over a finite field, *Arch. Math.* **17** (1966), 50—55.

[6] A. Duane Porter, Some systems of equations in a finite field, *Math. Z.* **100** (1967), 141—145.

[7] B. L. van der Waerden, Modern Algebra Vol. I, 1949.

(Received January 2, 1968.)