Systems of one quadratic and two bilinear equations in a finite field

By A. DUANE PORTER (Laramie, Wyo.)

1. Introduction

Let $F=GF(q)$ be the finite field of $q=p^r$ elements, p odd. At the turn of this century, L. E. DICKSON ([5], pp. 46—48) found the number of solutions in F of a single qudratic equation, and in 1954 L. CARLITZ [3] found the number of simultaneous solutions in F of certain pairs of quadratic equations. These results were followed in 1957 by the formulas of E. COHEN [4] for the number of simultaneous solutions in F of pairs of linear and quadratic equations. In this paper, we wish to generalize to the system of three equations

$$(1.1) \qquad \sum_{j=1}^{n} a_j x_j^2 = a; \quad \sum_{j=1}^{n} b_j x_j y_j = b; \quad \sum_{j=1}^{n} d_j x_j y_j = d,$$

where all coefficients are from F, and $a_j b_j d_j \neq 0$, all $l \leqq j \leqq n$. Explicit formulas are obtained for the number of simultaneous solutions in F of this system. As is the case in Dickson's results, the number of solutions depends upon whether n is even or odd. We remark that among the systems (1.1), there occur also unsolvable ones. Consider, e. g. the case when $b_j=d_j$, $1 \leqq j \leqq n$ and $b \neq d$.

2. Notation and preliminaries

If α is an element of F, we define

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

where by its definition $t(\alpha)$ is an element of $GF(p)$. From (2.1), we may prove

$$(2.2) \qquad e(\alpha+\beta) = e(\alpha)e(\beta),$$

$$(2.3) \qquad \sum_{\beta} e(\alpha\beta) = \begin{cases} q, & \text{if } \alpha=0, \\ 0, & \text{if } \alpha \neq 0, \end{cases}$$

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

$$(2.4) \qquad v(\alpha) = 1 - \psi^2(\alpha).$$

In view of (2. 3) and (2. 4), one may easily prove

$$\sum_{\beta} e(\alpha\beta) = v(\alpha)q - \sum_{i=1}^{t} e(\alpha\beta_i), \qquad \beta \neq \beta_1, \beta_2, \ldots, \beta_t. \tag{2. 5}$$

The well known Gauss-sum ([1], § 3) for F and its values will be denoted by

$$G(\alpha) = \sum_{\beta} e(\alpha\beta^2) = \begin{cases} q, & \alpha = 0, \\ \sum_{\beta} \psi(\beta)e(\alpha\beta) = \psi(\alpha)G(1), & \alpha \neq 0, \end{cases} \tag{2. 6}$$

where

$$G^2(1) = \psi(-1)q. \tag{2. 7}$$

The Cauchy—Gauss sum will be denoted by $G(\alpha, \beta)$ and has, by [2], § 1, the values

$$G(\alpha, \beta) = \sum_{\gamma} e(\alpha\gamma^2 + 2\beta\gamma) = \begin{cases} q, & \alpha = 0, \quad \beta = 0, \\ 0, & \alpha = 0, \quad \beta \neq 0, \\ e(-\beta^2/\alpha)G(\alpha), & \alpha \neq 0. \end{cases} \tag{2. 8}$$

If $s_1, \ldots, s_k$ are nonzero integers such that $s_1 + \ldots + s_k = n$, and $f_1, \ldots, f_k$ are distinct nonzero elements of F, then we rearrange the system (1. 1) such that

$$\begin{cases} f_i = -d_j/b_j, \; s_1 + \ldots + s_{i-1} < j \leqq s_1 + \ldots + s_i, \\ \text{for} \quad i = 2, \ldots, k, \quad \text{and for} \quad i = 1, \quad \text{we define} \quad s_0 = 1. \end{cases} \tag{2. 9}$$

It is clear that (2. 9) does not impose any restrictions on the system (1. 1).

Finally, we define

$$\begin{cases} A = a_1 a_2 \ldots a_n, \\ A_i = a_{s_{i-1}+1} \ldots a_{s_i}, \; 2 \leqq i \leqq k, \text{ and for } \quad i = 1, \\ S_0 = 0. \end{cases} \tag{2. 10}$$

3. The number $N = N(A, n, a, b, d, f_i, s_i)$

We may now prove the

Theorem. *The number* $N = N(A, n, a, b, d, f_i, s_i)$ *of simultaneous solutions in* F *of the system* (1. 1) *when* $a_j b_j d_j \neq 0$, $1 \leqq j \leqq n$, *is given by*

$$\begin{cases} N = q^{2n-3} + v(a)\left[\{v(b)q - 1\}q^{n-2} + v(b)\{v(d)q - 1\}q^{n-1}\right] + \\ + \sum_{i=1}^{k} [v(bf_i + d) - 1][q^{n+s_i-3} - v(a)q^{n-2} + \\ + q^{s_i-3}\psi(A_i)H(s_i)] + \begin{cases} R, & n \quad \textit{even}, \\ T, & n \quad \textit{odd}, \end{cases} \end{cases} \tag{3. 1}$$

where

$$R = \psi(A)\psi^{n/2}(-1)[v(a)q-1]q^{(3n-6)/2}$$

$$T = \psi(aA)\psi^{(n+3)/2}(-1)q^{(3n-5)/2},$$

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

ψ is the Legendre function for F; $v(\alpha)$ is defined by (2. 4); *s_i and f_i are defined by* (2. 9); *A and A_i are defined by* (2. 10).

PROOF. In view of (2. 3), we have

$$\text{(3. 2)} \qquad \begin{cases} N = q^{-3} \sum\limits_{x_j, y_j} \sum\limits_{\alpha} e\left\{\left(\sum\limits_{j=1}^{n} a_j x_j^2 - a\right)\alpha\right\} \cdot \\ \cdot \sum\limits_{\beta} e\left\{2\left(\sum\limits_{j=1}^{n} b_j x_j y_j - b\right)\beta\right\} \sum\limits_{\gamma} e\left\{2\left(\sum\limits_{j=1}^{n} d_j x_j y_j - d\right)\gamma\right\}, \end{cases}$$

where the first sum to the right of the equality sign indicates a sum in which each x_j, y_j, $1 \leqq j \leqq n$, takes on all values of F independently, and we have multiplied the bilinear equations by the constant 2 in order to simplify application of the Cauchy—Gauss sum below. If we now note (2. 2), interchange the order of sums and products, collect terms involving x_j, and sum over x_j in accordance with (2. 8), we obtain

$$\text{(3. 3)} \qquad N = q^{-3} \sum_{\alpha, \beta, \gamma} e(-a\alpha - 2b\beta - 2d\gamma) \prod_{j=1}^{n} \sum_{y_j} G(a_j\alpha, y_j[b_j\beta + d_j\gamma]).$$

To evaluate N, we write $N = N_1 + N_2$, where

$$\text{(3. 4)} \qquad \begin{cases} N_1 = \text{sum of terms of (3. 3) corresponding to } \alpha = 0, \\ N_2 = \text{sum of terms of (3. 3) corresponding to } \alpha \neq 0. \end{cases}$$

When $\alpha = 0$, we must have $y_j[b_j\beta + d_j\gamma) = 0$, $1 \leqq j \leqq n$, or in view of (2. 8), the value of the product over j in (3. 3) will be zero. Hence, we break N_1 into $M_1 + M_2$, where

$$\text{(3. 5)} \qquad \begin{cases} M_1 = \text{sum of terms of } N_1 \text{ corresponding to } \gamma = 0, \\ M_2 = \text{sum of terms of } N_1 \text{ corresponding to } \gamma \neq 0. \end{cases}$$

When $\gamma = 0$, by the same reasoning as above, we must have $y_j(b_j\beta) = 0$, $1 \leqq j \leqq n$. Thus, to evaluate M_1, we break the sum over β in (3. 3) into $\beta = 0$ plus the sum over $\beta \neq 0$. If we recall that $b_j \neq 0$, $1 \leqq j \leqq n$, so when $\beta \neq 0$, then $y_j = 0$, $1 \leqq j \leqq n$, we obtain

$$\text{(3. 6)} \qquad M_1 = q^{2n-3} + [v(b)q-1]q^{n-3}.$$

When $\gamma \neq 0$, then $b_j\beta + d_j\gamma = 0$ if and only if $\beta = -d_j/b_j\gamma$ so, in view of (2. 9), if and only if $\beta = f_i\gamma$ for some $1 \leqq i \leqq k$. Since the f_i, $1 \leqq i \leqq k$, are distinct, if $\beta = f_i\gamma$, then $\beta \neq f_j\gamma$ for all $j \neq i$. Thus, if we choose $\beta = f_i\gamma$, then y_j must be zero for all j except $s_1 + \ldots + s_{i-1} < j \leqq s_1 + \ldots + s_i$, or else $y_j[b_j\beta + d_j\gamma]$ will not be zero for all $1 \leqq j \leqq n$.

With these comments, simple calculations will show that if we pick $\beta = f_i\gamma$, the product over j in (3. 3) has the value q^{n+s_i}. Also if $\beta \neq f_i\gamma$, all $1 \leqq i \leqq k$, then the product over j in (3. 3) equals q^n. If we now break the sum over β in (3. 3) into $\beta = f_i\gamma$, $1 \leqq i \leqq k$, plus the sum over $\beta \neq f_i\gamma$, $1 \leqq i \leqq k$, and for each β use the corresponding values of the inner product indicated above, we have after rearranging terms

$$M_2 = q^{-3}\left[\sum_{i=1}^{k}\Big(q^{n+s_i}\sum_{\gamma\neq 0} e\{-2(bf_i+d)\gamma\}\Big) + \sum_{\gamma\neq 0} e(-2d\gamma)\sum_{\beta}{}' e(-2b\beta)q^n\right],$$

where the indicated sum over β is a sum over all $\beta \neq f_i\gamma$, $1 \leqq i \leqq k$. Thus, in view of (2. 5)

$$\sum_{\beta}{}' e(-2b\beta) = v(b)q - \sum_{i=1}^{k} e(-2bf_i\gamma). \tag{3. 7}$$

If we substitute (3. 7) into the above expression for M_2, regroup terms involving γ and f_i, sum over γ in accordance with (2. 5), and note that $e(0)=1$, we obtain

$$M_2 = \sum_{i=1}^{k}[v(bf_i+d)q-1](q^{n+s_i-3}-q^{n-3}) + v(b)[v(d)q-1]q^{n-2}. \tag{3. 8}$$

When $\alpha \neq 0$, if we recall $a_j \neq 0$ and make the substitution required by (2. 8) into (3. 3), note also (2. 6) and (2. 10), sum over y_j, and recall that ψ is multiplicative, we have

$$N_2 = q^{-3}\sum_{\alpha\neq 0}\sum_{\beta,\gamma} e(-a\alpha-2b\beta-2d\gamma)\psi(A)G^n(1)\psi^n(\alpha)\prod_{j=1}^{n} G(-[b_j\beta+d_j\gamma]^2/a_j\alpha). \tag{3. 9}$$

We now let

$$\begin{cases} Q_1 = \text{sum of terms of (3. 9) corresponding to } \gamma = 0,\\ Q_2 = \text{sum of terms of (3. 9) corresponding to } \gamma \neq 0. \end{cases} \tag{3. 10}$$

For $\gamma = 0$, if we note (2. 6), break the sum over β in (3. 9) into $\beta = 0$ plus the sum over $\beta \neq 0$, and note (2. 6), (2. 10), Q_1 may be written as

$$Q_1 = q^{-3}\sum_{\alpha\neq 0}\psi^n(\alpha)e(-a\alpha)\psi(A)G^n(1)[q^n + [v(b)q-1]\psi^n(-1)\psi(A)\psi^n(\alpha)G^n(1)].$$

We can see by (2. 6) that the value of Q_1 depends upon whether n is even or odd.

If n is even (so $\psi^n(\alpha) = \psi^n(-1) = 1$), then

$$Q_1 = \psi(A)[v(a)q-1]\psi^{n/2}(-1)q^{(3n-6)/2} + [v(a)q-1][v(b)q-1]q^{n-3}, \tag{3. 11}$$

where $v(\alpha)$ is defined by (2. 4).

If n is odd (so $\psi^n(\alpha) = \psi(\alpha)$, $\psi^n(-1) = \psi(-1)$), then

$$Q_1 = \psi(aA)\psi^{(n+3)/2}(-1)q^{(3n-5)/2} + [v(a)q-1][v(b)q-1]q^{n-3}. \tag{3. 12}$$

For $\gamma \neq 0$, if we use the same reasoning as used in the first paragraph under (3. 6), and choose $\beta = f_i\gamma$, for some fixed $1 \leqq i \leqq k$, the product over j in (3. 9) has the value

$$q^{s_i}\psi(A)\psi(A_i)\psi^{n-s_i}(\alpha)G^{n-s_i}(1)\psi^{n-s_i}(-1), \tag{3. 13}$$

where A and A_i are defined by (2. 10). Similarly, when $\beta \neq f_i \gamma$, all $1 \leqq i \leqq k$, this product over j has the value

$$\psi(A)\psi^n(\alpha)G^n(1)\psi^n(-1). \tag{3. 14}$$

To evaluate Q_2, we break the sum over β in (3. 9) into $\beta = f_i \gamma$, $1 \leqq i \leqq k$, plus the sum over $\beta \neq f_i \gamma$, and for each choice of β use (3. 13) or (3. 14) as the value of the corresponding value of the product over j. Thus, we have

$$\tag{3. 15} \begin{cases} Q_2 = q^{-3}\psi(A)G^n(1)\sum\limits_{a\neq 0} e(-a\alpha)\psi^n(\alpha)\left[\sum\limits_{i=1}^{k}\left(\sum\limits_{\gamma\neq 0} e\{-2(bf_i+d)\gamma\}\right)\cdot\right. \\ \cdot q^{s_i}\psi(A)\psi(A_i)\psi^{n-s_i}(\alpha)G^{n-s_i}(1)\psi^{n-s_i}(-1) + \sum\limits_{\gamma\neq 0} e(-2d\gamma)\cdot \\ \left.\cdot \sum\limits_{\beta}{}' e(-2b\beta)\psi(A)\psi^n(\alpha)G^n(1)\psi^n(-1)\right], \end{cases}$$

where the indicated sum over β is a sum over all $\beta \neq f_i \gamma$, $1 \leqq i \leqq k$. If we substitute the value of this sum, given by (3. 7), into (3. 15), regroup terms involving γ, α, and f_i, sum over γ and α in accordance with (2. 5), we obtain

$$\tag{3. 16} \begin{cases} Q_2 = \sum\limits_{i=1}^{k} [v(bf_i+d)-1][q^{s_i-3}\psi(A_i)\psi^{n-s_i}(-1)G^{2n-s_i}(1) \\ \sum\limits_{\alpha\neq 0}\psi^{s_i}(\alpha)e(-a\alpha) - [v(a)q-1]q^{n-3}] + v(b)[v(a)q-1][v(d)q-1]q^{n-2}. \end{cases}$$

If we let

$$H(s_i) = \psi^{n-s_i}(-1)G^{2n-s_i}(1)\sum_{\alpha\neq 0}\psi^{s_i}(\alpha)e(-a\alpha),$$

then, in view of (2. 6) and (2. 7), the value of $H(s_i)$ depends upon whether s_i is even or odd.

If s_i is even (so $\psi^{s_i}(\alpha)=1$), then

$$H(s_i) = \psi^{s_i/2}(-1)[v(a)q-1]q^{(2n-s_i)/2}. \tag{3. 17}$$

If s_i is odd (so $\psi^{s_i}(\alpha)=\psi(\alpha)$), then

$$H(s_i) = \psi(a)\psi^{3(s_i+1)/2}q^{(2n-s_i+1)/2}. \tag{3. 18}$$

Hence, recalling that $N = N_1 + N_2 = M_1 + M_2 + Q_1 + Q_2$, noting (3. 6), (3. 8), (3. 11), (3. 12), (3. 16), (3. 17), (3. 18), and regrouping terms, the Theorem is established.

References

[1] L. CARLITZ, The singular series for 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, Pairs of quadratic equations in a finite field, *Amer. J. Math.* **76** (1954), 137—153.

[4] E. COHEN, Simultaneous pairs of linear and quadratic equations in a finite field, *Canad. J. Math.* **9** (1957), 74—78.

[5] L. E. DICKSON, Linear Groups, *Leipzig*, 1901.

(Received June 10, 1965.)