

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 quadratic 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

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

where all coefficients are from F , and $a_j b_j d_j \neq 0$, all $1 \leq j \leq n$. 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 $b_j = d_j$, $1 \leq j \leq n$ and $b \neq d$.

2. Notation and preliminaries

If α is an element of F , we define

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

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

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

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

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

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

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

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

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

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

where

$$(2. 7) \quad G^2(1) = \psi(-1)q.$$

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

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

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

$$(2. 9) \quad \begin{cases} f_i = -d_j/b_j, & s_1 + \dots + s_{i-1} < j \leq s_1 + \dots + s_i, \\ \text{for } i=2, \dots, k, \text{ and for } i=1, \text{ we define } s_0=1. \end{cases}$$

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

Finally, we define

$$(2. 10) \quad \begin{cases} A = a_1 a_2 \dots a_n, \\ A_i = a_{s_{i-1}+1} \dots a_{s_i}, \quad 2 \leq i \leq k, \text{ and for } i=1, \\ S_0 = 0. \end{cases}$$

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 $a_j b_j d_j \neq 0$, $1 \leq j \leq n$, is given by

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

where

$$\begin{aligned} R &= \psi(A)\psi^{n/2}(-1)[v(a)q-1]q^{(3n-6)/2} \\ T &= \psi(aA)\psi^{(n+3)/2}(-1)q^{(3n-5)/2}, \\ H(s_i) &= \begin{cases} \psi^{s_i/2}(-1)[v(a)q-1]q^{(2n-s_i)/2}, & s_i \text{ even}, \\ \psi(a)\psi^{3(s_i+1)/2}(-1)q^{(2n-s_i+1)/2}, & s_i \text{ odd}, \end{cases} \end{aligned}$$

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

$$(3.2) \quad \left\{ \begin{aligned} N &= q^{-3} \sum_{x_j, y_j} \sum_{\alpha} e \left\{ \left(\sum_{j=1}^n a_j x_j^2 - a \right) \alpha \right\} \cdot \\ &\quad \cdot \sum_{\beta} e \left\{ 2 \left(\sum_{j=1}^n b_j x_j y_j - b \right) \beta \right\} \sum_{\gamma} e \left\{ 2 \left(\sum_{j=1}^n d_j x_j y_j - d \right) \gamma \right\}, \end{aligned} \right.$$

where the first sum to the right of the equality sign indicates a sum in which each $x_j, y_j, 1 \leq j \leq n$, 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

$$(3.3) \quad N = q^{-3} \sum_{\alpha, \beta, \gamma} e(-a\alpha - 2b\beta - 2d\gamma) \prod_{j=1}^n \sum_{y_j} G(a_j \alpha, y_j [b_j \beta + d_j \gamma]).$$

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

$$(3.4) \quad \begin{cases} N_1 = \text{sum of terms of (3. 3) corresponding to } \alpha = 0, \\ N_2 = \text{sum of terms of (3. 3) corresponding to } \alpha \neq 0. \end{cases}$$

When $\alpha = 0$, we must have $y_j [b_j \beta + d_j \gamma] = 0, 1 \leq j \leq n$, 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

$$(3.5) \quad \begin{cases} M_1 = \text{sum of terms of } N_1 \text{ corresponding to } \gamma = 0, \\ M_2 = \text{sum of terms of } N_1 \text{ corresponding to } \gamma \neq 0. \end{cases}$$

When $\gamma = 0$, by the same reasoning as above, we must have $y_j (b_j \beta) = 0, 1 \leq j \leq n$. 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 $b_j \neq 0, 1 \leq j \leq n$, so when $\beta \neq 0$, then $y_j = 0, 1 \leq j \leq n$, we obtain

$$(3.6) \quad M_1 = q^{2n-3} + [v(b)q-1]q^{n-3}.$$

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 $1 \leq i \leq k$. Since the $f_i, 1 \leq i \leq k$, 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 $s_1 + \dots + s_{i-1} < j \leq s_1 + \dots + s_i$, or else $y_j [b_j \beta + d_j \gamma]$ will not be zero for all $1 \leq j \leq n$.

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 $1 \leq i \leq k$, then the product over j in (3. 3) equals q^n . If we now break the sum over β in (3. 3) into $\beta = f_i \gamma$, $1 \leq i \leq k$, plus the sum over $\beta \neq f_i \gamma$, $1 \leq i \leq k$, and for each β use the corresponding values of the inner product indicated above, we have after rearranging terms

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

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

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

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

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

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

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

We now let

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

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

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

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

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

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

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 $1 \leq i \leq k$, the product over j in (3. 9) has the value

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

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

$$(3. 14) \quad \psi(A)\psi^n(\alpha)G^n(1)\psi^n(-1).$$

To evaluate Q_2 , we break the sum over β in (3. 9) into $\beta = f_i \gamma$, $1 \leq i \leq k$, 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

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

where the indicated sum over β is a sum over all $\beta \neq f_i \gamma$, $1 \leq i \leq k$. 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

$$(3. 16) \quad \left\{ \begin{aligned} Q_2 &= \sum_{i=1}^k [v(bf_i + d) - 1][q^{s_i-3}\psi(A_i)\psi^{n-s_i}(-1)G^{2n-s_i}(1) \\ &\quad \sum_{\alpha \neq 0} \psi^{s_i}(\alpha)e(-\alpha\alpha) - [v(a)q - 1]q^{n-3}] + v(b)[v(a)q - 1][v(d)q - 1]q^{n-2}. \end{aligned} \right.$$

If we let

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

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

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

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

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

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.)