# PAIRS OF BILINEAR EQUATIONS IN A FINITE FIELD

A. DUANE PORTER

**1. Introduction.** Let $F = \mathrm{GF}(q)$ be the finite field of $q = p^r$ elements, $p$ arbitrary. We wish to consider the system of bilinear equations

$$(1.1)\qquad \sum_{j=1}^{u} a_j x_j y_j = a, \qquad \sum_{j=1}^{u} b_j x_j y_j = b,$$

where all coefficients are from $F$. The number of solutions in $F$ of a single bilinear equation may be obtained from a theorem of John H. Hodges (**3**, Theorem 3) by properly defining the matrices $U$, $V$, $A$, $B$. In 1954, L. Carlitz (**1**) obtained, as a special case of his work on quadratic forms, the number of simultaneous solutions in $F$ of (1.1) when all $a_j = 1$ and $p$ is odd. Carlitz considered the case $p = 2$ separately.

In this paper we are able to remove all restrictions on the coefficients of (1.1). In §3 we obtain an explicit value for the number of simultaneous solutions in $F$ of (1.1). It is of interest to note that no solvability criterion, such as the one given by E. Cohen (**2**), depending only on the number of variables, can be given here, for, if we take $a_j = b_j = 1$, $1 \leqslant j \leqslant u$, $a = 0$, $b = 1$ in (1.1), it is easy to see that this corresponding system will be unsolvable for every $u \geqslant 1$ and every field $F$.

The proof in §3 is independent of whether the characteristic of $F$ is even or odd. However, in order to simplify the calculations, we rearrange the coefficients as follows. Let $s_0, \ldots, s_{k+1}$ be integers such that $s_0 + \ldots + s_{k+1} = u$, with $s_1 > 0$, $1 \leqslant i \leqslant k$, and $s_i \geqslant 0$, $i = 0, k+1$. Let $f_1, \ldots, f_k$ be distinct non-zero elements of $F$. Then we have

$$(1.2)\qquad \begin{cases} a_j = 0 & \text{if } 1 \leqslant j \leqslant s_0, \\ b_j = 0 & \text{if } s_0 + \ldots + s_k < j \leqslant s_0 + \ldots + s_{k+1}, \\ a_j \neq 0,\, b_j \neq 0 & \text{otherwise,} \end{cases}$$

$$(1.3)\qquad a_j/b_j = f_i \qquad \text{if } s_0 + \ldots + s_{i-1} < j \leqslant s_0 + \ldots + s_i,\ 1 \leqslant i \leqslant k,$$

so that for $1 \leqslant i \leqslant k$, $s_i$ is the number of ratios $a_j/b_j$ that have the common value $f_i$. We further let $n = u - s_0 - s_{k+1}$; thus $n$ is the number of $x_j$ with non-zero coefficients. We suppose $n \geqslant 1$ so that the problem is not trivial.

This paper is part of a doctoral thesis written at the University of Colorado under the direction of Professor John H. Hodges. The author wishes to

Received January 22, 1965.



https://doi.org/10.4153/CJM-1966-054-9 Published online by Cambridge University Press acknowledge with gratitude his indebtedness to Professor Hodges for his assistance in the preparation of this paper.

**2. Notation and preliminaries.** If $\alpha \in F$, we define

$$e(\alpha) = \exp[2\pi i t(\alpha)/p], \qquad t(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{r-1}}, \tag{2.1}$$

so that $t(\alpha)$ is an element of GF$(p)$. One may prove from (2.1) that

$$e(\alpha + \beta) = e(\alpha)e(\beta) \tag{2.2}$$

and

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

where the indicated sum in (2.3) is over all $\beta \in F$. We denote this sum by $R(\alpha)$. Obviously,

$$\sum_{\beta \neq \beta_1, \ldots, \beta_k} e(\alpha\beta) = R(\alpha) - \sum_{j=1}^{k} e(\alpha\beta_j). \tag{2.4}$$

For any choice of $x_j$ and $y_j$ in $F$, $1 \leqslant j \leqslant s_0$, $s_0 + n < j \leqslant u$, let

$$\begin{cases} A = A(a, a_j, x_j, y_j) = a - \displaystyle\sum_{j=s_0+n+1}^{u} a_j x_j y_j, \\ B = B(b, b_j, x_j, y_j) = b - \displaystyle\sum_{j=1}^{s_0} b_j x_j y_j. \end{cases} \tag{2.5}$$

If we properly define $U$, $V$, $A$, $B$ (**3**, Theorem 3), then the number of solutions in $F$ of the single bilinear equation

$$\alpha_1 x_1 y_1 + \ldots + \alpha_n x_n y_n = \alpha$$

is given by

$$\begin{cases} q^{2n-1} - q^{n-1} & \text{if } \alpha \neq 0, \\ q^{2n-1} + q^n - q^{n-1} & \text{if } \alpha = 0. \end{cases} \tag{2.6}$$

Finally, let $\psi$ denote the Legendre function for $F$; thus $\psi(\alpha) = 0, 1, -1$, according as $\alpha$ is 0, a non-zero square, or a non-square of $F$.

**3. The number** $N(a, b, a_j, b_j, n)$**.** We now prove the following result.

THEOREM. *The number* $N = N(a, b, a_j, b_j, n)$ *of simultaneous solutions in* $F$ *of the system* (1.1) *is given by*

$$N = q^{2(n+s-1)} + q^n[N(A)N(B) - q^{2(s-1)}] + \sum_{i=1}^{k} (q^{n+s_i-2} - q^{n-2})(N_i q - q^{2s}) \tag{3.1}$$

*where* $s = s_0 + s_{k+1}$. *If* $s_{k+1} = 0$, *then* $N(A) = 1 - \psi^2(a)$; *otherwise* $N(A)$ *is the number of solutions as given by* (2.6) *of the bilinear equation* $A = 0$; *cf.* (2.5).

https://doi.org/10.4153/CJM-1966-054-9 Published online by Cambridge University Press

*If* $s_0 = 0$, *then* $N(B) = 1 - \psi^2(b)$; *otherwise* $N(B)$ *is the number of solutions of the bilinear equation* $B = 0$; *cf.* (2.5). *If* $s_0 = s_{k+1} = 0$, *then* $N_i = 1 - \psi^2 (a - bf_i)$, *where* $f_i$ *is defined by* (1.3), *and otherwise* $N_i$ *is the number of solutions of the bilinear equation* $A - Bf_i = 0$.

*Proof.* If we move the last $s_{k+1}$ terms $a_j x_j y_j$ and the first $s_0$ terms $b_j x_j y_j$ to the right side of the corresponding equations (1.1), we obtain the equivalent system of equations

$$\sum_{j=s_0+1}^{s_0+n} a_j x_j y_j = A, \qquad \sum_{j=s_0+1}^{s_0+n} b_j x_j y_j = B, \tag{3.2}$$

where in (3.2) all $a_j \neq 0$, $b_j \neq 0$, and $A$, $B$ are defined by (2.5).

We now let $S_x$, $S_y$ indicate sums in which each $x_j$, $y_j$, respectively,

$$s_0 < j \leqslant s_0 + n,$$

takes on all values of $F$ independently. Then if we define

$$T = S_x S_y q^{-2} R\left(\sum_{j=s_0+1}^{s_0+n} a_j x_j y_j - A\right) R\left(\sum_{j=s_0+1}^{s_0+n} b_j x_j y_j - B\right), \tag{3.3}$$

we have, in view of (2.3), that the number of solutions of (3.2) is given by

$$N = \sum_{x_j, y_j}^{\circ} T \tag{3.4}$$

where the symbol immediately to the right of the equality sign indicates a sum in which each $x_j$, $y_j$, $1 \leqslant j \leqslant s_0$, $s_0 + n < j \leqslant u$ takes on all values of $F$ independently. Clearly, if $s_0 = S_{k+1} = 0$, then (3.4) reduces to $N = T$, with $A = a$ and $B = b$.

If we apply (2.3) to (3.3), we obtain

$$T = S_x S_y q^{-2} \sum_{\alpha} e\left\{\left(\sum_{j=s_0+1}^{s_0+n} a_j x_j y_j - A\right)\alpha\right\} \sum_{\beta} e\left\{\left(\sum_{j=s_0+1}^{s_0+n} b_j x_j y_j - B\right)\beta\right\}.$$

In view of (2.2), (2.3), and the definitions of $S_x$ and $S_y$, if we multiply out the above expression, interchange the order of sums and products, collect terms involving $y_j$ and sum over $y_j$, we obtain

$$T = q^{-2} \sum_{\alpha,\beta} e(-A\alpha - B\beta) \prod_{j=s_0+1}^{s_0+n} \sum_{x_j} R(x_j[a_j \alpha + b_j \beta]). \tag{3.5}$$

Clearly, $T = 0$ unless $x_j[a_j \alpha + b_j \beta] = 0$, for all $s_0 + 1 \leqslant j \leqslant s_0 + n$, and for $\alpha \neq 0$, $a_j \alpha + b_j \beta = 0$ if and only if $\beta = -f_i \alpha$ for some fixed $1 \leqslant i \leqslant k$. Hence, we write $T = P + Q$, where

$$\begin{cases} P \text{ equals the sum of terms of } T \text{ corresponding to } \alpha = 0, \\ Q \text{ equals the sum of terms of } T \text{ corresponding to } \alpha \neq 0. \end{cases} \tag{3.6}$$

When $\alpha = 0$, if we note (2.3) and hence break the sum over $\beta$ in (3.5) into the term with $\beta = 0$ and the sum over $\beta \neq 0$, a straightforward calculation will yield

$$P = q^{2n-2} - q^{n-2} + R(B)q^{n-2}. \tag{3.7}$$

If in (3.5), for arbitrary but fixed $\alpha \neq 0$, we choose $\beta = -f_i \alpha$, then since there are exactly $s_i$ ratios $a_j/b_j = f_i$, $x_j$ may be arbitrary for

$$s_0 + \ldots + s_{i-1} < j \leqslant s_0 + \ldots + s_i,$$

but $x_j$ must be zero for all other $j$ or else $Q = 0$. With $x_j$ defined as above, the inner product in (3.5) equals

$$q^{n+s_i}. \tag{3.8}$$

When $\alpha \neq 0$, if we break up the sum over $\beta$ in (3.5) into the term with $\beta = -f_i \alpha$ plus the sum over $\beta \neq -f_i \alpha$, $1 \leqslant i \leqslant k$, and for each $i$ use (3.8) as the value of the inner product, we obtain

$$Q = q^{-2} \sum_{\alpha \neq 0} \left( \sum_{i=1}^{k} q^{n+s_i} e[Bf_i \alpha] \right) e(-A\alpha) + q^{-2} \sum_{\alpha \neq 0} \sum_{\beta \neq -f_i\alpha, 1 \leqslant i \leqslant k} \prod_{j=s_0+1}^{s_0+n} R(0) e(-A\alpha - B\beta).$$

In view of (2.3), (2.4), and a rearrangement of terms, the above equals

$$Q = q^{n-2} \sum_{i=1}^{k} (q^{s_i} - 1)[R(Bf_i - A) - 1] + q^{n-2} R(B)[R(A) - 1]. \tag{3.9}$$

We may now write, in view of (3.4) and (3.6),

$$N = \sum_{x_j, y_j}^{\circ} (P + Q), \tag{3.10}$$

where $P$ is given by (3.7) and $Q$ by (3.9). If not both $s_0 = 0$ and $S_{k+1} = 0$, then as the $x_j, y_j$, $1 \leqslant j \leqslant s_0$, $s_0 + n < j \leqslant u$, take on all values of $F$, it is clear that $A, B$ will be equal to zero for some choices of $x_j$, $y_j$ and not equal to zero for others. In particular, for a fixed set

$$(x_1, y_1, \ldots, x_{s_0}, y_{s_0}, x_{s_0+n+1}, y_{s_0+n+1}, \ldots, x_u, y_u),$$

exactly one of the following combinations will hold:

$$\begin{cases} A = 0, B = 0; & A = 0, B \neq 0, \\ A \neq 0, B = 0; & A \neq 0, B \neq 0. \end{cases} \tag{3.11}$$

The terms of (3.10) that do not contain $A$ or $B$ are independent of the choices of $x_j$, $y_j$ described above; thus as we sum over the $x_j, y_j$, $1 \leqslant j \leqslant s_0$, $s_0 + n < j \leqslant u$, these terms obtain a factor of $q^{2s}$ where $s = s_0 + s_{k+1}$. Thus, if we substitute the values for $P$ and $Q$ into (3.10), carry out the indicated summation for those terms that are independent of $x_j$, $y_j$, $j$ in the above range, and combine the remaining terms, we have

$$(3.12)\quad N = q^{2(n+s-1)} - q^{2s}\left[q^{n-2} + q^{n-2}\sum_{i=1}^{k}(q^{s_i} - 1)\right] + q^{n-2}\sum_{x_j,y_j}^{\circ}\left[R(A)R(B) + \sum_{i=1}^{k}(q^{s_i} - 1)R(Bf_i - A)\right].$$

We now break the indicated sum over $s_j$, $y_j$ into the four cases of (3.11) to evaluate the third term of (3.12).

1. When $A = 0$, $B = 0$, then $R(A) = q$, $R(B) = q$, and $R(Bf_i - A) = q$. These values will be assumed $N(A)$, $N(B)$, and $N(A)N(B)$ times, respectively, so the contribution to (3.12) from this case is

$$(3.13)\qquad N(A)N(B)q^n + q^{n-1}\sum_{i=1}^{k}(q^{s_i} - 1)N(A)N(B).$$

2. When $A = 0$, $B \neq 0$, then $A - Bf_i = -Bf_i$. Thus $R(B) = 0$ and $R(A - Bf_i) = 0$ so the contribution to (3.12) from this case is zero.

3. When $A \neq 0$, $B = 0$, then $A - Bf_i = A$; hence the contribution from this case is likewise zero.

4. When $A \neq 0$, $B \neq 0$, then $R(A) = 0$, $R(B) = 0$, and $R(A - Bf_i)$ will equal $q$ exactly $N_i - N(A)N(B)$ times, since by (2) and (3) $A - Bf_i = 0$ has no solution in which $A = 0$, $B \neq 0$, or $A \neq 0$, $B = 0$. Thus the contribution to (3.12) from the terms corresponding to this case is

$$(3.14)\qquad q^{n-1}\sum_{i=1}^{k}(q^{s_i} - 1)[N_i - N(A)N(B)].$$

If $s_0 = 0$ or $s_{k+1} = 0$ or both, then we interpret the conditions on $A$ and $B$ as conditions on the constants $a$ and $b$ so that exactly one of the conditions (3.11) will hold for a given set of equations (1.1). The definitions of $N(A)$, $N(B)$, $N_i$ in the theorem take this possibility into consideration. Thus, if we replace the third term of (3.12) by its value, which is the sum of (3.13) and (3.14), and rearrange terms, we obtain (3.1), so the theorem is established.

## References


1. L. Carlitz, *Pairs of quadratic equations in a finite field*, Amer. J. Math., *76* (1954), 137–153.
2. E. Cohen, *Simultaneous pairs of linear and quadratic equations in a Galois field*, Can. J. Math., *9* (1957), 74–78.
3. J. H. Hodges, *Representations by bilinear forms in a finite field*, Duke Math. J., *22* (1955), 497–509.


*University of Wyoming*