Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

A. Duane Porter

Trilinear equations in a finite field

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **40** (1966), n.3, p. 361–365.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1966_8_40_3_361_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1966.

NOTE PRESENTATE DA SOCI

Algebra. — *Trilinear equations in a finite field.* Nota di A. DUANE PORTER, presentata (*) dal Socio B. SEGRE.

SUNTO. — Si determina il numero delle soluzioni di una o due equazioni trilineari, in un qualunque numero di variabili, sopra un campo di Galois.

1. INTRODUCTION.—Let $F = GF(q)$ be the finite field of $q = p^r$ elements, p arbitrary. We wish to consider the trilinear equations

$$\sum_{j=1}^{n} a_j x_j y_j z_j = a \quad ; \quad \sum_{j=1}^{n} b_j x_j y_j z_j = b \,, \tag{1.1}$$

with all coefficients from F. In the case of bilinear equations, the number of solutions of a single bilinear equation may be obtained from a theorem of John H. Hodges [2; Th. 3]. Also, the number of simultaneous solutions of 2 bilinear equations may be found in a result of the author [3].

In this paper, we are able to obtain corresponding results for trilinear equations. In Theorem I, we obtain the number of solutions in F of a single trilinear equation, and in Theorem II, we obtain the number of simultaneous solutions in F of the system (1.1), when $a_j b_j \neq 0$, $1 \leq j \leq n$. Finally, in Theorem III we find the number of simultaneous solutions of (1.1) without any restrictions on the coefficients. The proof of Theorem III is not included since it is similar to that of Theorem II, although much more cumbersome to write down.

It is of interest to note that no solvability criterion, such as given by E. Cohen [1], depending only on the number of variables, can be given here, for, if we take $a_j = b_j = 1$, $1 \leq j \leq n$, $a = 0$, $b = 1$ in (1.1) it is easy to see that this corresponding system will be unsolvable for every $n \geq 1$ and every field F.

2. NOTATION AND PRELIMINARIES.—If α is an element of F, we define

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

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

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

(*) Nella seduta del 12 febbraio 1966.

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 may define,

$$v(\alpha) = 1 - \psi^2(\alpha). \tag{2.4}$$

In view of (2.3) and (2.4), one can easily verify

$$\sum_{\beta+\beta_1,\cdots,\beta_t} e(\alpha\beta) = v(\alpha)\, q - \sum_{j=1}^{t} e(\alpha\beta_j). \tag{2.5}$$

3. ONE TRILINEAR.—We now prove

THEOREM I.—*The number* $N = N(n, a)$ *of solutions in* F *of the single trilinear equation* $a_1x_1y_1z_1 + \cdots + a_nx_ny_nz_n = a$ *is given by*

$$N = q^{3n-1} + [v(a)\, q - 1]\,[2q - 1]^n\, q^{n-1},$$

where $v(a)$ *is defined by* (2.5).

Proof. In view of (2.3), we have

$$N = \sum_{x_j, y_j, z_j}{}' q^{-1} \sum_{\alpha} e\left\{\left[\sum_{j=1}^{n} a_j x_j y_j z_j - a\right]\alpha\right\},$$

where the sum over x_j, y_j, z_j indicates a sum in which these elements, for $1 \leq j \leq n$, take on all values of F independently. If we now multiply out the above expression, interchange the order of sums and products, and sum over z_j, we have

$$N = q^{-1} \sum_{\alpha} e(-a\alpha) \prod_{j=1}^{n} \sum_{x_j} \sum_{y_j} v(a_j x_j y_j \alpha)\, q. \tag{3.1}$$

Clearly, we must have $a_j x_j y_j \alpha = 0$, all $1 \leq j \leq n$, or the value of the product over j is zero. Hence, we break the sum over α into $\alpha = 0$ plus the sum over $\alpha \neq 0$.

When $\alpha = 0$, x_j and y_j may be arbitrary for all $1 \leq j \leq n$, so the sum of the corresponding terms of (3.1) is q^{3n-1}.

When $\alpha \neq 0$, we must have $x_j y_j = 0$, all $1 \leq j \leq n$. To this end, we may have, for each j, as the x_j and y_j take on all values of F, either

$$\begin{cases} \text{(a)} & x_j = 0 \ , & y_j \text{ arbitrary, and} \\ \text{(b)} & x_j \neq 0 \ , & y_j = 0, \end{cases} \tag{3.2}$$

or

$$\begin{cases} \text{(a)} & y_j = 0 \ , & x_j \text{ arbitrary, and} \\ \text{(b)} & y_j \neq 0 \ , & x_j = 0. \end{cases} \tag{3.3}$$

However, both (3.2) and (3.3) yield $q + (q - 1)$ choices for $x_j y_j = 0$. Hence, for each j we have the same number of choices, regardless of how the sums

over x_j and y_j are formed. Hence, we may write (3.1) as

$$N = q^{-1} \sum_{\alpha} e(-a\alpha) \prod_{j=1}^{n} [2q-1]\, q,$$

which in view of (2.3) and (2.5) yields

$$N = [v(a)\, q - 1]\, [2q-1]^n q^n. \tag{3.4}$$

Combining (3.4) with the value of (3.1), Theorem I is established.

4. TWO TRILINEAR EQUATIONS.—To shorten the details of the proof, we only consider systems (1.1) in which $a_j b_j \neq 0$, $1 \leq j \leq n$. We then rearrange the coefficients of (1.1) in the following way: Let $s_1, s_2, \cdots s_k$ be nonzero integers such that $s_1 + \cdots + s_k = n$. Let $f_1, \cdots, f_k$ be distinct nonzero elements of F such that

$$\left\{\begin{array}{ll} -a_j/b_j = f_i, & \text{all } s_1 + \cdots + s_{i-1} < j \leq s_1 + \cdots + s_i, \\ & \text{for } 2 \leq i \leq k, \text{ and for } i = 1, \\ & \text{we define } s_0 = 0. \end{array}\right. \tag{4.1}$$

We now state

THEOREM II.—*If* $a_j b_j \neq 0$, $1 \leq j \leq n$, *then the number* $N = N(n, a, b)$ *of simultaneous solutions in* F *of the system* (1.1) *is given by*

$$N = q^{3n-2} + (2q-1)^n [v(a)\, v(b)\, q^2 - 1]\, q^{n-2} + \tag{4.2}$$

$$+ \sum_{i=1}^{k} [v(a + bf_i) - 1]\, [(2q-1)^{n-s_i} q^{n+2s_i-2} - (2q-1)^n q^{n-2}],$$

where $v(\alpha)$ *is defined by* (2.5); f_i *and* s_i *by* (4.1).

Proof. Clearly, noting (2.3), we have

$$N = \sum_{x_j, y_j, z_j}{}' q^{-2} \sum_{\alpha} e\left\{\left(\sum_{j=1}^{n} a_j x_j y_j z_j - a\right)\alpha\right\} \sum_{\beta} e\left\{\left(\sum_{j=1}^{n} b_j x_j y_j z_j - b\right)\beta\right\},$$

where the sum immediately to the right of the equality sign is defined as in the paragraph above (3.1). If we multiply out the above expression, interchange the order of sums and products, and sum over z_j in accordance with (2.3) and (2.5), we obtain

$$N = q^{-2} \sum_{\alpha, \beta} e(-a\alpha - b\beta) \prod_{j=1}^{n} \sum_{x_j} \sum_{y_j} v(x_j y_j [a_j \alpha + b_j \beta])\, q. \tag{4.3}$$

We now write $N = N_1 + N_2$, where

$$\left\{\begin{array}{l} N_1 = \text{sum of terms of (4.3) for which } \alpha = 0, \\ N_2 = \text{sum of terms of (4.3) for which } \alpha \neq 0. \end{array}\right. \tag{4.4}$$

When $\alpha = 0$, if we note (2.5), break the sum over β into $\beta = 0$ plus the sum over $\beta \neq 0$, and for $\beta \neq 0$, use the same reasoning as in (3.2) and (3.3), then a straightforward calculation will yield

$$N_1 = q^{3n-2} + [v(b)\, q - 1]\,[2q - 1]^n q^{n-2}. \tag{4.5}$$

If in (4.3), for an 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 and y_j may be arbitrary for $s_1 + \cdots + s_{i-1} < j \leq s_1 + \cdots + s_i$, but $x_j y_j$ must be zero for all other j or else $N_2 = 0$. Hence, for these j, we must use the same reasoning as in (3.2) and (3.3), so that if $\beta = f_i \alpha$, the product over j in (4.3) equals

$$(2q - 1)^{n-s_i} q^{n-2s_i}. \tag{4.6}$$

When $\alpha \neq 0$, if we break up the sum over β in (4.3) into $\beta = f_i \alpha$, $1 \leq i \leq k$, plus the sum over $\beta \neq f_i \alpha$, $1 \leq i \leq k$, and for each i use (4.6) as the value of the product over j, we obtain

$$N_2 = q^{-2} \sum_{\alpha \neq 0} \sum_{i=1}^{k} (2q - 1)^{n-s_i} q^{n+2s_i}\, e[(-a - bf_i)\alpha] +$$

$$+ q^{-2} \sum_{\alpha \neq 0} \sum_{\beta \neq f_i \alpha, 1 \leq i \leq k} e(-a\alpha - b\beta) \prod_{j=1}^{n} (2q - 1)\, q\,.$$

If we substitute the value of the sum over β, given by (2.5), into the above equation, regroup terms, and sum over α in accordance with (2.3), we obtain

$$N_2 = \sum_{i=1}^{k} [v(a + bf_i)\, q - 1]\,[(2q - 1)^{n-s_i} q^{n+2s_i-2} - (2q - 1)^n q^{n-2}] + \tag{4.7}$$

$$+ v(b)\,[v(a)\, q - 1]\,(2q - 1)^n q^{n-1}.$$

Hence, combining (4.5) and (4.7), and cancelling like terms, Theorem II is established.

5. THE NUMBER $N(n, a, b, a_j, b_j)$.—We now relax the restriction $a_j b_j \neq 0$, $1 \leq j \leq n$, of Theorem II. We let $s_0, \cdots, s_k, s_{k+1}$ be integers such that $s_0 + \cdots + s_{k+1} = n$ with $s_0, s_{k+1} \geq 0$, $s_i > 0$ for $1 \leq i \leq k$, and $f_1, \cdots, f_k$ be distinct nonzero elements of F. We then rearrange the coefficients of (1.1) as follows:

$$\begin{cases} a_j = 0 \quad , & 1 \leq j \leq s_0\,, \qquad a_j \neq 0 \text{ otherwise,} \\ b_j = 0 \quad , & s_0 + \cdots + s_k < j \leq n\,, \qquad b_j \neq 0 \text{ otherwise,} \\ a_j/b_j = -f_i\,, & s_0 + \cdots + s_{i-1} < j \leq s_0 + \cdots + s_i\,, \; 1 \leq i \leq k. \end{cases} \tag{5.1}$$

We further let $u = n - s_0 - s_{k+1}$, so u is the number of x_j, y_j, z_j with nonzero coefficients in both equations. We suppose $u \geq 1$ so the problem is not trivial. Finally, for any choice of x_j, y_j, z_j, $1 \leq j \leq s_0$, $s_0 + u \leq j \leq n$, in F, we

define

$$(5.2)\qquad \begin{cases} \mathrm{A} = \mathrm{A}(a, a_j, x_j, y_j, z_j) = a - \sum_{j=s_0+u+1}^{n} a_j x_j y_j z_j, \\ \mathrm{B} = \mathrm{B}(b, b_j, x_j, y_j, z_j) = b - \sum_{j=1}^{s_0} b_j x_j y_j z_j. \end{cases}$$

It is now possible to prove

THEOREM III.—*The number* $\mathrm{N} = \mathrm{N}(n, a, b, a_j, b_j)$ *of simultaneous solutions of the system* (1.1) *is given by*

$$\mathrm{N} = q^{3(u+s)-2} + (2q-1)^u q^{2u-2}[\mathrm{N}(\mathrm{A})\,\mathrm{N}(\mathrm{B})\,q^2 - q^{3s}] + \\ + \sum_{i=1}^{k} [\mathrm{N}(\mathrm{A} + \mathrm{B}f_i) - q^{3s}][(2q-1)^{u-s_i} q^{u+2s_i-2} - (2q-1)^u q^{u-2}],$$

where

$s = s_0 + s_{k+1}$ *and both* f_i *and* s_i *are as defined in* (4.1). *If* $s_{k+1} = 0$, *then* $\mathrm{N}(a) = v(a)$, *where* $v(a)$ *is given by* (2.5), *and otherwise* $\mathrm{N}(\mathrm{A})$ *is the number of solutions as given by Theorem I of the trilinear equation* $\mathrm{A}=0$, *where* A *is given by* (5.2). *If* $s_0 = 0$, *then* $\mathrm{N}(\mathrm{B}) = v(b)$, *and otherwise* $\mathrm{N}(\mathrm{B})$ *is the number of solutions of the trilinear equation* $\mathrm{B} = 0$, *where* B *is given by* (5.2). If $s_0 = s_{k+1} = 0$, *then* $\mathrm{N}(\mathrm{A} + \mathrm{B}f_i) = v(a + bf_i)$, *and otherwise* $\mathrm{N}(\mathrm{A} + \mathrm{B}f_i)$ *is the number of solutions of the trilinear equation* $\mathrm{A} + \mathrm{B}f_i = 0$.

The proof will not be included, however for interests sake, we note that the key to the proof lies in writing the first equation in the proof of Theorem II as

$$\mathrm{N} = \mathrm{S}_{xyz}\,\overline{\mathrm{S}}_{xyz}\,q^{-2} \sum_{\alpha} e\left\{\left(\sum_{j=s_0+1}^{s_0+u} a_j x_j y_j z_j - \mathrm{A}\right)\alpha\right\} \cdot \sum_{\beta} e\left\{\left(\sum_{j=s_0+1}^{s_0+u} b_j x_j y_j z_j - \mathrm{B}\right)\beta\right\},$$

where S_{xyz} indicates a summation in which each x_j, y_j, z_j, $1 \leq j \leq s_0$, $s_0 + u < j \leq n$ takes on all values of F independently, and $\overline{\mathrm{S}}_{xyz}$ indicates a similar sum in which j varies $s_0 + 1 \leq j \leq s_0 + u$.

REFERENCES.

[1] COHEN ECKFORD, *Simultaneous Pairs of Linear and Quadratic Equations in a Galois Field*, «Canadian Journal of Mathematics», 9, 74–78 (1957).

[2] HODGES JOHN H., *Representations by Bilinear Forms in a Finite Field*, «Duke Mathematical Journal», *22*, 497–501 (1955).

[3] PORTER A. DUANE, *Pairs of Bilinear Equations in a Finite Field*, Accepted by «Canadian Journal of Mathematics». Will appear in 1966.