ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

382

ON SYSTEMS OF LINEAR AND QUADRATIC EQUATIONS IN FINITE FIELDS

BY

AIMO TIETÄVÄINEN

HELSINKI 1965
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1966.382

Communicated 8 October 1965 by P. J. Myrberg and K. Inkeri.

KESKUSKIRJAPAINO
HELSINKI 1965

On systems of linear and quadratic equations in finite fields

1. Introduction. Let $K = GF(q)$ be a finite field of q elements where $q = p^n$, p is an odd prime and n a positive integer. Consider the system

$$(1)\qquad \begin{cases} \sum_{j=1}^{s} \alpha_j \xi_j^2 = \alpha \\ \sum_{j=1}^{s} \beta_{ij} \xi_j = \beta_i \ (i = 1, \ldots, t) \end{cases}$$

where $\alpha_1, \ldots, \alpha_s$ are non-zero, $\alpha, \beta_1, \ldots, \beta_t$ arbitrary elements of K, and the β_{ij}'s are elements of K such that the $t \times s$ matrix (β_{ij}) has rank t. The purpose of this note is to prove the following result.

Theorem. *The system* (1) *has a solution* $(\xi_1, \ldots, \xi_s)$ *in* K *if* $s = 2t + 2$. *On the other hand, in case* $s = 2t + 1$ *there exist, in every* K, *systems* (1) *which are insolvable in* K.

This theorem has been proved by Dickson [4] in case $t = 0$ and by Cohen ([2], remark 4; [3]) in case $t = 1$. It is a conjecture of Cohen [2].

2. Preliminary remarks. Let $\sigma, \sigma_1, \ldots, \sigma_v$ be elements of K. Define the trace of σ as

$$\mathrm{tr}(\sigma) = \sigma + \sigma^p + \ldots + \sigma^{p^{n-1}}$$

so that $\mathrm{tr}(\sigma)$ may be considered as an integer (mod p). Define, furthermore,

$$e(\sigma) = e^{2\pi i\, \mathrm{tr}(\sigma)/p} .$$

Then we have

$$(2)\qquad e\Big(\sum_{j=1}^{v} \sigma_j\Big) = \prod_{j=1}^{v} e(\sigma_j) .$$

Consider the system

$$(3)\qquad f_i(\xi_1, \ldots, \xi_s) = \delta_i \ (i = 1, \ldots, u)$$

where the f_i's are polynomials with coefficients in K and the δ_i's are elements of K. It has been proved in [1] that the number of solutions $(\xi_1, \ldots, \xi_s)$ of the system (3) is equal to

$$q^{-u} \sum_{\mathbf{c}} e(-\sum_{i=1}^{u} \gamma_i \delta_i) \sum_{\xi_1} \cdots \sum_{\xi_s} e(\sum_{i=1}^{u} \gamma_i f_i (\xi_1, \ldots, \xi_s)) . \tag{4}$$

Here and hereafter, in the sums of type $\sum\limits_{\mathbf{c}}$ the summation is over all the vectors $\mathbf{c} = (\gamma_1, \ldots, \gamma_u)$ with the γ_i's in K. Moreover, in the sums of type $\sum\limits_{\xi}$ the variable runs through all the elements of K. By (2) and (4), the number of solutions of the system

$$\sum_{j=1}^{s} f_{ij}(\xi_j) = \delta_i \quad (i = 1, \ldots, u),$$

where the f_{ij}'s are polynomials over K, is equal to

$$q^{-u} \sum_{\mathbf{c}} e(-\sum_{i=1}^{u} \gamma_i \delta_i) \prod_{j=1}^{s} \sum_{\xi_j} e(\sum_{i=1}^{u} \gamma_i f_{ij}(\xi_j)) . \tag{5}$$

Let us denote

$$S(\gamma, \delta) = \sum_{\xi} e(\gamma \xi^2 + \delta \xi) .$$

It is well known (see, for example, [2]) that $|S(\gamma, \delta)| = q^{1/2}$ if $\gamma \neq 0$.

3. Proof of the theorem. Let $s = 2t + 2$. Then the number of solutions of the system (1) is, by (5), equal to

$$N = q^{-t-1} \sum_{\mathbf{c}} e(-\varkappa \alpha - \sum_{i=1}^{t} \lambda_i \beta_i) \prod_{j=1}^{2t+2} S(\varkappa \alpha_j, \sum_{i=1}^{t} \lambda_i \beta_{ij})$$

where $\mathbf{c} = (\varkappa, \lambda_1, \ldots, \lambda_t)$. We break up this summation into two parts according as $\varkappa = 0$ or $\varkappa \neq 0$, writing

$$N = q^{-t-1}(\sum_{\varkappa=0} + \sum_{\varkappa \neq 0}) = q^{-t-1}(U_1 + U_2) .$$

In case $t = 0$ we have $U_1 = q^2$. In case $t \geqq 1$ U_1 is, by (5), equal to $q^t N_1$ where N_1 is the number of solutions of the system

$$\sum_{j=1}^{2t+2} \beta_{ij} \xi_j = \beta_i \quad (i = 1, \ldots, t) .$$

Because the matrix (β_{ij}) has rank t then $N_1 = q^{t+2}$. Consequently $U_1 = q^{2t+2}$, for every t. In the sum U_2 we have $\varkappa \alpha_j \neq 0$, for every $\mathbf{c}$. Therefore $|S(\varkappa \alpha_j, \sum\limits_{i=1}^{t} \lambda_i \beta_{ij})| = q^{1/2}$ and hence

$$|U_2| \leqq (q^{t+1} - q^t)q^{t+1} = q^{2t+2} - q^{2t+1} .$$

Consequently

$$N \geqq q^{-t-1} (U_1 - |U_2|) \geqq q^t > 0 .$$

This proves the former part of the theorem.

For the proof of the latter part of the theorem it is sufficient to note that the system

$$\begin{cases} -\sum_{j=1}^{t} \xi_j^2 + \sum_{j=t+1}^{2t+1} \xi_j^2 = \alpha \\ \xi_i + \xi_{t+i} = 0 \quad (i = 1, \ldots, t) , \end{cases}$$

where α is a non-square of K, is insolvable in K.

University of Turku
Turku, Finland

References

[1] CARLITZ, L.: Invariant theory of systems of equations in a finite field. - J. Analyse Math. 3 (1954), 382—413.

[2] COHEN, E.: The number of simultaneous solutions of a quadratic equation and a pair of linear equations over a Galois field. - Rev. Math. Pures Appl. 8 (1963), 297—303.

[3] —»— The number of planes contained in the complement of a quadric in an affine Galois space. - J. Tennessee Acad. Sci. 38 (1963), 133—134.

[4] DICKSON, L. E.: Linear groups with an exposition of the Galois field theory. Dover (1958).

Printed October 1965