ON SYSTEMS OF LINEAR AND QUADRATIC EQUATIONS IN FINITE FIELDS

BY

AIMO TIEÄVÄINEN

HELSINKI 1965
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1966.382
Communicated 8 October 1965 by P. J. Myrberg and K. Inkeri.
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

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

(1)

where $\alpha_1, \ldots, \alpha_s$ are non-zero, $\alpha, \beta_1, \ldots, \beta_t$ arbitrary elements of $K$, and the $\beta_j$’s are elements of $K$ such that the $t \times s$ matrix $(\beta_{ij})$ 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 $\sigma, \sigma_1, \ldots, \sigma_r$ be elements of $K$. Define the trace of $\sigma$ as

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

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

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

Then we have

$$e(\sum_{j=1}^{r} \sigma_j) = \prod_{j=1}^{r} e(\sigma_j).$$

(2)

Consider the system

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

(3)
where the \( f_i \)'s are polynomials with coefficients in \( K \) and the \( \delta_i \)'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

\[
q^{-u} \sum_{\mathbf{c}} e \left( - \sum_{i=1}^{u} \gamma_i \delta_i \right) \sum_{\mathbf{e}} \sum_{i=1}^{u} e \left( \sum_{i=1}^{u} \gamma_i f_i (\xi_1, \ldots, \xi_s) \right).
\]

Here and hereafter, in the sums of type \( \sum_{\mathbf{c}} \) the summation is over all the vectors \( \mathbf{c} = (\gamma_1, \ldots, \gamma_u) \) with the \( \gamma_i \)'s in \( K \). Moreover, in the sums of type \( \sum_{\mathbf{e}} \) 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

\[
q^{-u} \sum_{\mathbf{c}} e \left( - \sum_{i=1}^{u} \gamma_i \delta_i \right) \prod_{j=1}^{s} e \left( \sum_{i=1}^{u} \gamma_i f_j(\xi_j) \right).
\]

Let us denote

\[
S(\gamma, \delta) = \sum_{\mathbf{c}} e(\gamma x^2 + \delta \xi).
\]

It is well known (see, for example, [2]) that \( |S(\gamma, \delta)| = q^{u/2} \) 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

\[
N = q^{-t-1} \sum_{\mathbf{c}} e \left( - \kappa x - \sum_{i=1}^{t} \lambda_i \beta_i \right) \prod_{j=1}^{t+2} S(\kappa y_j, \sum_{i=1}^{t} \lambda_i \beta_j)
\]

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

\[
N = q^{-t-1}(\sum_{\kappa=0} + \sum_{\kappa=0}) = q^{-t-1}(U_1 + U_2).
\]

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

\[
\sum_{j=1}^{t+2} \beta_j \xi_j = \beta_i \quad (i = 1, \ldots, t).
\]

Because the matrix \( (\beta_{ij}) \) 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 \( \kappa y_j \neq 0 \), for every \( \mathbf{c} \). Therefore \( |S(\kappa y_j, \sum_{i=1}^{t} \lambda_i \beta_j)| = q^{u/2} \) and hence
\[ |U_2| \leq (q^{t+1} - q')q^{t+1} = q^{2t+2} - q^{2t+1}. \]

Consequently
\[ N \geq q^{-t-1}(U_1 - |U_2|) \geq q^t > 0. \]

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
\[
\begin{align*}
- \sum_{j=1}^{t} \xi_j^2 + \sum_{j=t+1}^{2t+1} \xi_j^2 &= \alpha \\
\xi_i + \xi_{t+i} &= 0 \quad (i = 1, \ldots, t),
\end{align*}
\]

where \( \alpha \) is a non-square of \( K \), is insolvable in \( K \).

University of Turku
Turku, Finland

References


Printed October 1965