THE NUMBER OF SOLUTIONS OF A SYSTEM OF A LINEAR EQUATION AND A QUADRATIC EQUATION IN GALOIS FIELDS OF CHARACTERISTIC 2

B. Zh. Kamaletdinov

Let $GF(q)$, $q = p^n$, be a Galois field of characteristic $p$. In the present note, we determine the number of solutions of a system of a linear equation and a nondegenerate quadratic equation over $F = GF(q)$, $q = 2^n$, where $n$ is a natural number. The proposed results, together with those obtained in [1, 2] for fields of characteristic $p > 2$, completely solve the problem of determination of the number of general solutions of a system of a linear equation and a quadratic equation in a field of arbitrary characteristic.

Let $e(x)$, $x \in F$, be a character of the additive group $F$ in the field of real numbers. Obviously, $e(x) = (-1)^{\text{tr} x}$, where

$$\text{tr} x = \sum_{i=0}^{n-1} x^i$$

is the trace of $x \in F$ in $GF(2)$. As we know [3, p. 191],

$$\sum_{x \in F} e(ax) = q \delta(a), \quad a \in F,$$

(1)

where $\delta(a)$ is the delta function on $F$ defined as

$$\delta(a) = \begin{cases} 1, & a = 0, \\ 0, & a \neq 0. \end{cases}$$

(2)

We also know (see, e.g., [4, p. 59]) that an arbitrary nondegenerate form

$$f(y_0, y_1, \ldots, y_{m-1}) = \sum_{i=0}^{m-1} \sum_{j=0}^{l-1} a_{ij} y_i y_j, \quad a_{ij} \in F,$$

can be reduced to one of the following two canonical forms $f_k(x_0, x_1, \ldots, x_{m-1})$:

$$f_k(x_0, x_1, \ldots, x_{m-1}) = \begin{cases} \beta (x_0^2 + x_1^2) + \sum_{i=0}^{l-1} x_i x_{i+1}, & m = 2l, \quad l \geq 1, \\ x_0^2 + \sum_{i=1}^{l} x_{2i-1} x_{2i}, & m = 2l + 1, \quad l \geq 1, \end{cases}$$

where $\beta$ is equal to zero or to one of the values of $\beta'$ for which the quadratic form $\beta'x_0^2 + \beta'x_1^2 + x_0x_1$ is irreducible in $F$. This means that an arbitrary system of a linear equation and a quadratic equation can be expressed as

$$\begin{cases} \sum_{i=0}^{m-1} \gamma_i x_i = a, \\ \beta (x_0^2 + x_1^2) + \sum_{i=0}^{l-1} x_i x_{i+1} = b \end{cases}$$

(3)

or as
where $s > i$ and $\gamma, \alpha, \beta$, and all $\gamma_i$ belong to $\mathcal{F}$, and at least one $\gamma_i$ is not equal to zero.

The following theorems contain the main results of this note.

**Theorem 1.** The number of solutions of the system (3) in the field $\mathcal{F}$ is given by the following formula:

$$N_1(a, b) = \begin{cases} q^{2i-1}, & \text{if } a \neq 0, \xi = 0, \\ q^{2i-1}, & \text{if } a = 0, \xi \neq 0, \\ q^{2i-1} + q^{i-1}(q\delta(b) - 1)(-1)^{tr \xi}, & \text{if } a = 0, \xi = 0, \\ q^{2i-1} + q^{i-1}(-1)^{tr \xi} \delta \gamma_1 \xi + tr \alpha, & \text{if } a \neq 0, \xi \neq 0, \end{cases}$$

where $\xi = (\gamma_0 + \gamma_1)^2 + \sum_{i=0}^{2i} \gamma_i \gamma_{2i+1}$.

**Theorem 2.** The number of solutions of the system (4) in the field $\mathcal{F}$ is given by the following formula:

$$N_2(a, b) = \begin{cases} q^{2i-1}, & \text{if } \gamma_0 = 0, \\ q^{2i-1} - q^{i-1}(q\delta(\gamma_0 \sqrt{\delta} - a) - 1)(-1)^{tr \gamma_0} \sum_{i=0}^{2i} \gamma_i \gamma_{2i+1}, & \text{if } \gamma_0 \neq 0. \end{cases}$$

**Proof of Theorem 1.** Using (1), we can write

$$q^2N_1(a, b) = \sum_{\lambda} \sum_{\gamma_i} \sum_{x_i, x_0, \ldots, x_{2i-1}} e(\lambda (\sum_{i=0}^{2i-1} \gamma_i x_i - a)) e(\mu (\beta x_0^2 + \beta x_i^2 + \sum_{i=0}^{2i-1} x_0 x_{2i+1} - b)).$$

We collect the terms corresponding to $\mu = 0$ on the right-hand side in the sum $\Sigma_1$ and the remaining terms in the sum $\Sigma_2$. By virtue of (1),

$$\Sigma_1 = q^{2i} \sum_{\lambda} e(-\lambda a) \prod_{i=0}^{2i-1} \delta(\lambda \gamma_i) = q^{2i},$$

since not all $\gamma_i = 0$.

To compute the sum $\Sigma_2$, we write it in the form

$$\Sigma_2 = \sum_{\mu} \sum_{\lambda} \sum_{x_i, x_0, \ldots, x_{2i-1}} e(\lambda (\sum_{i=0}^{2i-1} \gamma_i x_i - a)) e(\mu (\beta x_0^2 + \sum_{i=0}^{2i-1} x_0 x_{2i+1} - b)) \sum_{\lambda} e(\lambda \gamma_0 x_0 + \mu \beta x_0^2 + \mu x_0 x_1).$$

Since

$$tr x^2 = tr x \quad \text{for all } x \in \mathcal{F},$$

it follows by virtue of the additive property of the trace and the existence of square roots of all elements of a field of characteristic 2 that

$$e(\eta x^2 + \xi y) = e((V \eta + \xi) y).$$

On the basis of (8) and (1), after summation with respect to $x_0$, we have

$$\Sigma_2 = q \sum_{\mu} \sum_{\lambda} e(\lambda a + \mu b) \sum_{x_i, x_0, \ldots, x_{2i-1}} e(\lambda \sum_{i=0}^{2i-1} \gamma_i x_i) e(\mu (\beta x_0^2 + \sum_{i=0}^{2i-1} x_0 x_{2i+1})) \delta(x_1 - \lambda \mu^{-1} \gamma_0 - \sqrt{\beta x_1}).$$

By (8), $e(\mu \beta x_1^2) = e(\sqrt{\mu} x_1)$. Moreover,

$$\sum_{i=0}^{2i-1} \gamma_i x_i = \sum_{i=1}^{i-1} (\gamma_i x_i + \gamma_{2i+1} x_{2i+1}).$$

Therefore, summing with respect to $x_1$, we get

$$\Sigma_3 = q \sum_{\mu} \sum_{\lambda} e(\lambda a + \mu b) e(\lambda \mu^{-1} \gamma_0 +$$