PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2018, **52**(3), p. 180–190

I n f o r m a t i c s

ON A LINEARIZED COVERINGS OF A CUBIC HOMOGENEOUS EQUATION OVER A FINITE FIELD. UPPER BOUNDS

V. P. GABRIELYAN *

Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia

We obtain upper bounds of the complexity of linearized coverings for some special solutions of the equation
$x_1x_2x_3+x_2x_3x_4+\cdots+x_{3n}x_1x_2+x_1x_3x_5+x_4x_6x_8+\cdots+x_{3n-2}x_{3n}x_2=b$
over an arbitrary finite field.

MSC2010: Primary 97H60; Secondary 14N20, 51E21.

***Keywords*:** linear algebra, finite field, coset of linear subspace, linearized covering.

Introduction. Throughout this paper F_q stands for a finite field with q elements [1] (q-power of a prime number), and F_q^n stands for an n-dimensional linear space over $F_q : F_q^n \equiv \{\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)|\alpha_i \in F_q,\ i=1,2,\ldots,n\}$. If L is a linear subspace in F_q^n and $\alpha \in F_q^n$, then the set $\alpha+L=\{\alpha+x|x\in L\}$ is a *coset* (or translate) of the subspace L and $\dim(\alpha+L)$ coincides with $\dim L$. An equivalent definition: a subset $H \subseteq F_q^n$ is a coset, if whenever $h_1,h_2,\ldots,h_m$ are in H, so is any affine combination of them, i.e. $\sum\limits_{i=1}^{m}\lambda_i h_i \in H$ for any $\lambda_1,\lambda_2,\ldots,\lambda_m$ in F_q such that $\sum\limits_{i=1}^{m}\lambda_i=1$. It can be readily verified that any m-dimensional coset in F_q^n can be represented as a set of solutions of a certain system of linear equations over F_q of rank $n-m$ and vice versa.

D e f i n i t i o n . Let M be a subset in F_q^n and $H_1,H_2,\ldots,H_m \subseteq M$ be cosets of linear subspaces in F_q^n. If $M=\bigcup\limits_{i=1}^{m}H_i$, then we say that $\{H_1,H_2,\ldots,H_m\}$ is a linearized covering of M of complexity (or length) m. The linearized covering of M with minimal length is the *shortest* linearized covering of M.

The problem of the shortest (minimal) linearized covering of the set of solutions of a polynomial equation over a finite field was first investigated in [2, 3] for a simple field F_2, and the theory of linearized disjunctive normal forms was introduced. Some metric characteristics of the linearized coverings of subsets of a finite

* E-mail: var.gabrielyan@ysu.am

field were investigated in [4, 5]. The problem of a linearized covering of symmetric subsets of a finite field was solved in [6], and for the sets of solutions of quadratic and some higher-degree equations over a finite field was solved in [7–15].

Main Theorem. For given $b \in F_q$ and $n \geqslant 1$ consider an equation

$$x_1x_2x_3 + x_2x_3x_4 + \cdots + x_{3n}x_1x_2 + x_1x_3x_5 + x_4x_6x_8 + \cdots + x_{3n-2}x_{3n}x_2 = b \qquad (1)$$

over F_q. We denote by M the set of solutions of (1). It is clear that $M \subseteq F_q^{3n}$. We rewrite Eq. (1) in the following form:

$$(x_1 + x_4)(x_2 + x_5)x_3 + (x_4 + x_7)(x_5 + x_8)x_6 + \cdots + (x_{3n-2} + x_1)(x_{3n-1} + x_2)x_{3n} = b. \qquad (2)$$

If $n \equiv 0(\mathrm{mod}\,2)$ or $q \equiv 0(\mathrm{mod}\,2)$, then

$$x_{3n-2} + x_1 = \sum_{i=1}^{n-1}(-1)^{i-1}(x_{3i-2} + x_{3i+1}) \quad \text{and} \quad x_{3n-1} + x_2 = \sum_{i=1}^{n-1}(-1)^{i-1}(x_{3i-1} + x_{3i+2}),$$

and Eq. (2) can be rewritten in the form

$$\begin{gathered}(x_1 + x_4)(x_2 + x_5)x_3 + (x_4 + x_7)(x_5 + x_8)x_6 + \cdots \\ \cdots + (x_{3n-5} + x_{3n-2})(x_{3n-4} + x_{3n-1})x_{3(n-1)} + \\ + \left[\sum_{i=1}^{n-1}(-1)^{i-1}(x_{3i-2} + x_{3i+1})\right]\left[\sum_{i=1}^{n-1}(-1)^{i-1}(x_{3i-1} + x_{3i+2})\right]x_{3n} = b.\end{gathered} \qquad (3)$$

For any vector $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_{3n}) \in F_{q^{3n}}$ when $n \equiv 1(\mathrm{mod}\,2)$ and $q \equiv 1(\mathrm{mod}\,2)$, we construct a new vector

$$\tilde{\boldsymbol{\alpha}} = ((\alpha_1 + \alpha_4)(\alpha_2 + \alpha_5), (\alpha_4 + \alpha_7)(\alpha_5 + \alpha_8), \ldots, (\alpha_{3n-2} + \alpha_1)(\alpha_{3n-1} + \alpha_2)) \in F_q^n,$$

and when $n \equiv 0(\mathrm{mod}\,2)$ or $q \equiv 0(\mathrm{mod}\,2)$, we construct a vector $\tilde{\boldsymbol{\alpha}} = ((\alpha_1 + \alpha_4)(\alpha_2 + \alpha_5), (\alpha_4 + \alpha_7)(\alpha_5 + \alpha_8), \ldots, (\alpha_{3n-5} + \alpha_{3n-2})(\alpha_{3n-4} + \alpha_{3n-1})) \in F_q^{n-1}$. Further everywhere $z(\boldsymbol{\gamma})$ denotes the number of zero coordinates of the vector $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_m) \in F_{q^m}$. Moreover, for any $s \in \{0, 1, \ldots, n\}$ we have the set

$$M_s \equiv \{\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_{3n}) \in M \,|\, z(\tilde{\boldsymbol{\alpha}}) = s\}.$$

It should be noted that for $n \equiv 0(\mathrm{mod}\,2)$ or $q \equiv 0(\mathrm{mod}\,2)$ the set M_n does not exist. It is clear that $M_s \cap M_t = \emptyset \Longleftrightarrow s \neq t$ and

$$M = \bigcup_s M_s.$$

We denote by $E_q(n,s)$ the minimal complexity of the linearized covering of the set M_s, and by $E_q(n)$ the complexity of the shortest covering of M by cosets that are entirely contained in one of the sets M_s, $s = 0, 1, \ldots, n$.

Our goal is to evaluate the values of $E_q(n,s)$ and $E_q(n)$.

Theorem 1. When $n \equiv 1(\mathrm{mod}\,2)$ and $q \equiv 1(\mathrm{mod}\,2)$, then

$$E_q(n,s) \leqslant \begin{cases} C_n^s(q-1)^{2(n-s)}2^s, & \text{if} \quad s < n, \\ 2^n, & \text{if} \quad s = n. \end{cases}$$

$$E_q(n,s) \geqslant \begin{cases} C_n^s (q-1)^{2(n-s)} \Big(2-\dfrac{1}{q}\Big)^s, & \text{if } \ s<n \ \text{ and } \ b\neq 0,\\ \dfrac{1}{q} C_n^s (q-1)^{2(n-s)} \Big(2-\dfrac{1}{q}\Big)^s, & \text{if } \ s<n \ \text{ and } \ b=0,\\ \Big(2-\dfrac{1}{q}\Big)^s, & \text{if } \ s=n \ \text{ and } \ b=0. \end{cases}$$

$$E_q(n) \leqslant \begin{cases} \big[(q-1)^2+2\big]^n - 2^n, & \text{if } \ b\neq 0,\\ \big[(q-1)^2+2\big]^n, & \text{if } \ b=0. \end{cases}$$

$$E_q(n) \geqslant \begin{cases} \Big[(q-1)^2+\Big(2-\dfrac{1}{q}\Big)\Big]^n - \Big(2-\dfrac{1}{q}\Big)^n, & \text{if } \ b\neq 0,\\ \dfrac{1}{q}\Big[(q-1)^2+\Big(2-\dfrac{1}{q}\Big)\Big]^n + \dfrac{q-1}{q}\Big(2-\dfrac{1}{q}\Big)^n, & \text{if } \ b=0. \end{cases}$$

Theorem 2. When $n \equiv 0 (\mathrm{mod}\, 2)$ or $q \equiv 0 (\mathrm{mod}\, 2)$, then

$$E_q(n,s) \leqslant \begin{cases} (q-1)^{2(n-1)}, & \text{if } \ s=0,\\ C_{n-1}^s (2^s-2)(q-1)^{2(n-s)} q^{-1} + o(q^{2(n-s)-1}), & \text{if } \ 0<s<n-1,\\ (q-1)^2(2^s-2), & \text{if } \ s=n-1 \ \text{ and } \ b\neq 0,\\ (q^2-2q+3)(2^s-2)+2, & \text{if } \ s=n-1 \ \text{ and } \ b=0; \end{cases}$$

$$E_q(n) \leqslant (q-1)^{2(n-1)} + o(q^{2(n-1)}).$$

Proof of Theorem 1. Let $n \equiv 1 (\mathrm{mod}\, 2)$ and $q \equiv 1 (\mathrm{mod}\, 2)$. Then the nondegenerate linear transformation

$$\begin{cases} y_1 = x_1 + x_4,\\ y_2 = x_4 + x_7,\\ \quad \vdots\\ y_n = x_{3n-2} + x_1,\\ z_1 = x_2 + x_5,\\ z_2 = x_5 + x_8,\\ \quad \vdots\\ z_n = x_{3n-1} + x_2,\\ t_i = x_{3i}, \quad i = \overline{1,n}, \end{cases}$$

converts Eq. (2) into equation

$$y_1 z_1 t_1 + y_2 z_2 t_2 + \dots + y_n z_n t_n = b.$$

It is obvious that the last equation is a particular case of equation

$$x_1 x_2 \cdots x_k + x_{k+1} x_{k+2} \cdots x_{2k} + \dots + x_{k(n-1)+1} x_{k(n-1)+2} \cdots x_{kn} = b \tag{4}$$

when $k=3$. The Eq. (4) is considered in [9] and

- N stands for the set of all solutions of Eq. (4);
- N_s stands the set of all solutions of Eq. (4), for which exactly s, $0 \leqslant s \leqslant n$, of n products $x_{k(i-1)+1} x_{k(i-1)+2} \cdots x_{k(i-1)+(k-1)}$ $(i = 1,2,\dots,n)$ are equal to zero;
- $L_q^k(n,s)$ denotes the complexity of the shortest linearized covering of the set N_s;

• $L_q^k(n)$ denotes the complexity of the covering of the set N by cosets, all vectors of which are entirely contained in one set N_s, $0 \leqslant s \leqslant n$, the following estimates are obtained:

$$L_q^k(n,s) \leqslant \begin{cases} C_n^s(q-1)^{(k-1)(n-s)}(k-1)^s, & \text{if } s<n, \\ (k-1)^n, & \text{if } s=n; \end{cases}$$

$$L_q^k(n,s) \geqslant \begin{cases} C_n^s(q-1)^{(k-1)(n-s)}\left(\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right)^s, & \text{if } s<n \text{ and } b\neq 0, \\ \dfrac{1}{q}C_n^s(q-1)^{(k-1)(n-s)}\left(\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right)^s, & \text{if } s<n \text{ and } b=0, \\ \left(\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right)^s, & \text{if } s=n \text{ and } b=0; \end{cases}$$

$$L_q^k(n) \leqslant \begin{cases} \left[(q-1)^{k-1}+(k-1)\right]^n-(k-1)^n, & \text{if } b\neq 0, \\ \left[(q-1)^{k-1}+(k-1)\right]^n, & \text{if } b=0; \end{cases}$$

$$L_q^k(n) \geqslant \begin{cases} \left[(q-1)^{k-1}+\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right]^n-\left(\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right)^n, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } b\neq 0, \\ \dfrac{1}{q}\left[(q-1)^{k-1}+\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right]^n+\dfrac{q-1}{q}\left(\dfrac{q^{k-1}-(q-1)^{k-1}}{q^{k-2}}\right)^n, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } b=0. \end{cases}$$

From the above, it is clear that for $n\equiv 1(\operatorname{mod}2)$ and $q\equiv 1(\operatorname{mod}2)$ and $k=3$ we have the following identities:

$$M\equiv N, \quad M_s\equiv N_s, \quad E_q(n,s)\equiv L_q^3(n,s), \quad E_q(n)\equiv L_q^3(n)$$

and, consequently, the estimates of Theorem 1. Note that the problem of the minimal linearized covering for $y_1z_1t_1+y_2z_2t_2+\cdots+y_nz_nt_n=b$ was solved in [8].

Theorem 1 is completely proved.

On the Number of Solutions of Certain Equations and Systems of Equations over a Finite Field.

Lemma 1.

(i) The number of solutions of the equation $x_1+x_2+\cdots+x_k=0$ over the multiplicative group F_q^* of the finite field F_q is equal to

$$\frac{(q-1)\left[(q-1)^{k-1}+(-1)^k\right]}{q}.$$

(ii) Over the multiplicative group F_q^* the inequality $x_1+x_2+\cdots+x_k\neq 0$ has exactly $\dfrac{(q-1)\left[(q-1)^k+(-1)^{k+1}\right]}{q}$ solutions.

Proof. We denote by s_k the number of solutions of the equation $x_1+x_2+\cdots+x_k=0$ in the group F_q^*. It is clear that the equation $x_1=0$ has no solutions in F_q^* and, therefore, $s_1=0$. Consider the general equation $x_1+x_2+\cdots+x_k=0$

for $k>1$. The variables of the latter can not take zero values, therefore, assigning the values $\alpha_i \in F_q^*$ to all variables x_i $(i=1,2,\ldots,k-1)$, we must require that $\alpha_1+\alpha_2+\ldots+\alpha_{k-1}\neq 0$, and the number of such different vectors $(\alpha_1,\alpha_2,\ldots,\alpha_{k-1})$ coincides with s_k and is equal to $(q-1)^{k-1}-s_{k-1}$. Thus $s_1=0$ and $s_k=(q-1)^{k-1}-s_{k-1}$ for $k>1$. Then

$$s_k=(q-1)^{k-1}-(q-1)^{k-2}+(q-1)^{k-3}-\cdots-(-1)^k(q-1)=$$
$$=\sum_{i=1}^{k-1}(-1)^{i-1}(q-1)^{k-i}=\frac{(q-1)\left[(q-1)^{k-1}+(-1)^k\right]}{q}.$$

Having the value s_k for any positive integer k, we can find the number of solutions of the inequality $x_1+x_2+\cdots+x_k\neq 0$ in the group F_q^*. It is obvious that it is equal to

$$(q-1)^k-s_k=\frac{(q-1)\left[(q-1)^k+(-1)^{k+1}\right]}{q}.$$

□

L e m m a 2. The number of solutions of systems

$$\begin{cases} x_iy_i=0, \qquad i=1,2,\ldots,k,\\ (x_1+x_2+\cdots+x_k)(y_1+y_2+\cdots+y_k)=0 \end{cases} \tag{5}$$

and

$$\begin{cases} x_iy_i=0, \qquad i=1,2,\ldots,k,\\ (x_1+x_2+\cdots+x_k)(y_1+y_2+\cdots+y_k)\neq 0 \end{cases} \tag{6}$$

over F_q are equal to

$$\left[(2q-1)^{k+1}+2(q-1)^{k+2}+(-1)^{k+1}(q-1)^2\right]\cdot q^{-2},$$
$$(q-1)^2\cdot\left[(2q-1)^k-2(q-1)^k+(-1)^k\right]\cdot q^{-2}.$$

P r o o f . We consider system (5). If $x_i=\alpha_i\in F_q^*$ for $i=1,2,\ldots,k$, then $y_1=y_2=\cdots=y_k=0$ and the vector $\Big(\alpha_1,\alpha_2,\ldots,\alpha_k,\underbrace{0,0,\ldots,0}_{k}\Big)$ is a solution of (5), this gives us $(q-1)^k$ solutions. Further, for a fixed number s $(1\leqslant s\leqslant k)$ suppose $x_1=x_2=\cdots=x_s=0$ and $x_i=\alpha_i\in F_q^*$ for $i=s+1,\ldots,k$. Then we have $y_{s+1}=y_{s+2}=\cdots=y_k=0$ and the last equation of system (5) will have the following form:

$$\left(\sum_{i=s+1}^{k}\alpha_i\right)\cdot(y_1+y_2+\cdots+y_s)=0. \tag{7}$$

If $\sum\limits_{i=s+1}^{k}\alpha_i=0$, then the Eq. (7) has q^s solutions, otherwise it has q^{s-1} solutions. The number of different $(\alpha_{s+1},\alpha_{s+2},\ldots,\alpha_k)$, for which $\sum\limits_{i=s+1}^{k}\alpha_i=0$, is equal to $(q-1)\left[(q-1)^{k-s-1}+(-1)^{k-s}\right]q^{-1}$ (Lemma 1). And the number of vectors satisfying the condition $\sum\limits_{i=s+1}^{k}\alpha_i\neq 0$ is equal to $(q-1)\left[(q-1)^{k-s}+(-1)^{k-s+1}\right]q^{-1}$.

Consequently, the total number of solutions of Eq. (7) is equal to

$$\frac{(q-1)\left[(q-1)^{k-s-1}+(-1)^{k-s}\right]}{q}\cdot q^{s}+\frac{(q-1)\left[(q-1)^{k-s}+(-1)^{k-s+1}\right]}{q}\cdot q^{s-1}=$$
$$=(2q-1)(q-1)^{k-s}q^{s-2}+(q-1)^{2}(-1)^{k-s}q^{s-2}.$$

After combining all possible cases, we find that the number of solutions of system (5) is equal to

$$T_k\equiv(q-1)^k+\sum_{i=1}^{k}C_k^i\left[(2q-1)(q-1)^{k-i}q^{i-2}+(q-1)^2(-1)^{k-i}q^{i-2}\right]=$$
$$=\left[(2q-1)^{k+1}+2(q-1)^{k+2}+(-1)^{k+1}(q-1)^2\right]\cdot q^{-2}.$$

Note that in F_q^2 the number of solutions of the equation $xy=0$ is equal to $(2q-1)$. Therefore, the system $\{x_iy_i=0, i=1,2,\ldots,k$, has $(2q-1)^k$ solutions in F_q^{2k}. Then the number of solutions of system (6) is equal to

$$(2q-1)^k-T_k=\frac{(q-1)^2\cdot\left[(2q-1)^k-2(q-1)^k+(-1)^k\right]}{q^2}.$$

□

Proof of Theorem 1.

Canonical Covering. Let $n\equiv 0(\mathrm{mod}\,2)$ or $q\equiv 0(\mathrm{mod}\,2)$. For the vectors $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\ldots,\alpha_{n-1})$, $\boldsymbol{\beta}=(\beta_1,\beta_2,\ldots,\beta_{n-1})\in F_q^{n-1}$ the product $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}$ is defined by the equality $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=(\alpha_1\beta_1,\alpha_2\beta_2,\ldots,\alpha_{n-1}\beta_{n-1})$. It is easy to verify that for a fixed vector $\boldsymbol{\gamma}\in F_q^{n-1}$ the number of ordered pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ such that $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_q^{n-1}$ and $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=\boldsymbol{\gamma}$ is equal to $(2q-1)^{z(\boldsymbol{\gamma})}(q-1)^{n-1-z(\boldsymbol{\gamma})}$. Hence, if $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_q^{n-1}$ satisfy the equatin $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=\boldsymbol{\gamma}$ and $\left(\sum_{i=1}^{n-1}(-1)^{i-1}\alpha_i\right)\left(\sum_{i=1}^{n-1}(-1)^{i-1}\beta_i\right)=\omega$, where $\boldsymbol{\gamma}\in F_q^{n-1}$ and $\omega\in F_q$, then we say that the vector pair $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generates a vector $(\boldsymbol{\gamma},\omega)\in F_q^n$, and this relation will be written by $(\boldsymbol{\alpha},\boldsymbol{\beta})\to(\boldsymbol{\gamma},\omega)$.

Now, for Eq. (3) we construct a system of cosets covering the set M_s. Cosets are defined using systems of linear equations over the field F_q. The set M_s, where $0\leqslant s\leqslant n-1$, is covered by the sets of the solutions of the following systems of linear equations:

$$\begin{cases} x_{3i-2}+x_{3i+1}=\alpha_i, & i=1,2,\ldots,n-1,\\ x_{3i-1}+x_{3i+2}=\beta_i, & i=1,2,\ldots,n-1,\\ \gamma_1x_3+\cdots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b, \end{cases} \tag{8}$$

where the vector pair $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generates a vector $(\gamma_1,\gamma_2,\ldots,\gamma_{n-1},\omega)\neq(0,0,\ldots,0,0)\in F_q^n$ and $z(\boldsymbol{\alpha\beta})=z(\boldsymbol{\gamma})=s$.

If $s=n-1$ and $b=0$ in Eq. (3), then we add sets of solutions of the following systems to the solution sets of systems (8):

$$\begin{cases} x_{3i-2}+x_{3i+1}=\alpha_i, & i=1,2,\ldots,n-1,\\ x_{3i-1}+x_{3i+2}=\beta_i, & i=1,2,\ldots,n-1, \end{cases} \tag{9}$$

where the vector pair $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generates a vector $(0,0,\dots,0,0)\in F_q^n$.

It is obvious that for different vector pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ the sets of solutions of the above constructed systems of equations lie in M_s, are pairwise disjoint and the union of all these sets coincides with M_s and hence it is a disjoint covering of this set.

The ranks of systems (8) and (9) are equal to $2(n-1)+1$ and $2(n-1)$ respectively. Therefore, the number of solutions of these systems is equal to q^{n+1} and q^{n+2} respectively. The number of vectors $\boldsymbol{\gamma}\in F_q^{n-1}$ with $z(\boldsymbol{\gamma})=s$, where $0\leqslant s\leqslant n-1$, is equal to $C_{n-1}^s(q-1)^{n-1-s}$. For a fixed $\boldsymbol{\gamma}$ with $z(\boldsymbol{\gamma})=s$ there exist exactly $(2q-1)^s(q-1)^{n-1-s}$ vector pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ such that $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=\boldsymbol{\gamma}$. Therefore,

$$|M_s|=C_{n-1}^s(q-1)^{2(n-1-s)}(2q-1)^sq^{n+1},\quad \text{if } 0\leqslant s<n-1.$$

By Lemma 2 we obtain that exactly

$$(q-1)^2\cdot\left[(2q-1)^{n-1}-2(q-1)^{n-1}+(-1)^{n-1}\right]q^{-2}$$

vector pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generate nonzero vectors $(0,\dots,0,\omega)\in F_q^n$, and exactly

$$\left[(2q-1)^n+2(q-1)^{n+1}+(-1)^n(q-1)^2\right]q^{-2}$$

vector pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ generate a zero vector $(0,0,\dots,0,0)\in F_q^n$. Therefore,

$$\begin{aligned}
&|M_{n-1}|=(q-1)^2\cdot\left[(2q-1)^{n-1}-2(q-1)^{n-1}+(-1)^{n-1}\right]q^{-2}q^{n+1}, && \text{if } b\neq 0,\\
&|M_{n-1}|=(q-1)^2\cdot\left[(2q-1)^{n-1}-2(q-1)^{n-1}+(-1)^{n-1}\right]q^{-2}q^{n+1}+\\
&\qquad +\left[(2q-1)^n+2(q-1)^{n+1}+(-1)^n(q-1)^2\right]q^{-2}q^{n+2}, && \text{if } b=0.
\end{aligned}$$

We also see that

$$\begin{aligned}
|M|&=\left[\sum_{s=0}^{n-2}C_{n-1}^s(q-1)^{2(n-1-s)}(2q-1)^s\right]q^{n+1}+\\
&\quad+(q-1)^2\cdot\left[(2q-1)^{n-1}-2(q-1)^{n-1}+(-1)^{n-1}\right]q^{-2}q^{n+1}=\\
&=\left[q^{2n}-(2q-1)^n-2(q-1)^{n+1}+(-1)^{n-1}(q-1)^2\right]q^{n-1}, && \text{if } b\neq 0,\\
|M|&=\left[q^{2n}-(2q-1)^n-2(q-1)^{n+1}+(-1)^{n-1}(q-1)^2\right]q^{n-1}+\\
&\quad+\left[(2q-1)^n+2(q-1)^{n+1}+(-1)^n(q-1)^2\right]q^{-2}q^{n+2}=\\
&=\left[q^{2n}+(q-1)(2q-1)^n+2(q-1)^{n+2}+(-1)^n(q-1)^3\right]q^{n-1}, && \text{if } b=0.
\end{aligned}$$

Now we construct the enlargement of the covering described above. Each $(\boldsymbol{\gamma},\omega)\in F_q^n$ is associated with a set of linear systems. Fix the vector $(\boldsymbol{\gamma},\omega)=$ $=(\gamma_1,\gamma_2,\dots,\gamma_{n-1},\omega)$, where $z(\boldsymbol{\gamma})=s$. If $s=0$, then the corresponding systems are formed in the same way as a system of the (8) type.

Suppose that $0<s\leqslant n-1$. Without loss of generality, we can assume that $\gamma_1=\gamma_2=\dots=\gamma_s=0$ and $\gamma_i\neq 0,\ i=s+1,\dots,n-1$. For each vector pair $(\boldsymbol{\alpha},\boldsymbol{\beta})=(\alpha_{s+1},\dots,\alpha_{n-1},\beta_{s+1},\dots,\beta_{n-1})$ such that $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=\boldsymbol{\gamma}=(\gamma_{s+1},\dots,\gamma_{n-1})$, the set of systems of equations is constructed as follows. We write $\alpha\equiv\sum\limits_{i=s+1}^{n-1}(-1)^{i-1}\alpha_i$ and $\beta\equiv\sum\limits_{i=s+1}^{n-1}(-1)^{i-1}\beta_i$.

If $\omega \neq 0$, then for each vector $(\mu_1, \ldots, \mu_s) \in F_2^s$, where $(\mu_1, \ldots, \mu_s) \neq (0, \ldots, 0)$ and $(\mu_1, \ldots, \mu_s) \neq (1, \ldots, 1)$, and an arbitrary non-zero element $\sigma \in F_q$, we construct the following system of equations:

$$\begin{cases} x_{3i-2} + x_{3i+1} = 0 \Longleftrightarrow \mu_i = 0, \\ x_{3i-1} + x_{3i+2} = 0 \Longleftrightarrow \mu_i = 1, \\ x_{3i-2} + x_{3i+1} = \alpha_i, \quad i = s+1, \ldots, n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, \quad i = s+1, \ldots, n-1, \\ \sum\limits_{i=1}^{s} (-1)^{i-1} \mu_i (x_{3i-2} + x_{3i+1}) + \alpha = \sigma, \\ \sum\limits_{i=1}^{s} (-1)^{i-1} (\mu_i \oplus 1)(x_{3i-1} + x_{3i+2}) + \beta = \sigma^{-1}\omega, \\ \gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b, \end{cases}$$

where the symbol $\oplus$ denotes the addition of modulo 2, and the notation $x_{3i-2} + x_{3i+1} = 0$ is equivalent to $\mu_i = 0$ that means the equation $x_{3i-2} + x_{3i+1} = 0$ is included in the system if and only if $\mu_i = 0$.

When $(\mu_1, \ldots, \mu_s) = (0, \ldots, 0)$ we form the system

$$\begin{cases} x_{3i-2} + x_{3i+1} = 0, \quad i = 1, 2, \ldots, s, \\ x_{3i-2} + x_{3i+1} = \alpha_i, \quad i = s+1, \ldots, n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, \quad i = s+1, \ldots, n-1, \\ \sum\limits_{i=1}^{s} (-1)^{i-1} (x_{3i-1} + x_{3i+2}) + \beta = \alpha^{-1}\omega, \\ \gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b, \end{cases}$$

if and only if $\alpha \neq 0$ and when $(\mu_1, \ldots, \mu_s) = (1, \ldots, 1)$, then the system

$$\begin{cases} x_{3i-1} + x_{3i+2} = 0, \quad i = 1, 2, \ldots, s, \\ x_{3i-2} + x_{3i+1} = \alpha_i, \quad i = s+1, \ldots, n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, \quad i = s+1, \ldots, n-1, \\ \sum\limits_{i=1}^{s} (-1)^{i-1} (x_{3i-2} + x_{3i+1}) + \alpha = \beta^{-1}\omega, \\ \gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b \end{cases}$$

is constructed if and only if $\beta \neq 0$.

Next, consider the construction of new systems for $\omega = 0$. In this case, also for each binary vector $(\mu_1, \ldots, \mu_s)$, where $(\mu_1, \ldots, \mu_s) \neq (0, \ldots, 0)$ and $(\mu_1, \ldots, \mu_s) \neq (1, \ldots, 1)$, we construct a system

$$\begin{cases} x_{3i-2} + x_{3i+1} = 0 \Longleftrightarrow \mu_i = 0, \\ x_{3i-1} + x_{3i+2} = 0 \Longleftrightarrow \mu_i = 1, \\ x_{3i-2} + x_{3i+1} = \alpha_i, \quad i = s+1, \ldots, n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, \quad i = s+1, \ldots, n-1, \\ \sum\limits_{i=1}^{s} (-1)^{i-1} \mu_i (x_{3i-2} + x_{3i+1}) + \alpha = 0, \\ \gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b \end{cases}$$

and the system

$$\begin{cases} x_{3i-2}+x_{3i+1}=0 \Longleftrightarrow \mu_i=0, \\ x_{3i-1}+x_{3i+2}=0 \Longleftrightarrow \mu_i=1, \\ x_{3i-2}+x_{3i+1}=\alpha_i, \quad i=s+1,\dots,n-1, \\ x_{3i-1}+x_{3i+2}=\beta_i, \quad i=s+1,\dots,n-1, \\ \sum\limits_{i=1}^{s}(-1)^{i-1}(\mu_i\oplus 1)(x_{3i-1}+x_{3i+2})+\beta=0, \\ \gamma_1 x_3+\dots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b. \end{cases}$$

When $(\mu_1,\dots,\mu_s)=(0,\dots,0)$, we compose the system

$$\begin{cases} x_{3i-2}+x_{3i+1}=0, \quad i=1,2,\dots,s, \\ x_{3i-2}+x_{3i+1}=\alpha_i, \quad i=s+1,\dots,n-1, \\ x_{3i-1}+x_{3i+2}=\beta_i, \quad i=s+1,\dots,n-1, \\ \gamma_1 x_3+\dots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b, \end{cases}$$

if $\alpha=0$, and in the case $\alpha\neq 0$ we compile the system

$$\begin{cases} x_{3i-2}+x_{3i+1}=0, \quad i=1,2,\dots,s, \\ x_{3i-2}+x_{3i+1}=\alpha_i, \quad i=s+1,\dots,n-1, \\ x_{3i-1}+x_{3i+2}=\beta_i, \quad i=s+1,\dots,n-1, \\ \sum\limits_{i=1}^{s}(-1)^{i-1}(x_{3i-1}+x_{3i+2})+\beta=0, \\ \gamma_1 x_3+\dots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b. \end{cases}$$

For $(\mu_1,\dots,\mu_s)=(1,\dots,1)$, we add a system

$$\begin{cases} x_{3i-1}+x_{3i+2}=0, \quad i=1,2,\dots,s, \\ x_{3i-2}+x_{3i+1}=\alpha_i, \quad i=s+1,\dots,n-1, \\ x_{3i-1}+x_{3i+2}=\beta_i, \quad i=s+1,\dots,n-1, \\ \gamma_1 x_3+\dots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b \end{cases}$$

to existing systems if $\beta=0$, otherwise we add the system

$$\begin{cases} x_{3i-1}+x_{3i+2}=0, \quad i=1,2,\dots,s, \\ x_{3i-2}+x_{3i+1}=\alpha_i, \quad i=s+1,\dots,n-1, \\ x_{3i-1}+x_{3i+2}=\beta_i, \quad i=s+1,\dots,n-1, \\ \sum\limits_{i=1}^{s}(-1)^{i-1}(x_{3i-2}+x_{3i+1})+\alpha=0, \\ \gamma_1 x_3+\dots+\gamma_{n-1}x_{3(n-1)}+\omega x_{3n}=b. \end{cases}$$

The covering of the set M_s constructed above is called *canonical*.

Now let us estimate the complexity of the canonical covering. The number of different vectors $(\boldsymbol{\alpha},\boldsymbol{\beta})=(\alpha_{s+1},\dots,\alpha_{n-1},\beta_{s+1},\dots,\beta_{n-1})\in F_q^{2(n-1-s)}$, where $\alpha_i,\beta_i\in F_q\setminus\{0\}$ for all $i=s+1,\dots,n-1$, for which (according to Lemma 1)

a) $\alpha\equiv\sum\limits_{i=s+1}^{n-1}(-1)^{i-1}\alpha_i=0$ and $\beta\equiv\sum\limits_{i=s+1}^{n-1}(-1)^{i-1}\beta_i=0$, is equal to

$$(q-1)^2\left[(q-1)^{n-s-2}+(-1)^{n-s-1}\right]^2 q^{-2};$$

b) $\alpha=0$ and $\beta\neq 0$, is equal to

$$(q-1)^2\left[(q-1)^{n-s-2}+(-1)^{n-s-1}\right]\left[(q-1)^{n-s-1}+(-1)^{n-s}\right]q^{-2};$$

$c)$ $\alpha \neq 0$ and $\beta = 0$, is equal to
$(q-1)^2\left[(q-1)^{n-s-1}+(-1)^{n-s}\right]\left[(q-1)^{n-s-2}+(-1)^{n-s-1}\right]q^{-2}$;

$d)$ $\alpha \neq 0$ and $\beta \neq 0$, is equal to

$$(q-1)^2\left[(q-1)^{n-s-1}+(-1)^{n-s}\right]^2 q^{-2}.$$

Then, for a fixed $0 \neq \omega \in F_q$ and $(\boldsymbol{\alpha},\boldsymbol{\beta}) = (\alpha_{s+1},\ldots,\alpha_{n-1},\beta_{s+1},\ldots,\beta_{n-1}) \in \in F_q^{2(n-1-s)}$ the number of new systems, when

$a)$ $\alpha = 0$ and $\beta = 0$, is equal to $(q-1)(2^s-2)$;
$b)$ $\alpha = 0$ and $\beta \neq 0$, is equal to $(q-1)(2^s-2)+1$;
$c)$ $\alpha \neq 0$ and $\beta = 0$, is equal to $(q-1)(2^s-2)+1$;
$d)$ $\alpha \neq 0$ and $\beta \neq 0$, is equal to $(q-1)(2^s-2)+2$;

and for $\omega = 0$ the number of new systems is equal to $2(2^s-2)+2$ (for all α and β).

Denote by D_s the length of the canonical covering. It is clear that $D_0 = (q-1)^{2(n-1)}$. If $0 < s < n-1$, then

$$D_s = C_{n-1}^s \frac{(q-1)^2\left[(q-1)^{n-s-2}+(-1)^{n-s-1}\right]^2}{q^2}\left[(q-1)^2(2^s-2)+2(2^s-2)+2\right]+$$
$$+2C_{n-1}^s \frac{(q-1)^2\left[(q-1)^{n-s-2}+(-1)^{n-s-1}\right]\left[(q-1)^{n-s-1}+(-1)^{n-s}\right]}{q^2}\times$$
$$\times\left[(q-1)^2(2^s-2)+(q-1)+2(2^s-2)+2\right]+$$
$$+C_{n-1}^s \frac{(q-1)^2\left[(q-1)^{n-s-1}+(-1)^{n-s}\right]^2}{q^2}\left[(q-1)^2(2^s-2)+2(q-1)+2(2^s-2)+2\right].$$

Simplifying the last expression, we get

$$D_s = C_{n-1}^s(2^s-2)(q-1)^{2(n-s)}q^{-1}+C_{n-1}^s(2^s-1)(q-1)^{2(n-s)-2}+$$
$$+2C_{n-1}^s(-1)^{n-s}(q-1)^{n-s-1}q^{-1} = C_{n-1}^s(2^s-2)(q-1)^{2(n-s)}q^{-1}+o(q^{2(n-s)-1}).$$

Finally, $D_s = C_{n-1}^s(2^s-2)(q-1)^{2(n-s)}q^{-1}+o(q^{2(n-s)-1})$ when $0 < s < n-1$, and if $s = n-1$, then

$$D_{n-1} = \begin{cases} (q-1)^2(2^s-2), & \text{if } b \neq 0, \\ (q^2-2q+3)(2^s-2)+2, & \text{if } b = 0. \end{cases}$$

Finally we have

$$D_s = \begin{cases} (q-1)^{2(n-1)}, & \text{if } s = 0, \\ C_{n-1}^s(2^s-2)(q-1)^{2(n-s)}q^{-1}+o\left(q^{2(n-s)-1}\right), & \text{if } 0 < s < n-1, \\ (q-1)^2(2^s-2), & \text{if } s = n-1 \text{ and } b \neq 0, \\ (q^2-2q+3)(2^s-2)+2, & \text{if } s = n-1 \text{ and } b = 0. \end{cases}$$

Obviously, the quantity D_s is the upper bound for $E_q(n,s)$. The number of cosets contained entirely in one of the sets M_s, $s = 0,1,\ldots,n-1$, is equal to

$$(q-1)^{2(n-1)}+\sum_{s=1}^{n-1} D_s = (q-1)^{2(n-1)}+o\left(q^{2(n-1)}\right),$$

which is an upper bound for $E_q(n)$.

Theorem 2 is completely proved.

Received 23.10.2018

R E F E R E N C E S

1. **Lidl R., Niederreiter H.** Finite Fields. Encyclopedia of Mathematics and Its Applications. V. 20: Section Algebra, 1983.
2. **Alexanyan A.A.** Realization of Boolean Functions by Disjunctions of Products of Linear Forms. // Soviet Math. Dokl., 1989, v. 39, № 1, p. 131–135 (in Russian).
3. **Alexanyan A.A.** Disjunctive Normal Forms over Linear Functions. Theory and Applications. Yer.: YSU Press, 1990 (in Russian).
4. **Gabrielyan V.** On Metric Characteristics Associated with Coverings of Subsets of Finite Fields by Cosets of Linear Subspaces. Preprint 04-0603. Yer.: Institute for Informatics and Automation Problems NAS of Armenia, 2004 (in Russian).
5. **Nurijanyan H.K.** On the Length of the Shortest Linearized Covering for "Almost All" Subsets in Finite Field. // Reports of NAS RA, 2010, v. 110, № 1, p. 30–34.
6. **Alexanian A., Gabrielyan V.** Coverings of Simmetric Subsets in Finite Fields with Cosets of Linear Subspaces. // Algebra, Geometry and Their Applications, YSU, 2004, v. 3–4, p. 110–124.
7. **Alexanyan A.A., Serobyan R.K.** Coverings Connected with Quadratic Equations over a Finite Field. // Dokl. Acad. Nauk Armenii, 1992, v. 93, № 1, p. 6–10 (in Russian).
8. **Aleksanyan A., Papikian M.** On Coset Coverings of Solutions of Homogeneous Cubic Equations over Finite Fields. // The Electronic Journal of Combinatorics, 2001, v. 8, № 22, p. 1–9.
9. **Gabrielyan V.** On the Complexity of Covering a System of Cosets of a Single Equation over a Finite Field. Preprint 04-0602. Yer.: Institute for Informatics and Automation Problems NAS of Armenia, 2004 (in Russian).
10. **Gabrielyan V.P.** Linearized Coverings of One Type Equations of Higher Degree over Finite Fields. // Reports of NAS RA, 2006, v. 106, № 2, p. 101–107 (in Russian).
11. **Gabrielyan V.P.** Cubical Diagonal Equation over Finite Fields of Characteristic 2. // Reports of NAS RA, 2010, v. 110, № 3, p. 220–227 (in Russian).
12. **Alexanian A.A., Minasyan A.V.** An Upper Bound for the Complexity of Coset Covering of Subsets in a Finite Field. // Reports of NAS RA, 2017, v. 117, № 4, p. 287–291.
13. **Minasyan A.V.** On the Minimal Coset Covering of the Set of Singular and of the Set of Nonsingular Matrices. // Proceedings of the YSU. Physical and Mathematical Sciences, 2018, v. 52, № 1, p. 8–11.
14. **Minasyan A.V.** On the Minimal Coset Covering for a Special Subset in Direct Product of Two Finite Fields. // Proceedings of the YSU. Physical and Mathematical Sciences, 2017, v. 51, № 3, p. 236–240.
15. **Gabrielyan V.P.** Linearized Coverings for Sets of Special Solutions of One Cubic Equation over a Finite Field. // Reports of NAS RA, 2018, v. 118, № 2, p. 115–118.