PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2019, **53**(2), p. 119–126

I n f o r m a t i c s

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

V. P. GABRIELYAN *

Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia

We obtain lower bounds for the complexity of linearized coverings for some sets of 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 is a power of a prime number), and F_q^n 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. $\sum_{i=1}^{m} \lambda_i h_i \in H$ for any $\lambda_1, \lambda_2, \ldots, \lambda_m$ in F_q such that $\sum_{i=1}^{m} \lambda_i = 1$. 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.

Let H be an m-dimensional coset in F_q^n. We identify H with a $(q^m \times n)$-dimensional matrix, whose rows coincide with vectors from H. Obviously, any affine combination of rows of H is also a row of this matrix, and any permutation of rows of the matrix H does not change the properties of the coset. The matrix H has the following *basic properties:*

(i) Any column in H either consists of q^m copies of the same element of F_q (such columns are referred to as *constant*) or each element of F_q occurs in the

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

column exactly q^{m-1} times. Indeed, H is the set of solutions of a certain system of linear equations over F_q of rank $n-m$ over unknowns $x_1, x_2, \ldots, x_n$. If the column that corresponds to x_i is a constant one, we add an equation $x_i = \beta$, $\beta \in F_q$, to the original linear system. Obviously, the new system is of rank $n-m+1$ and has exactly q^{m-1} solutions, which coincide with those rows in H with i-th coordinate equal to β. The matrix formed by these rows will be denoted by H_β. Each H_β is a $(m-1)$-dimensional coset. Applying an appropriate permutation of rows in H, which does not change the coset, one can rearrange the rows in such an order that all rows in each H_β follow each other in H. All matrices H_β for different $\beta \in F_q$ are translates of the same linear $(m-1)$-dimensional subspace in F_q^n, and thus, translates of each other.

(ii) Let $n = n_1 + n_2$ and the first n_1 columns of the matrix H form a submatrix H^1, and the remaining n_2 columns form a submatrix H^2. We denote this by $H = H^1|H^2$. Rows in each H^i form a coset in $F_q^{n_i}$ and $\dim H^i \leq \dim H$. It is clear that $H \subseteq H^1 \times H^2$ and $\dim H \leq \dim H^1 + \dim H^2$.

Definition . *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 $M = \bigcup_{i=1}^{m} H_i$, 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 minimal covering of a set of solutions of a polynomial equation over a finite field by cosets of linear subspaces was first investigated in [2, 3] for the simple field F_2, in which the theory of disjunctive normal forms (DNF) over linear functions (linearized DNF) was constructed. This is a natural generalization of the theory of ordinary DNF, adequate to the problem of solving systems of nonlinear Boolean equations. In the new mathematical model a transition was made from the representation of Boolean functions by covering their carriers with n-dimensional unit cube intervals to coverings using cosets of linear subspaces of the finite field F_{2^n}, which, as a linear space, is isomorphic to the set of n-dimensional unit cube. The new model naturally summarizes the model of the ordinary DNF and in the framework of the new theory, significant progress was obtained in the minimization problem of Boolean functions, which is fundamentally unattainable in the framework of the theory of ordinary DNF. For example, for Boolean functions that can be represented as quadratic polynomials over F_2, the members of the minimal covering were written out in an explicit analytic form [4].

It was realized that the representation of functions by covering with cosets of linear subspaces can be transferred to the case of an arbitrary finite field. Such a representation is very useful in solving systems of equations over a finite field, as well as a number of problems. Generally speaking, coverings with cosets are a very convenient and efficient way to enumerate solutions of both single equations and systems of equations in finite fields.

Some metric characteristics of the linearized coverings of subsets of a finite field were investigated in [5, 6]. The problem of a linearized covering of symmetric

subsets of a finite field was solved in [7], and other results on this topic can be found in [4, 8–14].

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

$$\begin{gathered} x_1x_2x_3 + x_2x_3x_4 + \cdots + x_{3n}x_1x_2 + x_1x_3x_5 + x_4x_6x_8 + \cdots + \\ + x_{3n-2}x_{3n}x_2 = b \end{gathered} \tag{1}$$

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:

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

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

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

and

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

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

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

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

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

and when $n \equiv 0 (\mathrm{mod}\, 2)$ or $q \equiv 0 (\mathrm{mod}\, 2)$, we construct a vector

$$\begin{gathered} \tilde{\alpha} = ((\alpha_1 + \alpha_4)(\alpha_2 + \alpha_5), (\alpha_4 + \alpha_7)(\alpha_5 + \alpha_8), \ldots, \\ (\alpha_{3n-5} + \alpha_{3n-2})(\alpha_{3n-4} + \alpha_{3n-1})) \in F_q^{n-1}. \end{gathered}$$

Further, everywhere $z(\gamma)$ denotes the number of zero coordinates of the vector $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m) \in F_{q^m}$. Moreover, for any $s \in \{0, 1, \ldots, n\}$ we have the set

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

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 $E_q(n)$ we denote 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 $E_q(n)$. The upper bounds and the case of $n \equiv 1 (\mathrm{mod} 2)$ and $q \equiv 1 (\mathrm{mod}\, 2)$ were obtained in [15].

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

$$E_q(n,s) \geq \begin{cases} C_{n-1}^s (q-1)^{2(n-s-1)} \left(2-\frac{1}{q}\right)^s, \quad if\ \ 0 \leq s < n-1\ \ and\ \ b \neq 0, \\ \frac{1}{q} C_{n-1}^s (q-1)^{2(n-s-1)} \left(2-\frac{1}{q}\right)^s, \ if\ \ 0 \leq s < n-1\ \ and\ \ b = 0, \\ \left(1-\frac{1}{q}\right)^2 \left[\left(2-\frac{1}{q}\right)^s - 2\left(1-\frac{1}{q}\right)^s + \frac{(-1)^s}{q^s}\right], \\ \qquad\qquad if\ s = n-1\ \ and\ \ b \neq 0, \\ \frac{1}{q}\left(3-\frac{3}{q}+\frac{1}{q^2}\right)^s \left(2-\frac{1}{q}\right)^2 + 2\left(1-\frac{1}{q}\right)^{s+1} - \\ \left(1-\frac{1}{q}\right)^3 \left(-\frac{1}{q}\right)^s, \qquad\qquad if\ s = n-1\ \ and\ \ b = 0. \end{cases}$$

$$E_q(n) \geq \begin{cases} (q-1)^{2(n-1)} + o(q^{2(n-1)}), \ \ if\ \ b \neq 0, \\ \frac{1}{q}(q-1)^{2(n-1)} + o(q^{2(n-1)-1}), \ \ if\ \ b = 0. \end{cases}$$

Proof. Let $n \equiv 0(\mathrm{mod}\, 2)$ or $q \equiv 0(\mathrm{mod}\, 2)$.

For vectors $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, $\beta = (\beta_1, \beta_2, \ldots, \beta_{n-1}) \in F_q^{n-1}$ the product $\alpha \cdot \beta$ is defined by the equality $\alpha \cdot \beta = (\alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_{n-1}\beta_{n-1})$. It is easy to verify that for a fixed vector $\gamma \in F_q^{n-1}$ the number of ordered pairs (α, β) such that $\alpha, \beta \in F_q^{n-1}$ and $\alpha \cdot \beta = \gamma$ is equal to $(2q-1)^{z(\gamma)}(q-1)^{n-1-z(\gamma)}$. Hence, if the vectors $\alpha, \beta \in F_q^{n-1}$ satisfy the equalities $\alpha \cdot \beta = \gamma$ 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 $\gamma \in F_q^{n-1}$ and $\omega \in F_q$, then we say that the vector pair (α, β) generates a vector $(\gamma, \omega) \in F_q^n$, and this fact is fixed by writing $(\alpha, \beta) \to (\gamma, \omega)$.

It was constructed in [15] a system of cosets covering the set M_s for the Eq. (3). Cosets are represented by systems of linear equations over the field F_q. The set M_s, where $0 \leq s \leq n-1$, is covered by the sets of the solutions of the following systems of linear equations:

$$\begin{cases} x_{3i-2} + x_{3i+1} = \alpha_i, & i = 1,2,\ldots,n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, & i = 1,2,\ldots,n-1, \\ \gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b, \end{cases} \tag{4}$$

where the vector pair (α, β) generates a vector

$$(\gamma_1, \gamma_2, \ldots, \gamma_{n-1}, \omega) \neq (0,0,\ldots,0,0) \in F_q^n \ \text{ and } \ z(\alpha\beta) = z(\gamma) = s.$$

If $s = n-1$ and $b = 0$ in Eq. (3), then the solution sets of systems (4) are supplemented by the solution sets of the following systems:

$$\begin{cases} x_{3i-2} + x_{3i+1} = \alpha_i, & i = 1,2,\ldots,n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, & i = 1,2,\ldots,n-1, \end{cases} \tag{5}$$

where the vector pair (α, β) generates a vector $(0,0,\ldots,0,0) \in F_q^n$.

It is obvious that for different vector pairs (α,β) 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 so it is a disjoint covering of this set.

In [15] it was also counted the values of the $|M_s|$ and $|M|$:

$$
\begin{aligned}
&|M_s| = C_{n-1}^{s}(q-1)^{2(n-1-s)}(2q-1)^s q^{n+1}, && \text{if } \ 0 \le s < n-1,\\
&|M_{n-1}| = (q-1)^2\cdot[(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}]q^{-2}q^{n+1}, && \text{if } b \neq 0,\\
&|M_{n-1}| = (q-1)^2\cdot[(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}]q^{-2}q^{n+1} + \\
&\qquad\qquad + [(2q-1)^n + 2(q-1)^{n+1} + (-1)^n(q-1)^2]q^{-2}q^{n+2}, && \text{if } \ b = 0,\\
&|M| = [q^{2n} - (2q-1)^n - 2(q-1)^{n+1} + (-1)^{n-1}(q-1)^2]q^{n-1}, && \text{if } b \neq 0,\\
&|M| = [q^{2n} + (q-1)(2q-1)^n + 2(q-1)^{n+2} + (-1)^n(q-1)^3]q^{n-1}, && \text{if } b = 0.
\end{aligned}
$$

Now we suppose that for $i = 1,2,\ldots,k$ the vectors $\alpha^i = (\alpha_1^i, \alpha_2^i, \ldots, \alpha_n^i)$ belong to F_q^n and their product is defined by the equality

$$\alpha^1\alpha^2\cdots\alpha^k = (\alpha_1^1\alpha_1^2\cdots\alpha_1^k, \alpha_2^1\alpha_2^2\cdots\alpha_2^k, \ldots, \alpha_n^1\alpha_n^2\cdots\alpha_n^k).$$

Then the following result was proved in [9]:

Lemma 1. *Suppose that the coset H consists of vectors of the form $(\alpha^1,\alpha^2,\ldots,\alpha^k) \in F_q^{kn}$ such that $\alpha^i = (\alpha_1^i,\alpha_2^i,\ldots,\alpha_n^i) \in F_q^n$ for all $i = 1,2,\ldots,k$, and $z(\alpha^1\alpha^2\cdots\alpha^k) = s$, $0 \le s \le n$. Then* $\dim H \le (k-1)s$.

Now suppose that $N(\alpha,\beta)$ denotes the cosets corresponding to the system (4) or (5) for the vector pair $(\alpha,\beta) = (\alpha_1,\alpha_2,\ldots,\alpha_{n-1},\beta_1,\beta_2,\ldots,\beta_{n-1}) \in F_q^{2(n-1)}$.

Lemma 2. *Let G be a coset in $F_q^{3n} \cap M_s$. Then*

$$\dim G \le \begin{cases} s+n+1, & \text{if } \ b \neq 0,\\ s+n+2, & \text{if } \ b = 0, \end{cases}$$

where b is the right-hand side of Eq. (3).

Proof. A coset G can be represented as

$$G = \bigcup_{z(\alpha\beta)=s} (G \cap N(\alpha,\beta)),$$

because $G \subseteq M_s$.

Let $H = \{(\alpha,\beta) | G \cap N(\alpha,\beta) \neq \emptyset\}$ and pairs $(\alpha^1,\beta^1),(\alpha^2,\beta^2),\ldots,(\alpha^m,\beta^m)$ belong to the set H. For elements $\lambda_1,\lambda_2,\ldots,\lambda_m \in F_q$ such that $\sum_{j=1}^{m}\lambda_j = 1$ consider the sum

$$\lambda_1\varphi_1 + \lambda_2\varphi_2 + \cdots + \lambda_m\varphi_m \equiv \varphi,$$

where $\varphi_j \in G \cap N(\alpha^j,\beta^j)$, $j = 1,2,\ldots,m$. The vectors $\varphi_1,\varphi_2,\ldots,\varphi_m$ belong to G and G is a coset, therefore $\varphi \in G$. It is clear that for all $i = 1,2,\ldots,n-1$, the sum of the $(3i-2)$-th and $(3i+1)$-th coordinates of the vectors $\varphi_1,\varphi_2,\ldots,\varphi_m$ respectively is $\alpha_i^1,\alpha_i^2,\ldots,\alpha_i^m$ (system (4) or (5)), and the sum of the $(3i-1)$-th and $(3i+2)$-th coordinates of the same vectors are respectively $\beta_i^1,\beta_i^2,\ldots,\beta_i^m$. Consequently, the sum of the $(3i-2)$-th and $(3i+1)$-th coordinates of the vector φ is equal to $\lambda_1\alpha_i^1 + \lambda_2\alpha_i^2 + \cdots + \lambda_m\alpha_i^m$, and the sum of the $(3i-1)$-th and $(3i+2)$-th coordinate of the same vector is equal to $\lambda_1\beta_i^1 + \lambda_2\beta_i^2 + \cdots + \lambda_m\beta_i^m$. Hence,

$$\varphi \in N(\lambda_1\alpha^1 + \lambda_2\alpha^2 + \cdots + \lambda_m\alpha^m, \lambda_1\beta^1 + \lambda_2\beta^2 + \cdots + \lambda_m\beta^m).$$

Therefore,

$$\varphi \in G \cap N(\lambda_1\alpha^1 + \lambda_2\alpha^2 + \cdots + \lambda_m\alpha^m, \lambda_1\beta^1 + \lambda_2\beta^2 + \cdots + \lambda_m\beta^m)$$

and

$$(\lambda_1\alpha^1 + \lambda_2\alpha^2 + \cdots + \lambda_m\ \alpha^m, \lambda_1\beta^1 + \lambda_2\beta^2 + \cdots + \lambda_m\beta^m) \in H.$$

That is H is a coset and satisfies the conditions of Lemma 1 for $k = 2$. Finally we have that $\dim H \leq s$, i. e. $|H| \leq q^s$.

Next, consider a matrix of the coset G. Columns of the matrix G with numbers of multiples of 3 form coset G_1, and the remaining columns coset G_2. For each pair $(\alpha, \beta) \in H$ there are rows in the matrix G_2 that satisfy a linear system of equations

$$\begin{cases} x_{3i-2} + x_{3i+1} = \alpha_i, & i = 1, 2, \ldots, n-1, \\ x_{3i-1} + x_{3i+2} = \beta_i, & i = 1, 2, \ldots, n-1, \end{cases} \tag{6}$$

and the corresponding rows in G_1 satisfy the equation

$$\gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b,$$

where $(\alpha, \beta) \to (\gamma, \omega)$. The number of solutions of the system (6) in F_q^{2n} is equal to $q^{2n-2(n-1)} = q^2$, and the number of systems (6) does not exceed $|H| \leq q^s$. Consequently, $|G_2| \leq q^s \cdot q^2 = q^{s+2}$ and $\dim G_2 \leq s + 2$. It is clear that $\dim G_1 \leq n$. Thus $\dim G \leq \dim G_1 + \dim G_2 \leq s + n + 2$.

When $b \neq 0$, the vector $(0, 0, \ldots, 0) \in F_q^n$ does not satisfy equations of the form $\gamma_1 x_3 + \cdots + \gamma_{n-1} x_{3(n-1)} + \omega x_{3n} = b$. Hence, for $b \neq 0$ we have $\dim G_1 \leq n - 1$ and $\dim G \leq \dim G_1 + \dim G_2 \leq n - 1 + s + 2 = s + n + 1$. □

Obviously, if G is a coset in M_s, then $L_q(n, s) \geq \dfrac{|M_s|}{q^{\max \dim G}}$, and therefore for $0 \leq s < n - 1$ we have the following:

$$E_q(n, s) \geq \frac{C_{n-1}^s (q-1)^{2(n-1-s)} (2q-1)^s q^{n+1}}{q^{s+n+1}} = C_{n-1}^s (q-1)^{2(n-1-s)} \left(2 - \frac{1}{q}\right)^s$$

if $b \neq 0$, and

$$E_q(n, s) \geq \frac{1}{q} C_{n-1}^s (q-1)^{2(n-1-s)} \left(2 - \frac{1}{q}\right)^s$$

if $b = 0$. And for $s = n - 1$ we have that

$$E_q(n, s) \geq \frac{(q-1)^2 \cdot [(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}] q^{-2} q^{n+1}}{q^{2n}} =$$

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

when $b \neq 0$, and

$$E_q(n, s) \geq \frac{(q-1)^2 \cdot [(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}] q^{-2} q^{n+1}}{q^{2n+1}} +$$

$$+ \frac{[(2q-1)^n + 2(q-1)^{n+1} + (-1)^n (q-1)^2] q^n}{q^{2n+1}} =$$

$$= \frac{1}{q}\left(3 - \frac{3}{q} + \frac{1}{q^2}\right)\left(2 - \frac{1}{q}\right)^{n-1} + 2\left(1 - \frac{1}{q}\right)^{n+2} - \left(1 - \frac{1}{q}\right)^3 \left(-\frac{1}{q}\right)^{n-1}$$

if $b = 0$.

It is also clear that the length of the covering of the set M of all solutions of equation (3) with cosets from the sets M_s, $s = 0, 1, \ldots, n-1$, satisfies the following inequalities:

$$E_q(n) \geq \sum_{s=0}^{n-2} \frac{C_{n-1}^s (q-1)^{2(n-1-s)} (2q-1)^s q^{n+1}}{q^{s+n+1}} + \\ + \frac{(q-1)^2 \cdot [(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}] q^{n-1}}{q^{2n}} = \\ = \left[(q-1)^2 + \left(2 - \frac{1}{q}\right) \right]^{n-1} - \frac{1}{q} \left(2 - \frac{1}{q}\right)^{n-1} - 2\left(1 - \frac{1}{q}\right)^{n+1} + \\ + \left(-\frac{1}{q}\right)^{n-1} \left(1 - \frac{1}{q}\right)^2 = (q-1)^{2(n-1)} + o\left(q^{2(n-1)}\right)$$

if $b \neq 0$, and

$$E_q(n) \geq \sum_{s=0}^{n-2} \frac{C_{n-1}^s (q-1)^{2(n-1-s)} (2q-1)^s q^{n+1}}{q^{s+n+2}} + \\ + \frac{(q-1)^2 \cdot [(2q-1)^{n-1} - 2(q-1)^{n-1} + (-1)^{n-1}] q^{n-1}}{q^{2n+1}} = \\ = \frac{1}{q}(q-1)^{2(n-1)} + o\left(q^{2(n-1)-1}\right)$$

if $b = 0$. □

Received 07.03.2019
Reviewed 21.05.2019
Accepted 10.06.2019

REFERENCES

1. Lidl R., Niederreiter H. Finite Fields. *Encyclopedia of Mathematics and Its Applications, Section: Algebra*, **20** (1987).
2. Alexanyan A.A. Realization of Boolean Functions by Disjunctions of Products of Linear Forms. *Soviet Math. Dokl.*, **39** : 1 (1989), 131–135 (in Russian).
3. Alexanyan A.A. *Disjunctive Normal Forms Over Linear Functions. Theory and Applications*. Yer., YSU Press (1990) (in Russian).
4. Alexanyan A.A., Serobyan R.K. Coverings Connected with Quadratic Equations over a Finite Field. *Dokl. Acad. Nauk Armenii*, **93** : 1 (1992), 6–10 (in Russian).
5. Gabrielyan V. On Metric Characteristics Associated with Coverings of Subsets of Finite Fields by Cosets of Linear Subspaces. *Institute for Informatics and Automation Problems NAS of Armenia*, Yer., Preprint 04-0603 (2004) (in Russian).
6. Nurijanyan H.K. On the Length of the Shortest Linearized Covering for "Almost All" Subsets in Finite Field. *Reports of NAS RA*, **10** : 1 (2010), 30–34.
7. Alexanian A., Gabrielyan V. Coverings of Simmetric Subsets in Finite Fields with Cosets of Linear Subspaces. *Algebra, Geometry & Their Applications. Seminar Proceedings*, Yer.,YSU, **3 – 4** (2004), 110–124.

8. Aleksanyan A., Papikian M. On Coset Coverings of Solutions of Homogeneous Cubic Equations over Finite Fields. *The Electronic Journal of Combinatorics*, **8** : R22 (2001), 1–9.
9. Gabrielyan V. On the Complexity of Covering a System of Cosets of a Single Equation Over a Finite Field. *Institute for Informatics and Automation Problems NAS of Armenia*, Yer., Preprint 04-0602 (2004) (in Russian).
10. Gabrielyan V.P. Linearized Coverings of One Type Equations of Higher Degree over Finite Fields. *Reports of NAS RA*, **106**:2 (2006), 101–107 (in Russian).
11. Gabrielyan V.P. Cubical Diagonal Equation over Finite Fields of Characteristic 2. *Reports of NAS RA*, **110**:3 (2010), 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*, **117**:4 (2017), 287–291.
13. Minasyan A.V. On the Minimal Coset Covering of the Sets of Singular and Nonsingular Matrices. *Proceedings of the YSU. Physical and Mathematical Sciences*, **52**:1 (2018), 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*, **51**:3 (2017), 236–240
15. Gabrielyan V.P. On a Linearized Coverings of a Cubic Homogeneous Equation Over a Finite Field. Upper Bounds. *Proceedings of the YSU. Physical and Mathematical Sciences*, **52**:3 (2018), 180–190.

Վ. Պ. ԳԱԲՐԻԵԼՅԱՆ

ՎԵՐՋԱՎՈՐ ԴԱՇՏՈՒՄ ՄԵԿ ԽՈՐԱՆԱՐԴԱՅԻՆ ՀԱՄԱՍԵՌ ՀԱՎԱՍԱՐՄԱՆ ԳԾԱՅՆԱՑՎԱԾ ԾԱԾԿՈՒՅԹՆԵՐԸ: ՍՏՈՐԻՆ ԳՆԱՀԱՏԱԿԱՆ

Հոդվածում ներքևից գնահատվում է գծայնացված ծածկույթների բարդությունը կամայական վերջավոր դաշտում մեկ խորանարդային համասեռ հավասարման հատուկ լուծումների որոշ բազմությունների համար: