ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 118 2018 № 2

APPLIED MATHEMATICS

УДК 512.62; 519.7

V. P. Gabrielyan

Linearized Coverings for Sets of Special Solutions of One Cubic Equation over a Finite Field

(Submitted by academician Yu. H. Shoukourian 26/II 2018)

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

1. **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 for a 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., $\sum_{i=1}^m h_j \lambda_i \in H$ 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.

Defination 1. 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* $M = \sum_{i=1}^m H_i$ *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 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 [7-12].

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

$$x_1x_2x_3 + x_2\,x_3x_4 + \ldots + x_{3n}x_1x_2 + x_1\,x_2\,x_5 + x_4x_6x_8 + \ldots + x_{3n-2}x_{3n}x_2 = b \qquad (1)$$

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

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

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

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

and equation (2) can be rewritten in the form

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

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

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

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

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

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

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

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 $M_s \cap M_t = \varnothing \Leftrightarrow s \neq t$ 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 $E_q(n)$.**

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

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

$$E_q(n,s)\ge\begin{cases} C_n^s(q-1)^{2(n-s)}\left(2-\frac{1}{q}\right)^s, \ if\ \ s<n\ and\ \ b\neq 0 \\ \frac{1}{q}C_n^s(q-1)^{2(n-s)}\left(2-\frac{1}{q}\right)^s, \ if\ \ s<n\ and\ \ b=0, \\ \left(2-\frac{1}{q}\right)^s, \qquad\qquad if\ s=n\ and\ b=0 \end{cases}$$

$$E_q(n)\le\begin{cases}\left[(q-1)^2+2\right]^n-2^n, if\ \ b\neq 0 \\ \left[(q-1)^2+2\right]^n, \qquad if\ \ b=0\end{cases}$$

$$E_q(n)\ge\begin{cases}\left[(q-1)^2+\left(2-\frac{1}{q}\right)\right]^n-\left(2-\frac{1}{q}\right)^n, \qquad if\ \ b\neq 0 \\ \frac{1}{q}\left[(q-1)^2+\left(2-\frac{1}{q}\right)\right]^n+\frac{q-1}{q}\left(2-\frac{1}{q}\right)^n, \qquad if\ \ b=0\end{cases}.$$

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

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

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

$$E_q(n)\le(q-1)^{2(n-1)}+o\left(q^{2(n-1)}\right),$$

$$E_q(n)\ge\begin{cases}(q-1)^{2(n-1)}+\mathrm{o}\left(q^{2(n-1)}\right), \qquad if\ \ b\neq 0 \\ \frac{1}{q}(q-1)^{2(n-1)}+\mathrm{o}\left(q^{2(n-1)-1}\right), \quad if\ \ b=0\end{cases}.$$

Yerevan State University
e-mail: var.gabrielyan@ysu.am

V. P. Gabrielyan

Linearized Coverings for Sets of Special Solutions of of One Cubic Equation over a Finite Field

The complexity of linearized covering is estimated for the set of special solutions of one cubic equation over an arbitrary finite field.

Վ. Պ. Գաբրիելյան

Վերջավոր դաշտի վրա մեկ խորանարդային հավասարման հատուկ լուծումների բազմությունների գծայնացված ծածկույթները

Գծայնացված ծածկույթների բարդությունը գնահատված է կամայական վերջավոր դաշտի վրա մեկ խորանարդային հավասարման հատուկ լուծումների բազմությունների համար:

В. П. Габриелян

Линеаризованные покрытия для множеств специальных решений одного кубического уравнения над конечным полем

Оценивается сложность линеаризованного покрытия для множеств специальных решений одного кубического уравнения над произвольным конечным полем.

References

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т. М. Мир. 1988. Т. 1, 430 с.; Т. 2. 390 с.
2. *Алексанян А. А.* – ДАН СССР. 1989. Т. 304. № 4.
3. *Алексанян А. А.* Дизъюнктивные нормальные формы над линейными функциями. Теория и приложения. Ереван. Изд. ЕГУ.1990.
4. *Габриелян В.* О метрических характеристиках, связанных с покрытиями подмножеств конечных полей смежными классами линейных подпространств. Препринт 04-0603. Ин-т проблем информатики и автоматизации НАН РА. Ереван. 2004.
5. *Nurijanyan H. K.* – RNAS RA. 2010. V. 110. № 1. P. 30-34
6. *Alexanian A., Gabrielyan V.* In: Algebra, Geometry & Their Applications. Seminar Proceedings. 2004. V. 3-4. Yerevan State University. P. 110-124.
7. *Алексанян А. А., Серобян Р. К.* – ДАН Армении. 1992. Т. 93. №1.
8. *Aleksanyan A., Papikian M.* – The Electronic Journal of Combinatorics. 2001. V. 8. R 22. P. 1-9.
9. *Габриелян В.* О сложности покрытия системой смежных классов одного уравнения над конечным полем. Препринт 04-0602. Ин-т проблем информатики и автоматизации НАН РА. Ереван. 2004.
10. *Габриелян В. П.* – ДНАН РА. 2006. Т.106. № 2. С. 101-107.
11. *Габриелян В. П.* – ДНАН РА. 2010. Т. 110. № 3. С. 220-227.
12. *Alexanian A. A., Minasyan A. V.* – RNAS RA. 2017. V. 117. № 4. P. 287-291.