On Coset Coverings of Solutions of Homogeneous Cubic Equations over Finite Fields

Ara Aleksanyan
Department of Informatics and Applied Mathematics
Yerevan State University, Yerevan 375049, Armenia.
alexara@sci.am

Mihran Papikian
Department of Mathematics
University of Michigan, Ann Arbor, MI 48109, U.S.A.
papikian@umich.edu

Submitted: April 21, 1999; Accepted: May 26, 2001.
MR Subject Classifications: Primary 11T30, Secondary 05B40

Abstract

Given a cubic equation $x_1y_1z_1 + x_2y_2z_2 + \cdots + x_ny_nz_n = b$ over a finite field, it is necessary to determine the minimal number of systems of linear equations over the same field such that the union of their solutions exactly coincides with the set of solutions of the initial equation. The problem is solved for arbitrary size of the field. A covering with almost minimum complexity is constructed.

1 Introduction

Throughout this paper F_q stands for a finite field with q elements, and F_q^n for an n-dimensional linear space over F_q. If L is a linear subspace in F_q^n, then the set $\bar{\alpha} + L \equiv \{\bar{\alpha} + \bar{x} \mid \bar{x} \in L\}$, $\bar{\alpha} \in F_q^n$ is a *coset* of the subspace L. An equivalent definition: a subset $N \subseteq F_q^n$ is a coset if whenever $\bar{x}^1, \bar{x}^2, ..., \bar{x}^m$ are in N, so is any affine combination of them, i.e., so is $\sum\limits_{i=1}^{m} \lambda_i \bar{x}^i$ for any $\lambda_1, ..., \lambda_m$ 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.

The purpose of this article is to estimate the minimum number of cosets of linear subspaces in F_q^{3n} one must choose in order to precisely cover the set of all solutions of the homogeneous cubic equation $x_1y_1z_1 + x_2y_2z_2 + \cdots + x_ny_nz_n = b$ over F_q.

The general covering problem was investigated by the first author in [1]-[3] in connection with linearized disjunctive normal forms of Boolean functions. A linearized disjunctive normal form (l.d.n.f.) of a Boolean function f is a representation of the form $f = f_1 \vee \cdots \vee f_p$, where each $f_j \in \prod L(n)$ is a product of linear functions; the latter term designates those functions which can be represented as linear polynomials over F_2. Since every literal x_i or $\overline{x}_i = x_i + 1$ is a linear function, it follows that every disjunctive normal form is an l.d.n.f. (in spite of this terminology, which may suggest the converse inclusion). The fact that the length (i.e., number of disjunctive terms) of an l.d.n.f. is invariant with respect to the affine group of transformations of the n-dimensional unit cube enables one to apply algebraic methods in the study of the set $\prod L(n)$ and of the l.d.n.f. representations. All major results of the theory of l.d.n.f. are summarized in [3].

Since in l.d.n.f. each linear conjunction is a product of linear polynomials over F_2, the problem of finding the shortest l.d.n.f. representation of a Boolean function can be reformulated as a problem of covering sets in F_2^n by the least possible number of cosets of linear subspaces. From this point of view one naturally can consider the same problem (coverings by cosets) in the case of a finite field of an arbitrary characteristic p. For quadratic equations this was done in [4]. The present work is a natural continuation of [4].

According to a well-known theorem [7], any quadratic form over F_q can be reduced by a nondegenerate linear transformation to the form $x_1x_2+x_3x_4+\cdots+x_{n-3}x_{n-2}+q(x_{n-1},x_n)$, where $q(x_{n-1},x_n)$ is possibly a degenerate quadratic. So one obtains general results on the coset coverings of quadratics just by investigating this form. Unfortunately, forms of higher degrees, in general, cannot be reduced to convenient representations, but one still can restrict the attention to homogeneous equations of a special form: $x_1x_2\ldots x_k + x_{k+1}x_{k+2}\ldots x_{2k} + \cdots + x_{k(n-1)}\ldots x_{kn}$. For cubics it is done in this paper.

In particular, if $\mathbf{sl}(q,n,3)$ is the minimum number of cosets required to cover precisely the set of solutions of $x_1y_1z_1 + x_2y_2z_2 + \cdots + x_ny_nz_n = b$ in F_q^{3n}, then we show that

$$\left(q^2-2q+3-\tfrac{1}{q}\right)^n - \left(2-\tfrac{1}{q}\right)^n - n \le \mathbf{sl}(q,n,3) \le \left(q^2-2q+3\right)^n - 2^n, \text{ when } b \neq 0,$$

$$\tfrac{1}{q}\left[\left(q^2-2q+3-\tfrac{1}{q}\right)^n + (q-1)\left(2-\tfrac{1}{q}\right)^n\right] - n - 1 \le \mathbf{sl}(q,n,3) \le \left(q^2-2q+3\right)^n, \; b=0. \tag{1}$$

Our upper bound is constructive and it provides a covering close to minimal. Comparing (1) with the estimates of $\mathbf{sl}(q,n,2)$ in [4]: $\mathbf{sl}(q,n,2) = q^n - 1$, when $b \neq 0$, and $q^{n-1} + 1 - \frac{1}{q} \le \mathbf{sl}(q,n,2) \le q^n$, when $b = 0$, one may cautiously conjecture that in general $\mathbf{sl}(q,n,k) = q^{n(k-1)} + o\left(q^{n(k-1)}\right)$, when $b \neq 0$, and $q^{n(k-1)-1} + o\left(q^{n(k-1)-1}\right) \le \mathbf{sl}(q,n,k) \le q^{n(k-1)} + o\left(q^{n(k-1)}\right)$, when $b = 0$.

Coverings by cosets were also considered by R. Jamison in the study of 1-intersection sets in affine spaces over finite fields. In [6] the minimum number of cosets of k-dimensional subspaces of a vector space V over a finite field F required to cover the nonzero points of V is established. Several generalizations of Jamison's results and applications to finite geometry have been obtained by A. Bruen in [5].

2 Upper bound: Canonical coverings

Let $\bar{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\bar{\beta} = (\beta_1, \beta_2, ..., \beta_n) \in F_q^n$. Define the product $\bar{\alpha} \cdot \bar{\beta}$ as

$$\bar{\alpha} \cdot \bar{\beta} = (\alpha_1 \cdot \beta_1, \alpha_2 \cdot \beta_2, \ldots, \alpha_n \cdot \beta_n).$$

Denote by $z(\bar{\alpha})$ the number of all coordinates of $\bar{\alpha}$ equal to zero. Observe that the number of all ordered vector pairs $\bar{\alpha}, \bar{\beta}$ such that $\bar{\alpha} \cdot \bar{\beta} = \bar{\gamma}$, for some particular $\bar{\gamma}$, is equal to $(2q-1)^{z(\bar{\gamma})} (q-1)^{n-z(\bar{\gamma})}$. Indeed, the equation $\alpha_i \cdot \beta_i = \gamma_i$ has $(q-1)$ solutions in F_q^2 if $\gamma_i \neq 0$ and $(2q-1)$ solutions if $\gamma_i = 0$.

The solutions of the equation

$$x_1 y_1 z_1 + x_2 y_2 z_2 + \cdots + x_n y_n z_n = b \tag{2}$$

can be covered by the cosets of solutions of the following linear systems

$$\left\{ \begin{array}{ll} x_i = \alpha_i \ , & i = 1, \ldots, n \\ y_i = \beta_i \ , & i = 1, \ldots, n \\ \gamma_1 z_1 + \gamma_2 z_2 + \cdots + \gamma_n z_n = b, & \text{where } \bar{\gamma} = \bar{\alpha} \cdot \bar{\beta} \neq \bar{0}. \end{array} \right. \tag{3}$$

When $b = 0$ we must also add the systems

$$\left\{ \begin{array}{ll} x_i = \alpha_i \ , & i = 1, \ldots, n \\ y_i = \beta_i \ , & i = 1, \ldots, n, \qquad \text{where } \bar{\alpha} \cdot \bar{\beta} = \bar{0}. \end{array} \right. \tag{4}$$

It is easy to see that the solutions of systems (3) (or (4)) for different $\bar{\alpha}$ and $\bar{\beta}$ do not intersect. Further we call a covering of solutions of (2) by the cosets corresponding to (3) and (4) a *disjoint* covering.

Each system (3) has q^{n-1} solutions, since its rank is $2n+1$ with the number of variables equal to $3n$, and similarly each system (4) has q^n solutions. For a fixed $\bar{\gamma}$ there are $(2q-1)^{z(\bar{\gamma})} (q-1)^{n-z(\bar{\gamma})}$ pairs $\bar{\alpha}, \bar{\beta}$ such that $\bar{\alpha} \cdot \bar{\beta} = \bar{\gamma}$. Moreover, in F_q^n the number of vectors $\bar{\gamma}$ in with $z(\bar{\gamma}) = k$ is equal to $\binom{n}{k}(q-1)^{(n-k)}$. Consequently, if N is the number of solutions of (2), then

$$N = \left(\sum_{i=0}^{n-1} (2q-1)^i (q-1)^{n-i} \binom{n}{i} (q-1)^{n-i} \right) q^{n-1} = \left(q^{2n} - (2q-1)^n \right) q^{n-1}, \text{ when } b \neq 0$$

and similarly

$$N = \left(q^{2n} - (2q-1)^n \right) q^{n-1} + (2q-1)^n q^n, \text{ when } b = 0.$$

Cosets corresponding to (3) and (4) can be unified into cosets having larger dimension in the following way. Consider (3) (for (4) the procedure is similar). Let $z(\gamma) = k$, say $\gamma_1 = \gamma_2 = \cdots = \gamma_k = 0$. Let us fix the coordinates $\alpha_{k+1}, \alpha_{k+2}, \ldots, \alpha_n$ and $\beta_{k+1}, \beta_{k+2}, \ldots, \beta_n$. For each vector $(\mu_1, \mu_2, \ldots, \mu_k)$ of the binary cube E_k we construct a system of linear equations which coincides with (3) by the equations $x_{k+1} = \alpha_{k+1}, \ldots, x_n = \alpha_n \quad ; \quad y_{k+1} =$

$\beta_{k+1}, \ldots, y_n = \beta_n$ and $\gamma_1 z_1 + \gamma_2 z_2 + \cdots + \gamma_n z_n = b$, but out of $x_1 = 0, \ldots, x_k = 0$ it contains only the equations $x_i = 0$ with an index i for which $\mu_i = 1$; similarly out of $y_1 = 0, \ldots, y_k = 0$ it contains only the equations $y_i = 0$ with an index i for which $\mu_i = 0$.

Further we refer to the covering of solutions of (2) by the cosets corresponding to these new constructed systems as *canonical.* The number of systems (3) for some $\bar{\gamma}$, and accordingly the number of disjoint cosets, was equal to $(2q-1)^{z(\bar{\gamma})}\,(q-1)^{n-z(\bar{\gamma})}$. After their unification into canonical cosets we have reduced the number of cosets down to $2^{z(\bar{\gamma})}\,(q-1)^{n-z((\bar{\gamma})}$.

Summing over all possible values of $z(\cdot)$ we obtain that the length of the canonical covering is equal to

$$\sum_{i=0}^{n-1} \binom{n}{i} (q-1)^{2(n-i)} \cdot 2^i = \left(q^2 - 2q + 3\right)^n - 2^n, \text{ when } b \neq 0$$

and

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^{2(n-i)} \cdot 2^i = \left(q^2 - 2q + 3\right)^n, \text{ when } b = 0.$$

This is the upper bound for $\mathbf{sl}(q, n, 3)$. Comparing with the lower bound for $\mathbf{sl}(q, n, 3)$ we see that the canonical covering is close to the minimal possible.

3 Lower bound for the length of covering

Let $N\left(\bar{\alpha}, \bar{\beta}\right)$ stand for a *disjoint* coset, i.e. one of the cosets in the disjoint covering. As it was shown in Section **2** the set N of all the solutions of (2) can be represented as

$$N = \bigcup_{\bar{\alpha}, \bar{\beta} \in F_q^n} N\left(\bar{\alpha}, \bar{\beta}\right) = \bigcup_{\bar{\gamma} \in F_q^n} \bigcup_{\bar{\alpha} \cdot \bar{\beta} = \bar{\gamma}} N\left(\bar{\alpha}, \bar{\beta}\right) = \bigcup_{\bar{\gamma} \in F_q^n} N\left(\bar{\gamma}\right), \qquad (5)$$

where $N(\bar{\gamma}) = \bigcup_{\bar{\alpha} \cdot \bar{\beta} = \bar{\gamma}} N\left(\bar{\alpha}, \bar{\beta}\right)$.

Obtaining a lower bound in (1) is equivalent to obtaining a bound on the dimension of an arbitrary coset in N. So suppose $M \subseteq N$, where M is a coset of a certain subspace H in F_q^{3n} and $\dim(M) = \dim(H) = m$. It is clear that M can be represented as $M = \cup \left(M \cap N\left(\bar{\alpha}, \bar{\beta}\right)\right) = \bigcup_{\bar{\gamma} \in F_q^n} \left(M \cap N\left(\bar{\gamma}\right)\right)$. We will consider in detail the set $T\left(\bar{\gamma}\right) \equiv M \cap N\left(\bar{\gamma}\right) = \bigcup_{\bar{\alpha} \cdot \bar{\beta} = \bar{\gamma}} \left(M \cap N\left(\bar{\alpha}, \bar{\beta}\right)\right)$, assuming it is nonempty.

Denote $\Gamma \equiv \{\bar{\gamma} \mid T\left(\bar{\gamma}\right) \neq \emptyset\} \equiv \left\{\bar{\gamma}^1, \bar{\gamma}^2, \ldots, \bar{\gamma}^k\right\}$. We will prove as separate lemmas the following statements, whose proofs are given in the next section:

i) each $T\left(\bar{\gamma}\right)$ is a coset, $\bar{\gamma} \in \Gamma$

ii) each $T\left(\bar{\gamma}\right)$ is embedded into some canonical coset

iii) all $T\left(\bar{\gamma}\right)$, $\bar{\gamma} \in \Gamma$, are translates of the same linear subspace of F_q^{3n}

Let $s = \min_{T(\bar{\gamma})\neq\emptyset} z(\bar{\gamma})$. Since $T(\bar{\gamma})$ can be covered by some canonical coset, let C be the linear subspace of solutions in F_q^{3n} of the system

$$\begin{cases} x_{i_1} = 0 \\ \dots \\ x_{i_k} = 0 \\ y_{j_1} = 0 \\ \dots \\ y_{j_l} = 0 \end{cases} \tag{6}$$

corresponding to the canonical system by which $T(\bar{\gamma})$ is covered, without the last equation in it. System (6) contains $2n - s$ equations. The coset $T(\bar{\gamma})$ is a shift of $H \cap C$, and such is any other $T(\bar{\gamma}') \neq \emptyset$ by (iii).

Let $\dim(H \cap C) = p$, $\dim(H) = m$. We define $S \equiv \{T(\bar{\gamma}^i)\}$. According to (iii) S is a coset in the factor-space $F_q^{3n}/(H \cap C)$. Clearly $\dim(S) = m - p$, and S is isomorphic to the coset $S_0 \equiv \left\{\bar{\gamma} \in F_q^n \quad | \quad T(\bar{\gamma}) \neq \emptyset\right\}$. Since each $T(\bar{\gamma}) \neq \emptyset$ is a shift of $H \cap C$, $H \cap C$ must satisfy the system

$$\begin{cases} Equations\ of\ (6) \\ \sum_{i=1}^n \bar{\gamma}_i z_i = 0 \qquad (\gamma_1, \gamma_2, \dots, \gamma_n) \in S_0 \end{cases} \tag{7}$$

So $p \leq 3n - rank((7)) = 3n - ((2n - s) + m - p + 1)$, when $b \neq 0$; observe that $\bar{\gamma} = \bar{0}$ is not in S_0 when $b \neq 0$. Similarly, $p \leq 3n - ((2n - s) + m - p)$, when $b = 0$. Finally, $\dim(M) = \dim(H) = m \leq n + s - 1$, when $b \neq 0$, and $m \leq n + s$, when $b = 0$.

Represent N as $\bigcup_{s=0}^n L_s$, where $L_s = \bigcup_{z(\bar{\alpha}\cdot\bar{\beta})=s} N(\bar{\alpha}, \bar{\beta})$. As we have seen the dimension of an arbitrary coset M in N is bounded by the minimal s such that $M \cap L_s \neq \emptyset$. The conditions of Lemma (4.4) will be satisfied if we treat a covering by cosets as a covering by a family of subsets. In this case $|L_s| = (2q-1)^s \cdot (q-1)^{n-s} \cdot q^{n-1} \cdot \binom{n}{s} \cdot (q-1)^{n-s}$, $|\pi_0| = q^{n-1}$ if $b \neq 0$ and $|\pi_0| = q^n$ if $b = 0$, along with $|\pi_{s+1}| = q\,|\pi_s|$ (as s increases the possible dimension of a coset in N also increases).

Using the estimate in Lemma (4.4) we get

$$\begin{aligned} \mathbf{sl}(q,n,3) &\geq \sum_{s=0}^{n-1} \frac{\binom{n}{s} (2q-1)^s q^{n-1} (q-1)^{2(n-s)}}{q^{n+s-1}} - n \\ &= \left(q^2 - 2q + 3 - \frac{1}{q}\right)^n - \left(2 - \frac{1}{q}\right)^n - n, \text{ when } b \neq 0, \end{aligned}$$

and

$$\begin{aligned} \mathbf{sl}(q,n,3) &\geq \sum_{s=0}^{n-1} \frac{\binom{n}{s} (2q-1)^s q^{n-1} (q-1)^{2(n-s)}}{q^{n+s}} + \frac{(2q-1)^n q^n}{q^{2n}} - n - 1 \\ &= \frac{1}{q}\left[\left(q^2 - 2q + 3 - \frac{1}{q}\right)^n + (q-1)\left(2 - \frac{1}{q}\right)^n\right] - n - 1, \text{ when } b = 0. \end{aligned}$$

4 Proofs of Lemmas

Definition 4.1 *We say that the set of vector pairs* $\left\{\left(\bar{\alpha}^1,\bar{\beta}^1\right),\left(\bar{\alpha}^2,\bar{\beta}^2\right),\ldots,\left(\bar{\alpha}^k,\bar{\beta}^k\right)\right\}$, *such that* $\bar{\alpha}^1\cdot\bar{\beta}^1=\bar{\alpha}^2\cdot\bar{\beta}^2=\cdots=\bar{\alpha}^k\cdot\bar{\beta}^k=\bar{\gamma}$, $\bar{\alpha}^i,\bar{\beta}^i,\bar{\gamma}\in F_q^n$, *forms a quadratic coset in* F_q^{2n}, *if*

$$\left(\mu_1\bar{\alpha}^1+\mu_2\bar{\alpha}^2+\cdots+\mu_k\bar{\alpha}^k\right)\cdot\left(\mu_1\bar{\beta}^1+\mu_2\bar{\beta}^2+\ \cdots\ +\mu_k\bar{\beta}^k\right)=\bar{\gamma},$$

for any $\mu_1,\ldots,\mu_k$ *in* F_q *satisfying* $\sum\limits_{i=1}^{k}\mu_i=1$.

Lemma 4.2 *If the set of vector pairs* $\{\left(\bar{\alpha}^i,\bar{\beta}^i\right)\mid\bar{\alpha}^i\cdot\bar{\beta}^i=\bar{\gamma},\ i=1,2,\ldots,k\}$ *forms a quadratic coset in* F_q^n *then* $\alpha_i^1=\alpha_i^2=\cdots=\alpha_i^k$ *and* $\beta_i^1=\beta_i^2=\cdots=\beta_i^k$ *whenever* $\gamma_i\neq 0$. *(Here* α_i^j *is the i-th coordinate of* $\bar{\alpha}^j$*).*

Proof

Let $\left(\bar{\alpha}^1,\bar{\beta}^1\right)$ and $\left(\bar{\alpha}^2,\bar{\beta}^2\right)$ be from the quadratic coset. Then

$$\left(\mu\alpha_i^1+(1-\mu)\,\alpha_i^2\right)\left(\mu\beta_i^1+(1-\mu)\,\beta_i^2\right)=\gamma_i,$$

for any $\mu\in F_q$. Rearranging, $\mu^2\gamma_i+(1-\mu)^2\gamma_i+\mu(1-\mu)\left(\alpha_i^2\beta_i^1+\alpha_i^1\beta_i^2\right)=\gamma_i\Rightarrow\left(\mu^2-1\right)\gamma_i+(1-\mu)^2\gamma_i+\mu(1-\mu)\left(\alpha_i^2\beta_i^1+\alpha_i^1\beta_i^2\right)=0\Rightarrow\left(\alpha_i^2\beta_i^1+\alpha_i^1\beta_i^2\right)=2\gamma_i\Rightarrow\alpha_i^2\beta_i^1+\alpha_i^1\beta_i^2=\alpha_i^1\beta_i^1+\alpha_i^2\beta_i^2\Rightarrow\left(\alpha_i^1-\alpha_i^2\right)\left(\beta_i^1-\beta_i^2\right)=0$. The last equation is valid iff $\alpha_i^1=\alpha_i^2$ or $\beta_i^1=\beta_i^2$. Moreover, since $\gamma_i\neq 0$ one of the equalities implies the other one.

As $\left(\bar{\alpha}^1,\bar{\beta}^1\right)$ and $\left(\bar{\alpha}^2,\bar{\beta}^2\right)$ were arbitrary this completes the proof. □

Corollary 4.3 *For* $\bar{\gamma}\in F_q^n$, *the number of vector pairs in a quadratic coset* $\{\left(\bar{\alpha}^i,\bar{\beta}^i\right)\mid\bar{\alpha}^i\cdot\bar{\beta}^i=\bar{\gamma},\ i=1,2,\ldots,k\}$ *is less or equal to* $q^{z(\gamma)}$. *In particular, if* $z(\bar{\gamma})=0$ *then the quadratic coset consists of a single pair* $\left(\bar{\alpha},\bar{\beta}\right),\ \bar{\alpha}\cdot\bar{\beta}=\bar{\gamma}$.

Now we prove a simple combinatorial lemma on set coverings which was used in Section **3** to obtain the lower bound in (1).

Lemma 4.4 *Suppose we have a finite set* N *represented as a union of disjoint sets* $L_0,L_1,\ldots,L_{n-1}$. *We consider the coverings of* N *by a family of subsets of types* $\Pi_0,\Pi_1,\ldots,\Pi_{n-1}$, *with the following conditions imposed on* π_i *as a subset of type* Π_i:

- π_0 *is nonempty,*
- *Order (number of elements) of* π_i *is fixed for* Π_i *and* $|\pi_i|>|\pi_{i-1}|$,
- $\pi_i\subset L_i\cup L_{i+1}\cup\ldots\cup L_{n-1}$.

Then the number of subsets of types $\Pi_0, \Pi_1, \ldots, \Pi_{n-1}$ *required to cover* N *is greater or equal to* $\sum\limits_{i=0}^{n-1} \frac{|L_i|}{|\pi_i|} - n$.

Proof

We use induction on n. When $n = 1$ the statement is trivial. Now suppose $n > 1$, and consider some covering of N. If there is π_0 such that $\pi_0 \cap L_0 = \emptyset$ then replace it by π_1, $\pi_1 \supset \pi_0$. If there are two subsets of type Π_0 not completely (only partially) in L_0, we replace them by two other subsets of the same type in such a way that ether one of them does not intersect L_0 or completely lies in it. These two procedures do not change the overall number of subsets used in the covering, and after repeating them a finite number of times, we will arrive at a covering where possibly only one π_0 is not completely in L_0. Now we replace $\pi_0 \cap L_0$ by some other subset of type Π_0, and $\pi_0 \backslash \pi_0 \cap L_0$ by some π_1. We have obtained a covering containing utmost one more subset than the number of subsets in our initial covering and where all π_0-s lie in L_0. Applying the induction hypothesis to $L_1 \cup L_2 \cup \ldots \cup L_{n-1}$ and $\Pi_1, \Pi_2, \ldots, \Pi_{n-1}$, and to L_0 and Π_0 we see that the statement of the lemma holds. □

Recall that in Section **3** we defined $T(\bar{\gamma}) = \bigcup_{\bar{\alpha}\cdot\bar{\beta}=\bar{\gamma}} \left(M \cap N\left(\bar{\alpha}, \bar{\beta}\right)\right)$, where $N\left(\bar{\alpha}, \bar{\beta}\right)$ is a disjoint coset and M is an arbitrary coset in the set of solutions N. We also defined $\Gamma \equiv \{\bar{\gamma} \mid T(\bar{\gamma}) \neq \emptyset\} \equiv \left\{\bar{\gamma}^1, \bar{\gamma}^2, \ldots, \bar{\gamma}^k\right\}$. Consider an affine sum of $T(\bar{\gamma})$-s, $\bar{\gamma} \in \Gamma$:

$$\lambda_1 T\left(\bar{\gamma}^1\right) + \lambda_2 T\left(\bar{\gamma}^2\right) + \cdots + \lambda_p T\left(\bar{\gamma}^p\right) \tag{8}$$

as the union of all sums of the form $\lambda_1\bar{\varphi}_1 + \lambda_2\bar{\varphi}_2 + \cdots + \lambda_p\bar{\varphi}_p$, $\bar{\varphi}_i \in T\left(\bar{\gamma}^i\right)$, $\sum_{i=1}^p \lambda_i = 1$. Taking into account that $T(\bar{\gamma})$-s are the parts of the same coset M one can easily check that

$$\lambda_1 T\left(\bar{\gamma}^1\right) + \lambda_2 T\left(\bar{\gamma}^2\right) + \cdots + \lambda_p T\left(\bar{\gamma}^p\right) \subseteq T\left(\lambda_1\bar{\gamma}^1 + \cdots + \lambda_p\bar{\gamma}^p\right) \tag{9}$$

Taking $\bar{\gamma}^1 = \cdots = \bar{\gamma}^p = \bar{\gamma}$ in (9) we get $\lambda_1 T(\bar{\gamma}) + \lambda_2 T(\bar{\gamma}) + \cdots + \lambda_p T(\bar{\gamma}) \subseteq T(\bar{\gamma})$. And this is the statement of

Lemma 4.5 $T(\bar{\gamma})$ *is a coset,* $\bar{\gamma} \in \Gamma$.

Lemma 4.6 $T(\bar{\gamma})$ *can be embedded into some canonical coset.*

Proof

Let $T(\bar{\gamma}) = \left(M \cap N\left(\bar{\alpha}^1, \bar{\beta}^1\right)\right) \cup \ldots \cup \left(M \cap N\left(\bar{\alpha}^t, \bar{\beta}^t\right)\right)$. Obviously $\lambda_1 N\left(\bar{\alpha}^1, \bar{\beta}^1\right) + \cdots + \lambda_t N\left(\bar{\alpha}^t, \bar{\beta}^t\right) = N\left(\lambda_1\bar{\alpha}^1 + \cdots + \lambda_t\bar{\alpha}^t, \lambda_1\bar{\beta}^1 + \cdots + \lambda_t\bar{\beta}^t\right)$. On the other hand, by Lemma (4.5) $N(\lambda_1\bar{\alpha}^1 + \cdots + \lambda_t\bar{\alpha}^t,\ \lambda_1\bar{\beta}^1 + \cdots + \lambda_t\bar{\beta}^t)$ must be one of the initial $N\left(\bar{\alpha}^i, \bar{\beta}^i\right)$-s.

So the pairs of vectors $\left(\bar{\alpha}^1, \bar{\beta}^1\right)$, …, $\left(\bar{\alpha}^t, \bar{\beta}^t\right)$ form a quadratic coset, see definition (4.1). Lemma (4.2) states that the parts of $\left(\bar{\alpha}^i, \bar{\beta}^i\right)$ corresponding to the coordinates of $\bar{\gamma}$ not equal to 0 coincide.

Let $z(\bar{\gamma}) = s > 0$ (when $s = 0$ there is only one $N\left(\bar{\alpha}, \bar{\beta}\right)$ such that $M \cap N\left(\bar{\alpha}, \bar{\beta}\right) \neq \emptyset$ and the statement of the lemma is trivial, see corollary 4.3). Let us suppose the contrary: $T(\bar{\gamma})$ cannot be covered by only one canonical coset. This implies that $T(\bar{\gamma})$ contains the vectors $(\cdots \underset{i}{0} \cdots \underset{n+i}{t_1} \cdots)$ and $(\cdots \underset{i}{t_2} \cdots \underset{n+i}{0} \cdots)$, $i \leq n$, for some $t_1,\ t_2$ nonzero. But then an affine sum of these vectors takes us out of $T\left(\bar{\gamma}\right)$, contradicting Lemma (4.5). □

Lemma 4.7 $\left|T\left(\bar{\gamma}'\right)\right| = \left|T\left(\bar{\gamma}''\right)\right|$, *for* $\bar{\gamma}', \bar{\gamma}'' \in \Gamma$.

Proof

Without loss of generality we suppose that $\lambda_1 \neq 0$ in (8) and $\left|T\left(\bar{\gamma}^1\right)\right|$ is maximal among $\left|T\left(\bar{\gamma}^i\right)\right|$ present in the sum (8). If we fix $\bar{\varphi}_i \in T\left(\bar{\gamma}^i\right)$, $i \geq 2$, and let $\bar{\varphi}_1$ run through the entire $T\left(\bar{\gamma}^1\right)$ we will get $\left|T\left(\bar{\gamma}^1\right)\right|$ different results since $\lambda_1\bar{\varphi}_1' + \lambda_2\bar{\varphi}_2 + \cdots + \lambda_p\bar{\varphi}_p = \lambda_1\bar{\varphi}_1'' + \lambda_2\bar{\varphi}_2 + \cdots + \lambda_p\bar{\varphi}_p$ implies $\bar{\varphi}_1' = \bar{\varphi}_1''$.
So we have

$$\left|\lambda_1 T\left(\bar{\gamma}^1\right) + \lambda_2 T\left(\bar{\gamma}^2\right) + \cdots + \lambda_p T\left(\bar{\gamma}^p\right)\right| \geq \max\left\{\left|T\left(\bar{\gamma}^1\right)\right|, \left|T\left(\bar{\gamma}^2\right)\right|, \ldots, \left|T\left(\bar{\gamma}^p\right)\right|\right\}. \tag{10}$$

Now suppose that not all of $\left|T\left(\bar{\gamma}^i\right)\right|$-s are equal. Let $\Delta \equiv \{\bar{\gamma}^1, \bar{\gamma}^2, \ldots, \bar{\gamma}^p\}$ be the set of all $\bar{\gamma}$-s for which $\left|T\left(\bar{\gamma}^i\right)\right|$ is maximal. Expressions (9) and (10) yield that any affine sum of $T\left(\bar{\gamma}^i\right)$-s, $\bar{\gamma}^i \in \Delta$, gives as a result one of the same $T\left(\bar{\gamma}^i\right)$-s, so for any $\lambda_1, ..., \lambda_p$ such that $\sum\limits_{i=1}^{p} \lambda_i = 1$,

$$\lambda_1\bar{\gamma}^1 + \cdots + \lambda_p\bar{\gamma}^p = \bar{\gamma} \quad , \quad \bar{\gamma} \in \Delta. \tag{11}$$

On the other hand, if $\left|T\left(\bar{\gamma}'\right)\right| < \left|T\left(\bar{\gamma}^i\right)\right|$ then $\lambda_1 T\left(\bar{\gamma}'\right) + \lambda_2 T\left(\bar{\gamma}^2\right) + \cdots + \lambda_{p+1} T\left(\bar{\gamma}^p\right)$, where not all $\lambda_2, \ldots, \lambda_{p+1}$ are equal to 0, according to (9) and (10) must give as a result one of $T\left(\bar{\gamma}^i\right)$, $\bar{\gamma}^i \in \Delta$. So $\lambda_1\bar{\gamma}' + \cdots + \lambda_{p+1}\bar{\gamma}^p = \bar{\gamma} \quad , \quad \bar{\gamma} \in \Delta$. But then $\bar{\gamma}' = \lambda_1^{-1}\bar{\gamma} - \lambda_1^{-1}\lambda_2\bar{\gamma}^1 - \cdots - \lambda_1^{-1}\lambda_{p+1}\bar{\gamma}^p$ and $\lambda_1^{-1}\left(1 - \sum_{i\geq 2}\lambda_i\right) = \lambda_1^{-1}\lambda_1 = 1$. Since $\bar{\gamma}' \notin \Delta$ we have a contradiction to (11). □

Note that along with the main proposition we have proved the following important equality:

$$\lambda_1 T\left(\bar{\gamma}^1\right) + \lambda_2 T\left(\bar{\gamma}^2\right) + \cdots + \lambda_k T\left(\bar{\gamma}^k\right) = T\left(\lambda_1\bar{\gamma}^1 + \cdots + \lambda_k\bar{\gamma}^k\right) \tag{12}$$

Lemma 4.8 *All* $T\left(\bar{\gamma}\right)$, $\bar{\gamma} \in \Gamma$, *are translates of the same linear subspace.*

Proof

By Lemma (4.5) $T\left(\bar{\gamma}^i\right)$ and $T\left(\bar{\gamma}^j\right)$ are cosets, so the equality $\left|T\left(\bar{\gamma}^i\right)\right| = \left|T\left(\bar{\gamma}^j\right)\right|$ implies $\dim T\left(\bar{\gamma}^i\right) = \dim T\left(\bar{\gamma}^j\right)$ since $\left|T\left(\bar{\gamma}\right)\right| = q^{\dim T(\bar{\gamma})}$.

To prove the lemma we use a well-known relation

$$\dim\left(L_1 + L_2\right) = \dim\left(L_1\right) + \dim\left(L_2\right) - \dim\left(L_1 \cap L_2\right),$$

where L_1 and L_2 are linear subspaces. From this relation it follows that $\dim(L_1 + L_2) > \dim(L_i)$, $(i = 1, 2)$ unless $L_1 \subseteq L_2$ or $L_1 \supseteq L_2$. In particular, if $\dim(L_1) = \dim(L_2)$ then $\dim(L_1 + L_2) = \dim(L_i)$ $(i = 1, 2)$ if and only if $L_1 \equiv L_2$.

As it was proven every $T(\bar{\gamma}^i)$ is a coset, so $T(\bar{\gamma}^i) = L_i + \bar{\varphi}_i$ for some linear subspace L_i and some vector $\bar{\varphi}_i$. Moreover, based on Lemma (4.7) $\dim(L_i) = d$, $1 \leq i \leq k$. Now (12) can be rewritten as

$$\lambda_1(L_1 + \bar{\varphi}_1) + \lambda_2(L_2 + \bar{\varphi}_2) + \cdots + \lambda_k(L_k + \bar{\varphi}_k) = \sum_{i=1}^{k} \lambda_i \bar{\varphi}_i + \sum_{i=1}^{k} L_i = \bar{\varphi} + L \tag{13}$$

where $L \in \{L_1, L_2, \ldots, L_k\}$. So we have $\dim\left(\sum_{i=1}^{k} L_i\right) = d$. From the above reasoning it follows that this is possible if and only if $L_1 \equiv L_2 \equiv \cdots \equiv L_k \equiv L$. □

References

[1] A. Aleksanyan, *Linearized disjunctive normal forms of Boolean functions*, Lecture Notes in Comp.Sci., **278**, Springer-Verlag (1988), 14-16.

[2] A. Aleksanyan, *Realization of quadratic Boolean functions by systems of linear equations*, Cybernetics **25** (1989), no. 1, 9-17.

[3] A. Aleksanyan, *Disjunctive normal forms over linear functions (Theory and Applications)*, Yerevan Univ., Yerevan, (1990), 201p., (in Russian)

[4] A. Aleksanyan and R. Serobyan, *Coverings associated with quadratic equations over a finite field*, Akad. Nauk Armenii Dokl, No. 1, **93** (1992), 6-10, (in Russian)

[5] A. A. Bruen, *Polynomial multiplicities over finite fields and intersection sets*, J. Combin. Theory Ser. A **60** (1992), 19-33.

[6] R. E. Jamison, *Covering finite fields with cosets of subspaces*, J. Combin. Theory Ser. A **22** (1977), 253-266.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol.20, Section: Algebra, Addison-Wesley, 1983.