PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2017, **51**(3), p. 236–240

Mathematics

ON THE MINIMAL COSET COVERING FOR A SPECIAL SUBSET IN DIRECT PRODUCT OF TWO FINITE FIELDS

A. V. MINASYAN *

Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia

In this paper we estimate the minimal number of systems of linear equations of $n+m$ variables over a finite field F_q such that the union of all solutions of all the systems coincides exactly with all elements of $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$.

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

***Keywords*:** linear algebra, covering with cosets.

Introduction. Let $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_q^n$ be n-dimensional linear space over $\mathbb{F}_q$. We denote by $\overset{*}{\mathbb{F}}{}_q^n$ the set of all nonzero vectors in $\mathbb{F}_q^n$. A coset of linear subspace L in $\mathbb{F}_q^n$ is a translation of L, i.e. a set $\alpha + L \equiv \{\alpha + x|\ x \in L\}$ for some $\alpha \in \mathbb{F}_q^n$. It is known that any k-dimensional coset in $\mathbb{F}_q^n$ can be represented as a set of solutions of a certain system of linear equations over $\mathbb{F}_q$ of rank $n-k$ and vice versa.

Let A be a set of vectors in $\mathbb{F}_q^n$. We say that a set of cosets $\{L_1, \dots, L_k\}$ is a covering for a set A if and only if $L_i \subseteq A$ for $1 \le i \le k$ and $A = \cup_{i=1}^k L_i$. The length of covering is the number of its cosets.

In [1] the following theorem is proved:

Theorem A. The minimal number of cosets needed to cover $\overset{*}{\mathbb{F}}{}_q^n$ is equal to $n(q-1)$.

Let $A \times B$ be direct product of two vector sets. In this paper we present several results related to coset covering of $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$.

Main Results. Let M be a subset of in $\mathbb{F}_q^n$. A coset $H \subseteq M$ is maximal in M, if it can not be enclosed in another coset $K \subseteq M$.

Proposition 1. If $A \subseteq \overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$ is maximal coset for $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$, then $A = A_1 \times A_2$, where A_1 is a coset in $\overset{*}{\mathbb{F}}{}_q^n$ and A_2 is a coset in $\overset{*}{\mathbb{F}}{}_q^m$ and $\dim(A_1) = n-1$, $\dim(A_2) = m-1$.

* E-mail: ashot.minasya@gmail.com

P r o o f . Consider all vectors of A, which are $n+m$-dimensional vectors. Let A'_1 be the set of all n-dimensional vectors that we get by omiting last m coordinates of vectors in A. Obviously, A'_1 is a coset in $\overset{*}{\mathbb{F}}{}_q^n$. It can be enclosed in a coset A_1 that has dimension $n-1$. Similarly, we can get the coset A_2. We have $A \subseteq A_1 \times A_2$, and since A is a maximal coset, we have $A = A_1 \times A_2$. □

Therefore, all maximal cosets of $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$ have dimension $n+m-2$ and are constructed by taking direct product of two maximal cosets from $\overset{*}{\mathbb{F}}{}_q^n$ and $\overset{*}{\mathbb{F}}{}_q^m$. Since for every covering we can construct a covering with the same number of maximal cosets we will use only maximal cosets [2–5].

Lets denote the minimal number of cosets needed to cover $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$ by $C_{n,m,q}$. One can cover $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$ by taking all direct products of cosets from coverings of $\overset{*}{\mathbb{F}}{}_q^n$ and $\overset{*}{\mathbb{F}}{}_q^m$. It will produce a covering of size $n(q-1) \times m(q-1)$. So, $C_{n,m,q} \leq nm(q-1)^2$.

P r o p o s i t i o n 2. $C_{n,1,q} = n(q-1)^2$.

P r o o f . A maximal coset in $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^1$ is a direct product of $n-1$ dimensional coset in $\overset{*}{\mathbb{F}}{}_q^n$ and one of $q-1$ elements from $\overset{*}{\mathbb{F}}{}_q^1$. To cover $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^1$ one should take a coset covering of $\overset{*}{\mathbb{F}}{}_q^n$ of size $n(q-1)$ (by Theorem A) for every element of $\overset{*}{\mathbb{F}}{}_q^1$. □

P r o p o s i t i o n 3. $C_{2n,2m,q} \leq 3C_{n,m,q}$.

P r o o f . Let $(x_1,\dots,x_n,x_{n+1},\dots,x_{2n},y_1,\dots,y_m,y_{m+1},\dots,y_{2m})$ be a vector in $\overset{*}{\mathbb{F}}{}_q^{2n} \times \overset{*}{\mathbb{F}}{}_q^{2m}$. We will divide all vectors of $\overset{*}{\mathbb{F}}{}_q^{2n} \times \overset{*}{\mathbb{F}}{}_q^{2m}$ into 3 groups (we say a vector is nonzero, if any of its coordinates is not zero):

1) $(x_1,\dots,x_n)$ and $(y_1,\dots,y_m)$ are nonzero;

2) $(x_{n+1},\dots,x_{2n})$ and $(y_{m+1},\dots,y_{2m})$ are nonzero;

3a) $(x_1,\dots,x_n)$; $(y_{m+1},\dots,y_{2m})$ are nonzero and $(x_{n+1},\dots,x_{2n})$; $(y_1,\dots,y_m)$ are zero;

3b) $(x_1,\dots,x_n)$; $(y_{m+1},\dots,y_{2m})$ are zero and $(x_{n+1},\dots,x_{2n})$; $(y_1,\dots,y_m)$ are nonzero.

We show here that covering of each of the 3 groups is equivalent to covering of $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$. For 1) and 2) cases it is easy to verify. For 3) case lets define $u_1 = x_1 + x_{n+1},\dots,u_n = x_n + x_{2n}$ and $v_1 = y_1 + y_{m+1},\dots,v_m = y_m + y_{2m}$. If we get covering for vectors $(u_1,\dots,u_n,v_1,\dots,v_m)$, where $(u_1,\dots,u_n)$ is nonzero and $(v_1,\dots,v_m)$ is nonzero, then we can replace u,v by their values depending on x,y in the system of equations of covering cosets and the set 3) will be covered. Obviously it can be covered using $C_{n,m,q}$ cosets. □

The same idea was used in [6] to find a minimal coset covering for a specific equation.

T h e o r e m 1. If $n \geq m$ and both are powers of 2, then

$$C_{n,m,q} \leq m^{\log_2 3} \times \times \frac{n}{m}(q-1)^2.$$

P r o o f . Let $n = 2^k, m = 2^t$. If the Proposition 1 is applied t times we get: $C_{n,m,q} = C_{2^k,2^t,q} \leq 3^t 2^{k-t}(q-1)^2 = 3^{\log_2 m} 2^{\log_2 n - \log_2 m}(q-1)^2 = m^{log_2 3} \frac{n}{m}(q-1)^2$. □

If $n = m$, we get $C_{n,n,q} \leq n^{\log_2 3}(q-1)^2$.

T h e o r e m 2. $C_{n,m,q} \geq n(q-1)(q-1/q^{m-1})$.

P r o o f . Let A be a set of cosets that cover $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^m$. We can replace a coset by maximal one and, by Proposition 2, we can represent each maximal coset by a solution of system of 2 equations of the following form:

$$\begin{cases} \alpha_1 x_1 + \ldots + \alpha_n x_n = \alpha_0, \\ \beta_1 y_1 + \ldots + \beta_m y_m = \beta_0. \end{cases}$$

All coefficients are in $\mathbb{F}_q$. Since there are no covering vectors, where the first n or the last m coordinates are 0, we can assume that α_0 and β_0 are nonzero. By multiplying both equations by appropriate elements of $\mathbb{F}_q$ we get systems of the following form:

$$\begin{cases} \alpha_1 x_1 + \ldots + \alpha_n x_n = 1, \\ \beta_1 y_1 + \ldots + \beta_m y_m = 1. \end{cases}$$

Let $\overset{*}{b} = (b_1, \ldots, b_m)$ be a vector in $\overset{*}{\mathbb{F}}{}_q^m$. If a coset $\beta_1 y_1 + \ldots + \beta_m y_m = 1$ covers it, then $\beta_1 b_1 + \ldots + \beta_m b_m = 1$, so the number of maximal cosets in $\overset{*}{\mathbb{F}}{}_q^m$ that cover $\overset{*}{b}$ is equal to the number of $(\beta_1, \ldots, \beta_m)$ solutions of the equation $\beta_1 b_1 + \ldots + \beta_m b_m = 1$. Since solution set is a $m-1$ dimensional coset, we have q^{m-1} maximal cosets that cover a single vector in $\overset{*}{\mathbb{F}}{}_q^m$.

Let $A_{\overset{*}{b}} \subseteq A$ be the set of cosets from A, where the bottom equation of the system of corresponding coset is one of the q^{m-1} equations covering $(b_1, \ldots, b_m)$. Their upper equation of the same system is coset in $\overset{*}{\mathbb{F}}{}_q^n$. The solutions of those upper equations of systems corresponding cosets in $A_{\overset{*}{b}}$ must form a covering for $\overset{*}{\mathbb{F}}{}_q^n$. If $(a_1, \ldots, a_n)$ is not covered by them, then $(a_1, \ldots, a_n, b_1, \ldots, b_m)$ is not covered by A. Since the minimal number of cosets necessary to cover $\overset{*}{\mathbb{F}}{}_q^n$ is $n(q-1)$, we get $|A_{\overset{*}{b}}| \geq n(q-1)$.

By summing all inequalities for all $\overset{*}{b} \in \overset{*}{\mathbb{F}}{}_q^m$, we get

$$\sum_{\overset{*}{b} \in \overset{*}{\mathbb{F}}{}_q^m} |A_{\overset{*}{b}}| \geq n(q-1)(q^m-1).$$

Since each bottom equation of the system of corresponding to a coset in A covers q^{m-1} vectors of $\overset{*}{\mathbb{F}}{}_q^m$, we have

$$\sum_{\overset{*}{b} \in \overset{*}{\mathbb{F}}{}_q^m} |A_{\overset{*}{b}}| = q^{m-1}|A|, \quad |A| \geq n(q-1)\frac{q^m-1}{q^{m-1}} = n(q-1)\left(q - \frac{1}{q^{m-1}}\right). \qquad \square$$

If $m = 1$ this result coincides with Proposition 3, where $C_{n,1,q} = n(q-1)^2$.

T h e o r e m 3. $C_{n,2,q} \leq 3\lceil \frac{n}{2} \rceil (q-1)^2$.

Proof. A vector in $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^2$ will be written by $(x_1, \ldots, x_n, y_1, y_2)$. Lets first prove that $C_{2,2,q} \leq 3(q-1)^2$. Consider the following set of cosets in $\overset{*}{\mathbb{F}}{}_q^2 \times \overset{*}{\mathbb{F}}{}_q^2$.

For all $a, b \in \overset{*}{\mathbb{F}}_q$:

$$(I)\begin{cases} x_1 = a \\ y_1 = b \end{cases} ; \quad (II)\begin{cases} x_2 = a \\ y_2 = b \end{cases} ; \quad (III)\begin{cases} x_1 + x_2 = a \\ y_1 + y_2 = b \end{cases} .$$

Each group has $(q-1)^2$ cosets, so there are $3(q-1)^2$ cosets. Consider a vector $v = (a_1, a_2, b_1, b_2) \in \overset{*}{\mathbb{F}}{}_q^2 \times \overset{*}{\mathbb{F}}{}_q^2$.

If a_1 and b_1 are not 0, then v is covered by a coset from (I) group. If a_2 and b_2 are not 0, then v is covered by a coset from (II) group. If one of a_1 and a_2 is 0 and one of b_1 and b_2 is 0, then v is covered by a coset from (III) group.

Therefore, we have a covering for $\overset{*}{\mathbb{F}}{}_q^2 \times \overset{*}{\mathbb{F}}{}_q^2$ of size $3(q-1)^2$. Now let $n = 2k$ and consider this set of cosets in $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^2$. For all $i = 1, 3, \ldots, 2k-1$ and $a, b \in \overset{*}{\mathbb{F}}_q$:

$$(I_i)\ \begin{cases} x_i = a \\ y_1 = b \end{cases} ; \quad (II_i)\ \begin{cases} x_{i+1} = a \\ y_2 = b \end{cases} ; \quad (III_i)\ \begin{cases} x_i + x_{i+1} = a \\ y_1 + y_2 = b \end{cases} .$$

If $v = (a_1, a_2, \ldots, a_n, b_1, b_2) \in \overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^2$, then for some $i \in \{1, 3, \ldots, 2k-1\}$ (a_i, a_{i+1}) is nonzero. Obviously, it will be covered by one of the cosets from (I_i), (II_i) or (III_i).

If n is odd, then several cosets will not be required and a covering of size $3\lceil \frac{n}{2} \rceil (q-1)^2$ for $\overset{*}{\mathbb{F}}{}_q^n \times \overset{*}{\mathbb{F}}{}_q^2$ is found. □

Corollary 1. If $q = 2$, then from Theorem 2 and 3 it follows that $C_{n,2,2} = 3\lceil \frac{n}{2} \rceil$.

When $n = m = 2$, we have $2(q-1)^2(q+1)/q \leq C_{2,2,q} \leq 3(q-1)^2$. Clearly, $C_{2,2,2} = 3$. From the inequalities it follows that $11 \leq C_{2,2,3} \leq 12$.

Theorem 4. $C_{2,2,3} = 12$.

Proof. The following set is to be covered: $\overset{*}{\mathbb{F}}{}_3^2 \times \overset{*}{\mathbb{F}}{}_3^2 = \begin{pmatrix} 0,1 \\ 0,2 \\ 1,0 \\ 1,1 \\ 1,2 \\ 2,0 \\ 2,1 \\ 2,2 \end{pmatrix} \times \begin{pmatrix} 0,1 \\ 0,2 \\ 1,0 \\ 1,1 \\ 1,2 \\ 2,0 \\ 2,1 \\ 2,2 \end{pmatrix}$. If A is a covering then every coset in A has the following form:

$$\begin{cases} \alpha_1 x_1 + \alpha_2 x_2 = 1, \\ \beta_1 y_1 + \beta_2 y_2 = 1, \end{cases}$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_3$, one of $\alpha_1, \alpha_2 \neq 0$ and one of $\beta_1, \beta_2 \neq 0$.

Let t_{ij} be the number of cosets in A, where the bottom equation of the system of corresponding system is of the form $iy_1 + jy_2 = 1$. The size of A is equal to the sum of all t_{ij}, $0 \le i \le 2$, $0 \le j \le 2$ and $t_{00} = 0$.

The cosets covering the vector $(0,1)$ are $y_2 = 1, y_1 + y_2 = 1$ and $2y_1 + y_2 = 1$. Using the same arguments as in Theorem 2, we get $t_{01} + t_{11} + t_{21} \ge 4$. If we do the same for all vectors of $\overset{*}{\mathbb{F}_3^2}$, then we get the system of inequalities:

$$\begin{cases} t_{01}+t_{11}+t_{21} \ge 4 \\ t_{02}+t_{12}+t_{22} \ge 4 \\ t_{10}+t_{11}+t_{12} \ge 4 \\ t_{10}+t_{01}+t_{22} \ge 4 \\ t_{10}+t_{02}+t_{21} \ge 4 \\ t_{20}+t_{21}+t_{22} \ge 4 \\ t_{20}+t_{01}+t_{12} \ge 4 \\ t_{20}+t_{02}+t_{11} \ge 4 \end{cases} .$$

There are 8 integer unknowns, $t_{ij} \ge 0,\ 0 \le i \le 2,\ 0 \le j \le 2,\ t_{00}$ is missing. Every unknown is used in exactly 3 inequalities. The problem is to find the solution of the system that minimize sum of all t_{ij}.

Let one of t_{ij} be 2 (if there is 3, using the same method we can even prove that the sum is ≥ 13).

Let $t_{02} = 2$.

If $t_{01} = 0$, then $t_{10} + t_{22} \ge 4$, $t_{11} + t_{21} \ge 4$ and $t_{12} + t_{20} \ge 4$, so the sum of all $t_{ij} \ge 2+0+4+4+4 = 14$.

Similarly:

if $t_{01} = 1$, then $t_{10}+t_{22} \ge 3$, $t_{11}+t_{21} \ge 3$ and $t_{12}+t_{20} \ge 3$, so $t_{ij} \ge 12$;

if $t_{01} = 2$, then $t_{10}+t_{11}+t_{12} \ge 4$ and $t_{20}+t_{21}+t_{22} \ge 4$, so $t_{ij} \ge 12$.

For all cases we have the sum of all $t_{ij} \ge 12$. It means that the covering has at least 12 cosets. □

Received 31.07.2017

REFERENCES

1. **Jamison R.** Covering Finite Fields with Cosets of Subspaces. // J. Combin. Theory, Ser. A, 1977, v. 22, p. 253–266.
2. **Alexanyan A.A.** Disjunctive Normal Forms over Linear Functions. // Theory and applications. Yer.: YSU Press, 1990 (in Russian).
3. **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).
4. **Alexanyan A.A., Serobyan R.K.** Covers Concerned with the Quadratic over Finite Field Equations. 1992, p. 6–10 (in Russian).
5. **Alexanyan A.A., Papikyan M.** On Blocking Sets of Affine Spaces. 1999, v. 1.
6. **Minasyan A.V.** On Minimal Coset Covering of Solutions of a Boolean Equation. // Proceedings of the YSU, Physical and Mathematical Sciences, 2015, № 1, p. 26–30.