PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2018, **52**(1), p. 8–11

M a t h e m a t i c s

ON THE MINIMAL COSET COVERINGS OF THE SET OF SINGULAR AND OF THE SET OF NONSINGULAR MATRICES

A. V. MINASYAN *

Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia

It is determined minimum number of cosets over linear subspaces in $\mathbb{F}_q$ necessary to cover following two sets of $A(n\times n)$ matrices. For one of the set of matrices $\det A = 0$ and for the other set $\det A \neq 0$. It is proved that for singular matrices this number is equal to $1+q+q^2+\ldots+q^{n-1}$ and for the nonsingular matrices it is equal to $(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})/q^{\binom{n}{2}}$.

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

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

Introduction. Let $\mathbb{F}_q$ be the finite field of q elements and $M_n(\mathbb{F}_q)$ be the vector space of matrices of size $n\times n$ over $\mathbb{F}_q$. A **coset** of subspace L in $M_n(\mathbb{F}_q)$ is a translate of L, i.e. it coincides with $m+L \equiv \{m+x \mid x\in L\}$ for some matrix m. It is known that any k-dimensional coset in $M_n(\mathbb{F}_q)$ can be represented as a set of solutions of a certain system of linear equations over $\mathbb{F}_q$ of rank n^2-k and vice versa.

Let S be a subset of $M_n(\mathbb{F}_q)$. We say that set of cosets $\{L_1, L_2, \ldots, L_k\}$ covers S if and only if $L_i \subseteq S$ for $1\le i\le k$ and $S=\bigcup_{i=1}^{k} L_i$. The length of the covering is the number of its cosets.

Matrix $m\in M_n(\mathbb{F}_q)$ is called singular (nonsingular), if its determinant is equal to 0 (is not equal to 0). The set of nonsingular matrices of $M_n(\mathbb{F}_q)$ forms the General Linear Group ($GL_n(\mathbb{F}_q)$).

A coset L is maximal for the set S if $L\subseteq S$ and no coset contained in S contains L.

We shall proved two results. First one determines the minimum number of cosets in $M_n(\mathbb{F}_q)$ that one must choose in order to cover the set of all solutions of the polynomial equation

$$\det\begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \ldots & x_{nn} \end{pmatrix} = 0, \tag{1}$$

where $x_{ij}, 1\le i,j\le n$, are variables in $\mathbb{F}_q$.

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

And second result establishes the minimal covering for the complement set ($\det(A) \neq 0$).

In other words, we look for the minimal cover with cosets for the:

$\diamond$ singular matrices: $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$;

$\diamond$ nonsingular matrices: $GL_n(\mathbb{F}_q)$.

The problem of the shortest or minimal coset covering of the subsets in finite fields was introduced and studied in [1–3].

Theorem 1. The minimum number of cosets necessary to cover $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$ (i.e. the set of all singular matrices) is equal to

$$\frac{q^n-1}{q-1} = 1+q+q^2+\ldots+q^{n-1}.$$

Theorem 2. The minimum number of cosets necessary to cover $GL_n(\mathbb{F}_q)$ is equal to $\dfrac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q^{\binom{n}{2}}}$.

Minimal Covering for $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$. A classification of maximal cosets in $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$ is given in [4–6]. It was proved that they are all the subspaces of dimension $n(n-1)$.

One can get such a coset by choosing some linear relation between several rows or several columns of matrices. For example matrices with a zero first row forms such a coset. Another example is given by matrices for which the first column is the sum of the second and the third columns.

Due to the below theorem from [6] all maximal cosets are formed in the described way.

Let $\mathbb{F}_q^n$ be a vector space of dimension n over $\mathbb{F}_q$. Denote by $x\otimes y \in M_n(\mathbb{F}_q)$, the Kronecker product of $x,y \in \mathbb{F}_q^n$. It is defined in the following way. If $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_n)$, then

$$x\otimes y = \begin{pmatrix} x_1y_1 & x_1y_2 & \ldots & x_1y_n \\ x_2y_1 & x_2y_2 & \ldots & x_2y_n \\ \vdots & \vdots & & \vdots \\ x_ny_1 & x_ny_2 & \ldots & x_ny_n \end{pmatrix}. \tag{2}$$

For $A,B \subseteq \mathbb{F}_q^n$, let $A\otimes B = span\{x\otimes y \mid x\in A, y\in B\}$, where $span\{S\}$ of set S is the set of all linear combinations of vectors in S.

Theorem 3. [6]. Suppose $W \subseteq M_n(\mathbb{F}_q)$ is a subspace of dimension $n(n-1)$, such that for all $A\in W$, $\det(A)=0$. Then either $W = E\otimes \mathbb{F}_q^n$ or $W = \mathbb{F}_q^n \otimes E$ for some $n-1$ dimensional subspace $E \subseteq \mathbb{F}_q^n$.

It follows that there is 2 to 1 matching between maximal cosets and $n-1$ dimensional subspaces of $\mathbb{F}_q^n$. $n-1$ dimensional subspace of $\mathbb{F}_q^n$ is defined as a solution set of a linear homogeneous equation $\alpha_1x_1+\ldots+\alpha_nx_n=0$, where $\alpha_1,\ldots,\alpha_n \in \mathbb{F}_q$ and not all coefficients are 0. Two matching cosets are constructed in the following way. In one of them the linear equation is applied on the rows of matrices (lets call it a row coset), and other one is constructed when the same equation is applied on the

columns of matrices (lets call it a column coset). It is easy to see, that if we transpose all matrices of a row coset, we will get matching column coset.

Since number of $n-1$ dimensional subspaces of $\mathbb{F}_q^n$ is equal to $\binom{n}{n-1}_q = \frac{q^n-1}{q-1}$, there are $\frac{q^n-1}{q-1}$ row cosets and $\frac{q^n-1}{q-1}$ column cosets.

It is easy to see that only row cosets or only column cosets cover $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$. It follows from the fact that each singular matrix has rows that are linearly dependent and has columns that are linearly dependent.

Following theorem states that those 2 coverings are minimal. One can not get covering with less cosets by taking several row cosets and several column cosets. There is no covering with less than $\frac{q^n-1}{q-1} = 1+q+q^2+\ldots+q^{n-1}$ cosets.

Theorem 4. In order to cover the set of singular matrices of $M_n(\mathbb{F}_q)$ one must take all row cosets or all column cosets.

Proof. Let L be a covering for the set of $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$ and it does not contain one of row cosets (call it R) and one of column cosets (call it C). In this case there exists a singular matrix that is not covered by cosets of L.

Since R is a row coset there is a linear relation on rows of matrices of R. It means that there is a row that is linearly dependent on other rows. In the same way there is a column that is linearly dependent on other columns in matrices of C. For the simplicity of proof we can assume that first row is dependent on other rows and first column is dependent on other columns.

It means that we have the following relations:

$\diamond\ r_1 = \alpha_2 r_2 + \ldots + \alpha_n r_n$;

$\diamond\ c_1 = \beta_2 c_2 + \ldots + \beta_n c_n$;

where $r_1, \ldots, r_n$ are row vectors and $c_1, \ldots, c_n$ are column vectors.

We construct the matrix m in the following way:

$$m = \begin{pmatrix} \beta_2\alpha_2 + \ldots + \beta_n\alpha_n & \alpha_2 & \ldots & \alpha_n \\ \beta_2 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ \beta_n & 0 & \ldots & 1 \end{pmatrix}. \tag{3}$$

The sub-matrix, where the first row and the first column are excluded, is filled by the identity matrix of size $(n-1)\times(n-1)$.

One can see that both linear relations are satisfied on m so it has the following properties:

$\diamond\ m \in R$;

$\diamond\ m \in C$;

$\diamond$ m does not belong to any other row coset;

$\diamond$ m does not belong to any other column coset.

Last two properties follow from the fact that all rows of m except first and all columns of m except first are linearly independent. Since L does not contain R and C, it does not cover m, so it is not a covering for $M_n(\mathbb{F}_q)\backslash GL_n(\mathbb{F}_q)$. □

Theorem 1 follows from this Theorem.

Minimal Covering for $GL_n(\mathbb{F}_q)$. The maximal cosets in the $GL_n(\mathbb{F}_q)$ are classified in [7]. It was proved that they have dimension at most $\binom{n}{2}$.

Proof of Theorem 2. We are going to cover $GL_n(\mathbb{F}_q)$ by maximal cosets. Let H be the linear subspace of strictly upper triangular matrices:

$$H = \left\{ \begin{pmatrix} 0 & \alpha_{12} & \dots & \alpha_{1n} \\ 0 & 0 & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \alpha_{n-1n} \\ 0 & 0 & \dots & 0 \end{pmatrix}, \ \alpha_{i,j} \in \mathbb{F}_q \right\}. \tag{4}$$

If e is the identity matrix, then the set $e+H$ is maximal coset in $GL_n(\mathbb{F}_q)$ because it has dimension $\binom{n}{2}$.

It is easy to verify that $e+H$ is a multiplicative subgroup in $GL_n(\mathbb{F}_q)$. Consider left cosets of $e+H$. Each of them is of the form $p(e+H) = p+pH$, where p is a nonsingular matrix. Since H is a subspace in $M_n(\mathbb{F}_q)$, then pH is also a subspace and $p+pH$ is a coset of the linear subspace pH in $GL_n(\mathbb{F}_q)$. Therefore any multiplicative left coset $p(e+H)$ is a coset of linear subspace in $GL_n(\mathbb{F}_q)$. The set of left cosets of $e+H$ obviously forms a minimal covering for $GL_n(\mathbb{F}_q)$.

The order of $GL_n(\mathbb{F}_q)$ is equal to $(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$. Thus the length of the minimal covering is equal to the index of $e+H$ in $GL_n(\mathbb{F}_q)$, which is $\dfrac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q^{\binom{n}{2}}}$. □

Received 21.12.2017

REFERENCES

1. **Alexanyan A.A.** Disjunctive Normal Forms over Linear Functions. Theory and Applications. Yer.: YSU Press, 1990 (in Russian).
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., Serobyan R.K.** Covers Concerned with the Quadratic over Finite Field Equations. // Reports of NAS RA, 1992, v. 92, p. 6–10 (in Russian).
4. **Dieudonne J.** Sur Une Generalisation Du Groupe Orthogonal a Quatre Variables. // Arch. Math., 1949, v. 1, p. 282–287.
5. **de Seguins Pazzis C.** The Affine Preservers of Non-Singular Matrices. // Arch. Math., 2010, v. 95, p. 333-342.
6. **Meshulam R.** On the Maximal Rank in a Subspace of Matrices. // The Quarterly Journal of Mathematics, 1985, v. 36, № 2, p. 225–229.
7. **de Seguins Pazzis C.** Large Affine Spaces of Non-Singular Matrices. // Transactions of the American Mathematical Society, 2013, v. 365, № 5, p. 2569–2596.