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

Հատոր Том Volume 117 2017 № 4

MATHEMATICS

УДК 519.7+512.62

A. A. Alexanian, A. V. Minasyan

An Upper Bound for the Complexity of Coset Covering of Subsets in a Finite Field

(Submitted by academician Yu. H. Shoukourian 3/VII 2017)

Keywords: *complexity, coset, covering, linearized disjunctive normal form, finite fileld, general affine group.*

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 (obviously F_q^n is isomorphic to F_{q^n}). If L is a linear subspace in F_q^n, then the set $\alpha + L \equiv \{\alpha + x \mid x \in L\}$, $\alpha \in F_q^n$ is a *coset* (or translate) of the subspace L and $\dim(\alpha + L)$ coincides with $\dim L$. An equivalent definition: a subset $N \subseteq F_q^n$ is a coset if whenever $x^1, x^2, \ldots, x^m$ are in N, so is any affine combination of them, i.e., so is $\sum_{i=1}^{m} \lambda_i x^i$ for any $\lambda_1, \ldots, \lambda_m$ in F_q such that $\sum_{i=1}^{m} \lambda_i = 1$. It can be readily verified that any k-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 $n-k$ and vice versa.

Definition 1. *A set M of cosets C form a coset covering for a subset N in F_q^n iff $N = \bigcup_{C \in M} C$. The number of cosets in M is the length (or complexity) of the covering. The shortest coset covering is the covering of the minimal possible length.*

The problem of finding of the shortest coset covering was introduced in [1] originally for F_2^n in relation with a natural generalization of the notion of Disjunctive Normal Forms of Boolean functions. The subset $N \subseteq F_q^n$ can be given in different ways: as a list of elements, as a set of solutions of a polynomial equation over F_q^n etc. Finding the shortest coset covering means finding the minimal number of systems of linear over F_q equations, such that

N coincides with the union of sets of solutions of the linear systems. Various aspects of this problem were investigated in [2-8].

In this paper we prove an upper bound for the length of the shortest coset covering based on some properties of the stabilizer of the subset N, considering the action of the General Affine Group on F_q^n.

2. General Affine Group and Coset Coverings. Consider affine transformations of F_q^n of the form $y = xA + b$, where x, y and $b \in F_q^n$, and A is an $(n \times n)$-dimensional non-degenerate matrix over F_q. We refer to an affine transformation as a pair (A,b).The General Affine Group acts naturally on F_q^n, on the set of all subsets in F_q^n and on the set of all cosets in F_q^n, and coset dimension remains invariant under this action. Thus, if two subsets N_1 and N_2 are in the same orbit then, obviously, any coset covering for N_1 can be transformed to a coset covering of the same length for N_2 by an appropriate affine transformation, and coset covering properties are invariant under the action of the General Affine Group.

Definition 2 *A set* T *of affine transformations is a coset if whenever* $(A_1,b_1),(A_2,b_2),...,(A_m,b_m)$ *are in* T, *so is* $\left(\sum_{i=1}^{m}\lambda_i A_i, \sum_{i=1}^{m}\lambda_i b_i\right)$ *for any* $\lambda_1,\ldots,\lambda_m$ *in* F_q *such that* $\sum_{i=1}^{m}\lambda_i = 1$.

For a given set of affine transformations one can consider coset covering and the shortest coset covering.

Definition 3. *Let* G *be a subgroup in the General Affine Group. The coset rank of* G *is the length of its shortest coset covering, which is denoted by* $CR(G)$.

Let $N \subseteq F_q^n$ and $Stab(N)$ be the stabilizer of N under the action of the General Affine Group. Any subgroup G in the stabilizer $Stab(N)$ acts on N splitting N into disjoint orbits of elements. We denote the number of orbits by $\#orb_G(N)$.

3. The main Theorem. Theorem 4. *The length of the shortest coset covering for a set* $N \subseteq F_q^n$ *is not greater than* $CR(G) \times \#orb_G(N)$ *for any subgroup* G *in* $Stab(N)$. *This upper bound is achievable and cannot be improved.*

Proof. For $x \in N$ consider its orbit $orb_G(x) = \{xA + b \mid (A,b) \in G\}$. Let L be the shortest coset covering for G and $C \in L$ be a coset of affine transformations. It can be readily verified that $M(x,C) \stackrel{def}{=} \{xA + b \,|\, (A,b) \in C\}$ is a coset in N. Indeed, for any $\lambda_1,\ldots,\lambda_m$ in F_q such that $\sum_{i=1}^{m}\lambda_i = 1$ and any $xA_1 + b_1$, $xA_2 + b_2, ..., xA_m + b_m$ from $M(x,C)$ we have

$$\sum_{i=1}^{m}\lambda_i\left(xA_i+b_i\right)=\sum_{i=1}^{m}x\lambda_iA_i+\sum_{i=1}^{m}\lambda_ib_i=x\sum_{i=1}^{m}\lambda_iA_i+\sum_{i=1}^{m}\lambda_ib_i.$$

Obviously, $\left(\sum_{i=1}^{m}\lambda_iA_i,\sum_{i=1}^{m}\lambda_ib_i\right)\in C$ and $x\sum_{i=1}^{m}\lambda_iA_i+\sum_{i=1}^{m}\lambda_ib_i\in M(x,C)$; therefore, $M(x,C)$ is a coset in N. This immediately implies that $orb_G(x)=\bigcup_{c\in L}M(x,C)$ is a coset covering for $orb_G(x)$ of the length $CR(G)$. Applying the same procedure to each orbit in N, we obtain a coset covering for N of the length $CR(G)\cdot\#orb_G(N)$. This completes the proof.

4. The Upper Bound is Exact. In this section we show that the upper bound in theorem 4 is achievable and, thus, exact.

Let $f(\theta)=\alpha_0+\alpha_1\theta+\ldots+\alpha_{n-1}\theta^{n-1}+\theta^n$ be a normalized primitive polynomial with $\deg(f)=n$ over F_q and

$$A=\begin{pmatrix}0&0&0&\ldots&0&-\alpha_0\\1&0&0&\ldots&0&-\alpha_1\\0&1&0&\ldots&0&-\alpha_2\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&0&\ldots&1&-\alpha_{n-1}\end{pmatrix}$$

be the companion matrix for $f(\theta)$. Obviously, $\alpha_0\neq0$ and $\det A=(-1)^n\alpha_0$. As known from algebra (see [9]), the set $F_{q^n}^*$ of non-zero elements of the finite field F_{q^n} that form a cyclic group can be represented by powers of A, i.e. $F_{q^n}^*=\left\{E,A,A^2,\ldots,A^{q^n-2}\right\}$. The elements of the field F_{q^n} can be represented by polynomials over A of degree less than n with coefficients in F_q, i.e. each element in F_{q^n} is represented by a unique polynomial $\beta_0E+\beta_1A+\ldots+\beta_{n-1}A^{n-1}$, $\beta_i\in F_q, i=1,2,\ldots,n$. The field F_{q^n} can be considered as an n-dimensional linear space over F_q, i.e. F_q^n.

Let us take $N\overset{def}{=}F_q^n\setminus\{0\}$ and $G\overset{def}{=}F_{q^n}^*=\left\{E,A,A^2,\ldots,A^{q^n-2}\right\}$. It is clear that G is a subgroup in the General Affine Group and also is a subgroup in the stabilizer of N. In [10] it is proven that the length of the shortest coset covering for $F_q^n\setminus\{0\}=F_{q^n}^*$ is equal to $n(q-1)$ and shortest covering can be chosen to consist of cosets of $\dim=n-1$. Therefore, $CR(G)=n(q-1)$ and the length of the shortest coset covering for N is also equal to $n(q-1)$. In fact all elements in N lie in a single orbit under the action of G. Indeed, affine transformation defined by the matrix A maps any vector $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})\in N$ into $\left(\gamma_1,\ldots,\gamma_{n-1},\gamma_n=-\alpha_0\gamma_0-\alpha_1\gamma_1-\ldots-\alpha_{n-1}\gamma_{n-1}\right)$. This means that the orbit of a non-zero vector $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})$ coincides with the sequence of states of a Linear

Feedback Shift Register that generates a periodic sequence with a connection (characterictic) polynomial $g(\theta)=1+\alpha_{n-1}\theta+\alpha_{n-2}\theta^2+\ldots+\alpha_1\theta^{n-1}+\alpha_0\theta^n$ with $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})$ as the initial state (see [9, 11]). But $g(\theta)=\theta^n f\left(\frac{1}{\theta}\right)$, thus $g(\theta)$ is the reciprocal polynomial of $f(\theta)$, which means that both polynomials have the same period equal to q^n-1 and the above Linear Feedback Shift Register generates a maximal-length sequence of the period q^n-1. Therefore, the length of the orbit is equal to q^n-1 and it consists of all non-zero vectors in F_q^n, i.e. coincides with N. According to the theorem 4 the length of the shortest coset covering for N is not greater than $CR(G)\times\#orb_G(N)=n(q-1)\times 1=n(q-1)$, but, in fact, as indicated above, it is exactly equal to $n(q-1)$, thus the upper bound from the theorem 4 is achieved.

If we define N as above equal to $F_q^n\setminus\{0\}$ and take G equal to the General Linear Group $GL_n(F_q)$ then clearly G is a subgroup in $Stab(N)$. Obviously all vectors in N lie in a single orbit, therefore, due to theorem 4 the length of the shortest coset covering for N is not greater than $CR\left(GL_n(F_q)\right)\times 1$.

Corollary 5. $CR\left(GL_n(F_q)\right)\geq n(q-1)$

.

Yerevan State University
e-mail: araalex@gmail.com

A. A.Alexanian, A. V. Minasyan

An Upper Bound for the Complexity of Coset Covering of Subsets in a Finite Field

An upper bound is proven for the length of the shortest coset covering of a subset in a finite field, based on some properties of the stabilizer of the subset, considering the action of the General Affine Group.

Ա. Ա. Ալեքսանյան, Ա. Վ. Մինասյան

Վերջավոր դաշտի ենթաբազմությունների հարակից դասերով ծածկույթի բարդության վերին գնահատականը

Ապացուցվել է վերջավոր դաշտի ենթաբազմության հարակից դասերով ամենակարճ ծածկույթի երկարության վերին գնահատականը, որը հիմնված է ենթաբազմության ստաբիլիզատորի որոշ հատկությունների վրա՝ դիտարկելով ընդհանուր աֆինական խմբի գործողությունը:

А. А. Алексанян, А. В. Минасян

Верхняя оценка сложности покрытия смежными классами подмножеств конечного поля

Доказана верхняя оценка длины кратчайшего покрытия смежными классами подмножества конечного поля, основанная на некоторых свойствах стабилизатора подмножества, рассматривая действие общей аффинной группы.

References

1. *Alexanian A.* Disjunctive Normal Forms Over Linear Functions (Theory and Applications), Yerevan State Univ. Press. 1990. 201 p. (Russian).
2. *Aleksanyan A.* – Soviet Math. Dokl. 1989. V. 39. N 1. P. 131-135.
3. *Alexanian A., Serobian R.* – RNAS RA. 1992. V. 93. N 1. P. 6-10. (Russian).
4. *Alexanian A., Gabrielyan V.* – ALGEBRA, GEOMETRY & THEIR APPLICATIONS, Seminar proceedings, Yerevan State University Press. 2004. V. 3-4. P. 97-111.
5. *Nurijanyan H.* – Proceedings of the Yerevan State University, Physical and Mathematical Sciences. 2010. V. 2(222). P. 41-48.
6. *Gabrielyan V.* On Metric Characterization Connected with Covering Subset of Finite Fields by Cosets of the Linear Subspaces, Institut Problem Informatiki i Avtomatizacii. Preprint 04-0603.Yer. 2004 (Russian).
7. *V. Gabrielyan* – RNAS RA. 2010. V. 110. N 3. P. 220-227.
8. *Gabrielyan V.* On Complexity of Coset Covering of an Equation over Finite Field. Institut Problem Informatiki i Avtomatizacii.Preprint 04-0602.Yer. 2004. (Russian).
9. *Lidl R., Niederreiter H.* Finite Fields (2nd ed.). Cambridge University Press. 1997.
10. *Jamison R.* – J. Combin. Theory. Ser. A. 1977. V. 22. P. 253-266.
11. *Golomb S.* Shift Register Sequences. Holden-Day, San Francisco. 1967. Reprinted by Aegean Park Press. 1982.