PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2010, № 2, p. 41–48

Informatics

AN UPPER BOUND FOR THE COMPLEXITY OF LINEARIZED COVERINGS IN A FINITE FIELD

H. K. NURIJANYAN*

Chair of Discrete Mathematics and Theoretical Informatics, YSU

The minimal number of systems of linear equations with n unknowns over a finite field F_q, such that the union of all solutions of the systems forms an exact cover for a given subset in F_q^n, is the complexity of a linearized covering. An upper bound for the complexity for "almost all" subsets in F_q^n is presented.

***Keywords*:** finite fields, system of linear equations over finite fields, linearized coverings.

Below 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 and $\tilde{\alpha} \in F_q^n$, then the set $\tilde{\alpha} + L \equiv \{\tilde{\alpha} + \tilde{x} \mid \tilde{x} \in L\}$ is a *coset* of the subspace L and its dimension coincides with $\dim L$. An equivalent definition: a subset $N \subseteq F_q^n$ is a *coset*, if whenever $\tilde{x}^1, \tilde{x}^2, ..., \tilde{x}^m$ are in N, so is any affine combination of them, i.e. $\sum_{i=1}^{m} \lambda_i \tilde{x}^i$ for any $\lambda_1, \lambda_2, ..., \lambda_m$ in F_q such that $\sum_{i=1}^{m} \lambda_i = 1$. It can be verified that any k-dimensional coset in F_q^n is 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 of cosets $\{H_1, H_2, ..., H_m\}$ in F_q^n forms a *linearized covering* of a subset N in F_q^n, if $N = \bigcup_{i=1}^{m} H_i$. The *length* of the covering is equal to the number m of cosets. A linearized covering is the *shortest* for the given N, if it has the smallest possible length.

Definition 2. Let π_n be the number of subsets in F_q^n that satisfy a certain property Π. If $\lim_{n\to\infty} \pi_n / 2^{q^n} = 1$, then we say that "almost all" subsets of F_q^n satisfy the property Π.

* E-mail: hovikn@gmail.com

The problem: for a given subset in F_q^n (usually a set of solutions of a polynomial equation with n unknowns over F_q) estimate the length of the shortest linearized covering and find an effective algorithm that constructs the shortest or "close" to the shortest linearized covering for N. This problem was originally considered in [1, 2] for $q=2$ in connection with minimization of Boolean functions. It was shown in [3], that the length of the shortest covering $L_q(N)$ for almost all subsets satisfies the following inequalities:

$$(1-\varepsilon_n)\frac{q^n}{2qn\log_q n} \le L_q(N) \le (1-\delta_n)\frac{3q^3q^n\log_q n}{2n\log_q e}, \text{ where } \lim_{n\to\infty}\varepsilon_n = \lim_{n\to\infty}\delta_n = 0.$$

Our aim is to improve the upper bound with the help of techniques developed in [4].

Theorem 1. $L_q(N) < c\dfrac{q^n}{n}$ for almost all subsets in F_q^n, where $c = \dfrac{q^{3-\ln 2}e^2(\ln 2+1)}{2\ln 2} \approx 18q^{3-\ln 2}$.

Denote by $\begin{bmatrix} n \\ k \end{bmatrix}_q$ the Gaussian coefficient – the number of k-dimensional linear subspaces in F_{q^n}. We use the following properties of the Gaussian coefficients:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}, \quad \begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q, \quad \begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n-r \\ n-k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} k \\ r \end{bmatrix}_q$$

and $\sum_{r=0}^{k} q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} k \\ r \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q$.

Let D_k stands for the set of all k-dimensional cosets in F_q^n (obviously $|D_k| = q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$), $F(n)$ stands for the set of all subsets in F_q^n, and $CK(n)$ – for the set of all cosets in F_q^n.

Theorem 1 is a result of Lemmas set out and proven below.

Definition 3. In a Boolean matrix $T = \{t_{i,j}\}$ the j-th column covers the i-th row, iff $t_{i,j} = 1$.

Definition 4. A sequence of columns of a Boolean matrix $a_1, a_2, \ldots, a_k$ is *gradient*, if for every $i = 1, 2, \ldots, k$ the column a_i covers the maximal possible number of rows, which are not covered by the columns $a_1, a_2, \ldots, a_{i-1}$. The number k is the *length* of a gradient sequence.

Denote the number of rows and columns in T by $p(T)$ and $q(T)$ respectively. Let $L_\delta(T)$, $\delta \ge 0$, be the minimal number k, such that for any gradient sequence with length k the portion of not covered rows in T is not greater than $e^{-\delta}$.

Lemma 1 [4]. Let $\tilde{T}$ be a submatrix in T, such that every row in $\tilde{T}$ is covered by not less than $\chi q(\tilde{T})$ columns, $\chi > 0$, and $p(\tilde{T}) \ge (1-\varepsilon)p(T)$, $\varepsilon \in (0,1)$, then $L_\delta(T) \le \frac{\delta}{\chi} + 1 + \varepsilon p(T)$.

Let a probability be defined on $F(n)$, such that random variables (RVs) $\xi_{\tilde{x}}(N) = \begin{cases} 1, & \tilde{x} \in N, \\ 0, & \tilde{x} \notin N, \end{cases}$ $\tilde{x} \in F_q^n, N \subseteq F_q^n$ are independent in aggregate, identically distributed and $\mathrm{P}(\xi_{\tilde{x}} = 1) = 2^{-\lambda}$.

Denote by $\psi_k(N)$ the number of k-dimensional cosets ($0 \le k \le n$) in a random subset N, and by $\eta_{\tilde{x}}^k(N)$ the number of such cosets H, for which $\tilde{x} \in H$ and $H \setminus \tilde{x} \subseteq N$. Below we calculate expectations and second moments for those RVs. Easily verify $M\psi_k = 2^{-\lambda q^k} q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q$,

$$M\psi_k^2 = 2^{-2\cdot\lambda q^k} \sum_{r=0}^{k} q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-r \\ k-r \end{bmatrix}_q q^{n-r} \begin{bmatrix} n \\ r \end{bmatrix}_q \left(2^{\lambda q^r} - 1\right) + \left(M\psi_k\right)^2,$$

$$M\eta_{\tilde{x}}^k = \begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda(q^k-1)} \text{ and } M\left(\eta_{\tilde{x}}^k\right)^2 = 2^{-\lambda(2q^k-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q \sum_{r=0}^{k} q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} k \\ r \end{bmatrix}_q 2^{\lambda q^r}.$$

Therefore,

$$D\psi_k = \left(M\psi_k\right)^2 - M\psi_k^2 = 2^{-2\cdot\lambda q^k} \sum_{r=0}^{k} q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} n-r \\ k-r \end{bmatrix}_q q^{n-r} \begin{bmatrix} n \\ r \end{bmatrix}_q \left(2^{\lambda q^r} - 1\right) \le$$

$$\le 2^{-2\cdot\lambda q^k} q^n \begin{bmatrix} n \\ k \end{bmatrix}_q \max_{0 \le r \le k} q^{-r} (2^{\lambda q^r} - 1) \sum_{r=0}^{k} q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} k \\ r \end{bmatrix}_q \le q^{n-k} 2^{-\lambda q^k} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 \text{ and}$$

$$\frac{D\psi_k}{\left(M\psi_k\right)^2} \le q^{n-k} 2^{-\lambda q^k} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 \Big/ q^{2(n-k)} 2^{-2\cdot\lambda q^k} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 = \frac{2^{\lambda q^k}}{q^{n-k}}. \qquad (*)$$

Lemma 2. $\frac{D\eta_{\tilde{x}}^k}{(M\eta_{\tilde{x}}^k)^2} \le \frac{k 2^{\lambda(q-1)} q^{3k}}{q^n}$ for $k = \left[\log_q n - \log_q \lambda - \delta - 1\right]$, $\delta \in (0,1)$.

Proof. The sequence $a_r \equiv q^{(k-r)^2} \begin{bmatrix} n-k \\ k-r \end{bmatrix}_q \begin{bmatrix} k \\ r \end{bmatrix}_q 2^{\lambda q^r}$, $0 \le r \le k$, decreases, so

$$M(\eta_{\tilde{x}}^k)^2 = 2^{-\lambda(2q^k-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q \sum_{r=0}^{k} a_r \le 2^{-\lambda(2q^k-1)} \begin{bmatrix} n \\ k \end{bmatrix}_q (a_0 + k a_1) \le 2^{-2\lambda(q^k-1)} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 \times$$

$$\times \left(1 + k 2^{\lambda(q-1)} q^{(k-1)^2} \frac{q^k-1}{q-1} \cdot \frac{\begin{bmatrix} n-k \\ k-1 \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q}\right) = 2^{-2\lambda(q^k-1)} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 \left(1 + k 2^{\lambda(q-1)} q^{(k-1)^2} \frac{q^k-1}{q-1} \cdot \frac{\begin{bmatrix} n-k \\ k-1 \end{bmatrix}_q}{\begin{bmatrix} n \\ k \end{bmatrix}_q}\right) \le$$

$$\le 2^{-2\lambda(q^k-1)}\left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right)^2 \left(1+k2^{\lambda(q-1)}q^{3k}q^{-n}\right)=\left(M\eta_{\tilde{x}}^k\right)^2\left(1+k2^{\lambda(q-1)}q^{3k}q^{-n}\right).$$

Finally we have $\dfrac{D\eta_{\tilde{x}}^k}{\left(M\eta_{\tilde{x}}^k\right)^2}=\dfrac{M\left(\eta_{\tilde{x}}^k\right)^2}{\left(M\eta_{\tilde{x}}^k\right)^2}-1\le\dfrac{k2^{\lambda(q-1)}q^{3k}}{q^n}$.

Definition 5. Let $N=\{\tilde{\alpha}_1,\tilde{\alpha}_2,...,\tilde{\alpha}_s\}$ and $\{H_1,H_2,...,H_p\}$ be the set of all cosets in N. We associate with N a Boolean matrix $T_N=\{t_{i,j}\}_{s\times p}$, such that $t_{i,j}=1$, iff $\tilde{\alpha}_i\in H_j$. Let $L_\delta(T_N)=L_\delta(N)$ and $\varphi_+(x)=x+|x|/2$.

Lemma 3. $M\varphi_+\left(L_\delta(N)-q^{2+\delta}\lambda\delta\dfrac{q^n2^{-\lambda}}{n}\right)\le\dfrac{q^n}{n\log_q^2 n}$ for $\lambda\ge1$, $\delta\in(0,1)$.

Proof. Suppose $k=\left[\log_q n-\log_q\lambda-\delta-1\right]$. By (*), $\dfrac{D\psi_k}{(M\psi_k)^2}\le\dfrac{2^{\lambda q^k}}{q^{n-k}}$. Thus, for large n $\dfrac{D\psi_k}{(M\psi_k)^2}\le\dfrac{2^{\lambda q^{\log_q n-\log_q\lambda-1}}}{q^n}q^{\log_q n}=q^{-n\left(1-\frac{1}{q\log_2 q}\right)+\log_q n}<\dfrac{1}{n^{12}}$.

For a random subset N using Chebyshev's inequality we obtain

$$\mathrm{P}\left(\psi_k\ge\left(1+\frac{1}{n^4}\right)q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda q^k}\right)=\mathrm{P}\left(\psi_k\ge\left(1+\frac{1}{n^4}\right)M\psi_k\right)\le$$
$$\le\mathrm{P}\left(\left|\psi_k-M\psi_k\right|\ge\frac{1}{n^4}M\psi_k\right)\le\frac{D\psi_k}{\left(\frac{1}{n^4}M\psi_k\right)^2}<\frac{n^8}{n^{12}}=\frac{1}{n^4}, \tag{1}$$

$$\mathrm{P}\left(\left|\psi_0-q^n2^{-\lambda}\right|\ge\frac{1}{n^4}q^n2^{-\lambda}\right)=\mathrm{P}\left(\left|\psi_0-M\psi_0\right|\ge M\psi_0\right)\le\frac{D\psi_0}{\left(\frac{1}{n^4}M\psi_0\right)^2}<\frac{n^8}{n^{12}}=\frac{1}{n^4}. \tag{2}$$

Denote by $T_{N,k}$ a submatrix in T_N, formed by columns that correspond to k-dimensional cosets in N, and rows in N, which are covered by not less than $S_0\equiv\left(1-\dfrac{1}{n^8}\right)\begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda(q^k-1)}$ k-dimensional cosets in N. Using Lemma 2 we can estimate

$$M\left(p(T_N)-p(T_{N,k})\right)=\frac{1}{2^{q^n}}\left|\left\{(\tilde{x},N)\mid\tilde{x}\in N;\ \ \eta_{\tilde{x}}^k(N)<S_0\right\}\right|=\frac{1}{2^{q^n}}\left|\left\{\tilde{x}\mid\tilde{x}\in F_{q^n};\eta_{\tilde{x}}^k(N)<S_0\right\}\right|\times$$
$$\times2^{q^n}2^{-\lambda}=q^n2^{-\lambda}P\left(\eta_{\tilde{x}}^k<\left(1-\frac{1}{n^8}\right)M\eta_{\tilde{x}}^k\right)\le q^n2^{-\lambda}P\left(\left|\eta_{\tilde{x}}^k-M\eta_{\tilde{x}}^k\right|\ge\frac{1}{n^8}M\eta_{\tilde{x}}^k\right)\le$$
$$\le q^n2^{-\lambda}\frac{D\eta_{\tilde{x}}^k}{\left(\frac{1}{n^8}M\eta_{\tilde{x}}^k\right)^2}\le q^n2^{-\lambda}\frac{k2^{\lambda(q-1)}q^{3k}}{q^n}n^{16}=k2^{\lambda(q-2)}q^{3k}n^{16}. \tag{3}$$

Let A^n be a subset of $F(n)$, such that for each $N \in A^n$ the following inequalities hold: $q(T_{N,K}) \le \left(1+\frac{1}{n^4}\right) q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda q^k}$, $\left|p(T_N) - q^n 2^{-\lambda}\right| \le \frac{1}{n^4} q^n 2^{-\lambda}$, $p(T_N) - p(T_{N,k}) \le p(T_N)\frac{1}{n^3}$.

Suppose that $N_0 \in F(n) \setminus A^n$ and at least one of the below inequalities holds: $q(T_{N_0,K}) > \left(1+\frac{1}{n^4}\right) q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda q^k}$, $\left|p(T_{N_0}) - q^n 2^{-\lambda}\right| > \frac{1}{n^4} q^n 2^{-\lambda}$, $p(T_{N_0}) - p(T_{N_0,k}) > p(T_{N_0})\frac{1}{n^3}$.

Due to (1), (2), $\psi_k(N) = q(T_{N,k})$, $\psi_0(N) = p(T_N)$, we obtain $\mathrm{P}\left(\psi_k > \left(1+\frac{1}{n^4}\right) q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda q^k}\right) < \frac{1}{n^4}$ and $\mathrm{P}\left(\left|\psi_0 - q^n 2^{-\lambda}\right| > \frac{1}{n^4} q^n 2^{-\lambda}\right) < \frac{1}{n^4}$ for the first two above inequalities. If the third inequality holds, but first two do not, then using Chebyshev's inequality and (3) we can estimate

$$\mathrm{P}\left(p(T_{N_0}) - p(T_{N_0,k}) > p(T_{N_0})\frac{1}{n^3}\right) < \frac{M(p(T_{N_0}) - p(T_{N_0,k}))}{\left(p(T_{N_0})\frac{1}{n^3}\right)^2} \le \frac{k 2^{\lambda(q-2)} q^{3k} n^{16}}{\left(1-\frac{1}{n^4}\right) q^n 2^{-\lambda}} n^3 < \frac{1}{n^3},$$

and, thus, $\mathrm{P}\left(F(n) \setminus A^n\right) < n^{-3}$. Obviously, for any $N \in A^n$ T_N meets the conditions of Lemma 1, thus, $L_\delta(N) \le (\delta / \chi) + 1 + \varepsilon p(N)$, where

$$\chi = \frac{\left(1-\frac{1}{n^8}\right)\begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda(q^k-1)}}{\left(1+\frac{1}{n^4}\right) q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_q 2^{-\lambda q^k}}, \quad \varepsilon = \frac{1}{n^3}.$$ Then

$$L_\delta(N) \le \delta \frac{\left(1+\frac{1}{n^4}\right)}{\left(1-\frac{1}{n^8}\right)} q^{n-k} 2^{-\lambda} + 1 + \frac{1}{n^3}\left(1+\frac{1}{n^4}\right) q^n 2^{-\lambda} \le \delta \frac{1}{\left(1-\frac{1}{n^4}\right)} q^{n-k} 2^{-\lambda} + \frac{2}{n^3} q^n 2^{-\lambda} \le$$

$$\le \delta q^{2+\delta} \lambda \frac{q^n 2^{-\lambda}}{n}\left(1+\frac{1}{n^2}\right) + \frac{2}{n^3} q^n 2^{-\lambda} < \delta q^{2+\delta} \lambda \frac{q^n 2^{-\lambda}}{n} + q^n 2^{-\lambda}\frac{1}{n^2} \le \delta q^{2+\delta} \lambda \frac{q^n 2^{-\lambda}}{n} + \frac{1}{n^2}\cdot\frac{q^n}{2}$$

and

$$M\varphi_+\left(L_\delta(N) - q^{2+\delta}\lambda\delta\frac{q^n 2^{-\lambda}}{n}\right) \le \frac{1}{n^2}\cdot\frac{q^n}{2}\mathrm{P}(A^n) + \mathrm{P}(F(n)\setminus A^n) q^n \le \frac{1}{n^2}\cdot\frac{q^n}{2}\mathrm{P}(A^n) + \frac{1}{n^3} q^n =$$

$$= \frac{q^n}{n^2}\left(\frac{\mathrm{P}\left(A^n\right)}{2} + \frac{1}{n}\right) < \frac{q^n}{n^2} < \frac{q^n}{n \log_q^2 n}.$$ This completes the proof.

As in [4] we split the set of coordinates X of vectors in F_{q^n} into non-intersecting subsets $X = X^1 \cup ... \cup X^k \cup Y$, such that

$$\left|X^i\right| = m, \quad i = \overline{1,k}, \quad k = \left[\log_q n\right], \quad m = \left[\frac{n}{\log_q n}\right].$$

Let υ_δ be an operator that associates with each $N \subseteq F_{q^n}$ a set of cosets in N that being taken in a certain order forms a gradient sequence, satisfying the condition that the fraction of uncovered rows does not exceed $e^{-\delta}$, and removal of the last member of this sequence breaches the condition.

For each subset $N \subseteq F_{q^n}$ we define a sequence of subsets $N_0, N_1, ..., N_k$ in the following way:

1) $N_0 = N$;

2) suppose that N_{i-1} $(i \le k)$ is already constructed and N_{i-1}^j, $j = 1, ..., q^{n-m}$, are subsets obtained from N_{i-1} by fixing the coordinates that are not in X^i in all vectors in N_{i-1}. We set $\upsilon_\delta^i(N) = \upsilon_\delta(N_{i-1}^1) \cup ... \cup \upsilon_\delta(N_{i-1}^{q^{n-m}})$. Then, $N_i = N_{i-1} \setminus \upsilon_\delta^i(N)$. Denote by $\upsilon^k(N)$ the longest gradient sequence for N_k, and $L_{\upsilon,\delta}(N) = \bigcup_{i=1}^{k} \upsilon_\delta^i(N) \cup \upsilon^k(N)$.

Lemma 4. $M\varphi_+\left(L_{\upsilon,\delta} - \frac{q^3 e^2}{2q^{\ln 2}} \frac{q^n}{n} 2^{-\lambda} \frac{\lambda \ln 2 + 1}{\ln 2}\right) \le \frac{q^n}{n \log_q n}$ for $\lambda \ge 1$, $\delta \ge 1 - \ln 2$.

Proof. Consider the i-th step of above construction scheme. Without a loss of generality we may assume that $X^i = \{1, 2, ..., m\}$, and all vectors in N_{i-1}^j are of the form $(x_1, ..., x_m, \sigma_1, ..., \sigma_{n-m})$, where $\sigma_k \in F_q$, $k = \overline{1, n-m}$. Define the following distribution on $F(m)$: $\mathrm{P}_j\left(\{G\}\right) = \mathrm{P}\left(\{N \mid N_{i-1}^j = G\}\right)$.

The RVs $\xi_{\tilde{x}}$ for each of the above distributions are independent in aggregate and identically distributed. Let $\mathrm{P}_j(\xi_{\tilde{x}} = 1) = 2^{-\lambda_{i,j}}$, $j = 1, ..., q^{n-m}$, $\lambda_{i,j} > 0$. According to the above construction scheme $\mathrm{P}(\tilde{x} \in N_{i-1}) = \frac{1}{s}\sum_{j=1}^{s} 2^{-\lambda_{i,j}}$, where $s = q^{n-m}$.

On the other hand, all the vectors, which were covered with gradient sequence in the previous step, are not in N_{i-1}, and the fraction of uncovered rows cannot exceed $e^{-\delta}$; therefore, $\mathrm{P}(\tilde{x} \in N_{i-1}) \le e^{-\delta(i-1)} 2^{-\lambda}$ and $\frac{1}{s}\sum_{j=1}^{s} 2^{-\lambda_{i,j}} \le e^{-\delta(i-1)} 2^{-\lambda} = 2^{-\lambda - \delta(i-1)\log_2 e}$.

Consequently, due to convexity, we state that

$$\frac{1}{s}\sum_{j=1}^{s} 2^{-\lambda_{i,j}} \lambda_{i,j} \le 2^{-\lambda - \delta(i-1)\log_2 e}\left(\lambda + \delta(i-1)\log_2 e\right) = e^{-\delta(i-1) - \lambda \ln 2} \frac{1}{\ln 2}\left(\delta(i-1) + \lambda \ln 2\right).$$

Denoting $t \equiv \delta(i-1) + \lambda \ln 2$, we have

$$\frac{1}{s}\sum_{j=1}^{s} 2^{-\lambda_{i,j}}\lambda_{i,j} \le e^{-t}t\frac{1}{\ln 2}. \tag{4}$$

As $e^{\delta} \ge \delta + 1$, we have $\frac{e^{\delta}}{\delta}\int_{t}^{t+d} xe^{-x}dx \ge e^{-t}\left(\frac{(\delta+1)(t+1)}{\delta} - \frac{t+\delta+1}{\delta}\right) = e^{-t}t.$ And combining with (4), we obtain

$$\sum_{j=1}^{s} 2^{-\lambda_{i,j}}\lambda_{i,j} \le s\frac{1}{\ln 2}\frac{e^{\delta}}{\delta}\int_{t}^{t+d} xe^{-x}dx. \tag{5}$$

As per construction of the operator υ_{δ}, we can state that $\left|\upsilon_{\delta}(N_{i-1}^{j})\right| \le L_{\delta}(N_{i-1}^{j})$ $\forall i = \overline{1,k}$ and $\forall j = \overline{1,s}$. By Lemma 4 we have

$$M\varphi_{+}\left(\left|\upsilon_{\delta}(N_{i-1}^{j})\right| - q^{2+\delta}\lambda_{i,j}\delta\frac{q^{m}2^{-\lambda_{i,j}}}{m}\right) \le M\varphi_{+}\left(L_{\delta}(N_{i-1}^{j}) - q^{2+\delta}\lambda_{i,j}\delta\frac{q^{m}2^{-\lambda_{i,j}}}{m}\right) \le \frac{q^{m}}{m\log_{q}^{2} m}.$$

Adding up over j $M\varphi_{+}\left(\left|\upsilon_{\delta}^{i}\right| - \sum_{j=1}^{s} q^{2+\delta}\lambda_{i,j}\delta\frac{q^{m}2^{-\lambda_{i,j}}}{m}\right) \le s\frac{q^{m}}{m\log_{q}^{2} m} = \frac{q^{n}}{m\log_{q}^{2} m}.$

Due to (5), $M\varphi_{+}\left(\left|\upsilon_{\delta}^{i}\right| - q^{2+\delta}\frac{q^{n}}{m}\cdot\frac{e^{\delta}}{\ln 2}\int_{\delta(i-1)+\lambda\ln 2}^{\delta i+\lambda\ln 2} xe^{-x}dx\right) \le \frac{q^{n}}{m\log_{q}^{2} m}$ or

$$M\varphi_{+}\left(\sum_{i=1}^{k}\left|\upsilon_{\delta}^{i}\right| - q^{2+\delta}\frac{q^{n}}{m}\cdot\frac{e^{\delta}}{\ln 2}\int_{\lambda\ln 2}^{\delta k+\lambda\ln 2} xe^{-x}dx\right) \le k\frac{q^{n}}{m\log_{q}^{2} m}. \tag{6}$$

Obviously,

$$\int_{\lambda\ln 2}^{\delta k+\lambda\ln 2} xe^{-x}dx < \int_{\lambda\ln 2}^{\infty} xe^{-x}dx = 2^{-\lambda}\left(\lambda\ln 2 + 1\right). \tag{7}$$

Taking into account the fact that for any set the length of a gradient sequence cannot be greater than the cardinality of the set, we estimate

$$M\left|\upsilon^{k}\right| \le \sum_{j=1}^{q^{n}} \mathrm{P}(\tilde{x} \in N_{k}) \le q^{n}2^{-\lambda}e^{-\delta k}. \tag{8}$$

Combining (6)–(8), we obtain

$$M\varphi_{+}\left(L_{\upsilon,\delta} - q^{2+\delta}e^{\delta}\frac{q^{n}2^{-\lambda}}{m}\cdot\frac{\lambda\ln 2+1}{\ln 2}\right) \le k\frac{q^{n}}{m\log_{q}^{2} m} + q^{n}2^{-\lambda}e^{-\delta k}.$$

Consequently, as $m \sim n$, $\log_{q} m \sim \log_{q} n$, $k \sim \log_{q} n$ when $n \to \infty$, and taking $\delta = 1 - \ln 2$, we prove the Lemma.

Proof of Theorem 1. Choosing $\lambda = 1$ in Lemma 4, we have

$$M\varphi_{+}\left(L_{\upsilon,\delta} - \frac{q^{3}e^{2}}{4q^{\ln 2}}\cdot\frac{q^{n}}{n}\cdot\frac{\ln 2+1}{\ln 2}\right) \le \frac{q^{n}}{n\log_{q} n}.$$

We define $A(n) = \frac{q^{3}e^{2}}{4q^{\ln 2}}\cdot\frac{q^{n}}{n}\cdot\frac{\ln 2+1}{\ln 2}$ and $B(n) = \frac{q^{n}}{n\log_{q} n}$. Then $\lim_{n\to\infty}\frac{B(n)}{A(n)} = 0$.

Using Chebyshev's inequality, we get

$$\mathrm{P}\left(L_{\upsilon,\delta}-2A(n)\geq 0\right)=\mathrm{P}\left(L_{\upsilon,\delta}-A(n)\geq A(n)\right)\leq\frac{M\left(L_{\upsilon,\delta}-A(n)\right)}{A(n)}\leq\frac{M\varphi_{+}\left(L_{\upsilon,\delta}-A(n)\right)}{A(n)}\leq\frac{B(n)}{A(n)}.$$

We come to a conclusion that $\mathrm{P}\left(L_{\upsilon,\delta}-2A(n)\geq 0\right)$ tends to 0, whenever $n\to\infty$, thus, for almost all subsets in F_q^n $L_{\upsilon,\delta}<2A(n)$, so we come to the statement of Theorem 1.

Received 01.03.2010

REFERENCES

1. **Alexanian A.** Disjunctive Normal Forms Over Linear Functions (Theory and Applications). Yer.: YSU press, 1990, 201 p. (in Russian).
2. **Aleksanyan A.** Soviet. Mat. Dokl., 1989, v. 39, № 1, p. 131–135 (in Russian).
3. **Gabrielian V.** On Metric Characterization Connected with Covering Subset of Finite Fields by Cosets of the Linear Subspaces. Institut Problem Informatiki i Avtomatizacii. Yer., 2004 (in Russian).
4. **Andreev A.** Vestnik Moskovskogo Universiteta, 1985, № 3, p. 29–35 (in Russian).

Հ. Ք. Նուրիջանյան

Գծայնացվող ծածկույթների բարդության վերին սահմանը վերջավոր դաշտում

F_q^n վերջավոր դաշտի վրա տրված փոփոխականների գծային հավասարումների համակարգերի նվազագույն քանակը, որոնց լուծումների միավորումը հանդիսանում է ճշգրիտ ծածկույթ -ում տրված ենթաբազմության համար, կոչվում է գծայնացվող ծածկույթի բարդություն: Աշխատանքում ներկայացված է այդ բարդության վերին սահմանը գծային տարածության "համարյա բոլոր" ենթաբազմությունների համար:

О. К. Нуриджанян.

Верхняя граница сложности линеаризуемых покрытий в конечном поле

Минимальное количество систем линейных над конечным полем F_q уравнений от n переменных, объединение решений которых образует точное покрытие для данного в F_q^n подмножества, называется сложностью линеаризированного покрытия. В настоящей статье мы представляем верхнюю границу этой сложности для "почти всех" подмножеств линейного пространства F_q^n.