

## ON SUBSPACES CONTAINED IN SUBSETS OF FINITE HOMOGENEOUS SPACES

M.G. KARPOVSKY and V.D. MILMAN

*The Institute for Advanced Studies, The Hebrew University, Jerusalem and Department of  
Mathematical Sciences, Tel Aviv University, Tel Aviv, Israel*

Received 22 April 1976  
Revised 22 June 1977

Let  $E(l) \subset E(l+1) \subset \dots \subset E(n)$  be a system of finite sets and  $H(l) \subset H(l+1) \subset \dots \subset H(n)$  be a system of groups, where  $H(k)$  is a transitive group of automorphisms of  $E(k)$ . Denote  $G(k, E(n)) = \{X \subset E(n) : \exists h \in H(n), h(E(k)) = X\}$ . We investigate the following problem: given  $n$ ,  $1 \leq l \leq k \leq n$ ,  $0 < \lambda \leq |E(k)|$ . What is the maximal cardinality  $L(n, k, \lambda)$  of a set  $M \subseteq E(n)$  such that for  $\forall X \in G(k, E(n))$ ,  $|X \cap M| < \lambda$ ? We shall establish an upper bound for  $L(n, k, \lambda)$  and prove that for some important cases it will coincide with the lower bound for  $L(n, k, \lambda)$ . We shall consider the three special cases of our problem: linear spaces, Grassmann spaces, Turan's problem. For linear spaces, we obtain the exact formula for the maximal cardinality  $L(n, k, q^k - 1)$  of a subset  $M$  in a linear  $n$ -space  $E_q^n$  over  $GF(q)$  such that  $M$  does not contain any  $k$ -subspace of  $E_q^n$ . We shall consider also some applications of this result.

### 1. Introduction

Let  $E(l) \subset E(l+1) \subset \dots \subset E(n)$  be a system of finite sets and  $H(l) \subset H(l+1) \subset \dots \subset H(n)$  be a system of groups, where  $H(k)$  is a transitive group of automorphisms of  $E(k)$ . Denote  $G(k, E(n)) = \{X \subset E(n) : \exists h \in H(n), h(E(k)) = X\}$ .

We investigate the following problem: given  $n$ ,  $1 \leq l \leq k \leq n$ ,  $0 < \lambda \leq |E(k)|$  ( $|E(k)|$  is the cardinality of  $E(k)$ ), what is the maximal cardinality  $L(n, k, \lambda)$  of a set  $M \subseteq E(n)$  such that for  $\forall X \in G(k, E(n))$ ,  $|X \cap M| < \lambda$ ? We shall consider particularly three special cases of this problem: linear spaces, Grassmann spaces, finite graphs.

(i) For linear spaces, we let  $E(n) = E_q^n - 0$  be a linear  $n$ -space over  $GF(q)$  without 0. Let  $\{e_i\}$  ( $i = 1, \dots, n$ ) be some basis in  $E_q^n$  and  $E_q^k$  be a linear span of  $\{e_i\}$  ( $i = 1, \dots, k$ ). Then we set  $E(k) = E_q^k - 0$  and  $H(k) = GL(n, k)$  is the group of linear automorphisms such that for  $\forall h \in H(k)$ ,  $h(e_i) = e_i$  ( $i = k+1, \dots, n$ ). For linear spaces, we are interested in the case  $l = 1$ ,  $\lambda = q^k - 1$  and denote for this case  $L(n, k, q^k - 1) = L_q(n, k)$ .

(ii) Using the same notations as in (i), let  $H(k) = GL(n, k)$  ( $k = l, \dots, n$ ) and  $E(k) = G(l, E_q^k)$  be the set of all  $l$ -subspaces in  $E_q^k$  (Grassmann space). For Grassmann spaces, we set  $\lambda = |G(l, E_q^k)|$  and denote  $L(n, k, |G(l, E_q^k)|) = L_q(n, k, l)$ .

(iii) Let  $G_n$  be a complete  $n$ -graph with vertices  $e_1, \dots, e_n$  and  $G_k$  ( $k = l, \dots, n$ ) be a complete subgraph of  $G_n$  with vertices  $e_1, \dots, e_k$ . Then  $E(k)$  is the set of edges of  $G_k$ ,  $H(k)$  is the group of automorphisms of vertices of  $G_k$  such that for  $\forall h \in H(k)$ ,  $h(e_i) = e_i$  ( $i = k+1, \dots, n$ ;  $k = l, \dots, n$ ).

For this case, we set  $l=1$  and  $L(n, k, \lambda) + 1 = f_T(n, k, \lambda)$ . We note that determination of  $f_T(n, k, \lambda)$  is the well-known problem of Turan and values of  $f_T(n, k, \lambda)$  are known only for some special cases [2, 6]. For example,  $f_T(n, 4, 4)$  is an open problem [2].

In Section 3, we shall obtain an upper bound for  $L(n, k, \lambda)$  for the general case of homogeneous spaces which will coincide with lower bounds for  $L(n, k, \lambda)$  for linear spaces, Grassmann spaces with  $l=1$  and some cases of Turan's problem. Since the case of linear spaces is the most interesting for us, we establish, in Section 2, the exact value of  $L_q(n, k)$ , and consider some corollaries from this result. Here we use the direct and shorter proof of the upper bound for  $L_q(n, k)$  due to the referee of this paper.

We note that the main difference between our problem and analogous "Ramsey-type" problems (see, e.g. [3]) is that we are looking for elements from  $G(k, E(n))$  in a given set  $M \subseteq E(n)$  and not in one of two sets ( $M$  and  $E(n) - M$ ).

## 2. Subspaces contained in subsets of linear spaces

In this section, we shall obtain the exact formula for the maximal cardinality  $L_q(n, k)$  of a set  $M \subseteq E_q^n - 0$  such that  $M$  does not contain any  $X_q^k - 0$  where  $X_q^k$  is a  $k$ -subspace of  $E_q^n$ .

**Theorem 2.1.** For  $1 \leq k \leq n$

$$L_q(n, k) = q^n - (q^{n-k+1} - 1)(q - 1)^{-1} - 1. \quad (1)$$

**Proof.** *Lower bound.* We fix  $X_q^{n-k+1}$  and  $M \subseteq E_q^n - 0$  such that for  $\forall X_q^1 \subseteq X_q^{n-k+1}$ ,  $|X_q^1 \cap M| < q - 1$ . Then

$$|M| \leq q^n - (q^{n-k+1} - 1)(q - 1)^{-1} - 1.$$

Now, let  $X_q^r$  be a subspace of maximal dimension such that  $X_q^r - 0 \subseteq M$ . If  $r \geq k$ , then  $\exists X_q^1$  such that  $X_q^1 \subseteq X_q^r \cap X_q^{n-k+1}$  and this contradicts the choice of  $M$ .

*Upper bound.* We use induction on  $k$ . For  $k=1$ , the result is trivial as each  $X_q^1 - 0$  has to contain an element that is not in  $M$ . Suppose, therefore, that

$$L_q(n, k-1) \leq q^n - (q^{n-k+2} - 1)(q - 1)^{-1} - 1.$$

Suppose  $M$  contains no  $X_q^k - 0$ . If  $M$  contains no  $X_q^{k-1} - 0$ , we are done by induction. Let, therefore  $V - 0 \subseteq M$ ,  $V$  is a  $(k-1)$ -dimensional subspace of  $E_q^n$ . Write  $E_q^n = V + W$ . (Direct sum of  $V$  and  $W$ .) For each 1-dimensional subspace  $T$  of  $W$ , choose  $a_T \in T - 0$ . Since  $M$  contains no  $X_q^k - 0$ , for each  $a_T$ , there must be a  $v_T \in V$  and  $\alpha_T \in GF(q) - 0$  such that  $v_T + \alpha_T a_T \notin M$ . If  $v_T + \alpha_T a_T = v_{T'} + \alpha_{T'} a_{T'}$ ,

then  $v_T - v_{T'} = \alpha_{T'} a_{T'} - \alpha_T a_T$ ,  $v_T = v_{T'}$ ,  $\alpha_{T'} a_{T'} = \alpha_T a_T$ ,  $T = T'$ . Hence, there are  $(q^{n-k+1} - 1)(q - 1)^{-1}$  distinct elements  $v_T + \alpha_T a_T \notin M$  and since  $0 \notin M$ , we have (1).

This proof implies the following result.

**Corollary 2.2.** *Let  $M \subset E_q^n - 0$  and  $M$  contains  $X_q^{k-1} - 0$ .*

*If*

$$|M| > q^n - (q^{n-k+1} - 1)(q - 1)^{-1} - 1,$$

*then there exists  $X_q^k$ , such that  $X_q^k - 0 \subseteq M$  and  $X_q^{k-1} \subseteq X_q^k$ .*

If  $M_1 \subseteq M_2 \subseteq \dots \subseteq M_r \subseteq E_q^n - 0$ , we say that  $M^{(r)} = (M_1, \dots, M_r)$  is an  $r$ -flag of sets and if  $X_q^{k_1} \subseteq \dots \subseteq X_q^{k_r}$ , we say that  $X^{(r)} = (X_q^{k_1}, \dots, X_q^{k_r})$  is an  $r$ -flag of spaces. We write  $X^{(r)} - 0 \subseteq M^{(r)}$  if  $X_q^{k_i} - 0 \subseteq M_i (i = 1, \dots, r)$ .

**Corollary 2.3.** *If  $M^{(r)} = (M_1, \dots, M_r)$  is an  $r$ -flag of sets and*

$$|M_i| > q^n - (q^{n-k_i+1} - 1)(q - 1)^{-1} - 1,$$

*then there exists an  $r$ -flag of spaces  $X^{(r)} = (X_q^{k_1}, \dots, X_q^{k_r})$  such that  $X^{(r)} - 0 \subseteq M^{(r)}$ .*

The proof follows immediately from Corollary 2.2.

Let  $E_q^\infty$  be a linear infinite-dimensional space over  $GF(q)$  consisting of all the finite sequences  $E_q^\infty = \{\alpha_1, \dots, \alpha_n, 0, 0, \dots\}$ :  $\alpha_i \in GF(q)$ ;  $i = 1, \dots, n$ ;  $n = 1, 2, \dots$ , and  $E_q^n = \{\alpha_1, \dots, \alpha_n, 0, 0, \dots\}$ :  $\alpha_i \in GF(q)$ ;  $i = 1, \dots, n$  be an  $n$ -dimensional subspace of  $E_q^\infty$ .

**Corollary 2.4.** *If  $M_\infty \subseteq E_q^\infty$  is such that  $0 \in M_\infty$  and  $\lim_{n \rightarrow \infty} \gamma_n = 1$ , where  $\gamma_n = q^{-n} |M_\infty \cap E_q^n| (n = 1, 2, \dots)$ , then there exists an infinite-dimensional space  $E$  such that  $E \subset M_\infty$ .*

**Proof.** It is sufficient to prove that there exists a sequence of numbers  $n_k (n_k < n_{k+1})$  and a sequence of subspaces  $X_q^k \subset E_q^\infty (k = 1, 2, \dots)$ , such that  $X_q^k \subseteq (M_\infty \cap E_q^{n_k})$  and  $X_q^k \subset X_q^{k+1}$ . Then we may put  $E = \bigcup_{k=1}^\infty X_q^k$ . We construct  $\{n_k\}$  and  $\{X_q^k\}$  by induction on  $k$ . Choose  $n_1$  such that  $\gamma_{n_1} > 1 - (q - 1)^{-1} + q^{-n_1}(q - 1)^{-1}$ . Then by Theorem 2.1, there exists  $X_q^1$  such that  $X_q^1 \subseteq (M_\infty \cap E_q^{n_1})$ . Suppose we have found  $n_1 < n_2 < \dots < n_{k-1}$  and  $X_q^1 \subset \dots \subset X_q^{k-1}$  such that  $X_q^i \subseteq (M_\infty \cap E_q^{n_i}) (i = 1, \dots, k - 1)$ . Choose  $n_k > n_{k-1}$  from the condition

$$\gamma_{n_k} > 1 - q^{-k+1}(q - 1)^{-1} + q^{-n_k}(q - 1)^{-1}$$

and by Theorem 2.1, there exists  $X_q^k$  such that  $X_q^{k-1} \subset X_q^k$  and  $X_q^k \subseteq (M_\infty \cap E_q^{n_k})$ .

Let us note that no analogue of this corollary for the case of fields  $R$  or  $C$  is known though it is of a great interest in functional analysis; while Ramsey analogues of Theorem 2.1 are well-known for these fields [4, 5].

### 3. Subspaces contained in subsets of finite homogeneous spaces

In this section, we investigate  $L(n, k, \lambda)$  for the general case of homogeneous spaces (see Section 1).

**Lemma 3.1.** For any  $M \subseteq E(n)$  and  $1 \leq t \leq n$

$$\frac{|M|}{|E(n)|} = \frac{1}{|G(t, E(n))| |E(t)|} \sum_{X \in G(t, E(n))} |X \cap M|. \tag{2}$$

**Proof.** In the sum on the right side of (2), each element of  $M$  is counted as many times as there are  $X \in G(t, E(n))$  which contain this element, i.e.  $|E(t)| |E(n)|^{-1} |G(t, E(n))|$  times.

We note that left and right sides of (2) are equal to the invariant normalized measure of  $M \subseteq E(n)$ ; and (2) follows from uniqueness of this measure on  $E(n)$ .

**Corollary 3.2.** For  $1 \leq k \leq n, 1 \leq \lambda \leq |E(k)|$

$$L(n, k, \lambda) \leq (\lambda - 1) |E(n)| |E(k)|^{-1}. \tag{3}$$

The proof follows from Lemma 3.1 with  $t = k$ .

By  $N(m, k, \lambda)$ , we denote a number of  $X \in G(k, E(n))$  such that for any  $M \subseteq E(n)$  with  $|M| = m$ , we have  $|X \cap M| \geq \lambda$  and we denote  $\mu(m, k, \lambda) = N(m, k, \lambda) |G(k, E(n))|^{-1}$ .

**Corollary 3.3.** For  $1 \leq m \leq |E(n)|, 1 \leq k \leq n, 1 \leq \lambda \leq |E(k)|$

$$(|E(k)| |E(n)|^{-1} m - \lambda + 1) \leq \mu(m, k, \lambda) \leq |E(k)| |E(n)|^{-1} m \lambda^{-1}. \tag{4}$$

**Proof.** By definition of  $\mu(m, k, \lambda)$  and (2) with  $t = k$ ,

$$\begin{aligned} \lambda \mu(m, k, \lambda) &\leq |G(k, E(n))|^{-1} \sum_{X \in G(k, E(n))} |X \cap M| = m |E(k)| |E(n)|^{-1} \\ &\leq (1 - \mu(m, k, \lambda)) (\lambda - 1) + \lambda \mu(m, k, \lambda) \end{aligned} \tag{5}$$

and (4) follows from (5).

**Theorem 3.4.** If for some function  $f(n, k, \lambda)$

$$\lceil |E(k)| |E(k+1)|^{-1} \cdot \dots \cdot \lceil |E(n-1)| |E(n)|^{-1} f(n, k, \lambda) \lceil \dots \lceil \geq \lambda, \tag{6}$$

then

$$L(n, k, \lambda) \leq f(n, k, \lambda) - 1. \tag{7}$$

( $\lceil a \lceil$  denotes the least integer  $\geq a$ ).

**Proof.** Let  $M \subseteq E(n)$  and  $|M| = f(n, k, \lambda)$ . Then by Lemma 3.1 with  $t = n - 1$ ,  $\exists X^{n-1} \in G(n - 1, E(n))$  such that

$$\lceil |E(n-1)| |E(n)|^{-1} f(n, k, \lambda) \lceil \leq |X^{n-1} \cap M|. \tag{8}$$

Next, using (8) and Lemma 3.1 for  $n - 1, M_1 = X^{n-1} \cap M, t = n - 2, \exists X^{n-2} \subseteq X^{n-1}$

$(X^{n-2} \in G(n-2, E(n)))$  such that

$$\begin{aligned} & ]|E(n-2)| |E(n-1)|^{-1}] |E(n-1)| |E(n)|^{-1} f(n, k, \lambda) [ [ \\ & \leq ]|E(n-2)| |E(n-1)|^{-1} |M_1| [ \leq |X^{n-2} \cap M_1| \leq |X^{n-2} \cap M|. \end{aligned}$$

Continuing this procedure for all  $t$  down to  $t = k$ , we find that  $\exists X^k \in G(k, E(n))$  such that

$$] |E(k)| |E(k+1)|^{-1} \dots ] |E(n-1)| |E(n)|^{-1} f(n, k, \lambda) [ \dots [ \leq |X_n^k \cap M|.$$

Hence by (6) and definition of  $L(n, k, \lambda)$ , we have (7).

We note that the upper bound from Theorem 2.1 immediately follows from Theorem 3.4 in a view of

$$\left[ \frac{q^k - 1}{q^{k+1} - 1} \right] \dots \left[ \frac{q^{n-1} - 1}{q^n - 1} \left( q^n - \frac{1}{q-1} (q^{n-k+1} - 1) \right) \right] \dots \left[ \dots \right] = q^k - 1$$

( $q \geq 2, i \leq k \leq n-1$ ).

For the case (ii) of Grassmann spaces  $E(n) = G(l, E_q^n)$  (see Section 1), we have the following bounds for  $L_q(n, k, l)$ .

**Corollary 3.5.** For any  $1 \leq l \leq k \leq n$

$$|G(l, E_q^n)| - |G(l, E_q^{n-k+l})| \leq L_q(n, k, l) \leq |G(l, E_q^n)| - |G(l, E_q^n)| |G(l, E_q^k)|^{-1}$$

(9)

where  $|G(l, E_q^i)| = [i]_q$  is the  $q$ -binomial coefficient,

$$|G(l, E_q^i)| = [i]_q = \prod_{i=0}^{l-1} (q^i - q^i)(q^i - q^i)^{-1}. \tag{10}$$

**Proof.** Define  $M = G(l, E_q^n) - G(l, E_q^{n-k+l})$ . Then  $\dim(X_q^k \cap E_q^{n-k+l}) \geq l$ , for every  $X_q^k \in G(k, E_q^n)$ . So there exists  $X_q^l \subseteq E_q^{n-k+l}, X_q^l \subseteq X_q^k$ . But then  $X_q^l \notin M$  and we have the lower bound from (9). Upper bound follows from Corollary 3.2 with  $E(k) = G(l, E_q^k)$  and  $\lambda = |G(l, E_q^k)|$ .

The difference between the lower and upper bounds (9) is not very large. For example, in the case  $k \rightarrow \infty, n - k \rightarrow \infty$  from (10) follows that for a large  $l$  and  $q$

$$\begin{aligned} \lim_{k \rightarrow \infty, n-k \rightarrow \infty} & |G(l, E_q^n)| |G(l, E_q^k)|^{-1} |G(l, E_q^{n-k+l})|^{-1} \\ & = \prod_{i=0}^{l-1} (1 - q^{-l+i}) \approx \exp(-(q-1)^{-1}). \end{aligned} \tag{11}$$

We note also that by the lower bound (9) and the upper bound from Theorem 3.4, we can establish sometimes the exact value for  $L_q(n, k, l)$ . For example

$$L_q(n, k, 1) = |G(1, E_q^n)| - |G(1, E_q^{n-k+1})| = (q^n - q^{n-k+1})(q-1)^{-1}. \tag{12}$$

We consider now the case (iii) when  $E(n)$  is the set of edges of a complete  $n$ -graph (problem of Turan, see Section 1). Turan [6] proved that if  $n = c(k-1) + r$  ( $c \in \{0, 1, \dots\}$ ,  $r \in \{0, \dots, k-2\}$ ), then

$$f_T\left(n, k, \binom{k}{2}\right) = 0.5(k-2)(k-1)^{-1}(n^2 - r^2) + \binom{r}{2} + 1. \tag{13}$$

We note here that the exact upper bound for  $f_T(n, k, \binom{k}{2})$  follows immediately from Theorem 3.4 since

$$\left] \binom{k}{2} \binom{k+1}{2}^{-1} \right] \cdots \left] \binom{n-1}{2} \binom{n}{2}^{-1} \left( \frac{k-2}{2(k-1)} (n^2 - r^2) + \binom{r}{2} + 1 \right) \left[ \cdots \left[ \left[ = \binom{k}{2}. \tag{14}$$

Other examples are given by formulas [4]:

$$f_T(n, k, [0.25k^2] + u) = [0.25n^2] + u \quad (u \leq [0.25(k+1)]), \tag{15}$$

$$f_T(n, k, [0.25k^2] + [0.5(k-1)]) = [0.25n^2] + [0.5(n-1)] \quad (k > 4) \tag{16}$$

([a] the greatest integer  $\leq a$ ). The exact upper bounds from (15) and (16) also follow from Theorem 3.4.

We shall give now one more corollary from Theorem 3.4 which may be useful for determination of  $f_T(n, k, \lambda)$ .

**Corollary 3.6.** Let  $f(n, k, \lambda) = L(n, k, \lambda) + 1$ . For any  $1 \leq s \leq k \leq n$ ,  $0 < \lambda \leq |E(s)|$

$$f(n, k, f(k, s, \lambda)) \geq f(n, s, \lambda) \tag{17}$$

and, if for all  $t \in \{k+1, \dots, n\}$

$$\left] |E(t-1)| |E(t)|^{-1} f(t, s, \lambda) \right[ = f(t-1, s, \lambda), \tag{18}$$

then

$$f(n, k, f(k, s, \lambda)) = f(n, s, \lambda). \tag{19}$$

**Proof.** Formula (17) follows from the definition of  $f(n, k, \lambda)$ . Let  $M \subseteq E(n)$  and  $|M| = f(n, s, \lambda)$ . Then as it was shown in the proof of Theorem 3.4,  $\exists X^k \in G(k, E(n))$  such that

$$\left] |E(k)| |E(k+1)|^{-1} \right] \cdots \left] |E(n-1)| |E(n)|^{-1} f(n, s, \lambda) \right[ \cdots \left[ \leq |X^k \cap M|$$

and in a view of (18)

$$f(k, s, \lambda) \leq |X^k \cap M|.$$

Hence,

$$f(n, k, f(k, s, \lambda)) \leq f(n, s, \lambda)$$

and by (17) we have (19).

By Corollary 3.6 with  $s = 4$ ,  $\lambda = 6$  and (13) we have, for example,

$$f_T(n, 5, 9) = f_T(n, 6, 13) = f_T(n, 7, 17) = 3^{-1}(n^2 - r^2) + \binom{r}{2} + 1 \quad (20)$$

where  $0 \leq r \leq 2$ ,  $n \equiv r \pmod{3}$ .

#### 4. Sufficient conditions for existence of linear error-correcting codes with given parameters

Let  $\rho(x, y)$  be a metric in  $E_q^n$ . A linear  $(n, k)$ -code with base  $q$  and distance  $d$  in the metric  $\rho$  is defined as a subspace  $X_q^k$  such that  $\min_{a, b \in X_q^k} \rho(a, b) = d$ .

**Theorem 4.1.** For any  $n, k < n$ , and any  $Q \subseteq E_q^n (0 \in Q)$ , a sufficient condition for the existence of an  $(n, k)$ -code  $X_q^k$  with base  $q$ , distance  $d$  in the metric  $\rho$ , such that  $X_q^k \subseteq Q$ , is that

$$|Q - \{a: \|a\|_\rho < d\}| \geq q^n - (q-1)^{-1}(q^{n-k+1} - 1) \quad (\|a\|_\rho = \rho(a, 0)). \quad (21)$$

**Proof.** A subspace  $X_q^k$  is an  $(n, k)$ -code with distance  $d$  in the metric  $\rho$  iff  $X_q^k \cap \{a: \|a\|_\rho < d\} = 0$ . We therefore set  $M = Q - \{a: 0 < \|a\|_\rho < d\}$ . Then  $|M| = 1 + |Q - \{a: \|a\|_\rho < d\}|$ , and by Theorem 2.1, if (21) holds, there exists an  $(n, k)$ -code  $X_q^k \subseteq Q$  with distance  $d$ .

Theorem 4.1 yields sufficient conditions for  $(n, k)$ -codes  $X_q^k$  satisfying constraints of the type  $X_q^k \subseteq Q$ . For example, let  $Q = \{a: \|a\|_\rho \leq d + \varepsilon\}$ , where  $\rho$  is the Hamming metric [1].

**Corollary 4.2.** For any  $n$  and  $k < n$ , a sufficient condition for the existence of an  $(n, k)$ -code  $X_q^k$  with base  $q$  and distance  $d$  in the Hamming metric  $\rho$ , such that

$$\max_{a, b \in X_q^k - 0} |(\|a\|_\rho - \|b\|_\rho)| \leq \varepsilon,$$

is that

$$\sum_{i=d}^{d+\varepsilon} \binom{n}{i} (q-1)^i \geq q^n - (q^{n-k+1} - 1)(q-1)^{-1}. \quad (22)$$

**Proof.** Set  $Q = \{a: \|a\|_\rho \leq d + \varepsilon\}$ ; then

$$|Q - \{a: \|a\|_\rho < d\}| = |\{a: d \leq \|a\|_\rho \leq d + \varepsilon\}| = \sum_{i=d}^{d+\varepsilon} \binom{n}{i} (q-1)^i,$$

and by Theorem 4.1 there exists an  $(n, k)$ -code  $X_q^k \subseteq Q$  with distance  $d$ , such that for any  $a \in X_q^k$  we have  $d \leq \|a\|_\rho \leq d + \varepsilon$ .

Note that in the case  $\varepsilon = n - d$  the condition (22) is very close to the well-known Varshamov-Gilbert bound [1].

**Note added in proof**

It came to our attention that the upper bound for  $L_q(n, k)$  also appeared in the paper by M. Deza and F. Hoffman, IEEE Int. Trans. (July 1977) 517-518.

**References**

- [1] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York 1968).
- [2] P. Erdős, Extremal problems in graph theory, in: Proc. Symp. on The Theory of Graph and its Applications, Smolenice, June (1963).
- [3] R.L. Graham and B.L. Rothschild, Ramsey's theorem for  $n$ -parameter sets, Trans. Am. Math. Soc. 159 (1971) 257-292.
- [4] V.D. Milman, A new proof of the theorem of A. Dvoretzky on sections of convex bodies, Functional Anal. Appl. 5 (1971) 28-37 (translated from Russian).
- [5] V.D. Milman, Asymptotic property of function of several variables, defined on homogeneous spaces, Dokl. Acad. Sci. USSR 199 (1971). (translated in: Soviet Math. Dokl. 12 (1971) 1277-1281).
- [6] P. Turan, On the Theory of Graphs, Colloq. Math. 3 (1954) 19-30.