Multiple packing in sum-type metric spaces

Rudolf Ahlswede and Vladimir Blinovsky

Abstract

We present the exact solution of the asymptotics of the multiple packing problem in a finite space with a sum-type metric. [1]

Consider the space Q^n of $n-$tuples over a finite set $Q = [q] = \{1, 2, \dots, q\}$ (by standard convention in Combinatorics) and a sum-type metric $d(x, y) = \sum_{i=1}^n d(x_i, y_i)$, $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, x_n)$. Let $B_n(x, r) := \{y \in Q^n : d(x, y) \le r\}$ be the ball of radius r in Q^n with the center in y. We say that a subset $\mathcal{A}_n \subset Q^n$ is an $L-$packing by the balls of radius r if

$$\max_{x \in Q^n} \left| B_n(x, r) \bigcap \mathcal{A}_n \right| \le L$$

or equivalently for an arbitrary set of $L + 1$ $n-$tuples $\{u_1, \dots, u_{L+1}\} \subset \mathcal{A}_n$

$$\bigcap_{j=1}^{L+1} B_n(u_j, r) = \emptyset.$$

We refer to papers [1-6] as literature about different properties and asymptotics of $L-$packings. $L-$packing finds applications in coding theory. Adopting the terminology from there we can consider the model when $n-$tuples from the set $\mathcal{A}_n$ are transmitted over the channel where up to t errors can occur (up to t coordinates of the output $y \in Q^n$ of the channel differ from the corresponding coordinates of the input $x \in \mathcal{A}_n$). In such a case there exist not more than L $n-$tuples from $\mathcal{A}_n$ at a distance less than $t + 1$ from the output of the channel $y \in Q^n$ and the transmitted $n-$tuple $x \in \mathcal{A}_n$ is among them. In this case we can decode the output of the channel into the list of not more than L codewords (elements of the code $\mathcal{A}_n$) such that the transmitted codeword x is among them i.e. realize the list–of–L decoding without error. More about the applications of list decoding one can find in [7]. Here we generalize the

[1] This work was partially supported by RFFI grants No 3-01-00592 and 03-01-00098 and INTAS grant No 00-738

work [6], where the Hamming metric was considered, to arbitrary sum-type metrics.

At a recent meeting in Valdivia (Chile) Guruswami pointed out that the results presented in this paper and results of earlier papers by Blinovsky ([2-6]) are the only exceptions of essential progress on list decoding bounds - a subject which through the work of Sudan in Coding Theory has become a very fruitful area in algorithms. There fortunately asymptotic ratewise optimality is presently often not needed. But definitely progress like in the present paper with a new setting via the general distance functions likely has an impact. Another application of this work can be found in [13]. There is also a close connection between list code problems and search.

We are interested in the case where for the sequence $(\mathcal{A}_n)_{n=1}^{\infty}$ $R_n = \frac{\ln|\mathcal{A}_n|}{n} \to 0$ and $M_n = |\mathcal{A}_n| \to \infty$ as $n \to \infty$. We call this case the zero rate case applying the terminology from coding theory where R_n is called the rate of the code $\mathcal{A}_n$. Also, we call such a sequence $(M_n)_{n=1}^{\infty}$ a zero rate sequence.

The restriction to the zero rate case concerns not the lower bound but the upper bound only, where we presently cannot – and it seems nobody else can – do better for the non-zero rate case.

For establishing the property that $L+1$ different points $(u_1, \ldots, u_{L+1}) \subset Q^n$ are an $L-$packing we follow [6] and introduce the moment inertia I_n of these $L+1$ points by the equation

$$I_n(u_1, \ldots, u_{L+1}) = \frac{1}{L+1} \min_{y \in Q^n} \sum_{j=1}^{L+1} d(y, u_j) = \frac{1}{L+1} \sum_{i=1}^{n} \min_{y_i \in Q} \sum_{j=1}^{L+1} d(y_i, u_{ji}). \quad (1)$$

A point $y \in Q^n$, which is an $\arg\min$ of the RHS, is called a center of inertia. Note that in general y is not unique.

If we denote

$$t_n(u_1, \ldots, u_{L+1}) = \max \left\{ r : \bigcap_{j=1}^{L+1} B_n(u_j, r) = \emptyset \right\},$$

then the following inequality can be easily verified

$$I_n(u_1, \ldots, u_{L+1}) \leq t_n(u_1, \ldots, u_{L+1}) + 1. \quad (2)$$

It means that the intersection of $L+1$ balls of radius $I_n(u_1, \ldots, u_{L+1}) - 1$ with the centers in $u_1, \ldots, u_{L+1}$ is empty and hence the set $\{u_1, \ldots, u_{L+1}\}$ is an $L-$packing (by the balls of radius $I_n(u_1, \ldots, u_{L+1}) - 1$). Let now

$$t_n^*(M_n) = \max\left\{ r : \exists \mathcal{A}_n \subset Q^n,\ |\mathcal{A}_n| = M_n, \forall y \in Q^n \left| B_n(y,r) \bigcap \mathcal{A}_n \right| \le L \right\},$$

$$I_n^*(M_n) = \max\{ r : \exists \mathcal{A}_n \subset Q^n,\ |\mathcal{A}_n| = M_n, \forall \{u_1, \ldots, u_{L+1}\} \subset \mathcal{A}_n,$$
$$u_i \ne u_j,\ i \ne j,\ I_n(u_1, \ldots, u_{L+1}) \ge r \}.$$

Denote for zero rate sequences $(M_n)_{n=1}^\infty$

$$\tau = \sup_{(M_n)_{n=1}^\infty} \limsup_{n \to \infty} \frac{t_n^*(M_n)}{n}, \rho = \sup_{(M_n)_{n=1}^\infty} \limsup_{n \to \infty} \frac{I_n^*(M_n)}{n}.$$

We write in short

$$\tau = \limsup_{M_n \to \infty} \frac{t_n^*(M_n)}{n}, \rho = \limsup_{M_n \to \infty} \frac{I_n^*(M_n)}{n}.$$

For the partition $j_1 + \ldots + j_q = L + 1,\ j_k \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$ let

$$f(j_1, \ldots, j_q) = \frac{1}{L+1} \min_{x \in Q} \sum_{y=1}^q j_s d(x,y). \tag{3}$$

The main purpose of this work is to determine τ exactly. The reason that we deal with the zero rate case only is that we are not able to find the proper upper bound for the rate R as a function of τ. At the same time the zero rate case is the first important non–trivial case of this problem: the value in the following (4), which is the exact value of τ at zero rate is the upper bound for τ at all rates. Note that we find (Theorem 2) the lower bound $\tau = \tau(R)$ for arbitrary rate $R \in [0,1]$, not only for zero rate. We formulate the main result.

Theorem 1

$$\tau = \varphi(L) := \max_{\substack{\lambda \in [0,1]^q: \\ \sum_{x=1}^q \lambda_x = 1}} \sum_{\substack{j_1, \ldots, j_q \in \mathbb{N}_0: \\ \sum_{x=1}^q j_x = L+1}} f(j_1, \ldots, j_q) \binom{L+1}{j_1, \ldots, j_q} \prod_{x=1}^q \lambda_x^{j_x}. \tag{4}$$

In the case of the Hamming metric it was shown in [6] that

$$\tau = \frac{1}{q^{L+1}} \sum_{j_1, \ldots, j_q \in \mathbb{N}_0 : \sum_{x=1}^q j_x = L+1} \left(1 - \frac{\max\{j_1, \ldots, j_q\}}{L+1} \right) \binom{L+1}{j_1, \ldots, j_q}.$$

It was shown in [2] (see also [3]) in the binary Hamming case that

$$\tau = \frac{1}{2} \left(1 - \frac{\binom{L}{\lceil \frac{L}{2} \rceil}}{2^L} \right).$$

It is interesting that in this case the value of τ for odd and next even values of L coincide. Note also that for Hamming metric it is possible to find the natural upper bounds for the rate R as the function of τ, not only at zero rate. The same we are able to do here in the case of a general sum–type metric.

The proof of Theorem 1 consists of several parts. First we prove the lower bound on ρ, which due to the relation (2) is a lower bound for τ. Then we will prove the upper bound for ρ. At last we will prove that this upper bound for ρ is still valid for τ. All these results are stated in the following lemmas.

Lemma 1 *The following relation is valid*

$$\rho \geq \varphi(L). \tag{5}$$

Lemma 2 *The following relation is valid*

$$\rho \leq \varphi(L). \tag{6}$$

Lemma 3 *The following relation is valid*

$$\tau \leq \varphi(L). \tag{7}$$

The proof of Lemma 1 we will give by the method of random choice with expurgation (about this method see for ex. [3], [9]). Consider the matrix of size $(L+1) \times n$ with symbols from Q which are chosen independently and with probability $P(x) = \lambda_x$, where $\{\lambda_x\}$ are values on which the maximum in (4) is achieved. Let $u_1, \ldots, u_{L+1}$ be $L+1$ rows of this matrix of length n. Then the average value of the moment inertia $EI_n(U_1, \ldots, U_{L+1})$, where $U_j = (U_{j1}, \ldots, U_{jn})$ is the random variable taking values $u_j = (u_{j1}, \ldots, u_{jn}) \in Q^n$, satisfies the relation

$$EI_n(U_1, \ldots, U_{L+1}) = n\varphi(L).$$

Now because

$$I_n(U_1, \ldots, U_{L+1}) = \sum_{i=1}^{n} I_1(U_{1i}, \ldots, U_{(L+1)i}) \text{ for } I = I_1$$

and variables $I_1 = I(U_{1i}, \ldots, U_{(L+1)i})$, $i = 1, \ldots, n$, are independent identically distributed random variables, we can apply the Chernoff bound to estimate the large deviation of the sum I_n of i.i.d. random variables from its mean value:

$$\begin{aligned} &P\left(I_n < n\rho = E(I_n) - \epsilon n\right) < E(\exp(-hI_n)) \exp(hn\rho) \\ &= \exp\left(n \ln(E(\exp(-hI_1))) + hn\rho\right) := \exp(n\delta(h, \rho)), h \geq 0, \end{aligned} \tag{8}$$

(The first line in (8) is exactly the Chernoff bound. More about such estimations one can find in [10]). Then consider the new matrix of size $M_n \times n$ whose elements are independently chosen from Q with distribution $P(x) = \lambda_x,\ x \in Q$. We say that the subset of different rows $u_{i_1}, \ldots, u_{i_{L+1}}$ of the matrix is bad if $I_n(u_{i_1}, \ldots, u_{i_{L+1}}) < n\rho$. According to (8) the average number of bad sets is less than

$$(M_n)^{L+1} \exp(n\delta(h,\rho)). \tag{9}$$

Hence if we choose one matrix with the number of bad sets less than the average and expurgate one vector from each bad subset of rows we obtain a matrix without bad subsets of rows. In order to expurgate the number of rows such that the whole number of rows does not decrease too much we impose the condition that the whole number of bad sets is less than $M_n/2$. This condition, using (9), can be expressed as

$$(M_n)^{L+1} \exp(n\delta(h,\rho)) < M_n/2. \tag{10}$$

It sets the restrictions on the possible values of M_n and ρ (for given h). Next we obtain the asymptotic representation of the inequality (10) which guarantees that this inequality is satisfied. Taking ln from both sides of this inequality we obtain the relation

$$\frac{\ln M_n}{n} + \frac{1}{L}\delta(h,\rho) \le o(1),\ \ M_n \to \infty. \tag{11}$$

If $M_n = [\exp(nR)]$, then we have the asymptotic relation

$$R = -\frac{1}{L}\delta(h,\rho).$$

Optimization of the RHS of the last relation over $h \ge 0$ (we put the derivative $\delta'_h(h,\rho) = 0$) gives the relations

$$\begin{aligned} R &= -\frac{1}{L}\left(h\rho + \ln Ee^{-hI_1}\right), \\ \rho &= \frac{E\left(I_1 e^{-hI_1}\right)}{Ee^{-hI_1}}. \end{aligned} \tag{12}$$

It is easy to calculate the mathematical expectations from the last formulas:

$$Ee^{-hI_1} = \sum_{(j_1,\dots,j_q):\sum_{x=1}^q j_x = L+1} e^{-hf(j_1,\dots,j_q)} \binom{L+1}{j_1 \dots j_q} \prod_{x=1}^q \lambda_x^{j_x} \tag{13}$$

$$E\left(I_1 e^{-hI_1}\right) = \sum_{(j_1,\dots,j_q):\sum_{x=1}^q j_x = L+1} f(j_i,\dots,j_q) e^{-hf(j_1,\dots,j_q)} \binom{L+1}{j_1 \dots j_q} \prod_{x=1}^q \lambda_x^{j_x}.$$

Substituting (13) into (12) we obtain the asymptotic bounds $R(\rho)$ in parametrical form. Obviously these bounds are lower bounds and as we mentioned before they are still valid if we substitute τ for ρ. We establish the lower bound $R = R(\tau)$ (or $\tau = \tau(R)$) in the following

Theorem 2 *The asymptotic lower bound in parametrical form (12) is valid (with parameter h and $\rho = \tau$), where Ee^{-hI_1} and $E\left(I_1 e^{-hI_1}\right)$ are determined by the equations (13).*

The bound (12) is general and to reach the particular case we are interested in, it is necessary to put $R = 0$. In this case we achieve the largest possible value of ρ (or τ) and still are in the limiting situation where $M_n \to \infty$. It is easy to see that in this case it is necessary to put $h = 0$ and obtain

$$\tau \geq EI_1 = \sum_{(j_1,\dots,j_q):\sum_{x=1}^q j_x = L+1} f(j_1,\dots,j_q) \binom{L+1}{j_1 \dots j_q} \prod_{x=1}^q \lambda_x^{j_x}. \tag{14}$$

This proves Lemma 1.

To obtain an upper bound on ρ we use Plotkin's method. Briefly this method consists in the following: the minimal value of some function of vectors over some set of vectors estimated from above by the average of this function over the choice of these vectors. Then due to the additivity property of the function over coordinates of vectors we can write the average componentwise and then find the maximum of the average in each component over the choice of elements from Q. More about Plotkin's technique one can find in [3], [11]. Now we apply Plotkin's method in our case. Consider the matrix of size $M_n \times n$ with elements from Q. The minimal moment inertia

$$I_n^{\min} = \min_{j_1,\dots,j_{L+1} \in [M_n]} I_n(u_{j_1},\dots,u_{j_{L+1}})$$

does not exceed the average moment inertia $< I_n >$ over choosing vectors $u_{j_1},\dots,u_{j_{L+1}}$,

$$I_n^{\min} \leq < I_n > = \frac{1}{\binom{M_n}{L+1}} \sum_{j_1,\dots,j_{L+1},\ j_m \neq j_{m'}, m \neq n'} I_n(u_{j_1},\dots,u_{j_{L+1}}).$$

At the same time, due to the additivity property of the metric, the sum in the RHS of this inequality can be decomposed into the sum of n coordinate sums:

$$\sum_{\substack{j_1,\dots,j_{L+1},\ j_{m'}\neq j_m,\\ m'\neq m}} I_n(u_{j_1},\dots,u_{j_{L+1}}) = \sum_{i=1}^{n} \sum_{\substack{j_1,\dots,j_{L+1},\ j_{m'}\neq j_m,\\ m'\neq m}} I_1(u_{j_1,i},\dots,u_{j_{L+1},i})$$

Let $g_i(k)$ be the number of times one meets symbol k in the i-th column of the matrix. Then the following relation can be easily verified:

$$\sum_{\substack{j_1,\dots,j_{L+1},\\ j_{m'}\neq j_m,\ m'\neq m}} I_1(u_{j_1,i},\dots,u_{j_{L+1},i}) = \sum_{j_1,\dots,j_q:\ \sum j_k=L+1} f(j_1,\dots,j_q)\prod_{k=1}^{q}\binom{g_i(k)}{j_k}. \tag{15}$$

Dividing the last sum by $\binom{M_n}{L+1}$ and using relations

$$\binom{a}{b} < \frac{a^b}{b!},\ \binom{a}{b} = \frac{a^b}{b!}(1+o(1))$$

as $a\to\infty,\ b=const$ we obtain the asymptotic inequality

$$\begin{aligned} < I_1 > &= \frac{1}{\binom{M_n}{L+1}} \sum_{j_1,\dots,j_{L+1},\ j_{k'}\neq j_k,\ k'\neq k} I_1(u_{j_1,i},\dots,u_{j_{L+1},i}) \qquad (16)\\ &= \sum_{j_1,\dots,j_q:\ \sum j_k=L+1} f(j_1,\dots,j_q)\binom{L+1}{j_1\dots j_q}\prod_{k=1}^{q}(\kappa_i(k))^{j_k}(1+o(1)) \end{aligned}$$

where $\kappa_i(k)=\frac{g_i(k)}{M_n}$. Now from (16) it follows that

$$\rho \le \max_{\{\kappa_i(k)\}:\ \sum_{k=1}^{q}\kappa_i(k)=1} \sum_{j_1,\dots,j_q:\ \sum j_k=L+1} f(j_1,\dots,j_q)\binom{L+1}{j_1\dots j_q}\prod_{k=1}^{q}(\kappa_i(k))^{j_k}. \tag{17}$$

This proves Lemma 2.

To prove Lemma 3 we need an involved technique. First we need Ramsey's Theorem. We next formulate the version of this theorem adapted to our purposes and for further information refer to [8]. $k-$uniform hypergraphs are those for which all edges contain k vertices. The complete $k-$uniform hypergraph with n vertices contains all $\binom{n}{k}$ edges.

Theorem 3 (Ramsey) *Let r and Z be positive integers. There exists n_0 such that for $n > n_0$ a $k-$uniform complete hypergraph with n vertices, whose edges* *are colored by Z numbers, contains a monochromatic complete subhypergraph with $n' > r$ vertices.*

The scheme of the proof is as follows. First we consider the $(L+1)$-uniform hypergraph $\mathcal{G}$ on M_n vertices of which all are vectors from some set $\mathcal{M}_n \subset Q^n$ and $|\mathcal{M}_n| = M_n \overset{n\to\infty}{\to} \infty$. Edges of this hypergraph are all subsets of $L+1$ vectors from $\mathcal{M}_n$. Using Ramsey's Theorem we extract from this hypergraph a subhypergraph such that for each sequence $(q_1, \ldots, q_{L+1}) \in Q^{L+1}$ all $L+1$ ordered vertices of this subhypergraph have the same up to $o(n)$ as $M_n \to \infty$ number of positions, where this sequence occurs. Then we will show that this is sufficient for the same property to be satisfied for non–ordered $L+1$ vertices from the subhypergraph. At last we will show that for such hypergraphs moment inertia of arbitrary $L+1$ vectors asymptotically coincide with the maximal radius of an $L-$packing of these vectors. The important thing is that after all these transformations of the initial set $\mathcal{M}_n$ we obtain a set whose cardinality still goes to infinity as $M_n \to \infty$. Now applying Lemma 2 to this set we obtain the upper bound for ρ and hence for τ of this set. Since the initial set has a τ only smaller than the obtained set, we can state that the initial set also satisfies the bound from (3) with τ instead of ρ. This proves Lemma 3.

Now we will realize our plan. Let $(\mathcal{M}_n)_{n=1}^{\infty}$ be the sequence of subsets from Q^n and $M_n \overset{n\to\infty}{\to} \infty$. First we order once and arbitrarily each set $\mathcal{M}_n$. Fix some ordered set $(q_1, \ldots, q_{L+1}) \in Q^{L+1}$ whose elements can repeat. For the arbitrarily ordered subset $(u_1, \ldots, u_{L+1}) \subset \mathcal{M}_n$ we denote by

$$T_{(q_1,\ldots,q_{L+1})}(u_1, \ldots, u_{L+1})$$

the number of positions i where $(u_{1i}, \ldots, u_{(L+1)i}) = (q_1, \ldots, q_{L+1})$. Dividing all such T by n we obtain values form interval $[0, 1]$. We divide this interval into S equal subintervals of length $1/S$. Then we number these intervals by the numbers $1, \ldots, S$ and color every edge $(u_1, \ldots, u_{L+1})$ of the hypergraph according to the number of the interval Δ_S such that

$$\frac{1}{n} T_{(q_1,\ldots,q_{L+1})}(u_1, \ldots, u_{L+1}) \in \Delta_S.$$

We call $\left(\frac{1}{n} T_{(q_1,\ldots,q_{L+1})}(u_1, \ldots, u_{L+1})\right)_{(q_1,\ldots,q_{L+1} \in Q^{L+1}}$ the type of the set $(u_1, \ldots, u_{L+1})$. If $M_n \to \infty$ then by Ramsey's Theorem we can extract a complete subhypergraph on ordered vertices such that for all ordered sets of $L+1$ edges $(u_1, \ldots, u_{L+1})$ from this hypergraph, $\frac{1}{n} T_{(q_1,\ldots,q_{L+1})}(u_1, \ldots, u_{L+1})$ belongs to the same interval δ. Note that for this extracted subhypergraph we still have for the number of edges $M_{1_n} \to \infty$. Moreover, if we let $S \to \infty$ sufficiently slowly, then we can preserve the property $M_{1_n} \to \infty$. Next we do this procedure for all ordered sets $(q_1, \ldots, q_{L+1})$ and receive a sequence of hypergraphs such that for an arbitrarily ordered set of vertices $(u_1, \ldots, u_{L+1})$ in the given hypergraph the interval Δ such that $\frac{1}{n}T_{(q_1,\ldots,q_{L+1})}(u_1,\ldots,u_{L+1}) \in \Delta$ does not depend on the choice of $(u_1,\ldots,u_{L+1})$ (but can depend on the choice of the hypergraph in the sequence). Hence all $\frac{1}{n}T_{(q_1,\ldots,q_{L+1})}(u_1,\ldots,u_{L+1})$ are equal for different $(u_1,\ldots,u_{L+1})$ up to $1/S = o(1)$.

Then we will show that, if for all ordered sets of vectors $(u_1,\ldots,u_{L+1})$ the values

$$\frac{1}{n}T_{(q_1,\ldots,q_{L+1})}(u_1,\ldots,u_{L+1})$$

coincide up to $o(1)$, then

$$T_{(q_1,\ldots,q_{L+1})}(u_1,\ldots,u_{L+1}) = T_{(\sigma(q_1),\ldots,\sigma(q_{L+1}))}(u_1,\ldots,u_{L+1}) + o(n).$$

Here σ is an arbitrary permutation of $(q_1,\ldots,q_{L+1})$. In words it is as follows: $\frac{1}{n}T_{(q_1,\ldots,q_{L+1})}(u_1,\ldots,u_{L+1})$ up to $o(1)$ depends only on the non–ordered set $(q_1,\ldots,q_{L+1})$.

It is not difficult to deduce that if the type has such a property, then the distance from the center of inertia $y(u_1,\ldots,u_{L+1})$ (if the center of inertia is not unique, then we make a special choice of it, as can be seen below) to the arbitrary vector $u \in \{u_1,\ldots,u_{L+1}\}$ does not depend (up to $o(n)$) on the choice of u i.e. the center of inertia asymptotically coincides with the center of the ball of minimal radius such that it contains all $L+1$ points $(u_1,\ldots,u_{L+1})$. From this property immediately follows that $I_n(u_1,\ldots,u_{L+1}) = t_n(u_1,\ldots,u_{L+1}) + o(n)$. Note that similar considerations where made in [6], [3], see also [4].

Introduce the following result of Komlos [12].

Lemma 4 *Let α_j and β_j, $j = 1,\ldots,M$, be square integrable functions under the probability measure P such that*

$$\left| \int \alpha_{j_1}\beta_{j_2}dP - r(j_1,j_2) \right| < \delta,$$

and

$$\max_j ||\alpha_j||_2 = \max_j ||\beta_j||_2 \le 1.$$

Then

$$|r(j_1,j_2) - r(j_2,j_1)| < \frac{6}{\sqrt{M}} + 6\sqrt{\delta} + 2\delta. \tag{18}$$

Actually we need a generalization of this lemma to the case of $L+1$ variables $\{\alpha_{j_1}(x_1),\ldots,\alpha_{j_{L+1}}(x_{L+1})); j_k \in [M_n], x_j \in [q]\}$ on $[n]$. In our case $\alpha_j(x)$ is the indicator function of the set of positions, where vector number j in ordered set of M_n vectors has symbol x. Also we do not need an estimate as precise as on the RHS of (18). It is enough for us that the rest term can be chosen such that it tends to zero as $M_n \to \infty$. For the finite ordered set $(q_1,\ldots,q_{L+1}) \in Q^{n+1}$ let

$(\sigma(q_1), \ldots, \sigma(q_{L+1}))$ be some transposition of this set. We have the following result.

Lemma 5 *If*

$$\left| \int \alpha_{j_1}(q_1) \cdot \ldots \cdot \alpha_{j_{L+1}}(q_{L+1}) dP - r(q_1, \ldots, q_{L+1}) \right| \to 0$$

as $M_n \to \infty$, *then*

$$|r(q_1, \ldots q_{L+1}) - r(\sigma(q_1), \ldots, \sigma(q_{L+1}))| \to 0.$$

i.e. r is asymptotically a symmetric function. Here P is the uniform distribution on the set of positions $\{1, \ldots, n\}$.

Proof Lemma 5. Denote by $\alpha_j(x)$ the indicator function of the positions, where vector u_j has symbol $x \in [q]$. From the Komlos Lemma follows that if the types of ordered pairs of vectors u_{j_1}, u_{j_2}, $j_1 < j_2$ asymptotically do not depend on the choice of this ordered pair, then the types of the arbitrary pair of vectors are symmetric functions and coincide (asymptotically). In these considerations we assume that the probability measure P is the uniform distribution on the set of n coordinates of the vectors.

Note that it is enough to prove the lemma only for permutations which fix the first $L-1$ elements $(q_1, \ldots, q_{L-1})$ and permutate the last two elements (q_L, q_{L+1}). Also we can assume that $u_{j_k} = u_j$. To prove Lemma 5 instead of the uniform distribution on the set of n coordinates we consider the distribution $(T_{(q_1, \ldots, q_{L-1})}(u_1, \ldots, u_{L-1}) \neq 0)$

$$\omega_{q_1, \ldots, q_{L-1}}(x) = \frac{\alpha_1(q_1), \ldots, \alpha_{L-1}(q_{L-1})}{T_{(q_1, \ldots, q_{L-1})}(x_1, \ldots, x_{L-1})}.$$

If $T_{(q_1, \ldots, q_{L-1})}(u_1, \ldots, u_{L-1}) = 0$, then

$$T_{(q_1, \ldots, q_{L-1}, q_L, q_{L+1})}(u_1, \ldots, u_{L-1}, u_{j_L}, u_{j_{L+1}}) = 0$$

for all $q_L, q_{L+1} \in Q$. We can apply Lemma 4 to this distribution and for the pair $(\alpha_{j_L}(q_L), \alpha_{j_{L+1}}(q_{L+1}))$ and obtain the relations

$$\left| \int \alpha_{j_L}(q_L) \alpha_{j_{L+1}}(q_{L+1}) d\omega - r(q_L, q_{L+1}) \right| = o(1). \tag{19}$$

We note that the range of possible values of j_L, j_{L+1} is $[L, M_n - 1]$ and $[L+1, M_n]$ correspondingly. The number of elements in each such set go to infinity as $M_n \to \infty$. Hence by Lemma 4

$$|r(q_L, q_{L+1}) - r(q_{L+1}, q_L)| = o(1) \tag{20}$$

and from (19) and (20) follows the relation

$$\Big|\int \alpha_{j_L}(q_L)\alpha_{j_{L+1}}(q_{L+1})\alpha_1(q_1)\dots\alpha_{L-1}(q_{L-1})dP -$$
$$\int \alpha_{j_L}(q_{L+1})\alpha_{j_{L+1}}(q_L)\alpha_1(q_1)\dots\alpha_{L-1}(q_{L-1})dP\Big| = o(1) \qquad (21)$$

Here P is once more the uniform distribution on the set of positions $1,\dots,n$. This proves Lemma 5.

To complete the proof of Lemma 3 we have to show that if for any $u_{i_1},\dots,u_{i_{L+1}} \in \mathcal{M}_n$ $T_{(q_1,\dots,q_{L+1})}(u_{i_1},\dots,u_{i_{L+1}})$ is asymptotically symmetric in $q_1,\dots,q_{L+1} \in Q$, then the center of inertia of the points $(u_{i_1},\dots,u_{i_{L+1}})$ coincides asymptotically with the center of the ball of minimal radius containing these $L+1$ points and in turn this radius is equal asymptotically to the moment of inertia $I_n(u_{i_1},\dots,u_{i_{L+1}})$. Precisely the last assertion is not true! Next we will show how to choose the center of inertia (it can be not a unique choice) in order to make our consideration valid.

We say that the word $(q_1,\dots,q_{L+1}) \in Q^{L+1}$ has composition $(k_1,\dots k_q)$ if the number of occurrences of symbol $x \in Q$ in the this word is equal to k_x. Write vectors $u_{i_1},\dots,u_{i_{L+1}}$ in the rows of a matrix of size $(L+1)\times n$. Then the columns of the matrix are words $(q_1,\dots,q_{L+1})$. Note that for a given $(q_1,\dots,q_{L+1}) \in Q^{L+1}$ such that symbol a is among elements $q_1,\dots,q_{L+1}$ exactly k_a times, we have (possibly) a not unique element $y_i \in Q$ which is arg min of the RHS of (1). We will choose the same value $y_i \in Q$ for all positions i such that the column of the matrix corresponding to this position is the permutation of $(q_1,\dots,q_{L+1})$. Since the number of positions with given column $(q_1,\dots,q_{L+1})$ is asymptotically equal to the number of positions, whose column is an arbitrary given permutation of $(q_1,\dots,q_{L+1})$, we conclude that every point u_{i_j} has each symbol from $\{q_1,\dots,q_{L+1}\}$ in the position with given composition asymptotically the same number of times, which does not depend on the choice of u_{i_j}. Hence the contribution to the distance $d(y,u_{i_j})$ from the positions with column of composition $(k_1,\dots,k_q)$ asymptotically does not depend on the choice of u_{i_j} and from this follows that distances $d(y,u_{i_j})$ are asymptotically the same for different u_{i_j}.

Therefore we have the sets of growing size such that arbitrary $L+1$ points from this set asymptotically lie on the sphere with the center in the center of inertia of these points.

From the relations

$$I_n(u_{i_1},\dots,u_{i_{L+1}}) \le t(u_{i_1},\dots,u_{i_{L+1}}) + 1 \le \max_j d(y,u_{i_j})$$
$$I_n(u_{i_1},\dots,u_{i_{L+1}}) = \max_j d(y,u_{i_j}) + o(n)$$

one can easily see that the moment inertia asymptotically coincide with $t(u_{i_1},\dots,u_{i_{L+1}})$. Hence the bound (6), which is valid for the moment of inertia, in our case is still valid for τ. At last, since our set is the extracted subset of the initial set and the minimal $L-$packing radius t of the initial set can be only smaller, we conclude that bound (6) is still valid with τ instead of ρ. This proves Lemma 3.

References

[1] P. Elias, Error– correcting codes for list decoding, IEEE Trans. Inf. Th., 37, 5–12, 1991.

[2] V. Blinovsky, Bounds for codes in the case of list decoding of finite volume, Probl. Inform. Transm., vol. 22, no.1, 7–19, 1986.

[3] V. Blinovsky, Asymptotic Combinatorial Coding Theory, Kluwer Acad. Publ., 1997.

[4] V. Blinovsky, Error probability exponent of list decoding at low rates, Probl. Inform. Trans., Vol.37, no.4, 277–287, 2001.

[5] V. Blinovsky, Lower bound for linear multiple packing of the binary Hamming space, J. Comb. Th., Ser.A, 92(1), 95–101, 2000.

[6] V. Blinovsky, Multiple packing of $q-$ary Hamming space, Probl. Inform. Transm., vol.41, no.1, 23–32, 2005.

[7] V. Guruswami, List decoding of error– correcting codes, Lect. Notes in Comp. Sci., 3282, Springer, 2004.

[8] B. Bollobás, Modern Graph Theory, Springer, 1998.

[9] R. Gallager, Information Theory and Reliable Communication, Wiley, 1968.

[10] A. Dembo and O. Zeitouni, Large Deviations Techniques and Applications, Springer, 1998.

[11] F. MacWilliams and N. Sloane, The Theory of Error Correcting Codes, Elsevier, 1977.

[12] J. Komlos, A strange pigeon-hole principle, Order, 7, Kluwer Acad. Publ., 107–113, 1990.

[13] R. Ahlswede, C. Deppe, and V. Lebedev, Nonbinary error correcting codes with noiseless feedback, localized errors or both, Annals of European Academy of Sciences, No. 1, 285 - 309, 2005.