# Bounds on Distance Distributions in Codes of Known Size

Alexei Ashikhmin [*], Gérard Cohen [†],
Michael Krivelevich [‡], Simon Litsyn [§]

May 30, 2004

**Abstract**

We treat the problem of bounding components of the possible distance distributions of codes given the knowledge of their size and possibly minimum distance. Using the Beckner inequality from Harmonic Analysis we derive upper bounds on distance distribution components which are sometimes better than earlier ones due to Ashikhmin, Barg and Litsyn. We use an alternative approach to derive upper bounds on distance distributions in linear codes. As an application of the suggested estimates we get an upper bound on the undetected error probability for an arbitrary code of given size. We also use the new bounds to derive better upper estimates on the covering radius, as well as a lower bound on the error-probability threshold, as a function of the code's size and minimum distance.

**Keywords**: Distance distributions, Beckner inequality, Undetected error probability, Covering radius, Error probability threshold.

[*] Bell Laboratories, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974, USA, e-mail: `aea@research.bell-labs.comi.`

[†] Département Informatique et Réseaux, ENST, 46 Rue Barrault, Paris, France; e-mail: `cohen@inf.enst.fr.`

[‡] School of Mathematics, Tel Aviv University, Ramat-Aviv, 69978 Israel; e-mail: `krivelev@math.tau.ac.il.`

[§] Department of Electrical Engineering-Systems, Tel Aviv University, Ramat Aviv, 69978 Israel; e-mail: `litsyn@eng.tau.ac.il.`

# 1 Introduction

An interest in the distance distributions of codes is due to the fact that they play an important role in estimating decoding error probabilities. In most recent studies bounds on the distance distributions are derived when the minimum distance or/and the dual distance of the code are known. These estimates prove reasonably tight when the size of the code is close to or satisfies linear programming bounds relating the minimum distance and the rate. In this paper we tackle a different problem, namely, we wish to bound the distance distribution of codes given their size and minimum distance. Thus the parameters of the considered codes may be essentially worse than those given by the known upper bounds on the rate of code as a function of minimum distance. However, as it will be demonstrated, this case is also of relevance in several problems of information and coding theory.

Let $F^n$ be the space of binary vectors of length $n$ endowed with the Hamming metric $d(\cdot,\cdot)$, for $\mathbf{x}=(x_1,...,x_n),\mathbf{y}=(y_1,...,y_n),\mathbf{x},\mathbf{y}\in F^n$,

$$d(\mathbf{x},\mathbf{y})=|\{i:x_i\neq y_i\}|.$$

Let the (Hamming) weight of $\mathbf{x}\in F^n$ be

$$wt(\mathbf{x})=|\{i:x_i=1\}|$$

i.e. the number of ones in $\mathbf{x}$. Let $B(\mathbf{x},r)\subseteq F^n$ stand for the ball of radius $r$ centered at $\mathbf{x}$,

$$V(r)=\sum_{i=0}^{r}\binom{n}{i}$$

being its volume. Let $C\subseteq F^n$ be a code of rate

$$R(C)=R=\frac{1}{n}\log_2|C|.$$

Assume that the minimum distance $d(C)$ of the code,

$$d(C)=d=\min_{\mathbf{c}_1,\mathbf{c}_2\in C,\,\mathbf{c}_1\neq\mathbf{c}_2}d(\mathbf{c}_1,\mathbf{c}_2),$$

is $d=\delta(C)n$, where $\delta=\delta(C)$ is the relative distance of the code. Denote by $\mathbf{B}(C)=(B_0(C)=1,B_1(C),\ldots,B_n(C))$ the distance distribution of the code, i.e.

$$B_i(C)=B_i=\frac{1}{|C|}\left|\{\mathbf{c}_1,\mathbf{c}_2:\mathbf{c}_1,\mathbf{c}_2\in C;d(\mathbf{c}_1,\mathbf{c}_2)=i\}\right|.$$

For $\mathbf{c} \in C$ let

$$A_i^C(\mathbf{c}) = A_i(\mathbf{c}) = |\{\mathbf{c}_1 \in C : d(\mathbf{c}, \mathbf{c}_1) = i\}|. \tag{1}$$

Notice that

$$B_i = \frac{1}{|C|} \sum_{\mathbf{c} \in C} A_i(\mathbf{c}). \tag{2}$$

Whenever we deal with a linear code (i.e. a code closed under componentwise modulo 2 sum) then for every $\mathbf{c} \in C$ we have $A_i(\mathbf{c}) = B_i$.

We will also be using the exponents $b_\xi(C)$ of $B_{\lfloor \xi n \rfloor}(C)$, namely,

$$b_\xi(C) = b_\xi = \frac{1}{n} \log_2 B_{\lfloor \xi n \rfloor}$$

We are interested in the problem of bounding possible distance distributions knowing the size of the code and, perhaps, its minimum distance.

**Problem statement:** *Given $R$, $\delta$, and $\xi$, such that $0 \le R \le 1$, $0 \le \delta \le 1/2$, and $\delta \le \xi \le 1$, we wish to estimate*

$$b_\xi(R, \delta) := \limsup_{n \to \infty} \max_C b_\xi(C) \tag{3}$$

*where the maximum is taken over all codes $C$ of length $n$, rate at most $R$ and minimum distance at least $\delta n$.*

When $\delta = 0$ we sometimes omit the second index and write $b_\xi(R)$.

Among others, we address the following very simply stated, but apparently non-trivial, question: *Is it possible that in a code of size exponentially smaller than $2^n$ there is an index $i$ such that $B_i$ has the same exponential order as $\binom{n}{i}$?* In what follows, among other results, we resolve this question negatively by providing upper bounds on the distance distribution components (see Corollary 2). The possible distance distributions are even more restricted if the minimum distance is given (see Theorem 7).

The bounds we derive are applied to three problems (though we believe that there are quite a few others where they can be efficiently used).

The first one is related to estimation of the undetected error probability, i.e. the average (over the code) probability that a codeword transmitted over a binary symmetric channel (BSC) is distorted in such a way that the received word, though different from the transmitted one, also belongs to the code. This probability for a code $C$ is expressed as

$$P_{ue}(C,\rho)=\sum_{i=1}^{n}B_i\rho^i(1-\rho)^{n-i}, \tag{4}$$

where $\rho$, $0\le\rho\le 1/2$, is the BSC bit transition probability. We are interested in bounding the undetected error probability from above, i.e. trying to answer the following question: *Given the BSC transition probability and the code size, what is the largest possible undetected error probability?* An answer is presented in Theorem 3. For earlier known bounds consult [11] and references therein.

Another problem deals with bounding the covering radius of a linear code of given size and dual distance. The covering radius of a code $C$ is

$$\mathcal{R}(C)=\max_{\mathbf{v}\in F^n}\min_{\mathbf{c}\in C}d(\mathbf{v},\mathbf{c}).$$

The dual distance is the minimum distance of the code $C^\perp$, dual to $C$,

$$C^\perp=\{\mathbf{c}^\perp:\forall\mathbf{c}\in C,\sum_{i=1}^{n}c_i^\perp c_i=0 \bmod 2\}.$$

It is well-known that codes with large dual distance have small covering radii. Using the obtained bound along with an inequality relating the value of the covering radius of the code to the distance distribution of its dual, we derive a better upper bound on the covering radius. It is given in Theorem 11, and improves on the earlier known bounds, see [3, 5, 7].

The third problem consists in finding the threshold for maximum- likelihood decoding error probability in a BSC as a function of code's minimum distance and size. Given a received distorted vector, such decoding outputs the closest (in the sense of Hamming distance) codeword. The error probability thus is the probability that the result of the decoding differs from the initial codeword. As it was proved in [18], for every code there exists a threshold $\theta$ of the BSC transition probability $\rho$ such that the decoding error probability is close to 0 if $\rho<\theta$, and is close to 1 if $\rho>\theta$. The problem is to locate $\theta$ given the parameters of the code. We give a lower bound on the threshold in Theorem 12. It is in many cases better than the corresponding estimates derived by Tillich and Zémor [18], see also [19, 20].

Our results provide also an upper bound on $m(n,k,w)$, the maximum number of vectors of constant weight $w$ belonging to a $k$-dimensional subspace of $F^n$. In Subsection 4 we extend results of Linial and Samorodnitsky [14], and provide another bound on the distance distributions of *linear* codes given their dimension and minimum distance, sometimes better than the general one. We discuss the tightness of our results in view of a conjecture due to Khachatrian [10]. For results and references on an analogous problem when the subspaces are picked from the Euclidean space, see e.g. [1].

Throughout the paper all logarithms are to the base 2, and

$$H(x) = -x\log x - (1-x)\log(1-x)$$

is the binary entropy.

The results of this paper extend and generalize those of the previous paper [8] of the last three authors, where mainly the case of unrestricted minimal distance was treated.

## 2 Basic inequalities

We use the Beckner inequality [6] (sometimes attributed to Bonami). The particular form of the inequality we use appears in [2, 9].

Let $f$ be a real-valued function defined on $F^n$. For a real positive $s$, the $s$-norm of $f$ is

$$||f||_s = \left(\frac{1}{2^n}\sum_{\mathbf{v}\in F^n}|f(\mathbf{v})|^s\right)^{1/s}.$$

For $\varepsilon \in (0,1)$, let $T_\varepsilon = T_\varepsilon(f)$ be the function defined on $F^n$ as

$$T_\varepsilon(\mathbf{v}) = \sum_{\mathbf{u}\in F^n} f(\mathbf{u})\left(\frac{1+\varepsilon}{2}\right)^{n-d(\mathbf{u},\mathbf{v})}\left(\frac{1-\varepsilon}{2}\right)^{d(\mathbf{u},\mathbf{v})}.$$

**Theorem 1 (Beckner)** *For any real-valued function $f$ on $F^n$ and any $\varepsilon \in (0,1)$,*

$$||T_\varepsilon||_2 \le ||f||_{1+\varepsilon^2}.$$

$\diamond$

Let $A(n,d,w)$ be the maximal possible number of binary $n$-vectors of weight $w$, being at Hamming distance at least $d$ one from another, and $A(n,d,\le w)$ stand for the corresponding quantity when the weight of the codewords is at most $w$. Clearly, $A(n,d,\le w) \le (w+1)\max_{i=1,\ldots,w} A(n,d,i)$. Thus known upper bounds on $A(n,d,w)$ can be used to estimate $A(n,d,\le w)$. All the known upper bounds are monotone in $i$ (for $w \le n/2$), so the maximum is achieved when $i = w$. Let

$$R(\delta,\gamma) := \limsup_{n\to\infty} \frac{1}{n}\log_2 A(n,\delta n,\le \gamma n).$$

The following summarizes the best known upper bounds on $R(\delta,\gamma)$.

**Lemma 1** *a)*

$$R(\delta,\gamma) \le R_1(\delta,\gamma) := H\left(\frac{1}{2}\left(1-\sqrt{1-(\sqrt{4\gamma(1-\gamma)-\delta(2-\delta)}-\delta)^2}\right)\right) \tag{5}$$

*where* $0 \le \delta \le 2\gamma(1-\gamma)$.
*b) Let*

$$\gamma_0 = \arg \min_{(1-\sqrt{1-2\delta})/2\le\alpha\le 1/2} 1 - H(\alpha) + R_1(\delta,\alpha),$$

*Then for* $\gamma_0 \le \gamma \le 1/2$

$$R(\delta,\gamma) \le H(\gamma) - H(\gamma_0) + R_1(\delta,\gamma_0) \tag{6}$$

◇

The first inequality (5) is the linear-programming bound [16], which is the best known bound for large distances. The second bound is due to a recurrence relation developed by Levenshtein [13] and is given here in the form suggested by Samorodnitsky [17].

Now we are in a position to state the basic inequality.

**Theorem 2** *For any code $C$ of length $n$, minimum distance $d$, and parameters $p \in [0,1/2]$, $g \in [0,\frac{n}{2}]$, $g$ being an integer, the following inequality holds:*

$$\sum_{i=0}^{n} B_i \sum_{l=0}^{n} h(i,l)p^l(1-p)^{n-l} \le \left(V(g)A^{1-2p}(n,d,\le g)\right)^{\frac{1}{1-p}} \left(\frac{|C|}{2^n}\right)^{\frac{p}{1-p}},$$

*where*

$$h(i,\ell) = |\{(\mathbf{u}_1,\mathbf{u}_2) : \mathbf{u}_1 \in B(0^n,g), \mathbf{u}_2 \in B(\mathbf{w},g) : wt(\mathbf{w}) = i, d(\mathbf{u}_1,\mathbf{u}_2) = \ell\}|.$$

**Proof** Define

$$f_g(\mathbf{v}) = |\{\mathbf{c} \in C : d(\mathbf{v}, \mathbf{c}) \le g\}|.$$

Clearly, for every $\mathbf{v} \in F^n$,

$$f_g(\mathbf{v}) \le A(n, d, \le g) \ .$$

Let

$$\{\mathbf{c}, \mathbf{v}\}_g = \{(\mathbf{c}, \mathbf{v}) : \mathbf{c} \in C, \mathbf{v} \in B(\mathbf{c}, g)\} \ .$$

Notice that

$$\sum_{\mathbf{v}} f_g(\mathbf{v}) = |\{\mathbf{c}, \mathbf{v}\}_g| = |C|V(g) \ .$$

Thus the maximum of

$$\sum_{\mathbf{v}} f_g^{1+\varepsilon^2}(\mathbf{v})$$

is achieved when $|C|V(g)/A(n, d, \le g)$ summands in the last sum assume their maximum value of $A(n, d, \le g)$, while the rest of the summands are 0, and this maximum is

$$|C|V(g)A^{\varepsilon^2}(n, d, \le g).$$

Therefore,

$$\|f_g\|_{1+\varepsilon^2} \le \left( \frac{|C|V(g)A^{\varepsilon^2}(n, d, \le g)}{2^n} \right)^{1/(1+\varepsilon^2)} .$$

This gives an estimate to the right-hand side of the Beckner inequality. To estimate the left-hand side, denote $\rho = (1 - \varepsilon)/2$. Then

$$T_\varepsilon(\mathbf{v}) = \sum_{\mathbf{u} \in F^n} f_g(\mathbf{u}) \rho^{d(\mathbf{u},\mathbf{v})} (1 - \rho)^{n - d(\mathbf{u},\mathbf{v})}$$

and

$$\begin{aligned}
\sum_{\mathbf{v} \in F^n} T_\varepsilon^2(\mathbf{v}) &= \sum_{\mathbf{v} \in F^n} \left( \sum_{\{\mathbf{c},\mathbf{u}\}_g} \rho^{d(\mathbf{u},\mathbf{v})} (1 - \rho)^{n - d(\mathbf{u},\mathbf{v})} \right)^2 \\
&= \sum_{\mathbf{v} \in F^n} \sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g, \{\mathbf{c}_2,\mathbf{u}_2\}_g} \rho^{d(\mathbf{u}_1,\mathbf{v}) + d(\mathbf{u}_2,\mathbf{v})} (1 - \rho)^{2n - d(\mathbf{u}_1,\mathbf{v}) - d(\mathbf{u}_2,\mathbf{v})} \\
&= \sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g, \{\mathbf{c}_2,\mathbf{u}_2\}_g} \sum_{\mathbf{v} \in F^n} \rho^{d(\mathbf{u}_1,\mathbf{v}) + d(\mathbf{u}_2,\mathbf{v})} (1 - \rho)^{2n - d(\mathbf{u}_1,\mathbf{v}) - d(\mathbf{u}_2,\mathbf{v})} \\
&= \sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g, \{\mathbf{c}_2,\mathbf{u}_2\}_g} G(\mathbf{u}_1, \mathbf{u}_2).
\end{aligned}$$

Now we calculate $G(\mathbf{u}_1, \mathbf{u}_2)$ defined by the previous equality. Clearly it depends only on the distance between $\mathbf{u}_1$ and $\mathbf{u}_2$. Let $d(\mathbf{u}_1, \mathbf{u}_2) = \ell$, and without loss of generality assume that $\mathbf{u}_1 = 0^n, \mathbf{u}_2 = 1^\ell 0^{n-\ell}$. Then

$$\begin{aligned} G(\mathbf{u}_1, \mathbf{u}_2) &= \sum_{i=0}^{\ell} \sum_{j=0}^{n-\ell} \binom{\ell}{i} \binom{n-\ell}{j} \rho^{i+j+\ell-i+j} (1-\rho)^{n-i-j+n-\ell+i-j} \\ &= \left( \sum_{i=0}^{\ell} \binom{\ell}{i} \rho^\ell (1-\rho)^\ell \right) \left( \sum_{j=0}^{n-\ell} \binom{n-\ell}{j} \rho^{2j} (1-\rho)^{2n-2\ell-2j} \right) \\ &= (2\rho(1-\rho))^\ell (\rho^2 + (1-\rho)^2)^{n-\ell} \end{aligned}$$

Denote $p = 2\rho(1-\rho)$, then $1 - p = \rho^2 + (1-\rho)^2$ and $p \in [0, 1/2]$ whenever $\rho \in [0, 1]$. Thus

$$G(\mathbf{u}_1, \mathbf{u}_2) = p^{d(\mathbf{u}_1, \mathbf{u}_2)} (1-p)^{n-d(\mathbf{u}_1, \mathbf{u}_2)}$$

Continuing the previous computation and using definition (1), we conclude that

$$\sum_{\mathbf{v} \in F^n} T_\varepsilon^2(\mathbf{v}) = \sum_{\mathbf{c} \in C} \sum_{i=0}^{n} A_i(\mathbf{c}) \sum_{\ell=0}^{n} h(i, \ell) p^\ell (1-p)^{n-\ell},$$

where $h(i, \ell)$ has been defined in Theorem 2. Now noticing that $1 + \varepsilon^2 = 2(1-p)$, $\varepsilon^2 = 1 - 2p$, applying the Beckner inequality, and using (2), we obtain the claimed result. ◇

The function $h(i, l)$ appearing in the statement of the theorem will be calculated later (in Lemma 3). However, choosing $g$ small enough we may consider a particular case where this function is essentially absent.

**Corollary 1** *With the above notation, for any $p \in [0, 1/2]$, and $0 \leq \gamma < \gamma_E := \frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}$,*

$$\sum_{i=0}^{n} B_i \sum_{\ell=0}^{n} h(i, \ell) p^\ell (1-p)^{n-\ell} \leq V^{\frac{1}{1-p}} (\gamma n) n^\alpha \left( \frac{|C|}{2^n} \right)^{\frac{p}{1-p}}.$$

*Here $\alpha$ is a non-negative constant depending on $\gamma$.* ◇

**Proof** If $\gamma$ satisfies the inequality

$$0 \leq \gamma < \frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta},$$

then, by Elias (see e.g. [15]), for every $\mathbf{v} \in F^n$, $f_{\gamma n}(\mathbf{v}) \leq n^\alpha$, for some constant $\alpha = \alpha(\gamma) > 0$. ◇

# 3 Estimates

In this section we use Theorem 2 to estimate components of distance distributions of codes. We start with the most straightforward application of the theorem to the problem of bounding the undetected error probability.

## 3.1 Undetected error probability in codes of given size

**Theorem 3** *Every code $C$ used on a BSC channel with transition probability $\rho \in [0, \frac{1}{2}]$ satisfies:*

$$P_{ue}(C, \rho) \leq \left(\frac{|C|}{2^n}\right)^{\frac{\rho}{1-\rho}} - (1-\rho)^n.$$

**Proof** Set $d = 1$ and choose $g = 0$ in Theorem 2. Then the balls $B(\mathbf{c}, g)$ are just codewords of $C$. Obviously $V(0) = 1$ and $A(n, 1, \leq 0) = 1$. It is easy to see that $h(i, \ell) = 0$ unless $i = \ell$, in which case $h(i, \ell) = 1$. Therefore, by the definition of $P_{ue}$, we have

$$\begin{aligned} P_{ue}(C, \rho) &= \sum_{i=1}^{n} B_i \rho^i (1-\rho)^{n-i} \\ &= -(1-\rho)^n + \sum_{i=0}^{n} B_i \rho^i (1-\rho)^{n-i} \\ &\leq -(1-\rho)^n + \left(\frac{|C|}{2^n}\right)^{\frac{\rho}{1-\rho}}. \end{aligned}$$

◇

Since for every code

$$P_{ue}(C, 1/2) = \frac{|C| - 1}{2^n} = \frac{|C|}{2^n} - \left(\frac{1}{2}\right)^n,$$

the bound of the theorem is tight at $\rho = 1/2$.

When $n$ grows we consider the undetected error exponent depending on $R$ and $\rho$,

$$p_{ue}(R, \rho) = \limsup_{n \to \infty} \left(-\frac{1}{n} \max_{C} \log_2 P_{ue}(C, \rho)\right),$$

where the maximum is taken over all codes of rate at most $R$.

**Lemma 2** *For $\rho \in [0, 1/2]$,*

$$p_{ue}(R, \rho) = p_{ue}(R, 1 - \rho)$$

**Proof** Given a code $C$ with distance components $B_{\mu n}(C)$ we construct a new code $C'$ of size at most $2|C|$ by "symmetrizing" it, i.e. adding to the code $C$ whenever possible the binary complements of codewords. The new code $C'$ has symmetric distance distribution with respect to $n/2$: $B_{\mu n}(C') = B_{(1-\mu)n}(C')$, and, asymptotically, the same rate as $C$. For a code $C'$ with symmetric distance distribution, it is immediate to check that:

$P_{ue}(C', \rho) + (1 - \rho)^n = P_{ue}(C', 1 - \rho) + \rho^n$.

Since the term $(1-\rho)^n$ is exponentially small in comparison with $P_{ue}(C', \rho)$, we have

$$\lim_{n \to \infty} -\frac{1}{n} \log_2 (P_{ue}(C', \rho) + (1 - \rho)^n) = \lim_{n \to \infty} -\frac{1}{n} \log_2 P_{ue}(C', \rho),$$

and any upper bound on $p_{ue}(R, \rho)$ is also valid for $p_{ue}(R, 1 - \rho)$. $\diamond$

For a lower bound consider the following code of given size $|C|$. Determine the maximum $w$ satisfying $\binom{n}{w} \leq |C|$. The code consisting of all vectors of weight $w$ has the distance distribution

$$B_{2i} = \binom{w}{i} \binom{n - w}{i},$$

and its probability of undetected error is

$$P_{ue}(C, \rho) = \sum_{i=1}^{w} \binom{w}{i} \binom{n - w}{i} \rho^{2i} (1 - \rho)^{n-2i} \tag{7}$$

**Theorem 4** *For the constant weight code consisting of all vectors of weight $w$ and $\rho \in [0, 1/2]$,*

$$\frac{\rho}{1 - \rho}(1 - R) \geq p_{ue}(R, \rho) = p_{ue}(R, 1 - \rho) \geq$$

$$-\left(\omega H\left(\frac{\xi}{\omega}\right) + (1 - \omega) H\left(\frac{\xi}{1 - \omega}\right) + 2\xi \log \rho + (1 - 2\xi) \log(1 - \rho)\right),$$

*where*

$$\omega = H^{-1}(R),$$

$$\xi = \frac{\rho^2 - \rho\sqrt{\rho^2 - 4\omega(1 - \omega)(2\rho - 1)}}{2(2\rho - 1)}.$$

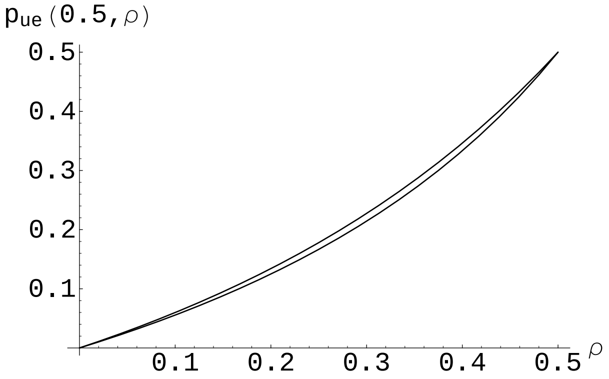

Figure 1: Lower and upper bounds on the probability of undetected error for $R = 0.5$

**Proof** The upper bound comes from the previous theorem. Optimizing (7) in $w$ we get the expression for the lower bound. Notice that the distance distribution of the defined constant weight code has its maximum at $i = \lfloor w(n-w)/n \rfloor$. However, it is possible to show that $\xi n$ is always less than this $i$. ◇

Figure 1 shows the upper and lower bounds on exponent of the probability of undetected error for the case $R = 0.5$. One can see that the bounds are quite tight.

## 3.2 Distance distributions ($g = 0$)

We start the analysis of distance distributions from the particular case of $g = 0$ in Theorem 2. Although the derived bounds are not always the best possible, they are given by explicit expressions.

**Theorem 5** *If* $0 < R < 1$*, and*

$$0 < \mu \le 1 - 2\sqrt{(1-R)\ln 2} + \ln 2 - R\ln 2\,,$$

*then*

$$b_\mu(R) \le -\frac{p^*}{1-p^*}(1-R) - \mu \log p^* - (1-\mu)\log(1-p^*) + o(1)\,, \qquad (8)$$

*where*

$$p^* = \frac{1}{2}\left(1+\mu-\ln 2+R\ln 2-\sqrt{-4\mu+(1+\mu-\ln 2+R\ln 2)^2}\right).$$

*Otherwise, the trivial bound holds:*

$$b_\mu(R) \leq R\ .$$

*The same bounds are valid also for $b_{1-\mu}(R)$.*

**Proof** Setting $g = 0$ in Theorem 2, we obtain

$$\left(\frac{|C|}{2^n}\right)^{\frac{p}{1-p}} \geq \sum_{i=0}^{n} B_i p^i (1-p)^{n-i} \geq B_m p^m (1-p)^{n-m},\ m \in [0,n].$$

Thus

$$B_m \leq \left(\frac{|C|}{2^n}\right)^{\frac{p}{1-p}} \cdot \frac{1}{p^m(1-p)^{n-m}}.$$

Optimization in $p$ gives the claim.

To see that the bounds are symmetric for $\mu$ and $1-\mu$ we use the same argument as in the previous section. ◇

**Corollary 2** *For any $\mu \in (0, 0.5)$*

$$b_\mu(R) = b_{1-\mu}(R) \leq -\frac{\mu}{1-\mu}(1-R) + H(\mu) + o(1).$$

**Proof** Notice that (8) is valid for any $\mu$ and any other value substituted instead of $p^*$. Plugging in $p^* = \mu$ we get the sought result. ◇

In particular, it is easily seen from the corollary that for any code of rate $R < 1$ every distance distribution component $B_i$ is exponentially smaller than the binomial coefficient $\binom{n}{i}$.

Let us now consider the code $C$ of even length $n$ and consisting of all vectors of weight $w$ and their complements. The size of this code is $2\binom{n}{w}$ and its distance distribution is

$$\begin{aligned} B_{2i} &= \binom{w}{i}\binom{n-w}{i} + \binom{w}{\frac{n}{2}-i}\binom{n-w}{\frac{n}{2}-i}, \\ B_{2i} &= B_{n-2i} \end{aligned}$$

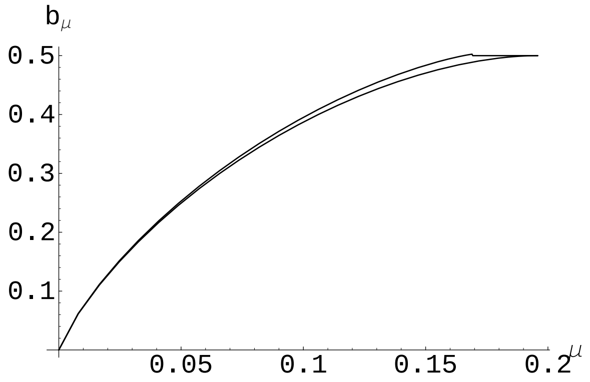

Figure 2: Lower and upper bounds on $b_\mu$ for $R = 0.5$

**Theorem 6** *Let $\omega = H^{-1}(R)$. For any $0 \le \mu \le 2\omega(1-\omega)$*

$$b_\mu(R) = b_{1-\mu}(R) \ge \omega H\left(\frac{\mu}{2\omega}\right) + (1-\omega)H\left(\frac{\mu}{2(1-\omega)}\right) \ .$$

*Otherwise, for $\mu \le 0.5$,*

$$b_\mu(R) = b_{1-\mu}(R) = R \ .$$

**Proof** The first estimate follows from the construction. For the second one, consider a random constant weight code of size $|C|$ and weight $w^*$, where $w^*$ satisfies $2w^*(1-w^*) = \mu n$. Its average distance distribution is

$$B_{2i} = \frac{|C|}{\binom{n}{w}}\binom{w}{i}\binom{n-w}{w-i}$$

Considering the union of the code and its complement, we conclude that the maximum of its distance distribution is attained when $2i = \lfloor 2w(1-w) \rfloor$ and is of order $2^{Rn(1-o(1))}$. $\diamond$

On Figure 2 the upper and lower bounds are presented for the distance distributions of codes of rate 0.5.

## 3.3 Distance distributions ($g > 0$)

Let $\hbar(\xi, \upsilon) = \frac{1}{n}\log h(\xi n, \upsilon n)$. The following lemma gives a lower bound for $\hbar(\xi, \upsilon)$.

**Lemma 3** *Let*

$$\sigma_1 = \begin{cases} \zeta\upsilon & \text{if } \zeta + \upsilon - \gamma \le 2\zeta\upsilon\,, \\ (\zeta + \upsilon - \gamma)/2 & \text{otherwise}\,, \end{cases}$$

$$\sigma_2 = \begin{cases} (\gamma - \zeta + \xi)/2 & \text{if } 2\xi(1-\zeta) > \gamma - \zeta + \xi\,, \\ \xi(1-\zeta) & \text{otherwise.} \end{cases}$$

*Then for* $\upsilon \in [\xi - 2\gamma, \xi + 2\gamma]$

$$\hbar(\xi, \upsilon) \ge \max_{\zeta} \zeta H\left(\frac{\sigma_1}{\zeta}\right) + (1-\zeta) H\left(\frac{\upsilon - \sigma_1}{1-\zeta}\right) +$$

$$+\xi H\left(\frac{\sigma_2}{\xi}\right) + (1-\xi) H\left(\frac{\zeta - \xi + \sigma_2}{1-\xi}\right)$$

*where the maximum is taken over* $\zeta$ *in the interval from* $\max\{0, \xi - \gamma, \upsilon - \gamma\}$ *up to* $\min\{1, \xi + \gamma, \upsilon + \gamma\}$.

**Proof** See Appendix. ◇

Using Theorem 2 in the most general form and Lemma 3, we derive the following bound.

**Theorem 7**

$$\begin{aligned} b_\mu(R, \delta) \quad \le \quad & \min\left\{ -\frac{p}{1-p}(1-R) + \frac{1}{1-p} H(\gamma) + \frac{1-2p}{1-p} R(\delta, \gamma) \right. \\ & \left. - \hbar(\mu, \upsilon) - \upsilon \log p - (1-\upsilon)\log(1-p) \right\}, \end{aligned} \qquad (9)$$

*where* $R(\delta, \gamma)$ *is defined in Lemma 1,* $\hbar(\mu, \upsilon)$ *defined in Lemma 3, and the minimum is taken for* $p \in [0, 1/2], \gamma \in [\frac{1}{2} - \sqrt{\frac{1}{4} - \frac{\delta}{2}}, 1/2]$*, and* $\upsilon \in [0, 1]$.

**Proof** It is an asymptotic form of Theorem 2 after we single out the corresponding term on the left-hand side of the inequality, and $g = \gamma n$ and $\ell = \upsilon n$. ◇

It is also possible to substitute the derived bounds in the expression for undetected error probability to obtain asymptotic upper bounds for this parameter as a function of rate and relative minimum distance. We omit details.

# 4 Distance distributions in linear codes

Below we present an upper bound on the distance distribution of linear codes. The bound is based on an extension of arguments used in [14].

Let $C$ be a linear code with relative minimum distance $\delta$ and rate $R$, and $R^*(\delta)$ any upper bound on $R$. We consider $b_\mu(R,\delta)$ defined by (3), the maximum being taken now over all *linear* codes; the corresponding value is denoted $b_\mu^L(R,\delta)$. Clearly $b_\mu^L(R,\delta) \le b_\mu(R,\delta)$, and the previous bounds apply. However, better bounds can be derived.

**Theorem 8** *The distance distribution of $C$ is bounded from above as follows*

$$b_\mu^L(R,\delta) \le \begin{cases} \min_{0\le\alpha\le1}\left\{\alpha R H\left(\frac{w}{\beta^*(\alpha)}\right) + (1-\alpha)R\right\}, & \textit{if } \beta^*(\alpha) > 2\mu, \\ R, & \textit{if } \beta^*(\alpha) \le 2\mu, \end{cases} \tag{10}$$

*where $\beta^*(\alpha)$ is the root of the equation*

$$\frac{(1-\alpha)R}{\beta} = R^*\left(\frac{\delta}{\beta}\right). \tag{11}$$

**Proof** Let $\{1,2,\ldots,n\}$ be the set of code coordinates of $C$, identified with columns of a generator matrix. Consider the following partition

$$\{1,2,\ldots,n\} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \ldots \cup \mathcal{A}_t \cup \mathcal{B},$$

where the $\mathcal{A}_i$'s are disjoint subsets consisting of $\lfloor \alpha R n \rfloor$ independent coordinates (i.e. columns of the generator matrix of $C$) and $\mathcal{B}$ is a subset with rank less than $\alpha R n$. We assume that such a partition is obtained greedily; we stop when no further $\mathcal{A}_{t+1}$ is possible. Let $D$ be the subcode of $C$ consisting of codewords with supports belonging to $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \ldots \cup \mathcal{A}_t$. Denote by $n' = \alpha t R n$ the length of $D$. Obviously $n' = \beta n$ for some $\beta \in [\delta, 1]$. It follows from the definition that the rate $R'$ and minimum distance $\delta'$ of $D$ satisfy

$$R' \ge \frac{(1-\alpha)R}{\beta},\ \delta' \ge \frac{\delta}{\beta}.$$

Hence we have

$$\frac{(1-\alpha)R}{\beta} \le R' \le R^*\left(\frac{\delta}{\beta}\right).$$

Since $(1-\alpha)R \leq R^*(\delta)$, $(1-\alpha)R/2\delta > R^*(\delta/2\delta) = 0$, and since the left and the right hand sides of (11) are decreasing and increasing in $\beta$ functions respectively, the equation (11) has a root $\beta^*(\alpha) = \beta^*$ on the interval $[2\delta, 1]$. Thus $\beta$ must belong to the interval $[\beta^*, 1]$.

Let $\mathbf{c} \in C$ be a codeword of weight $m$. By the pigeon-hole principle, there exists at least one set of coordinates $\mathcal{A}_i$ on which $\mathbf{c}$ has $\lfloor m/t \rfloor$ or less nonzero entries. Let's say $\mathbf{c}$ is *bad* for $i$. On the other hand, since $|\mathcal{A}_i| = \mathrm{rank}(\mathcal{A}_i) = \alpha Rn$, there are exactly

$$\left( \sum_{i=0}^{\lfloor m/t \rfloor} \binom{\alpha Rn}{i} \right) 2^{(1-\alpha)Rn}$$

bad codewords for every $i$, and in total $t$ times this number of bad codewords.

Thus if $\lfloor m/t \rfloor \leq \alpha Rn/2$ we have

$$B_m \leq t \left( \sum_{i=0}^{\lfloor m/t \rfloor} \binom{\alpha Rn}{i} \right) 2^{(1-\alpha)Rn},$$

or equivalently

$$b_\mu^L(R, \delta) \leq \alpha RH \left( \frac{\mu}{\beta} \right) + (1-\alpha)R. \qquad (12)$$

The condition $\lfloor m/t \rfloor \leq \alpha Rn/2$ is equivalent to $\beta \geq 2\mu$. Hence the worst case in (12) is achieved:

- if $\beta^* \geq 2\mu$, when $\beta = \beta^*$, giving the first part of the theorem;

- if $\beta^* \leq 2\mu$, when $\mu/\beta = 1/2$, giving the second part. ◇

Our previous considerations are relevant to the following combinatorial problem. Let $m(n, k, w)$ stand for the maximum number of vectors of weight $w$ in $F^n$ belonging to a $k$-dimensional linear subspace. Khachatrian [10] conjectured the following exact values.

Case 1: $w < k < 2w$, $w$ is even, $k$ is odd, then

$$m(n, k, w) = 2^{2w-k} \binom{2k-2w}{k-w} + \sum_{i=0}^{k-w} \binom{2k-2w}{2i} \binom{2w-k}{\frac{w-2i}{2}}.$$

The non-zero part of the generator matrix is given by the following construction:

$$k\left\{\begin{array}{ccc|ccc|ccc}
1 & \dots & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 \\
\hline
0 & \dots & 0 & 1 & \dots & 0 & 1 & \dots & 0 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & \dots & 0 & 0 & \dots & 1 & 0 & \dots & 1
\end{array}\right.$$

$$\underbrace{\hphantom{0\ \dots\ 0}}_{2k-2w}\quad\underbrace{\hphantom{0\ \dots\ 0}}_{2w-k}\quad\underbrace{\hphantom{0\ \dots\ 0}}_{2w-k}$$

Case 2: $k \geq 2w$

$$m(n,k,w) = \begin{cases} \binom{k+1}{w}, & \text{if } w \text{ is even} \\ \\ \binom{k}{w}, & \text{if } w \text{ is odd} \end{cases} .$$

In the odd case the non-zero part of the generator matrix is the $k \times k$ identity matrix. In the even case it is the identity matrix along with the all-one column.

Clearly,

$$\frac{1}{n}\log_2 m(n,k,w) = b_\mu^L(R)$$

where $\mu = w/n$, and $R = k/n$.

Combining the lower bound from Khachatrian's conjecture with simple arguments on random codes on a subset of positions, and symmetrizing the distance distribution by adding the all-one vector to the code, we arrive at the following lower bound on $b_\mu^L(R)$, conjectured to be the correct value:

$$b_\mu^L(R) \geq \begin{cases} RH\left(\frac{\mu}{R}\right) & \text{if } \mu \leq R/2\,, \\ R & \text{if } R/2 < \mu < 1 - R/2\,, \\ RH\left(\frac{1-\mu}{R}\right) & \text{if } \mu \geq 1 - R/2\,. \end{cases} \tag{13}$$

# 5 Comparison with known bounds

The best known bounds for the distance distribution components were derived earlier only when assuming the minimum distance known. Let us quote such a bound from [4].

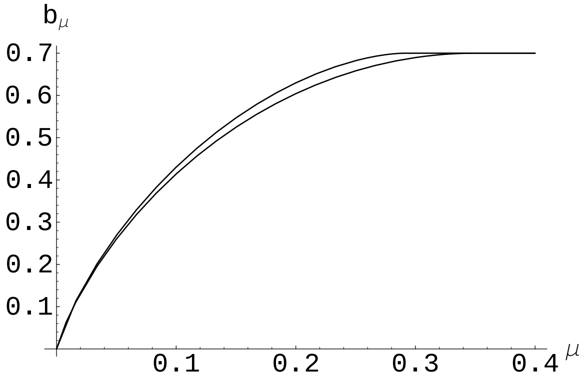

Figure 3: Lower and upper bounds on $b^L_\mu(0.5)$

**Theorem 9**

$$b_\mu(R,\delta) \le \min\{H\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) + H(\mu) - 1, R(\delta,\mu)\}. \qquad (14)$$

Notice that the left-hand side of the inequality depends only on $\delta$.

Figure 4 presents bounds from Theorem 9, Theorem 2 and Theorem 8 for the case $R = 0.4$ and $\delta = 0.1$. One can see that on almost the entire interval $[\delta, 1/2]$ the bound (9) is significantly better than other bounds. At the same time on a small interval around minimum distance, bounds from Theorem 9 are a little bit better than (9) and for sufficiently large $\mu$ the bound from Theorem 8 becomes the best one.

# 6 Applications

In this section we present some applications of the derived estimates on the distance distribution components.

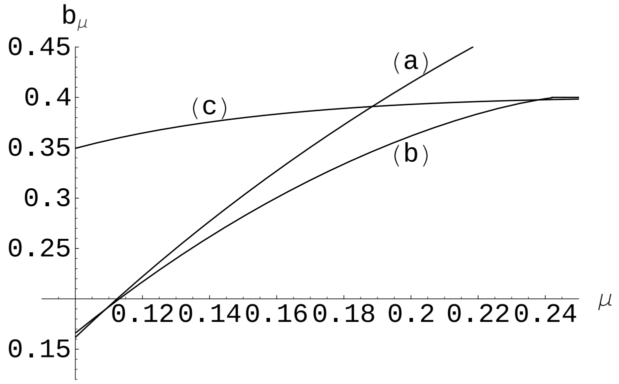

Figure 4: Upper bounds on $b_\mu$ for $R = 0.4$ and $d = 0.1$, (a) is the best of the bounds from Theorem 9, (b) is (9), and (c), which holds only for linear codes, is (10).

## 6.1 Covering radius as function of the size and dual distance of linear codes

Let $C$, $C \neq F^n$, be a linear code of rate $R$. Let $C^\perp$ be its dual code, of rate $1-R$, with the (dual) distance distribution

$$B^\perp = (B_0^\perp, B_1^\perp, ..., B_n^\perp),$$

such that $B_0^\perp = 1, B_1^\perp = ... = B_{d^\perp-1}^\perp = 0, B_{d^\perp}^\perp > 0$. Then $d^\perp$ is called the dual distance of code $C$. The following theorem was proved in [7, Theorem 8.3.5].

**Theorem 10** *Let $r$ be an integer and let*

$$\beta(x) = \sum_{i=0}^{n} \beta_i K_i(x), \tag{15}$$

*where $K_i(x)$ is the Krawtchouk polynomial of degree $i$. Let also*

$$\beta_0 > n \max_{j=1,...,n} \{\beta_j B_j^\perp\}$$

*and*

$$\beta(i) \leq 0 \quad \text{for } i = r+1, ..., n.$$

*Then $C$ has covering radius $\mathcal{R}(C) \leq r$.* ◇

We use the standard polynomial employed in the linear programming bound on the minimum distance [16]:

$$\beta(x) = \frac{(K_{t+1}(x) + K_t(x))^2}{a - x},$$

where $K_t(x)$ is the Krawtchouk polynomial of degree $t$ and $a$ is the smallest root of the numerator. Computing the coefficients $\beta_i$ of this polynomial and substituting them into (15), we obtain the following theorem.

**Theorem 11** *[3] Let $\rho$ be the minimal number such that*

$$\max_{\delta^\perp \le \xi \le 2\rho} \{(1-\xi)H\left(\frac{\rho - \xi/2}{1-\xi}\right) - H(\rho) + \xi + b_\xi(R, \delta^\perp)\} < 0.$$

*Then $\mathcal{R}(C)/n \le \rho$.* $\diamond$

Substitution of bounds from Theorem 9 into the theorem gives the best currently known bounds on the covering radius for $\delta^\perp \le 0.273$ [5],[12]. These bounds are functions of the dual minimum distance only. One can consider improvements of the bounds by using the code rate as an extra parameter. As we have seen in Section 3.3 bounds on $b_\xi(R, \delta^\perp)$ from Theorems 2, 8, and 9 are intersecting with each other when $\xi$ runs from $\delta^\perp$ to 1. Hence it makes sense to choose the best of them for each particular value of $\xi$. Substituting such an estimate into Theorem 11 yields significant improvements. For instance for $\delta^\perp = 0.25$ the best of the bounds from [5],[12] equals 0.1291. The bounds obtained as function of both $R$ and $\delta^\perp$ are presented in the following table.

| $R$ | 0.1 | 0.12 | 0.14 | 0.16 | 0.18 |
|---|---|---|---|---|---|
| $\mathcal{R}/n$ | 0.0854 | 0.0985 | 0.110 | 0.1213 | 0.1288 |

## 6.2 A lower bound on the threshold probability

In [18, 19, 20] Zémor et al. formulated the asymptotic problem of locating the threshold probability $\theta$ given the rate $R$ and relative distance $\delta$ of a code. They obtained the following theorem, which we present here with a proof for the sake of completeness.

**Theorem 12**

$$\theta > \vartheta$$

*whenever*

$$\max_{(\delta/\vartheta)<\alpha\le 2}\left\{b_{\alpha\vartheta}(R,\delta)+\alpha\vartheta+(1-\alpha\vartheta)H\left(\frac{(1-\alpha/2)\vartheta}{1-\alpha\vartheta}\right)\right\}<H(\vartheta).$$

**Proof** Let the all-zero codeword $\mathbf{0}$ be transmitted. Consider the vectors of weight $w$. If such a vector is at distance greater than $w$ from any codeword, it will be correctly decoded. To estimate the number of incorrectly decoded vectors of weight $w$ we apply the following argument. There are

$$N(\alpha,w)=\sum_{i=\alpha w/2}^{\alpha w}\binom{\alpha w}{i}\binom{n-\alpha w}{w-i}$$

vectors of weight $w$ which are closer to a given codeword of weight $\alpha w$ than to the zero word. Thus there are at most

$$\sum_{\alpha}A_{\alpha w}(\mathbf{0})N(\alpha,w)$$

such vectors of weight $w$. If this number is exponentially smaller than $\binom{n}{w}$, then most vectors of weight $w$ will be decoded correctly. Averaging over the codewords, substituting bounds on the distance distribution components and passing to asymptotics we obtain the result. ◇

The only previously known bounds were obtained with the help of upper estimates $b_\xi$ as functions of the code minimum distance only (bounds from Theorem 9). One can obtain better results constructing bounds on the threshold probability as a function of both parameters - the code rate and the minimum distance. Let, for instance, $\delta = 0.25$. The best bound on the threshold probability as a function of the minimum distance equals 0.165. In the following table we present lower bounds on the threshold probability depending on the code rate and minimum distance. One can observe significant improvements provided by the suggested method.

| $R$ | 0.1 | 0.12 | 0.14 | 0.16 | 0.18 |
|---|---|---|---|---|---|
| $\theta$ | 0.2204 | 0.2019 | 0.1866 | 0.1736 | 0.1626 |

# Acknowledgement

The authors are grateful to the anonymous referees for comments and suggestions.

# Appendix

## Proof of Lemma 3: Calculation of $h(i, \ell)$

Remind ourselves that

$$h(i, \ell) = |\{(\mathbf{u}_1, \mathbf{u}_2) : \mathbf{u}_1 \in B(0^n, g), \mathbf{u}_2 \in B(1^i 0^{n-i}, g) : d(\mathbf{u}_1, \mathbf{u}_2) = \ell\}|.$$

In this section we provide an explicit expression for this function, which counts the number of pairs of vectors being at distance $\ell$ and belonging to two different Hamming balls of radius $g$ with centers being at distance $i$ apart. Then, we use a simple lower bound on $h(i, \ell)$.

We accomplish the computation in two steps.

**Step 1** For a given vector $\mathbf{w} = 1^j 0^{n-j}$ let us find the number $p(j, \ell)$ of vectors being at distance $\ell$ from $\mathbf{w}$ and belonging to $B(0^n, g)$ (or, which is the same, having weight at most $g$). It is easy to verify that

$$p(j, \ell) = \sum_{s=\max\{0,(j+\ell-g)/2\}}^{\min\{j,\ell\}} \binom{j}{s}\binom{n-j}{\ell-s}$$

and

$$p(j, \ell) \geq \begin{cases} 0 & \text{if } \frac{j+\ell-g}{2} > \min\{j, \ell\} \\ \binom{j}{s_1}\binom{n-j}{\ell-s_1} & \text{otherwise}, \end{cases}$$

where

$$s_1 = \begin{cases} \frac{j\ell}{n} & \text{if } \frac{j+\ell-g}{2} \leq \frac{j\ell}{n} \\ \frac{j+\ell-g}{2} & \text{otherwise}. \end{cases}$$

**Step 2** We find the number of vectors $q(i, j)$ of weight $j$ in the ball $B(1^i 0^{n-i}, g)$. It is easy to check that

$$q(i, j) = \sum_{s=\max\{0,i-j\}}^{\min\{i,(g-j+i)/2\}} \binom{i}{s}\binom{n-i}{j-i+s}$$

and

$$q(i, j) \geq \begin{cases} 0 & \text{if } i - j > \frac{g-j+i}{2} \\ \binom{i}{s_2}\binom{n-i}{j-i+s_2} & \text{otherwise} \end{cases}$$

where

$$s_2 = \begin{cases} \frac{g-j+i}{2} & \text{if } \frac{i(n-j)}{n} > \frac{g-j+i}{2} \\ \frac{i(n-j)}{n} & \text{otherwise} \end{cases}$$

Finally,

$$\begin{aligned} h(i,\ell) &= \sum_{j=\max\{0,i-g\}}^{\min\{n,i+g\}} p(j,\ell)q(i,j) \\ &\geq \max_{j\in J} p(j,\ell)q(i,j)\,, \end{aligned}$$

where $J = [\max\{0, i-g\}, \min\{n, i+g\}]$.

Denoting $i = \xi n$, $g = \gamma n$, $\ell = \upsilon n$, and $\hbar(\xi,\upsilon) = \frac{1}{n}\log h(\xi n, \upsilon n)$, we obtain the claim of Lemma 3.

# References

[1] R.Ahlswede, H.Aydinian, and L.Khachatrian, Maximal number of constant weight vertices of the unit $n$-cube contained in a $k$-dimensional subspace, 1999, preprint.

[2] N.Alon, G.Kalai, M.Ricklin, and L.Stockmeyer, Lower bounds on the competitive ratio for mobile user tracking and distributed job scheduling, *Theoretical Computer Science*, vol.130, 1994, pp.175–201.

[3] A.Ashikhmin, and A.Barg, Bounds on the covering radius of linear codes, *Designs, Codes and Cryptography*, vol.27, no. 3, 2002, pp.261–269.

[4] A.Ashikhmin, A.Barg, and S.Litsyn, Estimates of the distance distribution of codes and designs, *IEEE Trans. Inform. Theory*, vol.45, 6, 1999, pp.1808–1816.

[5] A.Ashikhmin, I.Honkala, T.Laihonen, and S.Litsyn, On relations between covering radius and dual distance, *IEEE Trans. Inform. Theory*, vol.45, 1999, pp.1808–1816.

[6] W.Beckner, Inequalities in Fourier analysis, *Ann. of Math.*, vol.102, 1975, pp.159–182.

[7] G.Cohen, I.Honkala, S.Litsyn, and A.Lobstein, *Covering Codes*, Amsterdam: Elsevier, 1997.

[8] G.Cohen, M.Krivelevich, and S.Litsyn, Bounds on distance distributions in codes of given size, *In book: Communications, Information and Network Security*, V.K.Bhargava, H. Vincent Poor, V. Tarokh, and S.Yoon (Eds.), Kluwer, 2003, pp.33–42.

[9] G.Kalai, and N.Linial, On the distance distribution of codes, *IEEE Trans. Inform. Theory*, vol.41, 1995, pp.1467–1472.

[10] L.Khachatrian, *Personal communication*, 1999.

[11] T. Kløve, and V. Korzhik, *Error Detecting Codes, General Theory and Applications in Feedback Communication Systems*, Kluwer Acad. Publ., Boston, 1995.

[12] T.Laihonen, On algebraic method for bounding the covering radius, in book: *Codes and Association Schemes*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol.56, 2001, pp.213–221.

[13] V.I.Levenshtein, Upper-bound estimates for fixed-weight codes, *Problemy Peredachi Informatsii*, vol.7, 4, 1971, pp.3–12.

[14] N.Linial, and A.Samorodnitsky, Linear codes and character sums, *Combinatorica*, vol. 22, 4, 2002, pp.497–522.

[15] F.J.MacWilliams, and N.J.A.Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[16] R.J.McEliece, E.R.Rodemich, H.Rumsey, and L.R.Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, *IEEE Trans. Inform. Theory*, vol.23, 2, 1977, pp.157–166.

[17] A.Samorodnitsky, On the optimum of Delsarte's linear program, *J. Combin. Th.* Ser. A 96 (2001), 261–287.

[18] J.-P.Tillich, and G.Zémor, Discrete isoperimetric inequalities and the probability of a decoding error, *Combin. Probab. Comput.*, vol. 9, 5, 2000, pp. 465–479.

[19] G. Zémor, Threshold effects in codes, in: Gerard D. Cohen, Simon Litsyn, Antoine Lobstein, Gilles Zemor (Eds.): *Algebraic Coding*, Lecture Notes in Computer Science, vol.781, Springer 1993, pp.278–286.

[20] G.Zémor, and G.Cohen, The threshold probability of a code, *IEEE Trans. Inform. Theory*, vol.41, 2, 1995, pp. 469–477.