Bounds on Distance Distributions in Codes of Given Size

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

Abstract

We prove a new upper bound on the possible distance distribution of a code of a given size. The main instrument of the proof is the Beckner inequality from Harmonic Analysis. We also show that the obtained bound is almost tight.

Keywords: Distance distributions, Beckner inequality.

1 Introduction

While there are quite a few papers on the computation of distance distributions of *given* codes or classes of codes (see, e.g., [4], [11]), *universal* upper bounds, i.e. bounds holding irrespectively of the code, given its rate only, are scarce (see however [8], [10], [2] for results bounding distance distribution components given the minimum distance of a code). We offer such a result here, proving, loosely speaking, that if the rate of a code is less than 1, then all its weight distribution components are exponentially smaller than corresponding binomial coefficients.

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

[†]School of Mathematics, Tel Aviv University, Tel Aviv, 69978 Israel; e-mail: krivelev@post.tau.ac.il

[‡]Department of Electrical Engineering-Systems, Tel Aviv University, Tel Aviv, 69978 Israel; e-mail: litsyn@eng.tau.ac.il. Supported in part by a USA-Israeli BSF Grant 1999-099.

This bears some similarity with results on codes with forbidden distances, where one looks for the largest possible (lim inf of) rates of a family of codes if one sets to 0 some weight component (see, e.g., [3]).

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. $wt(x)$ is equal to the number of ones in $\mathbf{x}$. Let $B(\mathbf{x}, r) \subseteq F^n$ stand for the ball of radius r centered in $\mathbf{x}$, with

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

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,

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

is $d = \delta(C)n$, where $\delta = \delta(C)$ is the code's relative distance. 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 a $\mathbf{c} \in C$ let

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

Notice that

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

If the code is linear (i.e. closed under component-wise modulo 2 sum), then for every $\mathbf{c} \in C$, $A_i(\mathbf{c}) = B_i$.

We also use 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 bounding possible distance distributions given the size of code. Namely, given R and ξ, such that $0 \leq R, \xi \leq 1$, we wish to estimate

$$b_\xi(R) := \max_C b_\xi(C),$$

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

Our main result supplies a negative answer to 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 a B_i of the same exponential order as $\binom{n}{i}$?* We do so by providing upper bounds on the distance distribution components.

The above cited result is a particular case of a much more general result, allowing to bound from above distance distribution components of a code, given *both* its rate and the minimal distance. This more general result can be applied to several other problems such as:

- estimating the undetected error probability over a binary symmetric channel (BSC) [9];

- bounding the covering radius of a linear code of given size and dual distance [6];

- estimating the threshold for maximum likelihood decoding error probability over a BSC as a function of code's minimum distance and size ([12], see also [13]).

These applications will be covered in a subsequent paper [7].

Throughout the paper all logarithms are binary, and

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

is the binary entropy.

2 Basic inequalities

We shall make use of the Beckner inequality [5], already appearing in a combinatorial context in e.g. [1, 8].

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 $0 < \varepsilon < 1$, 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 $0 < \varepsilon < 1$,*

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

$\diamond$

Let $A(n, d, \leq w)$ be the maximal possible number of binary n-vectors of weight at most w, being at Hamming distance at least d one from another.

We are now in a position to state the basic inequality.

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

$$\frac{1}{|C|} \sum_{\mathbf{c} \in C} \sum_{i=0}^{n} A_i(\mathbf{c}) \sum_{\ell=0}^{n} h(i,\ell) p^\ell (1-p)^{n-\ell} \leq \left(V(g) A^{1-2p}(n, d, \leq g) \right)^{\frac{1}{1-p}} \left(\frac{|C|}{2^n} \right)^{\frac{p}{1-p}},$$

where

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

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

Proof Set

$$\epsilon = \sqrt{1-2p}.$$

Define

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

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

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

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 $|C|V(g)/A(n,d,\leq g)$ summands in the last sum assume their maximum value of $A(n,d,\leq g)$, and this maximum is

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

Therefore,

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

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

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

Therefore

$$\sum_{\mathbf{v}\in F^n} T_\varepsilon^2(\mathbf{v}) = \sum_{\mathbf{v}\in F^n}\left(\sum_{\{\mathbf{c},\mathbf{u}\}_g} \rho^{d(\mathbf{u},\mathbf{v})}(1-\rho)^{n-d(\mathbf{u},\mathbf{v})}\right)^2$$

$$= \sum_{\mathbf{v}\in F^n}\sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g,\{\mathbf{c}_2,\mathbf{u}_2\}_g} \rho^{d(\mathbf{u}_1,\mathbf{v})+d(\mathbf{u}_2,\mathbf{v})}(1-\rho)^{2n-d(\mathbf{u}_1,\mathbf{v})-d(\mathbf{u}_2,\mathbf{v})}$$

$$= \sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g,\{\mathbf{c}_2,\mathbf{u}_2\}_g}\sum_{\mathbf{v}\in F^n} \rho^{d(\mathbf{u}_1,\mathbf{v})+d(\mathbf{u}_2,\mathbf{v})}(1-\rho)^{2n-d(\mathbf{u}_1,\mathbf{v})-d(\mathbf{u}_2,\mathbf{v})}$$

$$=: \sum_{\{\mathbf{c}_1,\mathbf{u}_1\}_g,\{\mathbf{c}_2,\mathbf{u}_2\}_g} G(\mathbf{u}_1,\mathbf{u}_2).$$

Now we calculate $G(\mathbf{u}_1,\mathbf{u}_2)$, which clearly 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

$$G(\mathbf{u}_1,\mathbf{u}_2) = \sum_{i=0}^{\ell}\sum_{j=0}^{n-\ell}\binom{\ell}{i}\binom{n-\ell}{j}\rho^{i+j+\ell-i+j}(1-\rho)^{n-i-j+n-\ell+i-j}$$

$$= \sum_{i=0}^{\ell} \sum_{j=0}^{n-\ell} \binom{\ell}{i} \binom{n-\ell}{j} \rho^{\ell+2j} (1-\rho)^{2n-\ell-2j}$$

$$= \left(\sum_{i=0}^{\ell} \binom{\ell}{i} \rho^{\ell} (1-\rho)^{\ell} \right) \left(\sum_{j=0}^{n-\ell} \binom{n-\ell}{j} \rho^{2j} (1-\rho)^{2n-2\ell-2j} \right)$$

$$= (2\rho(1-\rho))^{\ell} (\rho^2 + (1-\rho)^2)^{n-\ell}$$

Observe that, since $p = 2\rho(1-\rho)$, 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 we conclude

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

Noticing that $1 + \varepsilon^2 = 2(1-p)$, $\varepsilon^2 = 1 - 2p$, and applying the Beckner inequality we obtain the claimed result. $\diamond$

The function $h(i,l)$ appearing in the statement of the theorem is estimated in [7]. However, we shall not need it here.

Given a code C we can construct a new code C' (its complemented version) of size at most $2|C|$ by adding to it the binary complements of every codeword (which does not have its complement already in C). The code C' has symmetric distance distribution, i.e. $B_{\mu n}(C') = B_{(1-\mu)n}(C')$, and, asymptotically, possesses the same rate as C. Thus, assuming our codes self-complementary entails no loss of generality.

3 Distance distributions

We now focus on the particular case of $g = 0$ in Theorem 2. This corresponds to the case where no restriction on the minimum distance of a code is imposed.

Theorem 3 *1) For every* $0 < \mu < 1$, $b_{\mu}(R) \leq R$;

2) Let

$$0 < \mu \leq 1 - 2\sqrt{(1-R)\ln 2} + \ln 2 - R \ln 2 \ . \tag{1}$$

Define

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

If

$$p^* \leq 0.5 \tag{2}$$

then:

$$b_\mu(R) \leq -\frac{p^*}{1-p^*}(1-R) - \mu\log p^* - (1-\mu)\log(1-p^*) + o(1) . \tag{3}$$

Proof Since the first bound of the theorem $b_\mu \leq R$ is trivial, we may assume that conditions (1) and (2) hold. Setting $g = 0$ in Theorem 2, we obtain

$$\frac{1}{|C|}\sum_{\mathbf{c}\in C}\sum_{i=0}^{n} A_i(\mathbf{c})p^i(1-p)^{n-i} \leq \left(\frac{|C|}{2^n}\right)^{\frac{p}{1-p}} .$$

The left-hand side of the above inequality is trivially estimated from below by singling out any weight m:

$$\begin{aligned}\frac{1}{|C|}\sum_{\mathbf{c}\in C}\sum_{i=0}^{n} A_i(\mathbf{c})p^i(1-p)^{n-i} \geq \\ \geq p^m(1-p)^{n-m}\frac{1}{|C|}\sum_{\mathbf{c}\in C} A_m(\mathbf{c}) = \\ = p^m(1-p)^{n-m}B_m.\end{aligned}$$

Thus we get

$$B_m \leq \left(\frac{|C|}{2^n}\right)^{\frac{p}{1-p}} \cdot \frac{1}{p^m(1-p)^{n-m}}. \tag{4}$$

Note that this holds true for any $p \in [0, 0.5]$ and m. Fixing $m := \mu n$, and minimizing the right-hand side of (4) as a function of p, gives $p^*(\mu)$ as stated. Plugging then $p^*(\mu)$ in (4) yields (3). ◇

Corollary 1 *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 Again, (3) is valid for any μ and any p instead of p^*. Setting $\mu = p$ in (3), we get the result. ◇

In fact, last corollary shows that for any code of rate $R < 1$, every distance distribution component B_i is exponentially smaller than the corresponding binomial coefficient $\binom{n}{i}$.

4 A Lower Bound

For a lower bound we use the following construction. First compute w^*, defined as the largest integer such that $2\binom{n}{w^*} < |C|$. Notice that for rates strictly less than 1 we have $w^* < 0.5$. Pick now for codewords all vectors of weight w^* and their complements. The distance distribution of such a code is (assuming without loss of generality that n is even)

$$B_{2i} = \binom{w^*}{i}\binom{n-w^*}{i} + \binom{w^*}{\frac{n}{2}-i}\binom{n-w^*}{\frac{n}{2}-i}$$

and

$$B_{2i} = B_{n-2i}.$$

Theorem 4 *For any* $0 \leq \mu \leq 2\omega(1-\omega)$

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

where $\omega = H^{-1}(R)$. *Otherwise, for* $\mu \leq 0.5$,

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

Proof The first estimate follows from the construction. For the second one, consider a random constant weight code of size $|C|$ and weight $w > w^*$. Its average distance distribution is

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

Taking for code the union of the previous one and its complement, we conclude that the maximum of its distance distribution occurs when $i = \lfloor 2w(1-w) \rfloor$ or $i = \lceil 2w(1-w) \rceil$, and is of order $2^{Rn(1-o(1))}$. ◇

On Figure 1 the upper and lower bounds are presented for the distance distributions of codes of rate 0.5.

References

[1] 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.

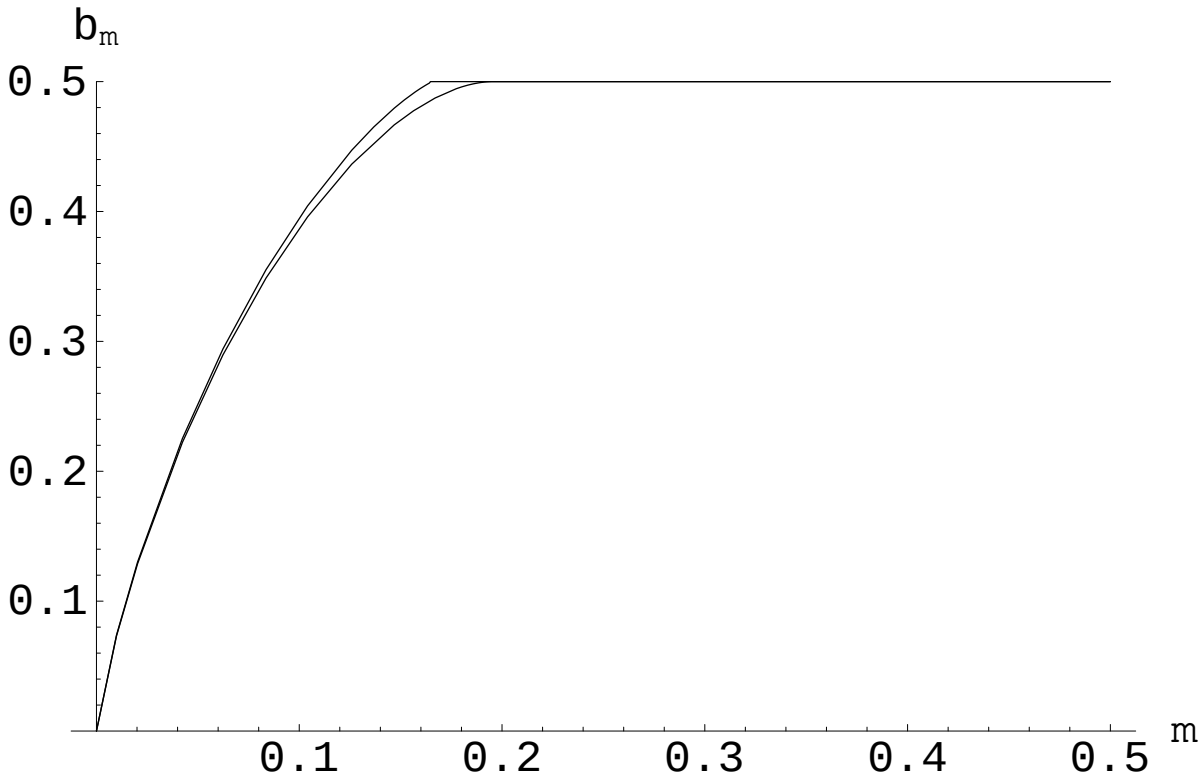

Figure 1: Upper and lower bounds on the distance distribution exponent for codes of rate 0.5

[2] 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.

[3] L. Bassalygo, G. Cohen, and G. Zémor, Codes with forbidden distances, *Discrete Mathematics*, 213, 2000, pp. 3-11.

[4] I.F. Blake, and R.C. Mullin, *The Mathematical Theory of Coding*, Academic Press, 1975.

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

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

[7] G. Cohen, M. Krivelevich, and S. Litsyn, manuscript.

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

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

[10] N. Linial and A. Samorodnitsky, Linear codes and character sums, manuscript.

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

[12] 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.

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