On Spectra of BCH Codes

Ilia Krasikov and Simon Litsyn

Abstract— **We derive an estimate for the error term in the binomial approximation of spectra of BCH codes. This estimate asymptotically improves on the earlier bounds by Sidelnikov, Kasami–Fujiwara–Lin, and Solé.**

Index Terms—**BCH codes, spectra of codes, Krawtchouk polynomials.**

I. Introduction

It is well known that the distance distribution of binary primitive BCH codes can be approximated by the binomial distribution. If C is the BCH code of length $n = 2^m - 1$ and with minimum distance $2t + 1 \le 2^{[(m+1)/2]} + 1$, the components of the distance distribution vector $\underline{b} = (b_0, \cdots, b_n)$ can be written as

$$b_i = \frac{\binom{n}{i}}{(n+1)^t}(1 + E_i) \tag{1}$$

where $|E_i|$ decreases with n. Several upper bounds on $|E_i|$ have been obtained. Sidelnikov [15] gave a bound of order $n^{-0.1}$ for i in the relevant range. Further improvements on this estimate have been derived by Kasami, Fujiwara, and Lin [3] and Solé [16].

The bound of [3] for n large enough, $t = o(\sqrt{n})$ and i linearly depending on n, $i = \sigma n$, gives

$$\frac{1}{n}\log_2 |E_{\sigma n}| \le \frac{\sigma}{2}((1 - \frac{5\sigma}{4})\log_2 e - \log_2 \sigma) \tag{2}$$

and the bound of [16] implies the following inequality:

$$\frac{1}{n}\log_2 |E_{\sigma n}| \le \frac{1}{2} - H(\sigma) \tag{3}$$

where $H(\sigma) = -\sigma \log_2(\sigma) - (1 - \sigma)\log_2(1 - \sigma)$.

In this correspondence we present new estimates of the relative error term improving the known results. Our approach is based on investigating upper bounds for absolute values of Krawtchouk polynomials. Actually, this is just a refinement of an idea due to P. Solé [16]. The bounds obtained are quite tight. Particularly, for t fixed our estimate is of order at most $O(n^{-1})$. This approach can be easily generalized to arbitrary codes with known dual distance width, see e.g., [3]. As it was mentioned by an anonymous referee, the approach works as well for wide classes of Goppa codes, Melas codes, etc., where bounds of Carlitz–Uchiyama type for the dual distance width are known (see, e.g. [5] ,[6], [11], [12]). Another upper estimates for values of Krawtchouk polynomials can be found in [4] where the expression for the envelope of absolute values of Krawtchouk polynomials was obtained.

Manuscript received March 16, 1994; revised October 2, 1994. The work of S. Litsyn was partly supported by the Guastallo Fellowship.

I. Krasikov is with Tel-Aviv University, School of Mathematical Sciences, Ramat-Aviv 69978 Tel-Aviv, Israel, and with Beit-Berl College, Kfar-Sava, Israel.

S. Litsyn is with Tel-Aviv University, Department of Electrical Engineering–Systems, Ramat-Aviv 69978 Tel-Aviv, Israel.

IEEE Log Number 9410123.

II. The Main Result

We will need some well known results about Krawtchouk polynomials (see, e.g., [7], [8], [10], [17]).

The binary Krawtchouk polynomial $P_k^n(x)$ (of degree k in x) is defined by the following generating function:

$$\sum_{k=0}^{\infty} P_k^n(x) z^k = (1 - z)^x (1 + z)^{n-x}. \tag{4}$$

Usually n is fixed and, when it does not lead to confusion, is omitted. We need some particular values of $P_k(i)$, namely,

$$P_k(0) = \binom{n}{k}. \qquad P_k(n) = (-1)^k \binom{n}{k}.$$

From Cauchy's integral formula we get for nonnegative integer x (see, e.g., [16]):

$$\begin{aligned} P_k(x) &= \frac{1}{2\pi i} \oint \frac{(1+z)^{n-x}(1-z)^x}{z^{k+1}}\, dz \\ &= \frac{(-i)^x}{2\pi} \int_0^{2\pi} \exp[i(n/2 - k)\theta] \cos^{n-x}(\theta/2) \sin^x(\theta/2)\, d\theta. \end{aligned}$$

Thus for n and x even we have

$$\begin{aligned} |P_k(x)| &= \frac{1}{2\pi} \left| \int_0^{2\pi} \exp[i(n/2 - k)] \cos^{n-x}(\theta/2) \sin^x(\theta/2)\, d\theta \right| \\ &\le \frac{1}{2\pi} \int_0^{2\pi} \cos^{n-x}(\theta/2) \sin^x(\theta/2)\, d\theta = |P_{n/2}(x)|. \end{aligned}$$

Hence, the following inequality holds (note, that in the sequel i is an integer, not $\sqrt{-1}$).

Lemma 1: For n and i even, $|P_k(i)| \le |P_{n/2}(i)|$.

Let us find the values $P_{n/2}(i)$ for even n and i's. The following symmetry relation holds for integer k and i (see, e.g. [8]):

$$\binom{n}{i} P_k(i) = \binom{n}{k} P_i(k). \tag{5}$$

From (4) we get

$$\sum_{k=0}^{\infty} P_k(n/2) z^k = (1 - z)^{n/2}(1 + z)^{n/2} = (1 - z^2)^{n/2}$$

thus

$$P_{2k}(n/2) = (-1)^k \binom{n/2}{k}$$

and

$$P_{n/2}(i) = (-1)^{i/2} \frac{\binom{n}{n/2}\binom{n/2}{i/2}}{\binom{n}{i}}. \tag{6}$$

So, from (5) and Lemma 1 we get for even n and i

$$|P_i(k)| = \frac{\binom{n}{i}}{\binom{n}{k}} |P_k(i)| \le \frac{\binom{n}{i}}{\binom{n}{k}} |P_{n/2}(i)|.$$

Employing (6) we obtain the following lemma.

Lemma 2: For k integer, and n and i even

$$|P_i(k)| \le \frac{\binom{n}{n/2}\binom{n/2}{i/2}}{\binom{n}{k}}.$$

Now we are in a position to analyze the weight distribution of BCH codes. Consider the extended BCH code C of length $n = 2^m$, cardinality 2^{n-mt-1}, and minimum distance $d = 2t+2 \le 2^{[(m+1)/2]}+2$. Let the distance distribution of the code be $\underline{B} = (B_0, \cdots, B_n)$, $B_0 = B_n = 1$, $B_{2i+1} = 0$ for $i = 0, \cdots, n/2-1$, and $B_i = B_{n-i} = 0$ for $i = 1, 2, \cdots, 2t+1$. For usual (nonextended) BCH code of length $n-1$ and minimum distance $2t+1$ we denote its spectrum by $\underline{b} = (b_0, \cdots, b_{n-1})$. Since the extended BCH code is doubly transitive we have the following result relating the values of odd and even components of the spectra of BCH codes (see, e.g., [10, ch. 8.5, Theorems 14 and 16]).

Lemma 3:

$$b_{2i-1} = \frac{2iB_{2i}}{n} \qquad b_{2i} = \frac{(n-2i)B_{2i}}{n}.$$

We start with estimating the spectrum of the extended BCH code. Let $\underline{B}' = (B'_0, \cdots, B'_n)$ stand for the spectrum of the dual C' of the extended BCH code, where $\underline{B}'$ is determined by the MacWilliams transform of $\underline{B}$

$$B'_k = \frac{|C'|}{2^n}\sum_{i=0}^{n} B_i P_k(i) \tag{7}$$

and $B'_i = B'_{n-i}$ for $i = 0, \cdots, n$, $B'_0 = B'_n = 1$, $B'_{2i+1} = 0$ for $i = 0, \cdots, n/2-1$, and for $2t+1 \le 2^{[(m+1)/2]}+1$

$$B'_i = B'_{n-i} = 0, \quad \text{for } i = 1, \cdots, d' = [n/2 - (t-1)\sqrt{n}]. \tag{8}$$

The last relation is due to Weil–Carlitz–Uchiyama (see [10, ch. 9.9] and [9], [13], [14] for further refinements). Denote by D' the segment $[d', \cdots, n-d']$. Note that for the considered range of t

$$\sum_{i=0}^{n} B'_i = |C'| = 2n^t.$$

Inverting (7) we have

$$\begin{aligned} B_i &= \frac{1}{2n^t}\sum_{k=0}^{n} B'_k P_i(k) \\ &= \frac{1}{2n^t}\left(B'_0 P_i(0) + B'_n P_i(n) + \sum_{k\in D'} B'_k P_i(k)\right). \end{aligned}$$

We consider only even i's, since, otherwise, $B_i = 0$. Hence

$$B_i = \frac{1}{2n^t}\left(2\binom{n}{i} + \sum_{k\in D'} B'_k P_i(k)\right)$$

i.e., for i even we have

$$B_i = \frac{\binom{n}{i}}{n^t}(1+E_i)$$

where

$$|E_i| = \frac{1}{2\binom{n}{i}}\left|\sum_{k\in D'} B'_k P_i(k)\right| \le \frac{n^t}{\binom{n}{i}}\max_{k\in D'}|P_i(k)|.$$

Now since n and i are even we may use Lemma 2, thus getting

Theorem 1: In the extended BCH code of length $n = 2^m$ and minimum distance $2t+2 \le 2^{[m+1]/2}+2$

$$B_i = 0, \text{ for } i \text{ odd}$$

$$B_i = \frac{\binom{n}{i}}{n^t}(1+E_i), \text{ for } i \text{ even}$$

where

$$|E_i| \le \frac{n^t\binom{n}{n/2}\binom{n/2}{i/2}}{\binom{n}{i}\binom{n}{d'}}. \tag{9}$$

Using Lemma 3 we obtain the following result for usual BCH codes.

Theorem 2: In the BCH code of length $\hat{n} = n-1 = 2^m - 1$ and minimum distance $2t+1 \le 2^{[(m+1)/2]}+1$

$$b_i = \frac{\binom{\hat{n}}{i}}{n^t}(1+E_{i^*})$$

where $i^* = i+1$ for i odd, and $i^* = i$ for i even, and $|E_i|$ is estimated in (9).

Using the theorems we can analyze some particular cases.

From standard estimates [1, ch. 7, § 2] of binomial coefficients we have

$$\ln\frac{\binom{n}{n/2}}{\binom{n}{d'}} = 2(t-1)^2 + O(\frac{(t-1)^4}{n}).$$

Therefore, for $t = o(n^{\frac{1}{4}})$,

$$\ln\frac{\binom{n}{n/2}}{\binom{n}{d'}} = 2(t-1)^2 + o(1),$$

and for $t = o(\sqrt{n})$

$$\ln\frac{\binom{n}{n/2}}{\binom{n}{d'}} = o(n).$$

This leads to straightforward corollaries from Theorems 1 and 2.

Corollary 1: If $t = o(\sqrt{n})$, and i grows linearly with n, $i/n = \sigma + o(1)$, then

$$\frac{1}{n}\log_2|E_{\sigma n}| \le -\frac{1}{2}H(\sigma) + o(1).$$

Comparing the result of the corollary with (2) and (3) we conclude that our estimate is better for all $\sigma \in (0,1)$.

Assuming $t = o(n^{\frac{1}{4}})$, we give somehow sharper estimates, particularly good for small i's. We use that for $i = o(\sqrt{n})$ from Stirling approximation we have

$$\frac{\binom{n/2}{i/2}}{\binom{n}{i}} = \sqrt{2}\,e^{-\frac{i}{2}}\,(\frac{i}{n})^{i/2}(1+o(1)).$$

Corollary 2: If $t = o(n^{\frac{1}{4}})$, $i = o(\sqrt{n})$, then

$$|E_i| \le \sqrt{2}\,i^{i/2}\,e^{2(t-1)^2 - i/2}\,n^{t-i/2}\,(1+o(1)).$$

If t and i are constants then we have $|E_i| = O(n^{t-i/2})$ (it was proven also in [3]). Since the maximum error occurs in $|E_{2t+2}|$, we always have $|E_i| = O(n^{-1})$.

Finally, for BCH codes we get

Theorem 3: Let $t = o(n^{\frac{1}{4}})$ and $l = [(i+1)/2]$, then in the BCH code of length $n = 2^m - 1$ and with minimum distance $2t+1$

$$b_i = \frac{\binom{n}{i}}{(n+1)^l}(1 + E_{2l})$$

where the error term is upperbounded as follows:

$$|E_{2l}| \leq \sqrt{2}\,(2l)^l \exp\left[2(t-1)^2 - \frac{l(n-2l)}{n}\right] n^{t-l}(1 + o(1)).$$

Note:

After the correspondence had been submitted we were informed that a similar, slightly weaker (by a factor $\sqrt{n}$), bound can be derived from arguments presented in [2]. Their approach is quite different from that of ours.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for helpful suggestions.

REFERENCES

[1] W. Feller, *An Introduction to Probability Theory and Its Applications*. New York: Wiley, 1970.
[2] I. Gashkov and V. Sidelnikov, "Linear ternary quasiperfect codes correcting double errors," *Probl. Peredachi Inform.*, vol. 22, no. 4, pp. 43–48, 1986.
[3] T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight distribution of binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 6, pp. 769–780, 1985.
[4] I. Krasikov and S. Litsyn, "Bounds for Krawtchouk polynomials," in preparation.
[5] G. Lachaud, "Distribution of the weights of the dual code of the Melas code," *Discrete Math.*, vol. 79, pp. 103–106, 1989.
[6] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 686–692, 1990.
[7] V. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," submitted for publication.
[8] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1992.
[9] S. Litsyn, C. J. Moreno, and O. Moreno, "Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables," *Applicable Algebra in Eng., Commun. Comput.*, vol. 5, pp. 105–116, 1994.
[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.
[11] C. J. Moreno and O. Moreno, "Exponential sums and Goppa codes I," *Proc. Amer. Math. Soc.*, vol. 111, pp. 523–531, 1991.
[12] ——, "Exponential sums and Goppa codes II," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1222–1229, 1992.
[13] O. Moreno and C. J. Moreno, "The MacWilliams-Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1894–1907, Nov. 1994.
[14] F. Rodier, "On the spectra of the duals of binary BCH codes of designed distance $\delta = 9$," *IEEE Trans. Inform. Theory*, vol. 38, pp. 478–479, 1992.
[15] V. M. Sidelnikov, "Weight spectrum of binary Bose–Chaudhuri–Hocquenghem codes," *Probl. Peredachi Inform.*, vol. 7, no. 1, pp. 14–22, 1971.
[16] P. Solé, "A limit law on the distance distribution of binary codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 229–232, 1990.
[17] G. Szegö, *Orthogonal Polynomials*. Providence, RI: Amer. Math. Soc. Colloq. Publ., vol. 23, 1975.

On Primitive BCH Codes with Unequal Error Protection Capabilities

Robert H. Morelos-Zaragoza, *Member, IEEE*, and Shu Lin, *Fellow, IEEE*

***Abstract*—We present a class of binary primitive BCH codes that have unequal-error-protection (UEP) capabilities. We use a recent result on the span of their minimum weight vectors to show that binary primitive BCH codes, containing second-order punctured Reed–Muller (RM) codes of the same minimum distance, are binary-cyclic UEP codes. The values of the error correction levels for this class of binary LUEP codes are estimated.**

***Index Terms*—Unequal error protection codes, binary primitive BCH codes.**

I. INTRODUCTION

Unequal error protection codes protect some of the encoded message symbols against more errors than the error correction level given by their minimum Hamming distance. Linear unequal error protection (LUEP) codes were first introduced by Masnick and Wolf [1]. They discussed linear codes, specified by their parity check matrices, providing a level of error correction beyond that given by the minimum distance of the code, for some codeword positions. Gore and Kilgus [2] introduced an example $(15, 9)$ binary-cyclic UEP code with minimum distance 4 that can correct one information bit against the occurrence of two errors. That is, the most significant bit can always be decoded in the presence of up to two random errors in a received vector. Since then, other cyclic UEP codes have been introduced [3], [4]. Binary BCH codes form a popular family of cyclic codes that have found numerous practical applications, due to their ability to correct multiple random errors, as well as their efficient coding and decoding procedures. Therefore, it is of interest to find conditions under which binary BCH codes are binary LUEP codes.

To analyze the multilevel error correcting capabilities of binary linear codes, the concept of set of minimum weight vectors is fundamental.

Definition [5]: Let C be an (n, k, d) linear code. The set of minimum-weight codewords, denoted $\mathcal{M}$, is defined as

$$\mathcal{M} \triangleq \{\bar{c} \in C : 0 < \mathrm{wt}(\bar{c}) \leq 2\epsilon, \epsilon > t\}$$

where $\mathrm{wt}(\bar{c})$ denotes the Hamming weight of vector $\bar{c}$, and $t = \lfloor (d-1)/2 \rfloor$.

With the above definition, Boyarinov and Katsman [5] found conditions for linear codes to be LUEP codes:

Lemma 1: To provide the protection level ϵ for at least k^* information digits of an (n, k, d) linear code C, it is necessary and

Manuscript received August 18, 1993; revised May 2, 1994. Part of this work was supported by NASA under Grant NAG 5-931, and by the NSF under Grants NCR-88813480 and NCR-9115400. The material in this correspondence was presented at the International Symposium on Information Theory, Trondheim, Norway, 1994.

R. H. Morelos-Zaragoza was with the Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka 560, Japan. He is now with the Third Department, Institute of Industrial Science, University of Tokyo, 7-22-1, Roppongi, Minatoku, Tokyo 106, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822 USA.

IEEE Log Number 9410417.