More on the distance distribution of BCH codes

Osnat Keren and **Simon Litsyn**
Department of Electrical Engineering – Systems,
Tel Aviv University,
Tel Aviv 69978 Israel
e-mail: {osnatk,litsyn}@eng.tau.ac.il

Abstract

We derive a new estimate for the error term in the binomial approximation to the distance distribution of BCH codes. This is an improvement on the earlier bounds by Kasami-Fujiwara-Lin, Vladuts-Skorobogatov, and Krasikov-Litsyn.

Keywords: BCH codes, distance distribution

1 Introduction

Consider the primitive t-error correcting BCH code of length $2^m - 1$ where $2t-2 < 2^{\frac{m}{2}}$. It is well known (see e.g. [4, §9.3]) that for such t, the dimension of the code is $2^m - 1 - mt$. Furthermore, the distance distribution of the code is approximately binomial [4, §9.10] . Namely, the number, b_i, of codewords of weight i is

$$b_i = \frac{\binom{2^m-1}{i}}{2^{mt}}(1 + E_i),$$

where the error term E_i tends to zero when m grows. Moreover, given m, the more i is, the less is the error term. Therefore, it is important to have tight estimates for small values of i.

The distance distributions of the BCH code and its extended code of length $n = 2^m$ are related [4, §8.5]. If B_i stands for the i-th component of the weight distribution of the extended code, then

$$b_{2k} = \frac{(n-2k)B_{2k}}{n}, \qquad b_{2k-1} = \frac{2kB_{2k}}{n}.$$

In earlier papers several upper bounds on the error term for the extended code were presented, see [2, 3, 5, 6, 7, 8] and references therein. The best known bounds for small values of k are due to Kasami-Fujiwara-Lin [3] and Vladuts-Skorobogatov [7, 8]. In [2], properties of Krawtchouk polynomials were used to obtain an upper bound on the error term. As k grows this bound becomes tighter.

As it was suggested in [3], one can obtain bounds on the distance distribution components of the BCH code by solving a linear programming problem. Namely, it is necessary to minimize or maximize the corresponding component under constraints implied by the non-negativity of the MacWilliams transform. This numerical approach is tractable for moderate lengths of codes. However, it is preferable to have analytical estimates applicable to codes of big lengths.

Here we use the linear programming approach to derive analytical upper and lower bounds on B_{2k} of the form

$$\frac{\binom{n}{2k}}{n^t}(1-\underline{E}_{2k}) \le B_{2k} \le \frac{\binom{n}{2k}}{n^t}(1+\overline{E}_{2k}), \tag{1}$$

where $\underline{E}_{2k}$ and $\overline{E}_{2k}$ are given by recursive expressions. We prove that for $t+1 \le k < 2(t-1)$, the derived bounds are tighter than those obtained in [2], [3] and [7, 8]. In particular we have

$$\overline{E}_{2k} \le n^{-(k-t)}\ 2\ t!\ (2(t-1))^{2(k-t)}\ (1+O(n^{-1}))$$

and

$$\underline{E}_{2k} \le \frac{k}{2}\overline{E}_{2k}.$$

The paper is organized as follows. We start from reducing the problem to a search for polynomials having special properties. Then we obtain recursive expressions for $\underline{E}_{2k}$ and $\overline{E}_{2k}$. We show that for $k = t+1$ it is in agreement with the Farr bound on the minimum length of BCH codes with the designed distance equal to the true minimum distance. Finally, for $k < 2(t-1)$ we give some estimates on the behavior of the error terms when n grows.

2 Estimates for the weight distribution

Denote by $P_i(x)$ the Krawtchouk polynomial of degree $i, i = 0, \ldots, n$,

$$P_i(x) = \sum_{k=0}^{i} (-1)^k \binom{x}{k} \binom{n-x}{i-k}.$$

The Krawtchouk polynomials satisfy the following orthogonal relation,

$$\sum_{i=0}^{n} P_k(i) P_i(l) = \delta_{k,l} 2^n.$$

For other properties of Krawtchouk polynomials see e.g. [1, §2.3] and [4].

Denote by $B'_i, i = 0, \ldots, n$, the weight distribution of the dual code, and let d' stand for its minimum distance. By the Weil-Carlitz-Uchiyama inequality [4, §9.9] we have $d' \geq n/2 - (t-1)\sqrt{n}$. Therefore,

$$\begin{aligned} B_0 &= B'_0 = 1, \\ B_n &= B'_n = 1, \\ B'_i &= B'_{n-i} = 0 \text{ for } i = 1, \ldots, d'-1, \\ B_i &= B_{n-i} = 0 \text{ for } i = 1, \ldots, 2t+1. \end{aligned}$$

Let $h(x) = \sum_{i=0}^{n} h_i P_i(x)$, where $h_i = (1/2^n) \sum_{j=0}^{n} h(j) P_j(i)$. The following relation follows from the MacWilliams identity [4, p.129]:

$$\sum_{i=0}^{n} B_i h_i = \frac{1}{2n^t} \sum_{k=0}^{n} \sum_{j=0}^{n} B'_j h(k) \frac{1}{2^n} \sum_{i=0}^{n} P_i(j) P_k(i) = \frac{1}{2n^t} \sum_{i=0}^{n} B'_i h(i) \qquad (2)$$

By choosing different polynomials $h(x)$ we can derive bounds on the weight distribution of the extended BCH code.

Theorem 1 *Let $f(x) = \sum_{i=0}^{k} f_{2i} P_{2i}(x)$ and $g(x) = \sum_{i=0}^{k} g_{2i} P_{2i}(x)$ be functions even with respect to $n/2$, such that $f_{2k} > 0, g_{2k} > 0$, and*

$$\begin{aligned} f(x) &\geq 0 \quad , \quad \forall x \\ g(x) &\leq 0 \quad , \quad d' \leq x \leq n - d' \end{aligned}$$

Then,

$$\underline{B}_{2k} \leq B_{2k} \leq \overline{B}_{2k}$$

where

$$\underline{B}_{2k} = \frac{\binom{n}{2k}}{n^t}(1-\underline{E}_{2k}) = \frac{\frac{f(0)}{n^t} - f_0 - \sum_{i=t+1}^{k-1} f_{2i}B_{2i}}{f_{2k}},$$
$$\overline{B}_{2k} = \frac{\binom{n}{2k}}{n^t}(1+\overline{E}_{2k}) = \frac{\frac{g(0)}{n^t} - g_0 - \sum_{i=t+1}^{k-1} g_{2i}B_{2i}}{g_{2k}}.$$

Proof ¿From (2) we have

$$f_0B_0 + \sum_{i=t+1}^{k} f_{2i}B_{2i} = \frac{f(0)}{n^t} + \frac{1}{n^t}\sum_{i=d'}^{n/2} B'_i f(i) \geq \frac{f(0)}{n^t}$$
$$g_0B_0 + \sum_{i=t+1}^{k} g_{2i}B_{2i} = \frac{g(0)}{n^t} + \frac{1}{n^t}\sum_{i=d'}^{n/2} B'_i g(i) \leq \frac{g(0)}{n^t}$$

□

Substitution of $f_{2i}, g_{2i}, \underline{B}_{2i}$ and $\overline{B}_{2i}$ gives bounds for B_{2k}. Notice that the upper and lower bound on the first weight distribution component, B_{2t+2}, depend only on $f(x)$ and $g(x)$. Therefore, one can calculate the bounds $\overline{B}_{2t+4}$, $\underline{B}_{2t+4}$ from $\overline{B}_{2t+2}$ and $\underline{B}_{2t+2}$. This process can be continued towards the higher spectra components, which are estimated using the recurrence relation given in Theorem 1.

We now proceed with the analysis of the error terms. The bounds on $\underline{E}_{2k}$ and $\overline{E}_{2k}$, will be obtained by choosing $f(x) = P_k^2(x)$ and $g(x) = (P_2(x) + C_t)P_{k-1}^2(x)$, where $C_t = -P_2(n/2 - (t-1)\sqrt{n})$. Indeed, the coefficients f_{2i} are always positive. The coefficients of $g(x)$, g_{2i}, are negative for small i, say in the interval $0 \leq i \leq \hat{i}(k)$, and are non-negative afterwards. Namely, (see Appendix)

$$f_{2i} = \binom{2i}{i}\binom{n-2i}{k-i} \tag{3}$$
$$g_{2i} = \begin{cases} \binom{2k}{k}\frac{k^2}{2} & i = k \\ \binom{2i}{i}\binom{n-2i}{k-i-1}A(k,i) & 0 \leq i < k \end{cases} \tag{4}$$
$$A(k,i) = C_t + \frac{i^2\binom{n-2(i-1)}{2}}{(k-i)(n-k-i+2)} + 2i(n-2i) + \frac{(2i+1)(k-i-1)(n-k-i+1)}{(i+1)}.$$

In what follows we use the notation $x \cong y$ for $x = y(1 + O(n^{-1}))$, and $x \preceq y$ for $x \leq y(1+O(n^{-1}))$. The proof of the following lemma is given in Appendix.

Lemma 1

$$\begin{aligned}
\underline{E}_{2k} &\cong \frac{\sum_{i=t}^{k-1} f_{2i}\binom{n}{2i}\overline{E}_{2i}}{f_{2k}\binom{n}{2k}} \\
\overline{E}_{2k} &\cong \frac{-g_{2t}\binom{n}{2t}\underline{E}_{2t} + \sum_{i=t+1}^{\hat{i}(k)} -g_{2i}\binom{n}{2i}\overline{E}_{2i} + \sum_{i=\hat{i}(k)+1}^{k-1} g_{2i}\binom{n}{2i}\underline{E}_{2i}}{g_{2k}\binom{n}{2k}}, \qquad (5)
\end{aligned}$$

where $\overline{E}_{2t} = \frac{f_0 n^t}{f_{2t}\binom{n}{2t}} - 1$, $\underline{E}_{2t} = \frac{g_0 n^t}{g_{2t}\binom{n}{2t}} - 1$, *and* f_{2i} *and* g_{2i} *are defined in (3) and (4).*

For $k = t + 1$ we obtain upper and lower bounds on the error terms of the first distance distribution component, B_{2t+2}.

Corollary 1

$$\begin{aligned}
\underline{E}_{2t+2} &\preceq n^{-1}\,(t+1)! \\
\overline{E}_{2t+2} &\preceq n^{-1}\,4\,t!(t-1)^2
\end{aligned}$$

Proof Since $\overline{E}_{2t} < \frac{f_0 n^t}{f_{2t}\binom{n}{2t}}$, we have

$$\begin{aligned}
\underline{E}_{2t+2} &= \frac{f_{2t}\binom{n}{2t}\overline{E}_{2t}}{f_{2(t+1)}\binom{n}{2t+2}} < \frac{f_0 n^t}{f_{2(t+1)}\binom{n}{2t+2}} \\
&= \frac{\binom{n}{t+1}n^t}{\binom{2t+2}{t+1}\binom{n}{2t+2}} \\
&= (t+1)!\frac{n^t}{(n-t-1)(n-t-2)\cdots(n-2t-1)} \\
&= n^{-1}(t+1)!\prod_{i=t+1}^{2t+1}(1+\frac{i}{n-i}) \\
&\cong n^{-1}\,(t+1)!
\end{aligned}$$

In a similar way we derive the second result;

$$\begin{aligned}
\overline{E}_{2t+2} &= \frac{-g_{2t}\binom{n}{2t}\underline{E}_{2t}}{g_{2(t+1)}\binom{n}{2t+2}} \\
&< \frac{-g_0 n^t}{g_{2t+2}\binom{n}{2t}} \\
&= \frac{n^t\binom{n}{t}(-C_t - t(n-t))}{\binom{2t+2}{t+1}\frac{(t+1)^2}{2}\binom{n}{2t+2}} \\
&\preceq n^{-1}\ 4t!(t-1)^2
\end{aligned}$$

□

The lower bound $\underline{E}_{2t+2}$ gives us an information about the true minimum distance of the code. Namely, if $\underline{E}_{2t+2} < 1$, then the designed distance equals to the true minimum distance. Indeed the code has at least $\frac{\binom{n}{2t+2}}{n^t}(1-\underline{E}_{2t+2})$ codewords of weight $2(t+1)$. Thus, our result is in agreement with the Farr bound [4, §9.2].

Table 1 compares the new bounds with the earlier known bounds on the error term E_{2t+2}. Our bounds are better by a factor of at least $2^{2t-2}/t^2$ than the known estimates.

In what follows we derive upper bounds on $\overline{E}_{2k}$ and $\underline{E}_{2k}$ for $k < 2(t-1)$, and compare them with earlier results. Define the *normalized* error terms as

$$\begin{aligned}
\underline{H}_{2k} &= n^{k-t}\underline{E}_{2k}, \\
\overline{H}_{2k} &= n^{k-t}\overline{E}_{2k},
\end{aligned}$$

Notice that both $\underline{H}_{2t}$ and $\overline{H}_{2t}$ are decreasing in k, namely,

$$\begin{aligned}
\overline{E}_{2t} &= \frac{f_0 n^t}{f_{2t}\binom{n}{2t}} - 1 \preceq \frac{t!}{\binom{k}{t}} \\
\underline{E}_{2t} &= \frac{g_0 n^t}{g_{2t}\binom{n}{2t}} - 1 \preceq \frac{2t!}{\binom{k-1}{t}}
\end{aligned}$$

The maximal values are attained for $k = t+1$, i.e. $\underline{H}_{2t}, \overline{H}_{2t} \preceq 2t!$.

Table 1: The error term in the binomial approximation of B_{2t+2}.

Bound	$n \cdot E_{2t+2}$
Vladuts-Skorobogatov [7]	$(2t+2)!\, e^{2t+2}$
Krasikov-Litsyn [2]	$2^{t+1}\ (t+1)!\, e^{2(t-1)^2}$
Kasami, Fujiwara and Lin [3]	$2^{2t}\ t!$
$\overline{E}_{2t+2}$	$4(t-1)^2\ t!$
$\underline{E}_{2t+2}$	$(t+1)!$

Lemma 2 *For $t+1 \leq k < 2(t-1)$,*

$$\begin{aligned} \overline{H}_{2k} &\preceq 2\ t!\ (2(t-1))^{2(k-t)} \\ \underline{H}_{2k} &\preceq \frac{k}{2}\overline{H}_{2k} \end{aligned}$$

Proof Notice that for $k < 2(t-1)$ the coefficients $A(k,m)$, $m = 0, \ldots, k-1$, are negative (see Appendix), thus $\hat{i}(k) = k-1$. From (5) we have

$$\begin{aligned} \overline{H}_{2k} &= n^{k-t} \frac{-g_{2t}\binom{n}{2t}\underline{E}_{2t} + \sum_{m=t+1}^{k-1} -g_{2m}\binom{n}{2m}\overline{E}_{2m}}{g_{2k}\binom{n}{2k}} \\ &\preceq \sum_{m=t}^{k-1} \frac{-A(k,m)k!^2}{nm!^2(k-m-1)!k^2/2}\overline{H}_{2m} \\ &\preceq \left(4(t-1)^2 - (k-1)^2\right)\overline{H}_{2(k-1)} + \\ &\quad \sum_{m=t}^{k-2} D(k,m)\frac{-A(k-1,m)(k-1)!^2}{nm!^2(k-m-2)!(k-1)^2/2}\overline{H}_{2m} \end{aligned}$$

where,

$$D(k,m) = \frac{A(k,m)k!^2(k-1)^2(k-m-2)!}{A(k-1,m)(k-1)!^2k^2(k-m-1)!}$$

$$
\begin{aligned}
&= (k-1)^2 \frac{A(k,m)}{A(k-1,m)(k-m-1)} \\
&\leq (k-1)^2 \frac{C_t - n + n\left(\frac{m^2}{2(k-m)} + \frac{2m+1}{m+1}\right)}{C_t - n + n\left(\frac{m^2}{2(k-1-m)} + \frac{(2m+1)(k-1)}{m+1}\right)} \\
&\leq (k-1)^2
\end{aligned}
$$

Therefore,

$$\overline{H}_{2k} \preceq \left(\left(4(t-1)^2 - (k-1)^2\right) + (k-1)^2\right)\overline{H}_{2(k-1)}$$

or

$$\overline{H}_{2k} \preceq 2\ t!\ (2(t-1))^{2(k-t)}.$$

As for the upper bound on $\underline{H}_{2k}$, notice that for $k < 2(t-1)$ we have

$$
\begin{aligned}
\underline{H}_{2k} &= n^{k-t} \frac{\sum_{m=t}^{k-1} f_{2m}\binom{n}{2m}\overline{E}_{2m}}{f_{2k}\binom{n}{2k}} \\
&= \sum_{m=t}^{k-1} n^{k-t} \frac{\binom{2m}{m}\binom{n-2m}{k-m}\binom{n}{2m}}{\binom{2k}{k}\binom{n}{2k}}\overline{E}_{2m} \\
&\preceq \sum_{m=t}^{k-1} \frac{k!^2}{m!^2(k-m)!}\overline{H}_{2m} \\
&\cong \sum_{m=t}^{k-1} \left(\frac{-A(k,m)k!^2}{nm!^2(k-m-1)!k^2/2}\overline{H}_{2m}\right)\left(\frac{nk^2/2}{-A(k,m)(k-m)}\right)
\end{aligned}
$$

Since both $-A(k,m)$ and $(k-m)$ are decreasing with m, the maximum is attained when $m = k-1$. Thus we have

$$\underline{H}_{2k} \preceq \overline{H}_{2k}\frac{k^2}{4(t-1)^2 - k^2} \preceq \frac{k}{2}\overline{H}_{2k}$$

□

Table 2 demonstrates the improvement on the earlier known bounds. To simplify the presentation of the results we use a lower bound on the error term given in [3] for $k \geq t+3$, and the upper bounds of Lemma 2. The lower bound on the error term of [3] was obtained by taking only one term of the sum given in [3, (73)].

Table 2: The normalized error term in the binomial approximation of B_{2k}, $t+1 \leq k < 2(t-1)$

Bound	H_{2k}
Vladuts-Skorobogatov	$(2k)!\ e^{2t+2}$
Krasikov-Litsyn	$2^k\ k!\ e^{2(t-1)^2}$
Kasami et al. $\succeq$	$2^t(t-1)!\ [2(t-1)]^{2k-2t}$
$\overline{H}_{2k}\ \preceq$	$2\ t!\ (2(t-1))^{2(k-t)}$
$\underline{H}_{2k}\ \preceq$	$t \cdot 2\ t!\ (2(t-1))^{2(k-t)}$

Table 3: Extended 3-error correcting BCH code over $GF(2^8)$

Error term E_{2k}	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
Exact	0.122	$-6.3E(-3)$	$2.2E(-4)$	$-4.6E(-6)$	$-4.74E(-8)$
$\overline{E}$	0.257	$6.76E(-3)$	$3.32E(-3)$	$8.50E(-4)$	$33.3E(-4)$
$-\underline{E}$	-0.0368	$-2.48E(-2)$	$-2.80E(-3)$	$-8.94E(-4)$	$-3.32E(-4)$
Kasami et al.	3.2	$2.58E(-1)$	$4.05E(-2)$	$4.17E(-3)$	$7.63E(-4)$
Vladuts-Skorobogatov	$4.69E(+5)$	$1.65E(+5)$	$8.51E(+4)$	$6.05E(+4)$	$5.67E(+4)$
Krasikov-Litsyn	$1.37E(+3)$	$5.01E(+1)$	2.25	$1.20E(-1)$	$7.48E(-3)$

Tables 3 and 4 present different numerical bounds on the error terms of the weight distribution of the extended 3-error correcting BCH codes of length 2^m, $m = 8, 12$. The exact values, taken from [3], are compared with the calculated bounds of Krasikov-Litsyn [2], Vladuts-Skorobogatov [7], Kasami et al. [3, (72),(73)] and the upper and lower bounds given in Lemma 1.

Table 4: Extended 3-error correcting BCH code over $GF(2^{12})$

Error term E_{2k}	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
Exact	$7.11E(-3)$	$-2.27E(-5)$	$5.0E(-8)$	$-7.24E(-11)$	$-6.65E(-16)$
$\overline{E}$	$1.47\,E(-2)$	$2.31E(-5)$	$6.93E(-7)$	$1.05E(-8)$	$2.44E(-10)$
$-\underline{E}$	$-1.97E(-3)$	$-8.53E(-5)$	$-5.76E(-7)$	$-1.10E(-8)$	$-2.42E(-10)$
Kasami et al.	$1.81E(-1)$	$8.54E(-4)$	$7.73E(-6)$	$4.53E(-8)$	$4.64E(-10)$
Vladuts-Skorobogatov	$2.93E(+4)$	$6.45E(+2)$	$2.08E(+1)$	$9.23E(-1)$	$5.41E(-2)$
Krasikov-Litsyn	$7.70E(+1)$	$1.69E(-1)$	$4.56E(-4)$	$1.45E(-6)$	$5.34E(-9)$

Appendix

Proof of Lemma 1 Let $f(x) = P_k^2(x)$, clearly $f(x)$ satisfies the restrictions of Theorem 1. The product of Krawtchouk polynomials can be calculated as follows:

$$P_k(x)P_i(x) = \sum_{j=Max(0,k+i-n)}^{Min(k,i)} a(k,i,j)P_{k+i-2j}(x)$$

where

$$a(k,i,j) = \binom{k+i-2j}{k-j}\binom{n-(k+i-2j)}{j}.$$

Therefore,

$$f(x) = \sum_{i=0}^{k} f_{2i}P_{2i}(x) = \sum_{i=0}^{k}\binom{2i}{i}\binom{n-2i}{k-i}P_{2i}(x).$$

Substituting the f_{2i}'s into the expression for $\underline{B}_{2k}$ of Theorem 1 we have

$$\begin{aligned}
\underline{B}_{2k} &= \frac{\frac{f(0)}{n^t} - \sum_{i=0}^{k-1} f_{2i}B_{2i}}{f_{2k}} \\
&= \frac{f_{2k}\binom{n}{2k}}{f_{2k}n^t} + \frac{\sum_{i=0}^{t} f_{2i}\binom{n}{2i}}{f_{2k}n^t} - \frac{f_0}{f_{2k}} + \frac{\sum_{i=t+1}^{k-1} f_{2i}\left(\binom{n}{2i} - n^t B_{2i}\right)}{f_{2k}n^t} \\
&\geq \frac{f_{2k}\binom{n}{2k}}{f_{2k}n^t} + \frac{\sum_{i=0}^{t} f_{2i}\binom{n}{2i}}{f_{2k}n^t} - \frac{f_0}{f_{2k}} - \frac{\sum_{i=t+1}^{k-1} f_{2i}\binom{n}{2i}\overline{E}_{2i}}{f_{2k}n^t}
\end{aligned}$$

Notice that the order of f_{2i} is n^{k-i}, and by [2] the order of E_{2i} is n^{t-i}. Therefore, if we neglect the terms of order less than n^k we get

$$\underline{B}_{2k} = \frac{\binom{n}{2k}}{n^t}\left(1 - \underline{E}_{2k}\right),$$

$$\underline{E}_{2k} \cong \frac{\sum_{i=t}^{k-1} f_{2i}\binom{n}{2i}\overline{E}_{2i}}{f_{2k}\binom{n}{2k}}$$

where $\overline{E}_{2t} = \frac{f_0 n^t}{f_{2t}\binom{n}{2t}} - 1$.

In a similar way we derive the **upper** bound $\overline{B}_{2k}$. Let

$$g(x) = \sum_{i=0}^{k} g_{2i} P_{2i}(x) = (P_2(x) + C_t) P_{k-1}^2(x),$$

be an even function in respect to $n/2$, of degree $2k$, $g(x) \leq 0$ for $x \in [d', n-d']$, where

$$C_t = -P_2(n/2 - (t-1)\sqrt{n}) = n/2(1 - 4(t-1)^2).$$

Indeed,

$$\begin{aligned}
g(x) &= C_t \sum_{m=0}^{k-1} a(k-1, k-m-1) P_{2m}(x) \\
&+ \sum_{m=0}^{k-1} \sum_{j=0}^{Min(2m,2)} a(k-1, k-m-1)\ a(2, 2m, j)\ P_{2(m+1-j)}(x) \\
&= C_t \sum_{m=0}^{k-1} a(k-1, k-m-1)\ P_{2m}(x) \\
&+ \binom{n}{k-1} P_2(x) \\
&+ \sum_{m=2}^{k} a(k-1, k-m)\ a(2, 2(m-1), 0)\ P_{2m}(x) \\
&+ \sum_{m=1}^{k-1} a(k-1, k-m-1)\ a(2, 2m, 1)\ P_{2m}(x) \\
&+ \sum_{m=0}^{k-2} a(k-1, k-m-2)\ a(2, 2(m+1), 2)\ P_{2m}(x) \\
&= \sum_{m=0}^{k} g_{2m}\ P_{2m}(x)
\end{aligned}$$

where,

$$a(k, j) = a(k, k, j) = \binom{2(k-j)}{k-j}\binom{n-2(k-j)}{j}$$

and

$$\begin{aligned} g_{2k} &= \binom{2k}{k}\frac{k^2}{2}, \\ g_{2m} &= C_t a(k-1,k-m-1) + a(k-1,k-m)\binom{2m}{2} \\ &+ a(k-1,k-1-m)2m(n-2m) + a(k-1,k-m-2)\binom{n-2m}{2} \\ &= \binom{2m}{m}\binom{n-2m}{k-m-1}A(k,m) \end{aligned}$$

where $A(k,m)$ is defined as follows,

$$\begin{aligned} A(k,m) &= C_t + \frac{m^2\binom{n-2(m-1)}{2}}{(k-m)(n-k-m+2)} \\ &+ 2m(n-2m) + \frac{(2m+1)(k-m-1)(n-k-m+1)}{(m+1)} \\ &= -\frac{n}{2}\left(4(t-1)^2+1-\frac{2k(2m+1)}{m+1}-\frac{m^2}{k-m}\right)+O(1) \end{aligned}$$

Notice that $A(k,m)$ is an increasing function in m, it achieves its maximum at $m=k-1$, i.e.

$$A(k,m) \le A(k,k-1) = -\frac{n}{2}(4(t-1)^2-(k-1)^2-4(k-1)-1).$$

The coefficient g_{2i} is of order n^{k-i} and it is negative for $0 \le i \le \hat{i}(k)$ where $\hat{i}(k) \le k-1$. Therefore, by Theorem 1 we have

$$B_{2k} \le \frac{\binom{n}{2k}}{n^t}\left(1+\frac{\sum_{i=0}^{t} g_{2i}\binom{n}{2i}}{g_{2k}\binom{n}{2k}} - \frac{g_0 n^t}{g_{2k}\binom{n}{2k}} + \frac{\sum_{i=t}^{\hat{i}(k)} -g_{2i}\binom{n}{2i}\overline{E}_{2i}}{g_{2k}\binom{n}{2k}} + \frac{\sum_{i=\hat{i}(k)+1}^{k-1} g_{2i}\binom{n}{2i}\underline{E}_{2i}}{g_{2k}\binom{n}{2k}}\right)$$

Again, ignoring terms of order less than n^k we get

$$\begin{aligned} \overline{B}_{2k} &= \frac{\binom{n}{2k}}{n^t}\left(1+\overline{E}_{2k}\right), \\ \overline{E}_{2k} &\cong \frac{-g_{2t}\binom{n}{2t}\underline{E}_{2t} + \sum_{i=t+1}^{\hat{i}(k)} -g_{2i}\binom{n}{2i}\overline{E}_{2i} + \sum_{i=\hat{i}(k)+1}^{k-1} g_{2i}\binom{n}{2i}\underline{E}_{2i}}{g_{2k}\binom{n}{2k}} \end{aligned}$$

where $\underline{E}_{2t} = \frac{g_0 n^t}{g_{2t}\binom{n}{2t}} - 1$ and $\overline{E}_{2k}$ is the error term of B_{2k}.

□

Acknowledgment

We are grateful to the anonymous referees for helpful comments and suggestions.

References

[1] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, Elsevier, 1997.

[2] I. Krasikov and S. Litsyn, On spectra of BCH codes, *IEEE Trans. Inform. Theory*, vol 41, 1995, pp. 786-788.

[3] T. Kasami, T. Fujiwara and S. Lin, An approximation to the weight distribution of binary linear codes, IEEE Trans. Inform. Theory, vol 31, No. 6, 1985, pp. 769-777.

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

[5] V. M. Sidelnikov, Weight spectrum of binary Bose-Chaudhuri-Hocquenghem codes, *Probl. Peredachi Inform.*, vol. 7, 1, 1971, pp.14–22 (In Russian).

[6] P. Solé, A limit law on the distance distribution of binary codes, *IEEE Trans. Inform.Theory*, vol. 36, 1990, pp.229–232.

[7] S. Vladuts and A. Skorobogatov, On spectra of binary cyclic codes, *Proceedings of the 9th All-Union Conference on Coding Theory and Information Transmission*, Odessa, 1988, pp.72–74 (in Russian)

[8] S. Vladuts and A. Skorobogatov, On spectra of subcodes over subfields of algebraic-geometric codes, *Probl. Peredachi Inform.*, vol. 27, 1, 1991, pp.24–36.