The Two Covering Radius of the Two Error Correcting BCH Code

Andrew Klapper
Department of Computer Science
University of Kentucky
Lexington, KY, 40506-0046
Email: klapper@cs.uky.edu

Andrew Mertz
Department of Mathematics and Computer Science
Eastern Illinois University
Email: aemertz@eiu.edu

***Abstract*— The m-*covering radii* of codes are natural generalizations of the covering radii of codes. In this paper we analyze the 2-covering radii of double error correcting BCH code.**

I. Introduction

Multicovering radii are generalizations of the covering radius. Let m and n be natural numbers. Denote the binary Hamming space of length n by $\boldsymbol{F}^n$. Given a code C of length n, the *m-covering radius of C*, denoted by $t_m(C)$, is the smallest natural number r such that every m-tuple of vectors in $\boldsymbol{F}^n$ is contained in a ball of radius r centered around some codeword of C. That is, $t_m(C)$ is the smallest integer r such that $\forall \mathbf{v}_1, \ldots, \mathbf{v}_m \in \boldsymbol{F}^n : \exists \mathbf{c} \in C : \forall i = 1, \ldots, m : \text{dist}(\mathbf{c}, \mathbf{v}_i) \leq r$.

General bounds on $t_m(C)$ are difficult, but it can be seen that $\lceil n/2 \rceil \leq t_2(C) \leq \lceil n/2 \rceil + s$, where s is the covering radius of C. In some cases — Hamming codes and Reed-Muller codes, for example – more precise results are known. In this paper we develop a technique (based on Krasikov's and Litsyn's method for studying the spectra of BCH codes) to tighten these bounds for some codes. Applying this technique, we show that the 2-covering radius of the double error correcting BCH code is $(n+1)/2$ for sufficiently large n.

We use the following notation:

- $\mathbf{0^n}$ and $\mathbf{1^n}$ are the all 0 and all 1 vectors of length n.
- $\overline{\mathbf{v}}$ is the bitwise complement of a vector $\mathbf{v}$.
- A code with length n, cardinality K, and minimum distance d is a (n, K, d) code or just a (n, K) code.
- A linear code with length n, dimension k, and minimum distance d is an $[n, k, d]$ or simply an $[n, k]$ code.
- $\text{cov}(\mathbf{x}, S) = \max\{\text{dist}(\mathbf{x}, \mathbf{y}) : \mathbf{y} \in S\}$ is the radius of the smallest ball centered at vector $\mathbf{x}$ and containing set S.
- Given subsets C and S of $\boldsymbol{F}^n$, $\text{cov}(C, S) = \min\{\text{cov}(\mathbf{c}, S) : \mathbf{c} \in C\}$.

Thus we have $t_m(C) = \max\{\text{cov}(C, S) : |S| = m\}$.

Theorem 1 (Klapper [1]): Let C be a code of length n. Then for a positive m, $t_m(C) \leq t_1(C) + t_m(\boldsymbol{F}^n)$.

Theorem 2 (Klapper [2], [1]): For every m and n satisfying $m \leq 2^n$, we have $t_m(\boldsymbol{F}^n) \geq \lceil (n + \lfloor \log_2(m) \rfloor - 1)/2 \rceil$, with equality for $m = 2, 3, 4, 5, 6$.

II. The multicovering radius of BCH codes

The binary primitive BCH code of length $2^m - 1$ and designed distance $2e + 1$ is a cyclic

$$[n = 2^m - 1, k \geq 2^m - me - 1, d \geq 2e + 1]$$

code, denoted BCH(e, m). BCH(e, m) is at least an e-error correcting code as its minimum distance is at least $2e + 1$. BCH$(1, m)$ is the Hamming code and $k = 2^m - me - 1$ if $2e - 1 \leq 2^{\lceil m/2 \rceil}$ (see [3] for details). BCH codes are important because their correction capabilities are known and they can be easily encoded. The covering radius of the 2 error correcting BCH codes are known.

Theorem 3 (Gorenstein, Peterson and Zierler [4]): The covering radius of the 2-error correcting BCH code, BCH$(2, m)$, for $m \geq 3$, is equal to 3.

Theorems 1 and 2 give the bounds

$$\lceil n/2 \rceil \leq t_2(\text{BCH}(2, m)) \leq \lceil n/2 \rceil + 3.$$

for $m \geq 3$. To obtain the 2-covering radius of BCH$(2, m)$ we use well known relations between the weight distribution of a code and the weight distribution of its dual. These relations depend on the Krawtchouk polynomials. Here we describe some properties of these polynomials (see [3] and [5] for details).

The binary Krawtchouk polynomial of degree i in x $P_i^n(x)$ is defined implicitly by the generating function

$$\sum_{i=0}^{\infty} P_i^n(x) z^i = (1 - z)^x (1 + z)^{n-x}.$$

Explicitly,

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

Usually n is fixed and is omitted. We will use the following relations involving Krawtchouk polynomials:

$$P_i(x) = \frac{(n - 2i)P_i(x - 1) - (x - 1)P_i(x - 2)}{n - x + 1}, \quad (1)$$

$$P_i(x) = (-1)^i P_i(n - x), \quad (2)$$

$$\binom{n}{x} P_i(x) = \binom{n}{i} P_x(i), \tag{3}$$

and if n is even,

$$P_i^n(n/2) = \begin{cases} 0 & \text{if } i \text{ is odd,} \\ (-1)^{i/2}\binom{n/2}{i/2} & \text{if } i \text{ is even.} \end{cases} \tag{4}$$

Lemma 4 (Krasikov and Litsyn [6]): For any integers x, n and i, with i even

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

Let $C \subseteq \boldsymbol{F}^n$ be a linear binary code. Its weight distribution $\mathbf{A}(C) = \mathbf{A} = (A_0, A_1, \ldots, A_n)$ is defined by

$$A_i = |\{\mathbf{c} \in C : \text{wt}(\mathbf{c}) = i\}|.$$

That is, the i^{th} component of $\mathbf{A}(C)$ is the number of codewords in C with weight i. The weight distribution of the dual code $C^\perp$, denoted $\mathbf{A}^\perp$, is called the dual spectrum of C.

Theorem 5 (MacWilliams identities [3]): For a linear code C of length n

$$A_i^\perp = \frac{1}{|C|} \sum_{x=0}^{n} A_x P_i^n(x),$$

where $P_i^n(x)$ is the Krawtchouk polynomial of degree i.

Let $\delta_m = 2^{m-1} - 2^{(m-1)/2}$ if m is odd and $\delta_m = 2^{m-1} - 2^{m/2}$ is m is even. If m is understood we just write δ.

Theorem 6 (Krasikov and Litsyn [6]): Let C be the 2-error correcting BCH code of length $n = 2^m - 1$. Then

$$A_i = \frac{\binom{n}{i}}{(n+1)^2}(1 + E_{i^*}),$$

where $i^* = i + 1$ if i is odd, $i^* = i$ if i is even, and

$$|E_{i^*}| \le \frac{(n+1)^2\binom{n+1}{(n+1)/2}\binom{(n+1)/2}{i^*/2}}{\binom{n+1}{i^*}\binom{n+1}{\delta_m}}.$$

We need Stirling's bound on factorials and the following bounds on binomial coefficients.

Lemma 7: For any natural numbers n and k,

1) $(n/k)^k \le \binom{n}{k} \le n^k$;

2) $n! \in \sqrt{2\pi n}(n/e)^n(1 + \Theta(1/n))$.

Lemma 8 ([3] §9.9): The weight of every nonzero codeword of the dual of BCH$(2, m)$ is in the range $[\delta_m, n - \delta_m]$.

Adding an overall parity check to a linear code appends a zero to each row of the parity check matrix and adds the all one vector as a new row. The result is called the *extended code*.

Corollary 9: The weight of every codeword of the dual of the extended BCH$(2, m)$ code is even and is in the range $[\delta_m, n + 1 - \delta_m]$ or is equal to 0 or $n + 1$.

Lemma 8 combined with Theorem 5 can be used to study the weight distribution of the BCH code. However, since certain calculations work best with even indices, we use the extended 2-error correcting BCH code.

Theorem 10: Let $0 \le a \le 4$ and $0 \le b \le 3$. Let S and T be disjoint sets of coordinates with $|S| = a$ and $|T| = b$. Then for sufficiently large m there exists a codeword $\mathbf{v}$ of BCH$(2, m)$ with $(n-1)/2 - a + b \le \text{wt}(\mathbf{v}) \le (n+1)/2 + b$ and with zeros at all of the coordinates in S and ones at all of the coordinates in T.

Proof: Suppose i is a positive integer and U and V are disjoint sets of coordinates. Let $A_{i,U,V}$ be the number of codewords in the extended 2-error correcting BCH code with weight i, zeros in all of the coordinates in U and ones in all of the coordinates in V. If V is the empty set then we may omit it from our notation. That is, $A_{i,U,\emptyset} = A_{i,U}$. Also, let $A^\perp_{i,U,V}$ denote the same quantity in the dual code. We next establish a useful equation for $A_{i,U}$.

Suppose U is a set of coordinates in $\boldsymbol{F}^n$ and the size of U is a. Let C_U be the subcode of the extended 2-error correcting BCH code with zeros in the coordinates of U and in the last coordinate of the extended code. Since every codeword of C_U has a zero in the last coordinate, we can remove this coordinate and obtain a BCH codeword that has the same weight. The code C_U can be constructed by adding $a+1$ parity checks, namely the $a+1$ vectors that are all zero except in one coordinate in U or in the last coordinate. From Corollary 9 we know that the minimal distance of the dual of the extended 2-error correcting BCH code is at least $\delta = (n+1)/2 - \sqrt{n+1}$. Therefore as long as $a + 1 < \delta$ the added parity checks are independent. It follows that

$$A^\perp_{i,U} = A^\perp_{n+1-i,U} = \begin{cases} \binom{a+1}{i} & \text{for } 0 \le i \le a+1 \\ 0 & \text{for } a+1 < i < \delta - a - 1. \end{cases}$$

Also,

$$\sum_{j=0}^{n+1} A^\perp_{j,U} = |C_U^\perp| = 2^{2m+1+a+1} = 2^{a+2}(n+1)^2.$$

Using Theorem 5 and the above values for $\mathbf{A}^\perp$ we have $A_{i,U} = 0$ if i is odd and, if i is even,

$$\begin{aligned} A_{i,U} &= \frac{1}{2^{a+2}(n+1)^2} \sum_{x=0}^{n+1} A^\perp_{x,U} P_i^{n+1}(x) \\ &= \frac{1}{2^{a+2}(n+1)^2} \left(\sum_{x=\delta-a-1}^{n+2-\delta+a} A^\perp_{x,U} P_i^{n+1}(x) + \right. \\ &\quad \left. \sum_{x=0}^{a+1} \binom{a+1}{x} \left(P_i^{n+1}(x) + P_i^{n+1}(n+1-x) \right) \right). \end{aligned}$$

When i is even we can use equation (2) to write $A_{i,U}$ as:

$$\begin{aligned} A_{i,U} &= \frac{1}{2^{a+2}(n+1)^2}\left(2\sum_{x=0}^{a+1}\binom{a+1}{x}P_i^{n+1}(x) + \right. \\ &\qquad \left.\sum_{x=\delta-a-1}^{n+2-\delta+a} A_{x,U}^{\perp}P_i^{n+1}(x)\right) \\ &= \alpha_{i,a}(1+\beta_{i,U}), \end{aligned}$$

where

$$\alpha_{i,a} = \frac{A_{i,a}}{2^{a+2}(n+1)^2}$$

and

$$\beta_{i,U} = \frac{1}{A_{i,a}}\sum_{x=\delta-a-1}^{n+2-\delta+a} A_{x,U}^{\perp}P_i^{n+1}(x)$$

with

$$A_{i,a} = 2\sum_{x=0}^{a+1}\binom{a+1}{x}P_i^{n+1}(x).$$

Since both n and i are even in this case, we may use Lemma 4 to bound the absolute value of $\beta_{i,U}$.

$$\begin{aligned} |\beta_{i,U}| &= \frac{1}{A_{i,a}}\ |\sum_{x=\delta-a-1}^{n+2-\delta+a} A_{x,U}^{\perp}P_i^{n+1}(x)| \\ &\le \frac{|C_U^{\perp}|}{A_{i,a}}\ \max\{|P_i^{n+1}(x)|\ : \\ &\qquad \delta-a-1 \le x \le n+2-\delta+a\} \\ &\le \frac{\binom{n+1}{(n+1)/2}\binom{(n+1)/2}{i/2}}{\alpha_{i,a}\binom{n+1}{\delta-a-1}}. \end{aligned}$$

We denote the last quantity by $\gamma_{i,a}$. We now proceed by cases for different a and b.

Case a = 4, b = 3: Suppose S and T are disjoint sets of coordinates with $|S| = 4$ and $|T| = 3$. It suffices to show that $A_{(n+1)/2,S,T} \ge 1$ for sufficiently large n. This implies the existence of a weight $(n+1)/2$ codeword with the appropriate structure. Such a codeword satisfies the requirements of other cases as well, namely when $(n+1)/2$ and $(n-1)/2$ are in the range of acceptable weights. Thus any case where $(n-1)/2-a+b \le (n-1)/2 \le (n+1)/2+b$, which is equivalent to $b \le a$, will also have been proved. Also, any case where $(n-1)/2-a+b \le (n+1)/2$ and $a \le 3$, i.e. $b-1 \le a \le 3$, will have been proved. This leaves only the cases $(a,b) = (0,2)$, $(0,3)$, and $(1,3)$.

Let $T = \{t_1, t_2, t_3\}$. Using the inclusion exclusion principal we can write $A_{i,S,T}$ as follows:

$$\begin{aligned} A_{i,S,T} &= A_{i,S} - A_{i,S\cup\{t_1\}} - A_{i,S\cup\{t_2\}} - A_{i,S\cup\{t_3\}} \\ &\quad + A_{i,S\cup\{t_1,t_2\}} + A_{i,S\cup\{t_1,t_3\}} + A_{i,S\cup\{t_2,t_3\}} \\ &\quad - A_{i,S\cup T}. \end{aligned}$$

Rewriting this equation in terms of α and β we have

$$\begin{aligned} &A_{\frac{n+1}{2},S,T} \\ &= \alpha_{\frac{n+1}{2},4}(1+\beta_{\frac{n+1}{2},S}) - \alpha_{\frac{n+1}{2},5}(3 + \\ &\quad \beta_{\frac{n+1}{2},S\cup\{t_1\}} + \beta_{\frac{n+1}{2},S\cup\{t_2\}} + \beta_{\frac{n+1}{2},S\cup\{t_3\}}) \\ &\quad + \alpha_{\frac{n+1}{2},6}(3 + \beta_{\frac{n+1}{2},S\cup\{t_1,t_2\}} + \beta_{\frac{n+1}{2},S\cup\{t_1,t_3\}} + \\ &\quad \beta_{\frac{n+1}{2},S\cup\{t_2,t_3\}}) - \alpha_{\frac{n+1}{2},7}(1+\beta_{\frac{n+1}{2},S\cup T}). \end{aligned} \tag{5}$$

To determine the asymptotic behavior of $A_{(n+1)/2,S,T}$ we consider the behavior of the α and β terms. Using equations (3) and (4) we can write $P_{(n+1)/2}^{n+1}(x)$ as

$$\begin{aligned} P_{(n+1)/2}^{n+1}(x) &= \frac{\binom{n+1}{(n+1)/2}P_x^{n+1}((n+1)/2)}{\binom{n+1}{x}} \\ &= \begin{cases} \frac{(-1)^{x/2}\binom{n+1}{(n+1)/2}\binom{(n+1)/2}{x/2}}{\binom{n+1}{x}} & \text{if } x \text{ is even,} \\ 0 & \text{if } x \text{ is odd.} \end{cases} \end{aligned}$$

Thus

$$\begin{aligned} \alpha_{\frac{n+1}{2},a} &= \frac{1}{2^{a+1}(n+1)^2}\sum_{x=0}^{a+1}\binom{a+1}{x}P_{(n+1)/2}^{n+1}(x) \\ &= \frac{\binom{n+1}{(n+1)/2}}{2^{a+1}(n+1)^2}\sum_{x=0}^{\lfloor\frac{a+1}{2}\rfloor}\frac{(-1)^x\binom{a+1}{2x}\binom{(n+1)/2}{x}}{\binom{n+1}{2x}} \\ &= \frac{\binom{n+1}{(n+1)/2}}{2^{a+1}(n+1)^2}\left(1+\sum_{x=1}^{\lfloor\frac{a+1}{2}\rfloor}\frac{(-1)^x\binom{a+1}{2x}\binom{\frac{n+1}{2}}{x}}{\binom{n+1}{2x}}\right). \end{aligned}$$

Since x and a are constant, $\binom{(n+1)/2}{x}$ is a polynomial of degree x in n, and $\binom{n+1}{2x}$ is a polynomial of degree $2x$ in n, we have

$$\begin{aligned} \frac{(-1)^x\binom{a+1}{2x}\binom{(n+1)/2}{x}}{\binom{n+1}{2x}} &\in \Theta\left(\frac{\binom{(n+1)/2}{x}}{\binom{n+1}{2x}}\right) \\ &\subseteq o(1). \end{aligned}$$

for $x \ge 1$. Therefore,

$$\alpha_{(n+1)/2,a} \in \frac{\binom{n+1}{(n+1)/2}}{2^{a+1}(n+1)^2}\left(1+o(1)\right).$$

Using our asymptotic bounds on α we can bound $\gamma_{(n+1)/2,a}$, which in turn bounds $\beta_{(n+1)/2,U}$ with $|U| = a$:

$$\begin{aligned} \gamma_{(n+1)/2,a} &= \frac{\binom{n+1}{(n+1)/2}\binom{(n+1)/2}{(n+1)/4}}{\alpha_{(n+1)/2,a}\binom{n+1}{\delta-a-1}} \\ &\in \frac{2^{a+1}(n+1)^2\binom{(n+1)/2}{(n+1)/4}}{\binom{n+1}{\delta-a-1}(1+o(1))}. \end{aligned}$$

Using Stirling's formula we obtain the usual estimate

$$\binom{\frac{n+1}{2}}{\frac{n+1}{4}} \subseteq \Theta\left(\frac{2^{(n+1)/2}}{\sqrt{n+1}}\right).$$

We can also estimate

$$\binom{n+1}{\delta-a-1} = \frac{\prod_{x=0}^{\delta-a-2}(n+1-x)}{\prod_{x=0}^{\delta-a-2}(\delta-a-1-x)}.$$

Since $(n+1)/2 - \sqrt{n+1} + 1 \geq \delta$, we have

$$\begin{aligned} n+1 &\geq n+1-2\sqrt{n+1}-2a-2x \\ &\geq 2(\delta-a-1-x). \end{aligned}$$

Also, if $x \geq (n+1-4\sqrt{n+1}-4a)/3$ then $n+1-x \geq 4(\lceil (n+1)/2 - \sqrt{n+1} \rceil - a - 1 - x)$. Let $\mu = n+1-4\sqrt{n+1}$. Then

$$\begin{aligned} \binom{n+1}{\delta-a-1} &\geq \left(\prod_{x=0}^{\lceil(\mu-4a)/3\rceil-1} 2\right)\left(\prod_{x=\lceil(\mu-4a)/3\rceil}^{\delta-a-2} 2^2\right) \\ &= 2^{2(\delta-a-2-\lceil(\mu-4a)/3\rceil+1)+\lceil(\mu-4a)/3\rceil} \\ &= 2^{2\delta-2a-2-\lceil(\mu-4a)/3\rceil} \\ &\geq 2^{2\delta-2a-2-((\mu-4a)/3+1)} \\ &= 2^{\frac{2}{3}\left(n-\sqrt{n+1}-a-\frac{7}{2}\right)}. \end{aligned}$$

For any $\epsilon > 0$, we have

$$2^{c\left(n-\sqrt{n+1}\right)} \in \Omega\left(2^{(c-\epsilon)n}\right).$$

Therefore

$$\binom{n+1}{\delta-a-1} \in \Omega\left(2^{\left(\frac{2}{3}-\epsilon\right)n}\right)$$

for any $\epsilon > 0$. Thus

$$\gamma_{(n+1)/2,a} \in \frac{2^{a+1}(n+1)^2\Theta\left(\frac{2^{(n+1)/2}}{\sqrt{n+1}}\right)}{\Omega\left(2^{\left(\frac{2}{3}-\epsilon\right)n}\right)(1+o(1))}.$$

This implies that $\gamma_{(n+1)/2,a}$ tends to 0 as n gets large and so must $\beta_{(n+1)/2,U}$, where U is of size a. Equation (5) becomes

$$\begin{aligned} &A_{(n+1)/2,S,T} \\ &= \alpha_{(n+1)/2,4} - 3\alpha_{(n+1)/2,5} + 3\alpha_{(n+1)/2,6} - \alpha_{(n+1)/2,7} \\ &\in \frac{\binom{n+1}{(n+1)/2}}{(n+1)^2}\left(\frac{1}{2^5} - \frac{3}{2^6} + \frac{3}{2^7} - \frac{1}{2^8} + o(1)\right) \\ &= \frac{\binom{n+1}{(n+1)/2}}{(n+1)^2}\left(\frac{1}{256} + o(1)\right). \end{aligned}$$

Therefore $A_{(n+1)/2,S,T}$ tends to infinity with n and there exist BCH codewords of weight $(n+1)/2$ with the sought after structure for large enough n (or, equivalently, large enough m).

Case a = 1, b = 3: Suppose S and T are disjoint sets of coordinates with $|S| = 1$ and $|T| = 3$. It suffices to show that $A_{(n+5)/2,S,T} \geq 1$ for sufficiently large n. This is equivalent to the existence of a weight $(n+5)/2$ codeword with the appropriate structure. Such a codeword also satisfies the requirements of cases $(a,b) = (0,2)$ and $(0,3)$ since $(n+5)/2$ is in the range of acceptable weights for those cases.

As before let $T = \{t_1, t_2, t_3\}$. Using the inclusion exclusion principal we can write $A_{(n+5)/2,S,T}$ in terms of α and β

$$\begin{aligned} &A_{\frac{n+5}{2},S,T} \\ &= \alpha_{\frac{n+5}{2},1}(1+\beta_{\frac{n+5}{2},S}) - \alpha_{\frac{n+5}{2},2}(3 + \\ &\quad \beta_{\frac{n+5}{2},S\cup\{t_1\}} + \beta_{\frac{n+5}{2},S\cup\{t_2\}} + \beta_{\frac{n+5}{2},S\cup\{t_3\}}) \\ &\quad + \alpha_{\frac{n+5}{2},3}(3 + \beta_{\frac{n+5}{2},S\cup\{t_1,t_2\}} + \beta_{\frac{n+5}{2},S\cup\{t_1,t_3\}} + \\ &\quad \beta_{\frac{n+5}{2},S\cup\{t_2,t_3\}}) - \alpha_{\frac{n+5}{2},4}(1+\beta_{\frac{n+5}{2},S\cup T}). \end{aligned} \quad (6)$$

To understand the asymptotic behavior of $A_{(n+5)/2,S,T}$ we consider the behavior of the α and β terms. From the explicit expression for a Krawtchouk polynomial, for any k we have

$$P_i^k(k/2+2) = \sum_{j=0}^{i}(-1)^j\binom{\frac{k}{2}+2}{j}\binom{\frac{k}{2}-2}{i-j}.$$

For fixed i this is a sum of $i+1$ polynomials in k of degree i and is therefore also a polynomial of degree at most i. Thus

$$P_i^k(k/2+2) \in O(k^i). \quad (7)$$

Also, $P_0^k(k/2+2) = 1$. Taking $k = n+1$ in equation (7) and using equation (3), we have

$$P^{n+1}_{(n+5)/2}(x) \in \frac{\binom{n+1}{(n+5)/2}O(n^x)}{\binom{n+1}{x}}$$

and $P^{n+1}_{(n+5)/2}(0) = \binom{n+1}{(n+5)/2}$. Thus

$$\begin{aligned} \alpha_{(n+5)/2,a} &= \frac{1}{2^{a+1}(n+1)^2}\sum_{x=0}^{a+1}\binom{a+1}{x}P^{n+1}_{(n+5)/2}(x) \\ &\in \frac{\binom{n+1}{(n+5)/2}}{2^{a+1}(n+1)^2}\left(1 + \sum_{x=1}^{a+1}\frac{\binom{a+1}{x}O(n^x)}{\binom{n+1}{x}}\right) \\ &\subseteq \frac{\binom{n+1}{(n+5)/2}}{2^{a+1}(n+1)^2}\Theta(1). \end{aligned}$$

Using this bound on $\alpha_{(n+5)/2,a}$ we obtain the bound

$$\begin{aligned} \gamma_{(n+5)/2,a} &= \frac{\binom{n+1}{(n+1)/2}\binom{(n+1)/2}{(n+5)/4}}{\alpha_{(n+5)/2,a}\binom{n+1}{\delta-a-1}} \\ &\in \frac{2^{a+1}(n+1)(n+5)(n+3)\binom{(n+1)/2}{(n+5)/4}}{(n-1)\binom{n+1}{\delta-a-1}\Theta(1)}. \end{aligned}$$

Using Stirling's formula we obtain the estimate

$$\binom{\frac{n+1}{2}}{\frac{n+5}{4}} \subseteq \Theta\left(\frac{2^{(n-3)/2}}{\sqrt{n-3}}\right).$$

As before

$$\binom{n+1}{\delta-a-1} \in \Omega\left(2^{\left(\frac{2}{3}-\epsilon\right)n}\right).$$

for any $\epsilon > 0$. Thus

$$\gamma_{(n+5)/2,a} \in \frac{2^{a+1}(n+5)(n+3)(n+1)\Theta\left(\frac{2^{(n-3)/2}}{\sqrt{n-3}}\right)}{(n-1)\Omega\left(2^{\left(\frac{2}{3}-\epsilon\right)n}\right)\Theta(1)}.$$

This implies that $\gamma_{(n+5)/2,a}$ tends to 0 as n gets large and so must $\beta_{(n+5)/2,U}$, where $|U| = a$. Thus equation (6) becomes

$$\begin{aligned} & A_{(n+5)/2,S,T} \\ &= \alpha_{(n+5)/2,1} - 3\alpha_{(n+5)/2,2} + 3\alpha_{(n+5)/2,3} - \alpha_{(n+5)/2,4} \\ &\in \frac{\binom{n+1}{(n+5)/2}\Theta(1)}{(n+1)^2}\left(\frac{1}{2^2} - \frac{3}{2^3} + \frac{3}{2^4} - \frac{1}{2^5}\right) \\ &= \frac{\binom{n+1}{(n+5)/2}\Theta(1)}{32(n+1)^2}. \end{aligned}$$

for large n. So $A_{(n+5)/2,S,T}$ tends to infinity as n gets large and therefore there exist BCH codewords of weight $(n+5)/2$ with the sought after structure for large enough n (or, equivalently, large enough m). ∎

Corollary 11: Given two vectors $\mathbf{x}$ and $\mathbf{y}$ with $a = n - \text{dist}(\mathbf{x}, \mathbf{y}) \leq 4$, let $\mathbf{z} = \overline{\mathbf{x}} + \mathbf{y}$. There exist codewords $\mathbf{u}$ and $\mathbf{v}$ of the code BCH$(2, m)$ that satisfy the following properties for sufficiently large m:

1) $b \triangleq \text{dist}(\mathbf{u}, \mathbf{x}) \leq 3$;
2) $(n-1)/2 - a + b \leq \text{wt}(\mathbf{v}) \leq (n+1)/2 + b$;
3) $\text{supp}(\mathbf{u} + \mathbf{x}) \subseteq \text{supp}(\mathbf{v})$;
4) $\text{supp}(\mathbf{z}) \cap \text{supp}(\mathbf{u} + \mathbf{x} + \mathbf{v}) = \emptyset$.

Proof: Property 1 can be satisfied since the covering radius of BCH$(2, m)$ is 3 for $m \geq 3$ by Theorem 3. Note that $\text{wt}(\mathbf{z}) = a$, $\text{wt}(\mathbf{x} + \mathbf{u}) = b$, and $\text{supp}(\mathbf{u} + \mathbf{x} + \mathbf{v}) = \text{supp}(\mathbf{v}) - \text{supp}(\mathbf{u} + \mathbf{x})$, so the fourth condition says that $\mathbf{v}$ has zeros wherever $\mathbf{z}$ is one and $\mathbf{u} + \mathbf{x}$ is zero. There are at most three such coordinates. The third condition says that $\mathbf{v}$ has ones wherever $\mathbf{u} + \mathbf{x}$ has ones. Thus by Theorem 10 with $S = \text{supp}(\mathbf{z})$ and $T = \text{supp}(\mathbf{x} + \mathbf{u})$ there exists a codeword $\mathbf{v}$ of BCH$(2, m)$ that satisfies properties 2, 3, and 4. ∎

Theorem 12: $t_2(\text{BCH}(2, m)) = (n+1)/2$ for sufficiently large m.

Proof: Consider vectors $\mathbf{x}$ and $\mathbf{y}$ with $\text{dist}(\mathbf{x}, \mathbf{y}) = n - a$. First suppose $a \geq 5$. There exists a vector $\mathbf{v}'$ with distance at most $(n-5)/2$ from both $\mathbf{x}$ and $\mathbf{y}$, and there exists a codeword $\mathbf{v}$ with $\text{dist}(\mathbf{v}, \mathbf{v}') \leq 3$. Thus the distance from $\mathbf{v}$ to both $\mathbf{x}$ and $\mathbf{y}$ is at most $(n-5)/2 + 3 = (n+1)/2$.

Now suppose that $a \leq 4$. Let $\mathbf{u}$, $\mathbf{v}$, $\mathbf{z}$, and let b be as in Corollary 11. Then

$$\begin{aligned} \text{dist}(\mathbf{x}, \mathbf{u} + \mathbf{v}) &= \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x}) \\ &= \text{wt}(\mathbf{v}) - \text{wt}(\mathbf{u} + \mathbf{x}) \\ &= \text{wt}(\mathbf{v}) - b \\ &\leq \frac{n+1}{2} \end{aligned}$$

and

$$\begin{aligned} \text{dist}(\mathbf{y}, \mathbf{u} + \mathbf{v}) &= \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{y}) \\ &= \text{wt}(\mathbf{u} + \mathbf{v} + \overline{\mathbf{x}} + \mathbf{z}) \\ &= n - \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x} + \mathbf{z}) \\ &= n - \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x}) - \text{wt}(\mathbf{z}) \\ &= n - \text{wt}(\mathbf{v}) + b - a \\ &\leq \frac{n+1}{2}. \end{aligned}$$

∎

III. Generalization

Our technique for determining the 2-covering radius of the 2-error correcting BCH code can be applied to other codes. We can generalize Corollary 11 as follows.

Theorem 13: Let C be a linear code with $t_1(C) = r$. Suppose that for any two vectors $\mathbf{x}$ and $\mathbf{y}$, with $a = n - \text{dist}(\mathbf{x}, \mathbf{y}) \leq r + 1$ and $\mathbf{z} = \overline{\mathbf{x}} + \mathbf{y}$, there exists codewords $\mathbf{u}$ and $\mathbf{v}$ such that

1) $b \triangleq \text{dist}(\mathbf{u}, \mathbf{x}) \leq r$
2) $\lfloor (n - r + 2)/2 \rfloor - a + b \leq \text{wt}(\mathbf{v}) \leq \lceil (n + r - 2)/2 \rceil + b$
3) $\text{supp}(\mathbf{u} + \mathbf{x}) \subseteq \text{supp}(\mathbf{v})$
4) $\text{supp}(\mathbf{z}) \cap \text{supp}(\mathbf{u} + \mathbf{x} + \mathbf{v}) = \emptyset$.

Then $t_2(C) \leq \left\lceil \frac{n+r-2}{2} \right\rceil$.

Proof: Consider vectors $\mathbf{x}$ and $\mathbf{y}$ with $\text{dist}(\mathbf{x}, \mathbf{y}) = n - a$, where $a \geq r + 2$. There exists a vector $\mathbf{v}'$ with distance at most $\lceil (n - r - 2)/2 \rceil$ to both $\mathbf{x}$ and $\mathbf{y}$ and there exists a codeword $\mathbf{v}$ with $\text{dist}(\mathbf{v}, \mathbf{v}') \leq r$. Thus the distance from $\mathbf{v}$ to both $\mathbf{x}$ and $\mathbf{y}$ is at most $\lceil (n - r - 2)/2 \rceil + r = \lceil (n + r - 2)/2 \rceil$.

Consider vectors $\mathbf{x}$ and $\mathbf{y}$ with $\text{dist}(\mathbf{x}, \mathbf{y}) = n - a$, where $a \leq r + 1$. Let $\mathbf{u}$, $\mathbf{v}$, $\mathbf{z}$, and $\mathbf{b}$ be as in the hypothesis. Then

$$\begin{aligned} \text{dist}(\mathbf{x}, \mathbf{u} + \mathbf{v}) &= \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x}) \\ &= \text{wt}(\mathbf{v}) - \text{wt}(\mathbf{u} + \mathbf{x}) \\ &= \text{wt}(\mathbf{v}) - b \\ &\leq \lceil (n + r - 2)/2 \rceil, \end{aligned}$$

and

$$\begin{aligned} \text{dist}(\mathbf{y}, \mathbf{u} + \mathbf{v}) &= \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{y}) \\ &= \text{wt}(\mathbf{u} + \mathbf{v} + \overline{\mathbf{x}} + \mathbf{z}) \\ &= n - \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x} + \mathbf{z}) \\ &= n - \text{wt}(\mathbf{u} + \mathbf{v} + \mathbf{x}) - \text{wt}(\mathbf{z}) \\ &= n - \text{wt}(\mathbf{v}) + b - a \\ &\leq \lceil (n + r - 2)/2 \rceil. \end{aligned}$$

∎

To prove the hypotheses of Corollary 11 we took advantage of the fact that both the covering radius and the dual distribution were known. In the case of the dual distribution we needed it to be concentrated around $n/2$. In other words no small or large weight codewords could be in the dual. Other codes, such as the 3-error correcting BCH code, have this property as well.

References

[1] A. Klapper, "The multicovering radii of codes," *IEEE Transactions on Information Theory*, vol. 43, pp. 1372–1377, 1997.

[2] I. Honkala and A. Klapper, "Multicovering bounds from relative covering radii," *SIAM Journal on Discrete Math*, pp. 228–234, 2002.

[3] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Elsevier Science B.V., 1977.

[4] W. P. D. Gorenstein and N. Zierler, "Two-error correcting bose-chaudhury codes are quasi-perfect," *Information and Control*, vol. 3, pp. 291–294, 1960.

[5] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Elsevier Science B.V., 1997.

[6] I. Krasikov and S. Litsyn, "On spectra of bch codes," *IEEE Transactions on Information Theory*, vol. 41, pp. 786–788, 1995.