Lower bounds on the minimum average distance of binary codes

Beniamin Mounits*

June 27, 2007

Abstract

Let $\beta(n, M)$ denote the minimum average Hamming distance of a binary code of length n and cardinality M. In this paper we consider lower bounds on $\beta(n, M)$. All the known lower bounds on $\beta(n, M)$ are useful when M is at least of size about $2^{n-1}/n$. We derive new lower bounds which give good estimations when size of M is about n. These bounds are obtained using linear programming approach. In particular, it is proved that $\lim_{n\to\infty} \beta(n, 2n) = 5/2$. We also give new recursive inequality for $\beta(n, M)$.

Keywords: Binary codes, minimum average distance, linear programming

*CWI, Amsterdam, The Netherlands, e-mail: B.Mounits@cwi.nl.

1 Introduction

Let $\mathcal{F}_2 = \{0, 1\}$ and let $\mathcal{F}_2^n$ denotes the set of all binary words of length n. For $x, y \in \mathcal{F}_2^n$, $d(x, y)$ denotes the Hamming distance between x and y and $wt(x) = d(x, \mathbf{0})$ is the weight of x, where $\mathbf{0}$ denotes all-zeros word. A binary code $\mathcal{C}$ of length n is a nonempty subset of $\mathcal{F}_2^n$. An (n, M) code $\mathcal{C}$ is a binary code of length n with cardinality M. In this paper we will consider only binary codes.

The average Hamming distance of an (n, M) code $\mathcal{C}$ is defined by

$$\overline{d}(\mathcal{C}) = \frac{1}{M^2} \sum_{c \in \mathcal{C}} \sum_{c' \in \mathcal{C}} d(c, c') \ .$$

The *minimum average Hamming distance* of an (n, M) code is defined by

$$\beta(n, M) = \min\{\ \overline{d}(\mathcal{C}) : \ \mathcal{C} \text{ is an } (n, M) \text{ code}\} \ .$$

An (n, M) code $\mathcal{C}$ for which $\overline{d}(\mathcal{C}) = \beta(n, M)$ will be called *extremal* code.

The problem of determining $\beta(n, M)$ was proposed by Ahlswede and Katona in [2]. Upper bounds on $\beta(n, M)$ are obtained by constructions. For survey on the known upper bounds the reader is referred to [9]. In this paper we consider the lower bounds on $\beta(n, M)$. We only have to consider the case where $1 \leq M \leq 2^{n-1}$ because of the following result which was proved in [6].

Lemma 1. *For* $1 \leq M \leq 2^n$

$$\beta(n, 2^n - M) = \frac{n}{2} - \frac{M^2}{(2^n - M)^2} \left(\frac{n}{2} - \beta(n, M) \right) \ .$$

First exact values of $\beta(n, M)$ were found by Jaeger et al. [7].

Theorem 1. *[7]* $\beta(n, 4) = 1$, $\beta(n, 8) = 3/2$, *whereas for* $M \leq n + 1$, $M \neq 4, 8$, *we have* $\beta(n, M) = 2 \left(\frac{M-1}{M} \right)^2$.

Next, Althöfer and Sillke [3] gave the following bound.

Theorem 2. *[3]*

$$\beta(n, M) \geq \frac{n+1}{2} - \frac{2^{n-1}}{M} \ ,$$

where equality holds only for $M = 2^n$ *and* $M = 2^{n-1}$.

Xia and Fu [10] improved Theorem 2 for odd M.

Theorem 3. *[10] If* M *is odd, then*

$$\beta(n, M) \geq \frac{n+1}{2} - \frac{2^{n-1}}{M} + \frac{2^n - n - 1}{2M^2} \ .$$

Further, Fu et al. [6] found the following bounds.

Theorem 4. *[6]*

$$\beta(n,M) \geq \frac{n+1}{2} - \frac{2^{n-1}}{M} + \frac{2^n - 2n}{M^2}\ , \quad \text{if} \quad M \equiv 2(mod\ 4)\ ,$$

$$\beta(n,M) \geq \frac{n}{2} - \frac{2^{n-2}}{M}\ , \quad \text{for} \quad M \leq 2^{n-1}\ ,$$

$$\beta(n,M) \geq \frac{n}{2} - \frac{2^{n-2}}{M} + \frac{2^{n-1} - n}{2M^2}\ , \quad \text{if} \quad M \text{ is odd and } \quad M \leq 2^{n-1} - 1\ .$$

Using Lemma 1 and Theorems 3, 4 the following values of $\beta(n,M)$ were determined: $\beta(n, 2^{n-1} \pm 1)$, $\beta(n, 2^{n-1} \pm 2)$, $\beta(n, 2^{n-2})$, $\beta(n, 2^{n-2} \pm 1)$, $\beta(n, 2^{n-1} + 2^{n-2})$, $\beta(n, 2^{n-1} + 2^{n-2} \pm 1)$. The bounds in Theorems 3, 4 were obtained by considering constraints on distance distribution of codes which were developed by Delsarte in [5]. We will recall these constraints in the next section.

Notice that the previous bounds are only useful when M is at least of size about $2^{n-1}/n$. Ahlswede and Althöfer determined $\beta(n,M)$ asymptotically.

Theorem 5. *[1] Let $\{M_n\}_{n=1}^{\infty}$ be a sequence of natural numbers with $0 \leq M_n \leq 2^n$ for all n and $\liminf_{n\to\infty} \left(M_n / \binom{n}{\lfloor \alpha n \rfloor} \right) > 0$ for some constant α, $0 < \alpha < 1/2$. Then*

$$\liminf_{n\to\infty} \frac{\beta(n,M_n)}{n} \geq 2\alpha(1-\alpha)\ .$$

The bound of Theorem 5 is asymptotically achieved by taking constant weight code $\mathcal{C} = \{x \in \mathcal{F}_2^n :\ wt(x) = \lfloor \alpha n \rfloor\}$.

The rest of the paper is organized as follows. In Section 2 we give necessary background in linear programming approach for deriving bounds for codes. This includes Delsarte's inequalities on distance distribution of a code and some properties of binary Krawtchouk polynomials. In Section 3 we obtain lower bounds on $\beta(n,M)$ which are useful in case when M is relatively large. In particular, we show that the bound of Theorem 2 is derived via linear programming technique. We also improve some bounds from Theorem 4 for $M < 2^{n-2}$. In Section 4, we obtain new lower bounds on $\beta(n,M)$ which are useful when M is at least of size about $n/3$. We also prove that these bounds are asymptotically tight for the case $M = 2n$. Finally, in Section 5, we give new recursive inequality for $\beta(n,M)$.

2 Preliminaries

The distance distribution of an (n,M) code $\mathcal{C}$ is the $(n+1)$-tuple of rational numbers $\{A_0, A_1, \cdots, A_n\}$, where

$$A_i = \frac{|\{(c,c') \in \mathcal{C} \times \mathcal{C} :\ d(c,c') = i\}|}{M}$$

is the average number of codewords which are at distance i from any given codeword $c \in \mathcal{C}$. It is clear that

$$A_0 = 1 \ , \quad \sum_{i=0}^{n} A_i = M \ \text{ and } \ A_i \geq 0 \ \text{ for } \ 0 \leq i \leq n \ . \tag{1}$$

If $\mathcal{C}$ is an (n, M) code with distance distribution $\{A_i\}_{i=0}^{n}$, the dual distance distribution $\{B_i\}_{i=0}^{n}$ is defined by

$$B_k = \frac{1}{M} \sum_{i=0}^{n} P_k^n(i) A_i \ , \tag{2}$$

where

$$P_k^n(i) = \sum_{j=0}^{k} (-1)^j \binom{i}{j} \binom{n-i}{k-j} \tag{3}$$

is the binary Krawtchouk polynomial of degree k. It was proved by Delsarte [5] that

$$B_k \geq 0 \ \text{ for } \ 0 \leq k \leq n \ . \tag{4}$$

Since the Krawtchouk polynomials satisfy the following orthogonal relation

$$\sum_{k=0}^{n} P_k^n(i) P_j^n(k) = \delta_{ij} 2^n \ , \tag{5}$$

we have

$$\sum_{k=0}^{n} P_j^n(k) B_k = \sum_{k=0}^{n} P_j^n(k) \frac{1}{M} \sum_{i=0}^{n} P_k^n(i) A_i = \frac{1}{M} \sum_{i=0}^{n} A_i \sum_{k=0}^{n} P_j^n(k) P_k^n(i) = \frac{2^n}{M} A_j \ . \tag{6}$$

It's easy to see from (1),(2),(3), and (6) that

$$B_0 = 1 \ \text{ and } \ \sum_{k=0}^{n} B_k = \frac{2^n}{M} \ . \tag{7}$$

Before we proceed, we list some of the properties of binary Krawtchouk polynomials (see for example [8]).

- Some examples are: $P_0^n(x) \equiv 1, \ P_1^n(x) = n - 2x$,

$$P_2^n(x) = \frac{(n-2x)^2 - n}{2}, \ P_3^n(x) = \frac{(n-2x)((n-2x)^2 - 3n + 2)}{6} \ .$$

- For any polynomial $f(x)$ of degree k there is the unique Krawtchouk expansion

$$f(x) = \sum_{i=0}^{k} f_i P_i^n(x) \ ,$$

where the coefficients are

$$f_i = \frac{1}{2^n} \sum_{j=0}^{n} f(j) P_j^n(i) \ .$$

- Krawtchouk polynomials satisfy the following recurrent relations:

$$P_{k+1}^n(x) = \frac{(n-2x)P_k^n(x) - (n-k+1)P_{k-1}^n(x)}{k+1} \ , \tag{8}$$

$$P_k^n(x) = P_k^{n-1}(x) + P_{k-1}^{n-1}(x) \ . \tag{9}$$

- Let i be nonnegative integer, $0 \le i \le n$. The following symmetry relations hold:

$$\binom{n}{i} P_k^n(i) = \binom{n}{k} P_i^n(k) \ , \tag{10}$$

$$P_k^n(i) = (-1)^i P_{n-k}^n(i) \ . \tag{11}$$

3 Bounds for "large" codes

The key observation for obtaining the bounds in Theorems 3, 4 is the following result.

Lemma 2. *[10] For an arbitrary (n, M) code $\mathcal{C}$ the following holds:*

$$\overline{d}(\mathcal{C}) = \frac{1}{2}(n - B_1) \ .$$

From Lemma 2 follows that any upper bound on B_1 will provide a lower bound on $\beta(n, M)$. We will obtain upper bounds on B_1 using linear programming technique.

Consider the following linear programming problem:

maximize B_1

subject to

$$\sum_{i=1}^n B_i = \frac{2^n}{M} - 1 \ ,$$

$$\sum_{i=1}^n P_k^n(i) B_i \ge -P_k(0) \ , \quad 1 \le k \le n \ ,$$

and $B_i \ge 0$ for $1 \le i \le n$.

Note that the constraints are obtained from (6) and (7).

The next theorem follows from the dual linear program. We will give an independent proof.

Theorem 6. *Let $\mathcal{C}$ be an (n, M) code such that for $2 \le i \le n$ and $1 \le j \le n$ there holds that $B_i \ne 0 \Leftrightarrow i \in I$ and $A_j \ne 0 \Leftrightarrow j \in J$.*

Suppose a polynomial $\lambda(x)$ of degree at most n can be found with the following properties. If the Krawtchouk expansion of $\lambda(x)$ is

$$\lambda(x) = \sum_{j=0}^{n} \lambda_j P_j^n(x) \ ,$$

then $\lambda(x)$ should satisfy

$$\begin{aligned} \lambda(1) &= -1 \ , \\ \lambda(i) &\le 0 \quad \textit{for} \quad i \in I \ , \\ \lambda_j &\ge 0 \quad \textit{for} \quad j \in J \ . \end{aligned}$$

Then

$$B_1 \le \lambda(0) - \frac{2^n}{M} \lambda_0 \ . \tag{12}$$

The equality in (12) holds iff $\lambda(i) = 0$ for $i \in I$ and $\lambda_j = 0$ for $j \in J$.

Proof. Let $\mathcal{C}$ be an (n, M) code which satisfies the above conditions. Thus, using (1), (2), (4) and (5), we have

$$-B_1 = \lambda(1)B_1 \ge \lambda(1)B_1 + \sum_{i \in I} \lambda(i)B_i = \sum_{i=1}^{n} \lambda(i)B_i = \sum_{i=1}^{n} \lambda(i) \frac{1}{M} \sum_{j=0}^{n} P_i^n(j)A_j$$

$$= \frac{1}{M} \sum_{j=0}^{n} A_j \sum_{i=1}^{n} \lambda(i) P_i^n(j) = \frac{1}{M} \sum_{j=0}^{n} A_j \sum_{i=1}^{n} \sum_{k=0}^{n} \lambda_k P_k^n(i) P_i^n(j)$$

$$= \frac{1}{M} \sum_{j=0}^{n} A_j \sum_{k=0}^{n} \lambda_k \left(\sum_{i=0}^{n} P_k^n(i) P_i^n(j) - P_k^n(0) P_0^n(j) \right) = \frac{1}{M} \sum_{j=0}^{n} A_j \sum_{k=0}^{n} \lambda_k \delta_{kj} 2^n$$

$$- \frac{1}{M} \sum_{j=0}^{n} A_j \sum_{k=0}^{n} \lambda_k P_k^n(0) = \frac{2^n}{M} \sum_{j=0}^{n} \lambda_j A_j - \lambda(0) = \frac{2^n}{M} \left(\lambda_0 A_0 + \sum_{j \in J} \lambda_j A_j \right) - \lambda(0)$$

$$\ge \frac{2^n}{M} \lambda_0 A_0 - \lambda(0) = \frac{2^n}{M} \lambda_0 - \lambda(0) \ .$$

□

Corollary 1. *If* $\lambda(x) = \sum_{j=0}^{n} \lambda_j P_j^n(x)$ *satisfies*

1. $\lambda(1) = -1$, $\lambda(i) \le 0$ *for* $2 \le i \le n$,
2. $\lambda_j \ge 0$ *for* $1 \le j \le n$,

then

$$\beta(n, M) \ge \frac{1}{2}\left(n - \lambda(0) + \frac{2^n}{M}\lambda_0\right) .$$

Example 1. *Consider the following polynomial:*

$$\lambda(x) \equiv -1 .$$

It is obvious that the conditions of the Corollary 1 are satisfied. Thus we have a bound

$$\beta(n, M) \ge \frac{n+1}{2} - \frac{2^{n-1}}{M}$$

which coincides with the one from Theorem 2.

Example 2. *[6, Theorem 4] Consider the following polynomial:*

$$\lambda(x) = -\frac{1}{2} + \frac{1}{2}P_n^n(x) .$$

From (11) we see that

$$P_n^n(i) = (-1)^i P_0^n(i) = \begin{cases} 1 & \text{if } i \text{ is even} \\ -1 & \text{if } i \text{ is odd} \end{cases} ,$$

and, therefore,

$$\lambda(i) = \begin{cases} 0 & \text{if } i \text{ is even} \\ -1 & \text{if } i \text{ is odd} . \end{cases}$$

Furthermore, $\lambda_j = 0$ for $1 \le j \le n-1$ and $\lambda_n = 1/2$. Thus, the conditions of the Corollary 1 are satisfied and we obtain

$$\beta(n, M) \ge \frac{1}{2}\left(n - \frac{2^{n-1}}{M}\right) = \frac{n}{2} - \frac{2^{n-2}}{M} .$$

This bound was obtained in [6, Theorem 4] and is tight for $M = 2^{n-1}, 2^{n-2}$.

Other bounds in Theorems 3, 4 were obtained by considering additional constraints on distance distribution coefficients given in the next theorem.

Theorem 7. *[4] Let $\mathcal{C}$ be an arbitrary binary (n, M) code. If M is odd, then*

$$B_i \geq \frac{1}{M^2}\binom{n}{i} \;, \quad 0 \leq i \leq n \;.$$

If $M \equiv 2 (mod\ 4)$, then there exists an $\ell \in \{0, 1, \cdots, n\}$ such that

$$B_i \geq \frac{2}{M^2}\left(\binom{n}{i} + P_i^n(\ell)\right) \;, \quad 0 \leq i \leq n \;.$$

Next, we will improve the bound of Example 2 for $M < 2^{n-2}$.

Theorem 8. *For $n > 2$*

$$\beta(n, M) \geq \begin{cases} \frac{n}{2} - \frac{2^{n-2}}{M} + \frac{1}{n-2}\left(\frac{2^{n-2}}{M} - 1\right) & \textit{if } n \textit{ is even} \\ \\ \frac{n}{2} - \frac{2^{n-2}}{M} + \frac{1}{n-1}\left(\frac{2^{n-2}}{M} - 1\right) & \textit{if } n \textit{ is odd} \;. \end{cases}$$

Proof. We distinguish between two cases.

- If n is even, $n > 2$, consider the following polynomial:

$$\lambda(x) = \frac{1}{2(n-2)}\left(3 - n + P_{n-1}^n(x) + P_n^n(x)\right) \;.$$

  Using (11), it's easy to see that

$$\lambda(i) = \begin{cases} \frac{2-i}{n-2} & \text{if } i \text{ is even} \\ \\ \frac{i+1-n}{n-2} & \text{if } i \text{ is odd} \;. \end{cases}$$

- If n is odd, $n > 1$, consider the following polynomial:

$$\lambda(x) = \frac{1}{2(n-1)}\left(2 - n + P_{n-1}^n(x) + 2P_n^n(x)\right) \;.$$

  Using (11), it's easy to see that

$$\lambda(i) = \begin{cases} \frac{2-i}{n-1} & \text{if } i \text{ is even} \\ \\ \frac{i-n}{n-1} & \text{if } i \text{ is odd} \;. \end{cases}$$

In both cases, the claim of the theorem follows from Corollary 1. □

4 Bounds for "small" codes

We will use the following lemma, whose proof easily follows from (5).

Lemma 3. *Let* $\lambda(x) = \sum_{i=0}^{n} \lambda_i P_i^n(x)$ *be an arbitrary polynomial. A polynomial* $\alpha(x) = \sum_{i=0}^{n} \alpha_i P_i^n(x)$ *satisfies* $\alpha(j) = 2^n \lambda_j$ *iff* $\alpha_i = \lambda(i)$.

By substituting the polynomial $\lambda(x)$ from Theorem 6 into Lemma 3, we have the following.

Theorem 9. *Let* $\mathcal{C}$ *be an* (n, M) *code such that for* $1 \le i \le n$ *and* $2 \le j \le n$ *there holds that* $A_i \neq 0 \Leftrightarrow i \in I$ *and* $B_j \neq 0 \Leftrightarrow j \in J$.

Suppose a polynomial $\alpha(x)$ *of degree at most* n *can be found with the following properties. If the Krawtchouk expansion of* $\alpha(x)$ *is*

$$\alpha(x) = \sum_{j=0}^{n} \alpha_j P_j^n(x) \ ,$$

then $\alpha(x)$ *should satisfy*

$$\begin{aligned} \alpha_1 &= 1 \ , \\ \alpha_j &\ge 0 \ , \ \ for \ \ j \in J \ , \\ \alpha(i) &\le 0 \ , \ \ for \ \ i \in I \ . \end{aligned}$$

Then

$$B_1 \le \frac{\alpha(0)}{M} - \alpha_0 \ . \tag{13}$$

The equality in (13) holds iff $\alpha(i) = 0$ *for* $i \in I$ *and* $\alpha_j = 0$ *for* $j \in J$.

Note that Theorem 9 follows from the dual linear program of the following one:

maximize $\sum_{i=1}^{n} P_1^n(i) A_i = M B_1 - n$

subject to

$$\sum_{i=1}^{n} A_i = M - 1 \ ,$$

$$\sum_{i=1}^{n} P_k^n(i) A_i \ge -P_k(0) \ , \quad 1 \le k \le n \ ,$$

and $A_i \ge 0$ for $1 \le i \le n$,

whose constraints are obtained from (1) and (4).

Corollary 2. *If* $\alpha(x) = \sum_{j=0}^{n} \alpha_j P_j^n(x)$ *satisfies*

1. $\alpha_1 = 1$, $\alpha_j \geq 0$ *for* $2 \leq j \leq n$,
2. $\alpha(i) \leq 0$ *for* $1 \leq i \leq n$,

then

$$\beta(n, M) \geq \frac{1}{2}\left(n + \alpha_0 - \frac{\alpha(0)}{M}\right) .$$

Example 3. *Consider*

$$\alpha(x) = 2 - n + P_1^n(x) = 2(1 - x) .$$

It's obvious that the conditions of the Corollary 2 are satisfied and we obtain

Theorem 10.

$$\beta(n, M) \geq 1 - \frac{1}{M} .$$

Note that the bound of Theorem 10 is tight for $M = 1, 2$.

Example 4. *Consider the following polynomial:*

$$\alpha(x) = 3 - n + P_1^n(x) + P_n^n(x) .$$

From (11) we obtain

$$\alpha(i) = \begin{cases} 4 - 2i & \text{if } i \text{ is even} \\ 2 - 2i & \text{if } i \text{ is odd} . \end{cases}$$

Thus, conditions of the Corollary 2 are satisfied and we have

Theorem 11.

$$\beta(n, M) \geq \frac{3}{2} - \frac{2}{M} .$$

Note that the bound of Theorem 11 is tight for $M = 2, 4$.

Example 5. *Let* n *be even integer. Consider the following polynomial:*

$$\alpha(x) = \frac{n(4-n)}{n+2} + P_1^n(x) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{\frac{n}{2}+1}} P_{\frac{n}{2}+1}^n(x) . \tag{14}$$

In this polynomial $\alpha_1 = 1$ and $\alpha_j \geq 0$ for $2 \leq j \leq n$. Thus, condition 1 in Corollary 2 is satisfied. From (10) we obtain that for nonnegative integer i, $0 \leq i \leq n$,

$$P^n_{\frac{n}{2}+1}(i) = \frac{\binom{n}{\frac{n}{2}+1}}{\binom{n}{i}} P^n_i\left(\frac{n}{2}+1\right)$$

and, therefore,

$$\alpha(i) = \frac{n(4-n)}{n+2} + P^n_1(i) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{i}} P^n_i\left(\frac{n}{2}+1\right) \ . \tag{15}$$

It follows from (8) that

$$P^n_1\left(\frac{n}{2}+1\right) = -2 \ , \quad P^n_2\left(\frac{n}{2}+1\right) = \frac{4-n}{2} \ , \quad P^n_3\left(\frac{n}{2}+1\right) = n-2 \ ,$$

$$P^n_4\left(\frac{n}{2}+1\right) = \frac{(n-2)(n-8)}{8} \ , \quad P^n_5\left(\frac{n}{2}+1\right) = \frac{(n-2)(4-n)}{4} \ . \tag{16}$$

Now it's easy to verify from (15) and (16) that $\alpha(1) = \alpha(2) = \alpha(3) = 0$. We define

$$\widetilde{\alpha}(i) := \frac{n(4-n)}{n+2} + P^n_1(i) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{i}} \left| P^n_i\left(\frac{n}{2}+1\right)\right| \ .$$

It is clear that $\alpha(i) \leq \widetilde{\alpha}(i)$ for $0 \leq i \leq n$. We will prove that $\widetilde{\alpha}(i) \leq 0$ for $4 \leq i \leq n$. From (11) and (16) one can verify that

$$\widetilde{\alpha}(n) = 0 \ , \quad \widetilde{\alpha}(n-1) = \widetilde{\alpha}(n-2) = \frac{2n(4-n)}{n+2} \ , \quad \text{and} \quad \widetilde{\alpha}(n-3) = 2(6-n) \tag{17}$$

which implies that $\widetilde{\alpha}(n-j) \leq 0$ for $0 \leq j \leq 3$ (of course, we are not interested in values $\widetilde{\alpha}(n-j)$, $0 \leq j \leq 3$, if $n-j \in \{1,2,3\}$). So, it is left to prove that for every integer i, $4 \leq i \leq n-4$, $\widetilde{\alpha}(i) \leq 0$. Note that for an integer i, $4 \leq i \leq n/2$,

$$\widetilde{\alpha}(n-i) = \frac{n(4-n)}{n+2} + P^n_1(n-i) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{n-i}} \left| P^n_{n-i}\left(\frac{n}{2}+1\right)\right|$$

$$= \frac{n(4-n)}{n+2} + (2i-n) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{i}} \left| (-1)^{\frac{n}{2}+1} P^n_i\left(\frac{n}{2}+1\right)\right|$$

$$\leq \frac{n(4-n)}{n+2} + (n-2i) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{i}} \left| P^n_i\left(\frac{n}{2}+1\right)\right| = \widetilde{\alpha}(i) \ .$$

Therefore, it is enough to check that $\widetilde{\alpha}(i) \leq 0$ only for $4 \leq i \leq n/2$.

From (16) we obtain that

$$\widetilde{\alpha}(4) = -2 - \frac{6}{n-3} < 0 \quad \text{and} \quad \widetilde{\alpha}(5) = -4 - \frac{12(n-8)}{(n+2)(n-3)} < 0 \ ,$$

where, in view of (17), we assume that $n \geq 8$. To prove that $\widetilde{\alpha}(i) \leq 0$ for $6 \leq i \leq n/2$ we will use the following lemma whose proof is given in the Appendix.

Lemma 4. *If n is an even positive integer and i is an arbitrary integer number, $2 \le i \le n/2$, then*

$$\left|P_i^n\left(\frac{n}{2}+1\right)\right| < \binom{n}{\lfloor \frac{i}{2} \rfloor} .$$

By Lemma 4, the following holds for $2 \le i \le n/2$.

$$\widetilde{\alpha}(i) = \frac{n(4-n)}{n+2} + P_1^n(i) + \frac{4\binom{n}{2}}{(n+2)\binom{n}{i}}\left|P_i^n\left(\frac{n}{2}+1\right)\right|$$

$$< \frac{n(4-n)}{n+2} + n - 2i + \frac{4\binom{n}{2}\binom{n}{\lfloor \frac{i}{2} \rfloor}}{(n+2)\binom{n}{i}} = \frac{6n}{n+2} - 2i + \frac{4\binom{n}{2}\binom{n}{\lfloor \frac{i}{2} \rfloor}}{(n+2)\binom{n}{i}}$$

$$= -\frac{12}{n+2} - 2(i-3) + \frac{4\binom{n}{2}\binom{n}{\lfloor \frac{i}{2} \rfloor}}{(n+2)\binom{n}{i}} .$$

Thus, to prove that $\widetilde{\alpha}(i) \le 0$ for $6 \le i \le n/2$, it's enough to prove that

$$-2(i-3) + \frac{4\binom{n}{2}\binom{n}{\lfloor \frac{i}{2} \rfloor}}{(n+2)\binom{n}{i}} < 0$$

for $6 \le i \le n/2$.

Lemma 5. *Let n be an even integer. For $6 \le i \le n/2$ we have*

$$\frac{(i-3)\binom{n}{i}}{\binom{n}{\lfloor \frac{i}{2} \rfloor}} > \frac{n(n-1)}{n+2} .$$

The proof of this lemma appears in the Appendix.

We have proved that the both conditions of the Corollary 2 are satisfied and, therefore, for even integer n, we have

$$\beta(n, M) \ge \frac{3n}{n+2} - \frac{n}{M} .$$

Once we have a bound for an even (odd) n, it's easy to deduce one for odd (even) n due to the following fact which follows from (9).

Lemma 6. *Let $\alpha(x) = \sum_{j=0}^{n} \alpha_j P_j^n(x)$ be an arbitrary polynomial. Then for a polynomial*

$$\mu(x) = \sum_{j=0}^{n-1} \mu_j P_j^{n-1}(x) ,$$

where

$$\mu_j = \alpha_j + \alpha_{j+1} , \quad 0 \le j \le n-1 ,$$

the following holds:

$$\mu(x) = \alpha(x) \quad \text{for} \quad 0 \le x \le n-1 .$$

Example 6. *Let n be odd integer, $n > 1$. Consider the following polynomial:*

$$\mu(x) = \frac{6+3n-n^2}{n+3} + P_1^n(x) + \frac{4\binom{n+1}{2}}{(n+3)\binom{n+1}{\frac{n+3}{2}}}\left(P^n_{\frac{n+1}{2}}(x) + P^n_{\frac{n+3}{2}}(x)\right) \tag{18}$$

which is obtained from $\alpha(x)$ given in (14) by the construction of Lemma 6. Thus, by Corollary 2, for odd integer n, we have

$$\beta(n, M) \geq \frac{3(n+1)}{n+3} - \frac{n+1}{M} \ .$$

We summarize the bounds from the Examples 5, 6 in the next theorem.

Theorem 12.

$$\beta(n, M) \geq \begin{cases} \frac{3n}{n+2} - \frac{n}{M} & \textit{if } n \textit{ is even} \\ \frac{3(n+1)}{n+3} - \frac{n+1}{M} & \textit{if } n \textit{ is odd} \ . \end{cases}$$

Example 7. *For $n \equiv 1 \ (mod\ 4)$, $n \neq 1$, consider*

$$\alpha(x) = \frac{(1-n)(n-5)}{n+1} + P_1^n(x) + \frac{4n(n-2)}{(n+1)\binom{n}{\frac{n+1}{2}}} P^n_{\frac{n+1}{2}}(x) + P^n_n(x) \ . \tag{19}$$

One can verify that

$$\alpha(0) = 4(n-1) \ , \quad \alpha(1) = \alpha(2) = \alpha(3) = \alpha(4) = 0 \ , \quad \alpha(5) = \alpha(6) = \frac{4(1-n)}{n-4} \ ,$$

and

$$\alpha(n) = -6\frac{(n-1)^2}{n+1} \ , \quad \alpha(n-1) = \alpha(n-2) = \alpha(n-3) = \alpha(n-4) = -2\frac{(n-5)(n-1)}{n+1} \ ,$$

$$\alpha(n-5) = \alpha(n-6) = -\frac{2(n-9)(n-2)(n-1)}{(n+1)(n-4)} \ .$$

We define

$$\widetilde{\alpha}(i) := \frac{(1-n)(n-5)}{n+1} + P_1^n(x) + \frac{4n(n-2)}{(n+1)\binom{n}{i}}\left|P_i^n\left(\frac{n+1}{2}\right)\right| + |P_n^n(i)| \ .$$

As in the previous example, it's easy to see that $\alpha(i) \leq \widetilde{\alpha}(i)$ for $0 \leq i \leq n$ and

$$\widetilde{\alpha}(n-i) \leq \widetilde{\alpha}(i) \ \text{ for } \ 0 \leq i \leq (n-1)/2 \ .$$

Therefore, to prove that $\alpha(i) \leq 0$ for $1 \leq i \leq n$, we only have to show that $\widetilde{\alpha}(i) \leq 0$ for $7 \leq i \leq (n-1)/2$. It is follows from the next two lemmas.

Lemma 7. *If n is odd positive integer and i is an arbitrary integer number, $2 \leq i \leq (n-1)/2$, then*

$$\left|P_i^n\left(\frac{n+1}{2}\right)\right| < \binom{n}{\lfloor \frac{i}{2} \rfloor} \ .$$

Lemma 8. *Let n be odd integer. For $7 \le i \le (n-1)/2$ we have*

$$\frac{(i-4)\binom{n}{i}}{\binom{n}{\lfloor \frac{i}{2} \rfloor}} > \frac{2n(n-2)}{n+1} \ .$$

Proofs of the Lemmas 7, 8 are very similar to those of Lemmas 4, 5, respectively, and they are omitted. Thus, we have proved that the conditions of the Corollary 2 are satisfied and we have the following bound.

$$\beta(n,M) \ge \frac{7n-5}{2(n+1)} - \frac{2(n-1)}{M} \ , \quad \text{if } n \equiv 1 \ (mod\ 4) \ , \quad n \ne 1 \ .$$

From Lemma 6, by choosing the following polynomials:

$$\mu(x) = \frac{2+5n-n^2}{n+2} + P_1^n(x) + \frac{4(n^2-1)}{(n+2)\binom{n+1}{\frac{n+2}{2}}} \left(P^n_{\frac{n}{2}}(x) + P^n_{\frac{n+2}{2}}(x) \right) + P^n_n(x) \ ,$$

if $n \equiv 0 \ (mod\ 4)$,

$$\widetilde{\mu}(x) = \frac{9+4n-n^2}{n+3} + P_1^n(x) + \frac{4n(n+2)}{(n+3)\binom{n+2}{\frac{n+3}{2}}} \left(P^n_{\frac{n-1}{2}}(x) + P^n_{\frac{n+3}{2}}(x) \right)$$
$$+ \frac{8n(n+2)}{(n+3)\binom{n+2}{\frac{n+3}{2}}} P^n_{\frac{n+1}{2}}(x) + P^n_n(x) \ ,$$

if $n \equiv 3 \ (mod\ 4), \ n \ne 3$, and

$$\widehat{\mu}(x) = \frac{16+3n-n^2}{n+4} + P_1^n(x) + \frac{4(n+1)(n+3)}{(n+4)\binom{n+3}{\frac{n+4}{2}}} \left(P^n_{\frac{n-2}{2}}(x) + P^n_{\frac{n+4}{2}}(x) \right)$$
$$+ \frac{12(n+1)(n+3)}{(n+4)\binom{n+3}{\frac{n+4}{2}}} \left(P^n_{\frac{n}{2}}(x) + P^n_{\frac{n+2}{2}}(x) \right) + P^n_n(x) \ ,$$

if $n \equiv 2 \ (mod\ 4), \ n \ne 2$, we obtain the bounds which are summarized in the next theorem.

Theorem 13. *For $n > 3$*

$$\beta(n,M) \ge \begin{cases} \frac{7n+2}{2(n+2)} - \frac{2n}{M} & \text{if } n \equiv 0 \ (mod\ 4) \\ \frac{7n-5}{2(n+1)} - \frac{2(n-1)}{M} & \text{if } n \equiv 1 \ (mod\ 4) \\ \frac{7n+16}{2(n+4)} - \frac{2(n+2)}{M} & \text{if } n \equiv 2 \ (mod\ 4) \\ \frac{7n+9}{2(n+3)} - \frac{2(n+1)}{M} & \text{if } n \equiv 3 \ (mod\ 4) \ . \end{cases}$$

It's easy to see that the bounds of Theorems 12 and 13 give similar estimations when the size of a code is about $2n$.

Theorem 14.

$$\lim_{n\to\infty} \beta(n, 2n) = \frac{5}{2} \ .$$

Proof. Let $\mathcal{C}$ be the following $(n, 2n)$ code:

$$\begin{array}{ccc} 000 & \cdots & 00 \\ \hline 100 & \cdots & 00 \\ 010 & \cdots & 00 \\ \vdots & \ddots & \vdots \\ 000 & \cdots & 01 \\ \hline 110 & \cdots & 00 \\ 101 & \cdots & 00 \\ \vdots & \ddots & \vdots \\ 100 & \cdots & 01 \end{array}$$

One can evaluate that

$$\beta(n, 2n) \leq \overline{d}(\mathcal{C}) = \frac{5}{2} - \frac{4n-2}{n^2} \ . \tag{20}$$

On the other hand, Theorem 12 gives

$$\beta(n, 2n) \geq \begin{cases} \frac{5}{2} - \frac{6}{n+2} & \text{if } n \text{ is even} \\ \\ \frac{5}{2} - \frac{13n+3}{2n(n+3)} & \text{if } n \text{ is odd} \ . \end{cases} \tag{21}$$

The claim of the theorem follows by combining (20) and (21). □

5 Recursive inequality on $\beta(n, M)$

The following recursive inequality was obtained in [10]:

$$\beta(n, M+1) \geq \frac{M^2}{(M+1)^2}\beta(n, M) + \frac{Mn}{(M+1)^2}\left(1 - \sqrt{1 - \frac{2}{n}\beta(n, M)}\right) \ . \tag{22}$$

In the next theorem we give a new recursive inequality.

Theorem 15. *For positive integers n and M, $2 \leq M \leq 2^n - 1$,*

$$\beta(n, M+1) \geq \frac{M^2}{M^2-1}\beta(n, M) \ . \tag{23}$$

Proof. Let $\mathcal{C}$ be an extremal $(n, M+1)$ code, i.e.,

$$\beta(n, M+1) = \overline{d}(\mathcal{C}) = \frac{1}{(M+1)^2} \sum_{c\in\mathcal{C}} \sum_{c'\in\mathcal{C}} d(c, c') \ .$$

Then there exists $c_0 \in \mathcal{C}$ such that

$$\sum_{c \in \mathcal{C}} d(c_0, c) \geq (M+1)\beta(n, M+1) \ . \tag{24}$$

Consider an (n, M) code $\widetilde{\mathcal{C}} = \mathcal{C} \setminus \{c_0\}$. Using (24) we obtain

$$\beta(n,M) \leq \overline{d}(\widetilde{\mathcal{C}}) = \frac{1}{M^2} \sum_{c \in \widetilde{\mathcal{C}}} \sum_{c' \in \widetilde{\mathcal{C}}} d(c, c') = \frac{1}{M^2} \left(\sum_{c \in \mathcal{C}} \sum_{c' \in \mathcal{C}} d(c, c') - 2 \sum_{c \in \mathcal{C}} d(c_0, c) \right)$$

$$\leq \frac{1}{M^2} \left((M+1)^2 \beta(n, M+1) - 2(M+1)\beta(n, M+1) \right) = \frac{M^2 - 1}{M^2} \beta(n, M+1) \ .$$

□

Lemma 9. *For positive integers n and M, $2 \leq M \leq 2^n - 1$, the RHS of (23) is not smaller than RHS of (22).*

Proof. One can verify that RHS of (23) is not smaller than RHS of (22) iff

$$\beta(n, M) \leq \frac{M^2 - 1}{M^2} \cdot \frac{n}{2} \ .$$

By (23) we have

$$\beta(n, M) \leq \frac{M^2 - 1}{M^2} \beta(n, M+1) \leq \frac{M^2 - 1}{M^2} \beta(n, 2^n) = \frac{M^2 - 1}{M^2} \cdot \frac{n}{2} \ ,$$

which completes the proof. □

6 Appendix

Proof of Lemma 4: The proof is by induction. One can easily see from (16) that the claim is true for $2 \leq i \leq 5$, where $i \leq n/2$. Assume that we have proved the claim for i, $4 \leq i \leq k \leq n/2 - 1$. Thus

$$\left| P_{k+1}^n \left(\frac{n}{2} + 1 \right) \right| = \left| \frac{(-2) P_k^n \left(\frac{n}{2} + 1 \right) - (n - k + 1) P_{k-1}^n \left(\frac{n}{2} + 1 \right)}{k+1} \right|$$

$$\leq \frac{2}{k+1} \left| P_k^n \left(\frac{n}{2} + 1 \right) \right| + \frac{n-k+1}{k+1} \left| P_{k-1}^n \left(\frac{n}{2} + 1 \right) \right|$$

$$< \frac{2}{k+1} \binom{n}{\lfloor \frac{k}{2} \rfloor} + \frac{n-k+1}{k+1} \binom{n}{\lfloor \frac{k-1}{2} \rfloor} = (*) \ .$$

We distinguish between two cases. If k is odd, then

$$(*) = \frac{2}{k+1}\binom{n}{\frac{k-1}{2}} + \frac{n-k+1}{k+1}\binom{n}{\frac{k-1}{2}} = \frac{2}{k+1}\binom{n}{\frac{k-1}{2}}\left(1+\frac{n-k+1}{2}\right)$$

$$= \frac{1}{n-\frac{k-1}{2}} \cdot \frac{n-\frac{k-1}{2}}{\frac{k+1}{2}}\binom{n}{\frac{k-1}{2}}\frac{n-k+3}{2} = \frac{n-k+3}{2n-k+1}\binom{n}{\frac{k+1}{2}} < \binom{n}{\frac{k+1}{2}} .$$

Therefore, for odd k, we obtain

$$\left|P_{k+1}\left(\frac{n}{2}+1\right)\right| < \binom{n}{\frac{k+1}{2}} = \binom{n}{\lfloor\frac{k+1}{2}\rfloor} .$$

If k is even, then

$$(*) = \frac{2}{k+1}\binom{n}{\frac{k}{2}} + \frac{n-k+1}{k+1}\binom{n}{\frac{k}{2}-1}$$

$$= \frac{2}{k+1}\binom{n}{\frac{k}{2}} + \frac{n-k+1}{k+1} \cdot \frac{\frac{k}{2}}{n-(\frac{k}{2}-1)} \cdot \frac{n-(\frac{k}{2}-1)}{\frac{k}{2}}\binom{n}{\frac{k}{2}-1}$$

$$= \binom{n}{\frac{k}{2}}\left(\frac{2}{k+1} + \frac{n-k+1}{2n-k+2} \cdot \frac{k}{k+1}\right) .$$

Since $k \geq 4$, we have

$$(*) = \binom{n}{\frac{k}{2}}\left(\frac{2}{k+1} + \overbrace{\frac{n-k+1}{2n-k+2}}^{<1/2} \cdot \overbrace{\frac{k}{k+1}}^{<1}\right) < \binom{n}{\frac{k}{2}}\left(\frac{2}{5}+\frac{1}{2}\right) < \binom{n}{\frac{k}{2}} .$$

Therefore, for even k, we obtain

$$\left|P_{k+1}\left(\frac{n}{2}+1\right)\right| < \binom{n}{\frac{k}{2}} = \binom{n}{\lfloor\frac{k+1}{2}\rfloor} .$$

□

Proof of Lemma 5: Denote

$$a_i = \frac{(i-3)\binom{n}{i}}{\binom{n}{\lfloor\frac{i}{2}\rfloor}} , \quad 6 \leq i \leq n/2 .$$

Thus,

$$\frac{a_6(n+2)}{n(n-1)} = \frac{(n+2)(n-3)(n-4)(n-5)}{40n(n-1)}$$

$$= \frac{(n-2)(n-7)}{40} + \frac{48n-120}{40n(n-1)} \overbrace{\geq}^{n\geq 12} \frac{5}{4} + \frac{48\cdot 12 - 120}{40n(n-1)} > \frac{5}{4}$$

and we have proved that $a_6 > \dfrac{n(n-1)}{n+2}$. Let's see that $a_i \geq a_6$ for $6 \leq i \leq n/2$. Let i be even integer such that $6 \leq i \leq n/2 - 2$. Then

$$\frac{a_{i+2}}{a_i} = \frac{(i-1)(n-i-1)(n-i)}{(i-3)(i+1)(n-2i)} \overbrace{>}^{i\geq 6} \frac{(i-3)(n-2i)(n-i)}{(i-3)(i+1)(n-2i)} = \frac{n-i}{i+1} \overbrace{>}^{i\leq n/2-2} 1\ .$$

Together with $a_6 > \dfrac{n(n-1)}{n+2}$, this implies that $a_i > \dfrac{n(n-1)}{n+2}$ for every even integer i, $6 \leq i \leq n/2$.

Now let i be even integer such that $6 \leq i \leq n/2 - 1$. Then

$$\frac{a_{i+1}}{a_i} = \frac{(i-2)(n-i)}{(i-3)(i+1)} > \frac{n-i}{i+1} \overbrace{>}^{i\leq n/2-1} 1\ ,$$

which completes the proof. □

References

[1] R. Ahlswede and I. Althöfer, "The asymptotic behaviour of diameters in the average", in *J. Combin. Theory Ser. B* 61, pp. 167–177, 1994.

[2] R. Ahlswede and G. Katona, "Contributions to the geometry of Hamming spaces", in *Discrete Math.* 17, pp. 1–22, 1977.

[3] I. Althöfer and T. Sillke, "An "average distance" inequality for large subsets of the cube", in *J. Combin. Theory Ser. B* 56, pp. 296–301, 1992.

[4] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, "Bounds for binary codes of length less than 25", *IEEE Trans. on Inform. Theory*, vol. 24, pp. 81–93, Jan. 1978.

[5] Ph. Delsarte, "An algebraic approach to the association schemes of coding theory ", *Philips Research Reports Supplements*, No. 10, 1973.

[6] F. -W. Fu, V. K. Wei and R. W. Yeung, "On the minimum average distance of binary codes: linear programming approach", in *Discrete Appl. Math.* 111, pp. 263–281, 2001.

[7] F. Jaeger, A. Khelladi and M. Mollard, "On shortest cocycle covers of graphs", in *J. Combin. Theory Ser. B* 39, pp. 153–163, 1985.

[8] I. Krasikov and S. Litsyn, *Survey of binary Krawtchouk polynomials*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **56** (2001), 199–211.

[9] A. Kündgen, "Minimum average distance subsets in the Hamming cube", in *Discrete Math.* 249, pp. 149–165, 2002.

[10] S. -T. Xia and F. -W. Fu, "On the average Hamming distance for binary codes", in *Discrete Appl. Math.* 89, pp. 269–276, 1998.