Bounds for binary codes with narrow distance distributions

Ron M. Roth, Gadiel Seroussi
Advanced Studies
HP Laboratories Palo Alto

HPL-2006-136
September 29, 2006*

constant-weight codes, distance distribution, equidistant codes, linear programming bound

New lower bounds are presented on the second moment of the distance distribution of binary codes, in terms of the first moment of the distribution. These bounds are used to obtain upper bounds on the size of codes whose maximum distance is close to their minimum distance. It is then demonstrated how such bounds can be applied to bound from below the smallest attainable ratio between the maximum distance and the minimum distance of codes. Finally, counterparts of the bounds are derived for the special case of constant-weight codes.

* Internal Accession Date Only

Approved for External Publication

Bounds for binary codes with narrow distance distributions[*]

Ron M. Roth[†] Gadiel Seroussi[‡]

September 18, 2006

Abstract

New lower bounds are presented on the second moment of the distance distribution of binary codes, in terms of the first moment of the distribution. These bounds are used to obtain upper bounds on the size of codes whose maximum distance is close to their minimum distance. It is then demonstrated how such bounds can be applied to bound from below the smallest attainable ratio between the maximum distance and the minimum distance of codes. Finally, counterparts of the bounds are derived for the special case of constant-weight codes.

Keywords: Constant-weight codes; Distance distribution; Equidistant codes; Grey–Rankin bound; Linear programming bound; Quasi-symmetric designs; Self-complementary codes.

1 Introduction

Let $\mathcal{C}$ be an (n, M, d) binary code (of length n, size $M > 1$, and minimum Hamming distance d). The *distance distribution* of $\mathcal{C}$ is a list $(B_0\ B_1\ \ldots\ B_n)$, where B_i is the average over all

[*] This work was done in part while both authors were at Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA. This work was supported in part by grant No. 2002197 from the United-States–Israel Binational Science Foundation (BSF), Jerusalem, Israel. This work was presented in part (under a different title) at the *IEEE International Symposium on Information Theory (ISIT'2005)*, Adelaide, Australia (September 2005), pp. 931–935 in the proceedings.

[†] Computer Science Department, Technion, Haifa 32000, Israel. E-mail: ronny@cs.technion.ac.il.

[‡] Mathematical Sciences Research Institute (MSRI), 17 Gauss Way, Berkeley CA 94720, USA. E-mail: gadiel@msri.org.

codewords $\mathbf{c} \in \mathcal{C}$ of the number of codewords at Hamming distance i from $\mathbf{c}$; that is, if $\mathsf{d}(\cdot, \cdot)$ denotes Hamming distance, then

$$B_i = \frac{1}{M} \sum_{\mathbf{c} \in \mathcal{C}} \left| \{ \mathbf{c}' \in \mathcal{C} \,:\, \mathsf{d}(\mathbf{c}, \mathbf{c}') = i \} \right| \;, \quad 0 \le i \le n \;.$$

Equivalently,

$$B_i = \frac{1}{M} \left| \{ (\mathbf{c}, \mathbf{c}') \in \mathcal{C} \times \mathcal{C} \,:\, \mathsf{d}(\mathbf{c}, \mathbf{c}') = i \} \right| \;.$$

Clearly, $B_0 = 1$ and $B_i = 0$ when $0 < i < d$.

Define $\beta_i = B_i/M$ for $0 \le i \le n$. Then $(\beta_i)_{i=0}^n$ is the probability measure on the distances in $\mathcal{C}$ that is induced by assuming a uniform distribution on the codewords of $\mathcal{C}$. In particular,

$$\mathsf{E}_{\mathcal{C}} = \sum_{i=0}^{n} i\beta_i$$

is the average distance between any two codewords in $\mathcal{C}$, and

$$\mathsf{S}_{\mathcal{C}} = \sum_{i=0}^{n} i^2\beta_i$$

is the second moment of the distances. It is known that $\mathsf{E}_{\mathcal{C}}$ is bounded from above by $n/2$ (in fact, this is the basis of the proof of the Plotkin bound: see [9, pp. 41–42]).

In this work, we obtain a new lower bound on the second moment $\mathsf{S}_{\mathcal{C}}$, in terms of the code parameters n and M and the average $\mathsf{E}_{\mathcal{C}}$. This bound will be presented in Section 3 (and a counterpart of that bound for constant-weight codes will be presented in Section 5). There are known bounds on the moments of codes, obtained from MacWilliams' identities, the Delsarte linear programming (DLP) bound, and enhancements thereof: see [1], [2], [3], [9, Sections 5.2 and 17.4]. We show that there is a range of code parameters for which the bound we present here is not implied by these techniques.

As an application of our new lower bound, we present in Section 4 an upper bound on the size M of a binary code $\mathcal{C}$, in terms of its length n, minimum distance d, and the *maximum distance* $d_{\max}$ between any two codewords in $\mathcal{C}$. The effectiveness of our bound can be seen in cases where $d_{\max}$ is close to d, i.e., when the distance distribution of the code is required to be narrow. As a concrete practical motivation for studying such codes, we refer the reader to [8], where it is demonstrated how binary constant-weight codes with narrow distance distribution can be incorporated into the design of demultiplexers for nano-scale memories.

The following definition will be useful throughout this work.

Let $A = A(\mathcal{C})$ be an $M \times n$ real matrix whose rows are indexed by the codewords of $\mathcal{C}$, and the row of A that is indexed by $\mathbf{c}$ is given by

$$(A)_{\mathbf{c}} = 2\mathbf{c} - \mathbf{1} \;;$$

here **1** denotes the real all-one vector of length n and the codeword $\mathbf{c}$ is regarded as an *integer* vector over $\{0,1\}^n$ (thus, the entries of A are in $\{-1,+1\}$). For $i = 0, 1, \ldots, n$, denote by E_i the $M \times M$ matrix whose rows and columns are indexed by the codewords of $\mathcal{C}$, and for every $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$,

$$(E_i)_{\mathbf{c},\mathbf{c}'} = \begin{cases} 1 & \text{if } \mathsf{d}(\mathbf{c},\mathbf{c}') = i \\ 0 & \text{otherwise} \end{cases} .$$

Let J denote the $M \times M$ all-one matrix. Clearly, we have $E_0 = I$ and $\sum_{i=0}^{n} E_i = J$. It follows that

$$AA^T = \sum_{i=0}^{n} (n-2i) \cdot E_i = n \cdot J - 2 \sum_{i=1}^{n} i \cdot E_i \ . \tag{1}$$

Example 1.1 An (n, M, d) binary code $\mathcal{C}$ is *equidistant* if $B_i \neq 0$ only if $i \in \{0, d\}$. For equidistant codes we have

$$E_i = \begin{cases} I & \text{if } i = 0 \\ J - I & \text{if } i = d \\ 0 & \text{otherwise} \end{cases}$$

and, so,

$$AA^T = (n{-}2d) \cdot J + (2d) \cdot I \ . \tag{2}$$

□

2 Bound on the size of equidistant codes

In this section, we present an upper bound on the size of equidistant codes. At first sight, this result might not seem to be related to the problem of bounding the second moment of the distances. However, the proof technique that we use here bears a common ground with the analyses in subsequent sections, through the properties of the matrix AA^T in (1).

Recall that the Plotkin bound states that for every (n, M, d) binary code $\mathcal{C}$ for which $n < 2d$,

$$M \le \frac{2d}{2d-n} ,$$

and equality can be attained only if $\mathcal{C}$ is equidistant (see [9, pp. 41–42]).

Proposition 2.1 *Let $\mathcal{C}$ be an equidistant (n, M, d) binary code. Then $M \le n{+}1$, and equality holds if and only if $n = 2d{-}1$ and $\mathcal{C}$ attains the Plotkin bound.*

Proof. The "if" part is straightforward: when $n = 2d{-}1$ and $\mathcal{C}$ attains the Plotkin bound, then

$$M = \frac{2d}{2d-n} = 2d = n{+}1 \ .$$

Turning to the "only if" part, the proof is similar to that of Fisher's inequality in block designs (see [4, p. 81] or [9, p. 62]). Specifically, we compute the rank of the matrix AA^T in two ways. On the one hand,

$$\text{rank}(AA^T) = \text{rank}(A) \le n \; . \tag{3}$$

On the other hand, we see from (2) that the eigenvalues of AA^T are $2d + M(n{-}2d)$ (with multiplicity 1) and $2d$ (with multiplicity $M{-}1$). Therefore,

$$\text{rank}(AA^T) = \left\{ \begin{array}{cl} M{-}1 & \text{if } 2d + M(n{-}2d) = 0 \\ M & \text{otherwise} \end{array} \right. \; . \tag{4}$$

We conclude from (3) and (4) that $M{-}1 \le n$, with equality holding only if $2d{+}M(n{-}2d) = 0$. In case of equality we have

$$n{+}1 = M = \frac{2d}{2d - n} \; ,$$

and it can be readily seen that $2d/(d{-}n)$ may exceed n only when $n = 2d{-}1$. □

The bound in Proposition 2.1 is attained by Hadamard codes [9, Section 2.3]. The $(n{>}3, M{=}n, d{=}2)$ code that consists of all binary words of length n and Hamming weight 1 is equidistant and its size is the largest possible for its length, given that $n > 2d{-}1$. See Tonchev [11, Section 4] (and the references therein) for conditions on the existence of equidistant codes that meet the Plotkin bound. A characterization of all *linear* equidistant codes can be found in Bonisoli [5].

3 Bound on the second moment

For a real $M \times M$ matrix $Y = (y_{i,j})_{i=1}^{M}{}_{j=1}^{M}$, denote by $\text{Tr}(Y)$ its trace and by $\|Y\|_F$ its Frobenius norm, i.e.,

$$\|Y\|_F = \Big(\sum_{i=1}^{M} \sum_{j=1}^{M} y_{i,j}^2 \Big)^{1/2} \; .$$

It is easy to verify that

$$\|Y\|_F = \text{Tr}(Y^2) \; .$$

We make use of the following theorem, which shows the effect on the eigenvalues of a given real symmetric matrix X, caused by subtracting from X a nonnegative definite symmetric matrix of rank 1 (see Wilkinson [12, pp. 94–97]).

Theorem 3.1 *Let X be a real symmetric $M \times M$ matrix with eigenvalues $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_M$ and let $\mathbf{v}$ be a real row vector of length M. Define the matrix Y by*

$$Y = X - \mathbf{v}^T \mathbf{v} \; ,$$

and let $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_M$ be the eigenvalues of Y. Then, for $r = 1, 2, \ldots, M{-}1$,

$$\lambda_{r+1} \leq \mu_r \leq \lambda_r \ ,$$

and

$$\mu_M \leq \lambda_M \ .$$

Proposition 3.2 *Let $M \cdot (\beta_i)_{i=0}^n$ be the distance distribution of an $(n, M{\geq}n, d)$ binary code. Then for every nonnegative real $\gamma \leq n/2$,*

$$\sum_{i=0}^{n} (i-\gamma)^2 \beta_i \geq \frac{\gamma^2}{n} \ .$$

Proof. From (1) we have,

$$AA^T = (n{-}2\gamma) \cdot J + 2 \sum_{i=0}^{n} (\gamma - i) \cdot E_i$$

and, so,

$$4M^2 \sum_{i=0}^{n} (i-\gamma)^2 \beta_i = \left\| 2 \sum_{i=0}^{n} (\gamma - i) \cdot E_i \right\|_F^2 = \left\| AA^T - (n{-}2\gamma) \cdot J \right\|_F^2 \ . \tag{5}$$

In what follows, we bound from below the right-hand side of (5). To this end, we apply Theorem 3.1 to the symmetric matrix $X = AA^T$ and the vector

$$\mathbf{v} = \sqrt{n{-}2\gamma} \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix} \ .$$

Then,

$$Y = AA^T - (n{-}2\gamma) \cdot J \ , \tag{6}$$

and the right-hand side of (5) equals $\|Y\|_F^2 = \mathrm{Tr}(Y^2)$. Note also that $\mathrm{Tr}(Y) = 2M\gamma$.

The matrix $X = AA^T$ is nonnegative definite (i.e., $\lambda_M \geq 0$), and $\mathrm{rank}(X) = \mathrm{rank}(A) \leq n$; hence,

$$\lambda_{n+1} = \lambda_{n+2} = \ldots = \lambda_M = 0 \ .$$

Therefore, by Theorem 3.1, the eigenvalues of Y satisfy

$$\mu_{n+1} = \mu_{n+2} = \ldots = \mu_{M-1} = 0 \tag{7}$$

and

$$\mu_M \leq 0 \ . \tag{8}$$

From (7)–(8) it follows that

$$\sum_{r=1}^{n} \mu_r \geq \sum_{r=1}^{M} \mu_r = \mathrm{Tr}(Y) = 2M\gamma \ \ (\geq 0) \ .$$

Thus,

$$\|Y\|_F^2 = \mathrm{Tr}(Y^2) = \sum_{r=1}^{M} \mu_r^2 \geq \sum_{r=1}^{n} \mu_r^2 \geq \frac{1}{n}\Big(\sum_{r=1}^{n} \mu_r\Big)^2 \geq \frac{4M^2\gamma^2}{n} \qquad (9)$$

(where the penultimate inequality follows from the convexity of $z \mapsto z^2$). The result is now obtained by combining (5), (6), and (9). □

Theorem 3.3 *Let $\mathcal{C}$ be an $(n, M{\geq}n, d)$ binary code. Then*

$$\mathsf{S}_{\mathcal{C}} \geq \begin{cases} \dfrac{n\mathsf{E}_{\mathcal{C}}^2}{n{-}1} & \text{if } \mathsf{E}_{\mathcal{C}} \leq \dfrac{n{-}1}{2} \\ n\mathsf{E}_{\mathcal{C}} - \dfrac{n(n{-}1)}{4} & \text{if } \dfrac{n{-}1}{2} < \mathsf{E}_{\mathcal{C}} \leq \dfrac{n}{2} \end{cases} .$$

Proof. We observe that

$$\sum_{i=0}^{n} (i-\gamma)^2 \beta_i = \mathsf{S}_{\mathcal{C}} - 2\gamma\mathsf{E}_{\mathcal{C}} + \gamma^2 \ ,$$

and by Proposition 3.2 we thus get

$$\mathsf{S}_{\mathcal{C}} \geq 2\gamma\mathsf{E}_{\mathcal{C}} - \frac{n{-}1}{n} \cdot \gamma^2 \ , \qquad (10)$$

for every real $\gamma \leq n/2$. The right-hand side of (10) attains its maximum at

$$\gamma = \begin{cases} \dfrac{n\mathsf{E}_{\mathcal{C}}}{n{-}1} & \text{if } \mathsf{E}_{\mathcal{C}} \leq \dfrac{n{-}1}{2} \\ \dfrac{n}{2} & \text{if } \dfrac{n{-}1}{2} < \mathsf{E}_{\mathcal{C}} \leq \dfrac{n}{2} \end{cases} ,$$

and the result is obtained by substituting this maximizing value of γ into (10). □

We point out that the inequality

$$\mathsf{S}_{\mathcal{C}} \geq n\mathsf{E}_{\mathcal{C}} - \frac{n(n{-}1)}{4} \qquad (11)$$

(obtained by substituting $\gamma = n/2$ in Proposition 3.2) is implied by the DLP bound. To see this, recall that MacWilliams' identities relate the distance distribution $(B_i)_{i=0}^n$ to its MacWilliams transform $(B'_\ell)_{\ell=0}^n$ by

$$B'_\ell = \frac{1}{M} \sum_{i=0}^{n} \mathcal{K}_\ell(i;n) \cdot B_i \ , \quad 0 \le \ell \le n \ , \tag{12}$$

where

$$\mathcal{K}_\ell(x;n) = \sum_{j=0}^{\ell} (-1)^j \binom{x}{j} \binom{n-x}{\ell-j} \ , \quad 0 \le \ell \le n \ .$$

The DLP bound on the code size is then given as the largest attainable value of the sum

$$B_0 + B_1 + \ldots + B_n \quad (= M) \ ,$$

where $(B_i)_{i=0}^n$ ranges over all nonnegative rational vectors whose MacWilliams transform satisfies the following constraints:

$$B'_\ell \ge 0 \ , \quad 0 \le \ell \le n \tag{13}$$

(strictly speaking, the rational entries B_i should also be such that their sum M is one of their integer common denominators). For $\ell = 2$ we have

$$\mathcal{K}_2(x;n) = 2x^2 - 2nx + \binom{n}{2}$$

and, so,

$$0 \le B'_2 = 2\mathsf{S}_{\mathcal{C}} - 2n\mathsf{E}_{\mathcal{C}} + \binom{n}{2} \ ,$$

thereby yielding (11).

From this analysis it follows that when $\mathsf{E}_{\mathcal{C}} \ge (n-1)/2$ (e.g., when $\mathcal{C}$ is a linear code with no all-zero coordinates), Theorem 3.3 offers no improvement over the DLP bound. However, as we see in the sequel, there are instances where Theorem 3.3 implies a stronger bound than the DLP bound.

Note that Theorem 3.3 is at least as strong as Proposition 3.2, for any $\gamma \le n/2$: Proposition 3.2 is equivalent to the *linear* constraint (10) on $\mathsf{S}_{\mathcal{C}}$ and $\mathsf{E}_{\mathcal{C}}$ for any fixed γ, while Theorem 3.3 is the intersection (or the envelope) of the constraints (10) over all $\gamma \le n/2$. The advantage in having the individual linear constraints (10) available is that they can be incorporated into any bounding technique that uses linear programming.

A (qualitative) illustration of the bound of Theorem 3.3 is shown Figure 1. The curve changes from quadratic to linear in $\mathsf{E}_{\mathcal{C}}$ at the point $(\mathsf{E}_{\mathcal{C}}, \mathsf{S}_{\mathcal{C}}) = (\frac{n-1}{2}, \frac{n(n-1)}{4})$: note that it is the quadratic region where the theorem strictly improves on the DLP-implied bound (11).

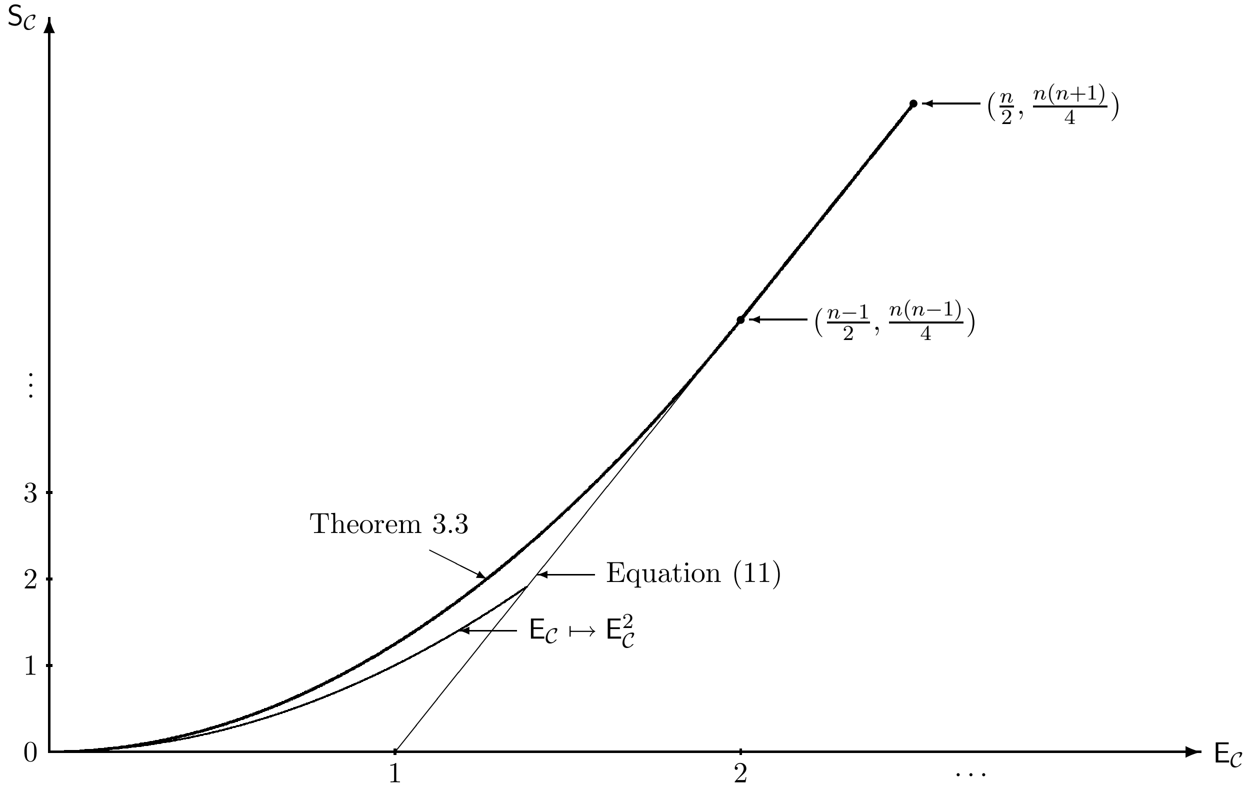

Figure 1: Bounds on $\mathsf{S}_{\mathcal{C}}$ in terms of $\mathsf{E}_{\mathcal{C}}$.

(The figure is, in fact, drawn to scale for the length value $n = 5$; as such, it exaggerates the proportions of the linear region of the bound. For larger n, the proportions change in favor of the quadratic region.) For reference, we have also included in the figure the curve $\mathsf{E}_{\mathcal{C}} \mapsto \mathsf{E}_{\mathcal{C}}^2$: the inequality $\mathsf{S}_{\mathcal{C}} \geq \mathsf{E}_{\mathcal{C}}^2$ must hold just from the fact that $(\beta_i)_{i=0}^n$ is a probability measure.

4 Bounds for narrow distance distributions

Theorem 3.3 can be used to obtain bounds on the parameters of codes whose distance distributions are limited to a narrow range of distances. Specifically, let $\mathcal{C}$ be an (n, M, d) binary code and denote by $d_{\max}$ the *maximum distance* between any two codewords in $\mathcal{C}$. We will be interested in cases where $d_{\max}$ is close to d. Equidistant codes are an extreme case where $d_{\max} = d$.

The next proposition yields an upper bound on the code size M, in terms of n, d, and $d_{\max}$.

Proposition 4.1 *Let $\mathcal{C}$ be an (n, M, d) binary code with maximum distance $d_{\max}$. Denote by $d_{\rm a}$ and $d_{\rm g}$ the arithmetic and geometric means, respectively, of d and $d_{\max}$; i.e.,*

$$d_{\rm a} = \frac{d_{\max} + d}{2} \quad \textit{and} \quad d_{\rm g} = \sqrt{d_{\max} d} \; .$$

Then

$$1 - \frac{1}{M} \le \begin{cases} \Bigl(1 - \dfrac{1}{n}\Bigr)\Bigl(\dfrac{d_{\rm a}}{d_{\rm g}}\Bigr)^2 & \textit{if } 2d_{\rm a} \notin \{n{+}1, n{+}2\} \\ \dfrac{n}{d_{\rm g}^2}\Bigl(d_{\rm a} - \dfrac{n{+}1}{4}\Bigr) & \textit{if } 2d_{\rm a} \in \{n{+}1, n{+}2\} \end{cases} .$$

Proof. For $d_{\max} = d$, the result follows from Proposition 2.1. In addition, the result can be easily verified to hold for the values $n = 2$, $d = 1$, and $d_{\max} = 2$. Therefore, we assume hereafter in the proof that $n \ge 3$ and $d_{\max} > d$.

For fixed value of $\mathsf{E}_{\mathcal{C}}$, the second moment $\mathsf{S}_{\mathcal{C}}$ attains its maximum when the distance distribution is concentrated at the boundary distance values, i.e., when $\beta_i \ne 0$ only for $i \in \{0, d, d_{\max}\}$. In our proof, we apply Theorem 3.3 to this extreme (worst case) distribution.

Assuming such a distribution, write $v = \beta_{d_{\max}}$; then $\beta_d = 1 - (1/M) - v$ and, so,

$$\mathsf{E}_{\mathcal{C}} = d\Bigl(1 - \frac{1}{M} - v\Bigr) + d_{\max} v = d\Bigl(1 - \frac{1}{M}\Bigr) + (d_{\max} - d)v \; ,$$

or

$$(d_{\max} - d)v = \mathsf{E}_{\mathcal{C}} - d\Bigl(1 - \frac{1}{M}\Bigr) \; . \tag{14}$$

Similarly,

$$\begin{aligned} \mathsf{S}_{\mathcal{C}} &= d^2\Bigl(1 - \frac{1}{M} - v\Bigr) + d_{\max}^2 v \\ &= d^2\Bigl(1 - \frac{1}{M}\Bigr) + (d_{\max}^2 - d^2)v \\ &= d^2\Bigl(1 - \frac{1}{M}\Bigr) + (d_{\max} + d)\left(\mathsf{E}_{\mathcal{C}} - d\Bigl(1 - \frac{1}{M}\Bigr)\right) \\ &= 2d_{\rm a}\mathsf{E}_{\mathcal{C}} - d_{\rm g}^2\Bigl(1 - \frac{1}{M}\Bigr) \; , \end{aligned}$$

where the third equality follows from (14). We now distinguish between two cases.

Case 1: $\mathsf{E}_{\mathcal{C}} \le (n{-}1)/2$. By Theorem 3.3 we have

$$\frac{n\mathsf{E}_{\mathcal{C}}^2}{n{-}1} - 2d_{\rm a}\mathsf{E}_{\mathcal{C}} + d_{\rm g}^2\Bigl(1 - \frac{1}{M}\Bigr) = \frac{n\mathsf{E}_{\mathcal{C}}^2}{n{-}1} - \mathsf{S}_{\mathcal{C}} \le 0 \; . \tag{15}$$

This inequality has a solution for $\mathsf{E}_{\mathcal{C}}$ only if the discriminant of the quadratic expression (in $\mathsf{E}_{\mathcal{C}}$) in (15) is nonnegative, namely,

$$4d_{\mathrm{a}}^2 - \frac{4d_{\mathrm{g}}^2 n}{n-1}\Bigl(1 - \frac{1}{M}\Bigr) \ge 0 \;,$$

which is the same as

$$1 - \frac{1}{M} \le \Bigl(1 - \frac{1}{n}\Bigr)\Bigl(\frac{d_{\mathrm{a}}}{d_{\mathrm{g}}}\Bigr)^2 \;. \tag{16}$$

Case 2: $\mathsf{E}_{\mathcal{C}} > (n-1)/2$. We again apply Theorem 3.3 to obtain

$$n\mathsf{E}_{\mathcal{C}} - \frac{n(n-1)}{4} - 2d_{\mathrm{a}}\mathsf{E}_{\mathcal{C}} + d_{\mathrm{g}}^2\Bigl(1 - \frac{1}{M}\Bigr) = n\mathsf{E}_{\mathcal{C}} - \frac{n(n-1)}{4} - \mathsf{S}_{\mathcal{C}} \le 0 \;,$$

or

$$1 - \frac{1}{M} \le \frac{1}{d_{\mathrm{g}}^2}\left((2d_{\mathrm{a}} - n)\mathsf{E}_{\mathcal{C}} + \frac{n(n-1)}{4}\right) \;. \tag{17}$$

For $d_{\mathrm{a}} \le n/2$, we bound from above the right-hand side of (17) by replacing $\mathsf{E}_{\mathcal{C}}$ with $(n-1)/2$; this yields

$$1 - \frac{1}{M} \le \frac{1}{d_{\mathrm{g}}^2}\left(d_{\mathrm{a}}(n-1) - \frac{n(n-1)}{4}\right) \;. \tag{18}$$

Similarly, for $d_{\mathrm{a}} > n/2$, we get the next bound from (17) by substituting $\mathsf{E}_{\mathcal{C}}$ for $n/2$:

$$1 - \frac{1}{M} \le \frac{1}{d_{\mathrm{g}}^2}\left(d_{\mathrm{a}}n - \frac{n(n+1)}{4}\right) \;. \tag{19}$$

A simple check reveals that the right-hand side of (18) is never greater than the right-hand side of (16); this means that the bound (16) prevails for $d_{\mathrm{a}} \le n/2$. On the other hand, the right-hand side of (19) exceeds that of (16) whenever

$$n < 2d_{\mathrm{a}} < \frac{n(n+1)}{n-1} \;; \tag{20}$$

observing that $n+2 < n(n+1)/(n-1) \le n+3$ for $n \ge 3$, we conclude from (20) that when $d_{\mathrm{a}} \in \{n+1, n+2\}$, the upper bound on $1 - (1/M)$ is dictated by (19). □

Remark. Since the last proof is based on putting the distribution mass on the extreme distance values, Proposition 4.1 is useful when $d_{\max}$ is bounded away from n; otherwise, our strategy would be too pessimistic. For example, it is easy to see that in every (n, M, d) binary code, the tail of the distance distribution satisfies

$$\sum_{i > n-(d/2)} B_i \le 1 \;,$$

and taking this inequality into account, our bound can then be improved when $d_{\max} > n-(d/2)$. □

We next present two applications of Proposition 4.1; both take advantage of the fact that the proposition yields the strongest bound when the distance distribution is two-valued (i.e., the distribution is nonzero only at two nonzero distance values). The first application is an alternate proof of the Grey–Rankin bound (see [7] and [9, p. 544]).

Theorem 4.2 (The Grey–Rankin bound) *Let $\mathcal{C}$ be an (n, M, d) binary code that is self-complementary, i.e., if* $\mathbf{c}$ *is a codeword in $\mathcal{C}$ then so is the word that is obtained by changing each* 1 *in* $\mathbf{c}$ *into* 0 *and each* 0 *into* 1*. If $(n-\sqrt{n})/2 < d \le n/2$ then*

$$M \le \frac{8d(n-d)}{n-(n-2d)^2} \; .$$

Proof. Let $\mathcal{C}'$ be the $(n, M/2, d')$ code obtained by taking one codeword of $\mathcal{C}$ from each complementary pair. The minimum distance d' of $\mathcal{C}'$ is at least d and its maximum distance $d_{\max}$ is at most $n-d$. Let d_{a} and d_{g} be given by $\frac{1}{2}(d_{\max}+d')$ and $d_{\mathrm{g}} = \sqrt{d_{\max}d'}$, respectively, and define the function $z \mapsto Q(z)$ over the positive reals by

$$Q(z) = \frac{1}{4}\Big(z + \frac{1}{z} + 2\Big) \; .$$

It is easy to verify that

$$\Big(\frac{d_{\mathrm{a}}}{d_{\mathrm{g}}}\Big)^2 = Q\Big(\frac{d'}{d_{\max}}\Big) \le Q\Big(\frac{d}{n-d}\Big) = \frac{n^2}{4d(n-d)} \; ,$$

where the inequality follows from the fact that $Q(z)$ is a decreasing function for $z \in (0,1]$. By Proposition 4.1 we thus have

$$1 - \frac{2}{M} \le \Big(1-\frac{1}{n}\Big)\Big(\frac{d_{\mathrm{a}}}{d_{\mathrm{g}}}\Big)^2 \le \Big(1-\frac{1}{n}\Big)Q\Big(\frac{d}{n-d}\Big) = \frac{n(n-1)}{4d(n-d)} \; ,$$

or

$$M\Big(n-(n-2d)^2\Big) \le 8d(n-d) \; .$$

The result follows. □

In our next application of Proposition 4.1, we consider the case where the equidistant property is slightly relaxed. As is commonly done in bounds that are based on the distance distribution, we will limit ourselves to even-distant codes, namely, $B_i \neq 0$ only if i is even (when d is even, this condition can be guaranteed simply by changing the last coordinate in each codeword of $\mathcal{C}$ into a parity bit; when d is odd, we apply the bounds to the $(n+1, M, d+1)$ code obtained by adding a parity bit as an $(n+1)$st coordinate).

An (n, M, d) binary code $\mathcal{C}$ is called *nearly-equidistant* if it is even-distant and $d_{\max} = d+2$.

Proposition 4.3 *Let $\mathcal{C}$ be a nearly-equidistant (n, M, d) binary code. Then the following holds.*

(i) If $\lfloor \sqrt{n} \rfloor \le d \le (n/2){-}1$ *then*

$$M \le \frac{d(d{+}2)n}{(d{+}1)^2 - n} .$$

(ii) If $(n/2){-}1 < d \le (n{+}1)/2$ *then*

$$M \le \begin{cases} (n{+}3)(n{-}1)/(n{-}3) & \text{if } d = (n{-}1)/2 \\ n{+}4 & \text{if } d = n/2 \\ n{+}1 & \text{if } d = (n{+}1)/2 \end{cases} .$$

Proof. Part (i) corresponds to the case where $2d_{\mathrm{a}} < n{+}1$ in Proposition 4.1. Part (ii) corresponds to the case where either $2d_{\mathrm{a}} \in \{n{+}1, n{+}2\}$ or the Plotkin bound is attained. □

Example 4.1 For $n = 13$ and $d = 4$, Proposition 4.3(i) yields the upper bound $M \le 26$. This bound is attained by a certain $(13, 26, 4)$ binary code whose codewords all have Hamming weight 3 (see Brouwer *et al.* [6, Table I-A]); thus, this code is nearly-equidistant. In comparison, the DLP bound yields $M \le 40$ for these parameters (with a feasible solution $B_4 = 13$ and $B_6 = 26$). □

Example 4.2 The linear $(n{=}9, M{=}2^4, d{=}4)$ binary code that is generated by the matrix

$$G = \begin{pmatrix} 1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,1\,0\,0\,0 \\ 1\,0\,1\,0\,0\,0\,1\,0\,1 \\ 1\,0\,0\,0\,1\,0\,0\,1\,1 \end{pmatrix}$$

can be verified to be nearly-equidistant with minimum distance $d = (n{-}1)/2 = 4$. This code attains the bound in Proposition 4.3(ii), which coincides with the DLP bound in this case.□

Example 4.3 As shown in [9, p. 549], by puncturing the binary simplex code, one can obtain linear nearly-equidistant $(n{=}2^m{-}4, M{=}2^m, d{=}2^{m-1}{-}2)$ binary codes; these codes attain the bound in Proposition 4.3(ii), which again, as expected, coincides with the DLP bound. □

For the code in Example 4.1 we have $2d_{\mathrm{a}} \notin \{n{+}1, n{+}2\}$, while the codes in Examples 4.2 and 4.3 satisfy $2d_{\mathrm{a}} \in \{n{+}1, n{+}2\}$. The former therefore belongs to the first range of values of d_{a} in Proposition 4.1, while the latter belong to the second range therein. Each of these examples attains the bound in Proposition 4.1 and violates the bound that corresponds to the range that it does not belong to. This shows that the distinction between the two ranges of values of d_{a} in Proposition 4.1 is necessary.

Table 1 shows the lower bounds on the length n, which are computed from Proposition 4.3 and the DLP bound, respectively, for nearly-equidistant (n, M, d) binary codes with $M = 64$ and $d = 2, 4, 6, 8, 10$ (the value 64 for M was selected to match the example in [8, Section 4]). Note that for $d = 2$, the DLP bound yields a better bound than Proposition 4.3.

d	Proposition 4.3	DLP Bound
2	8	12
4	19	15
6	28	19
8	36	21
10	43	25

Table 1: Lower bounds on the length n of nearly-equidistant $(n, M{=}64, d)$ binary codes.

There are coding applications where the parameters of interest are the code length n, size M, and the *ratio* $d_{\max}/d$ (rather than the specific values of d and $d_{\max}$). One such application is the design of demultiplexers for nano-scale memory platforms, where M stands for the memory size and n is the number of address lines, and the goal is to have $d_{\max}/d$ as small as possible [8] (in this application, the codes are also required to be of the constant-weight type; we consider such codes in Section 5). Propositions 4.1 and 4.3 can be used to find a trade-off between the parameters n, M, and $d_{\max}/d$ for even-distant codes, as demonstrated in the next example.

Example 4.4 We find the largest even-distant binary code with $n = 27$ and $d_{\max}/d = 4/3$. From Proposition 4.3 it follows that every nearly-equidistant $(n{=}27, M, d{=}6)$ binary code has size $M \leq 58$ (in comparison, the DLP bound provides a feasible solution for $M = 309$). We next check the values $d = 12$ and $d_{\max} = 16$. In this case, either bound—Proposition 4.1 or the DLP bound—implies the upper bound $M \leq 64$. There actually exists a linear $(n{=}27, M{=}2^6, d{=}12)$ code with $d_{\max} = 16$: it is obtained by shortening a self-complementary linear $(28, 2^7, 12)$ code which attains the Grey–Rankin bound (see Parker *et al.* [10] and Tonchev [11, p. 1263]).

The ratio $d_{\max}/d = 4/3$ can also be realized by $d = 18$ and $d_{\max} = 24$, yet by the Plotkin bound, the largest $(27, M, 18)$ binary code has size $M = 4$. □

Using Propositions 4.1 and 4.3 and the DLP bound (combined), we have created Table 2: this table provides a lower bound on $d_{\max}/d$ as a function of n, where we have taken the size M to be 64.

Range of n	$d_{\max}/d \geq$
$7 \leq n \leq 10$	3
$11 \leq n \leq 13$	2
$14 \leq n \leq 17$	5/3
$18 \leq n \leq 22$	3/2
$23 \leq n \leq 26$	7/5
$27 \leq n \leq 32$	4/3

Table 2: Lower bounds on the ratio $d_{\max}/d$ for even-distant $(n, M{=}64)$ binary codes, as a function of n.

The lower bounds in Table 2 are known to be tight, except possibly for the penultimate row. For $n = 7$ (and therefore for every $n \geq 7$), the ratio $d_{\max}/d = 3$ is attained by the $(7, 2^6, 2)$ parity code (for $n > 7$ we just pad each codeword with a tail of $n{-}7$ zeros), and a ratio of $d_{\max}/d = 2$ is attained by the $(11, 72, 4)$ code defined in [9, pp. 70–71]. By shortening the $(16, 256, 6)$ Nordstrom–Robinson code, we get a code that attains a ratio of 5/3 for $n = 14$ (see [9, pp. 73–74]); similarly, by shortening the extended binary Golay code one can obtain a linear $(18, 2^6, 8)$ code with a ratio of 3/2. Finally, the code described in Example 4.4 attains a ratio of 4/3 for $n = 27$. As of yet, we do not know whether $n = 23$ is the smallest length for which a ratio of 7/5 is achievable.

5 The constant-weight case

An (n, M, d) binary code $\mathcal{C}$ is called a *constant-weight code* if all the codewords in $\mathcal{C}$ have the same Hamming weight. We then say that $\mathcal{C}$ is an (n, M, d, w) code, where w is the Hamming weight of each codeword. There is no loss of generality in assuming that $w \leq n/2$, and we will indeed assume this inequality throughout this section. Constant-weight codes are always even-distant.

Proposition 3.2 can be slightly improved in the case of constant-weight codes, as we show next.

Proposition 5.1 *Let $M \cdot (\beta_i)_{i=0}^n$ be the distance distribution of an $(n, M{\geq}n, d, w)$ code, and denote by θ the ratio w/n. Then for every nonnegative real $\gamma \leq 2\theta(1{-}\theta)n$,*

$$\sum_{i=0}^{n} (i - \gamma)^2 \beta_i \geq \frac{\gamma^2}{n{-}1} \, .$$

Proof. The proof is similar to that of Proposition 3.2, except that we re-define the $M \times n$

matrix A so that its rows are now given by

$$(A)_{\mathbf{c}} = 2(\mathbf{c} - \theta \cdot \mathbf{1})$$

(the multiplier 2 in this definition is not essential to derive our results: it is inserted only to make the definition here closer to the one in Section 1). It follows that for every codeword $\mathbf{c} \in \mathcal{C}$,

$$(A)_{\mathbf{c}} \cdot \mathbf{1}^T = 2\underbrace{(\mathbf{c} \cdot \mathbf{1}^T)}_{w} - 2\theta \cdot \underbrace{(\mathbf{1} \cdot \mathbf{1}^T)}_{n} = 0 \; .$$

This implies that $A\mathbf{1}^T = \mathbf{0}$, which readily means that $\operatorname{rank}(A) \le n{-}1$. Also, for any two codewords $\mathbf{c}$ and $\mathbf{c}'$,

$$\begin{aligned} (A)_{\mathbf{c}'} \cdot (A)_{\mathbf{c}}^T &= 4(\mathbf{c}' - \theta \cdot \mathbf{1}) \cdot (\mathbf{c} - \theta \cdot \mathbf{1})^T \\ &= \underbrace{4(\mathbf{c}' \cdot \mathbf{c}^T)}_{4w-2\mathsf{d}(\mathbf{c},\mathbf{c}')} - 4\theta \cdot \Big(\underbrace{(\mathbf{c}' \cdot \mathbf{1}^T)}_{w} + \underbrace{(\mathbf{1} \cdot \mathbf{c}^T)}_{w} - \theta \cdot \underbrace{(\mathbf{1} \cdot \mathbf{1}^T)}_{n} \Big) \\ &= 4\theta(1{-}\theta)n - 2\,\mathsf{d}(\mathbf{c}, \mathbf{c}') \; . \end{aligned}$$

Hence, (the counterparts of) Equations (1) and (5) become, respectively,

$$AA^T = \sum_{i=0}^{n} (4\theta(1{-}\theta)n - 2i) \cdot E_i = 4\theta(1{-}\theta)n \cdot J - 2\sum_{i=1}^{n} i \cdot E_i$$

and

$$4M^2 \sum_{i=0}^{n} (i-\gamma)^2 \beta_i = \Big\| 2\sum_{i=0}^{n} (\gamma - i) \cdot E_i \Big\|_F^2 = \big\| AA^T - (4\theta(1{-}\theta)n - 2\gamma) \cdot J \big\|_F^2 \; . \qquad (21)$$

Next, we apply Theorem 3.1 to $X = AA^T$ and

$$\mathbf{v} = \sqrt{4\theta(1{-}\theta)n - 2\gamma} \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix} \; .$$

Here

$$Y = AA^T - (4\theta(1{-}\theta)n - 2\gamma) \cdot J$$

and, since $\operatorname{rank}(X) = \operatorname{rank}(A) \le n{-}1$, we get that

$$\lambda_n = \lambda_{n+1} = \ldots = \lambda_M = 0$$

(i.e., λ_n is also zero); thus, (7) becomes

$$\mu_n = \mu_{n+1} = \ldots = \mu_{M-1} = 0 \; ,$$

and (8) still holds. It follows that

$$\sum_{r=1}^{n-1} \mu_r \ge \sum_{r=1}^{M} \mu_r = \operatorname{Tr}(Y) = 2M\gamma \;\; (\ge 0)$$

and, so,

$$\|Y\|_F^2 = \mathrm{Tr}(Y^2) \geq \sum_{r=1}^{n-1} \mu_r^2 \geq \frac{1}{n-1}\Big(\sum_{r=1}^{n-1} \mu_r\Big)^2 \geq \frac{4M^2\gamma^2}{n-1} \;.$$

Finally, we combine the latter equation with (21). □

Theorem 5.2 *Let $\mathcal{C}$ be an $(n, M{\geq}n, d, w)$ code and define $\alpha = \alpha(n, w)$ by*

$$\alpha = 2w\Big(1 - \frac{w}{n}\Big) \;.$$

Then

$$\mathsf{S}_{\mathcal{C}} \geq \begin{cases} \dfrac{n-1}{n-2} \cdot \mathsf{E}_{\mathcal{C}}^2 & \text{if } \mathsf{E}_{\mathcal{C}} \leq \dfrac{(n-2)\alpha}{n-1} \\ 2\alpha \cdot \mathsf{E}_{\mathcal{C}} - \dfrac{(n-2)\alpha^2}{n-1} & \text{if } \dfrac{(n-2)\alpha}{n-1} < \mathsf{E}_{\mathcal{C}} \leq \alpha \end{cases} \;.$$

Proof. Similarly to (10), we get from Proposition 5.1 that

$$\mathsf{S}_{\mathcal{C}} \geq 2\gamma \mathsf{E}_{\mathcal{C}} - \frac{n-2}{n-1} \cdot \gamma^2 \;, \tag{22}$$

for every real $\gamma \leq \alpha$. The right-hand side of (22), in turn, attains its maximum at

$$\gamma = \begin{cases} \dfrac{n-1}{n-2} \cdot \mathsf{E}_{\mathcal{C}} & \text{if } \mathsf{E}_{\mathcal{C}} \leq \dfrac{(n-2)\alpha}{n-1} \\ \alpha & \text{if } \mathsf{E}_{\mathcal{C}} > \dfrac{(n-2)\alpha}{n-1} \end{cases} \;.$$

The result is obtained by substituting this value of γ into (22) and recalling the known fact that $\mathsf{E}_{\mathcal{C}} \leq \alpha$ (see, e.g., [9, pp. 525–526], where this fact is used in proving the Johnson bound). □

We next compare Theorem 5.2 with the DLP bound for constant-weight codes. The counterpart of (12) for the constant-weight case is given by

$$B'_{2\ell} = \frac{1}{M} \sum_{i=0}^{w} \mathcal{E}_\ell(i; n, w) \cdot B_{2i} \;, \quad 0 \leq \ell \leq w \;, \tag{23}$$

where

$$\mathcal{E}_\ell(x; n, w) = \frac{\displaystyle\sum_{j=0}^{\ell} (-1)^j \binom{x}{j}\binom{w-x}{\ell-j}\binom{n-w-x}{\ell-j}}{\dbinom{w}{\ell}\dbinom{n-w}{\ell}} \;, \quad 0 \leq \ell \leq w \;,$$

and the constraints (13) now become

$$B'_{2\ell} \geq 0 \; , \quad 0 \leq \ell \leq w \tag{24}$$

(see [1, Proposition 16] and [9, p. 665]). In particular, for $\ell = 2$ we get

$$\mathcal{E}_2(x; n, w) = \frac{\binom{n-1}{2} x^2 - \binom{n}{2} \Big(\alpha(n,w) - 1 \Big) x}{2 \binom{w}{2} \binom{n-w}{2}} + 1$$

and, so,

$$\begin{aligned} 0 \;\; &\leq \;\; 16 \binom{w}{2} \binom{n-w}{2} B'_4 \\ &= \;\; 2 \binom{n-1}{2} \mathsf{S}_{\mathcal{C}} - 4 \binom{n}{2} (\alpha - 1) \mathsf{E}_{\mathcal{C}} + 16 \binom{w}{2} \binom{n-w}{2} \\ &= \;\; (n-1) \left((n-2) \mathsf{S}_{\mathcal{C}} - 2n(\alpha-1)\mathsf{E}_{\mathcal{C}} + \frac{n^2\alpha^2}{n-1} - 2n\alpha \right) \; . \end{aligned}$$

Hence,

$$\mathsf{S}_{\mathcal{C}} \geq \frac{1}{n-2} \left(2n(\alpha-1)\mathsf{E}_{\mathcal{C}} - \frac{n^2\alpha^2}{n-1} + 2n\alpha \right) \; . \tag{25}$$

A simple check reveals that the bound of Theorem 5.2 is stronger than (25) whenever

$$\mathsf{E}_{\mathcal{C}} < \frac{n(\alpha-1) - \sqrt{n^2 - 2n\alpha}}{n-1} \; .$$

For larger values of $\mathsf{E}_{\mathcal{C}}$, the bound (25) becomes tighter, until the bounds coincide again at $\mathsf{E}_{\mathcal{C}} = \alpha$. When $w = n/2$, the value of α is $n/2$, in which case the bound (25) coincides with the bound of Theorem 5.2 whenever $\mathsf{E}_{\mathcal{C}}$ is in the range

$$\frac{n(n-2)}{2(n-1)} = \frac{(n-2)\alpha}{n-1} \leq \mathsf{E}_{\mathcal{C}} \leq \alpha = \frac{n}{2} \; ;$$

this range is precisely where the bound of Theorem 5.2 is linear in $\mathsf{E}_{\mathcal{C}}$.

Example 5.1 We consider the parameters $n = 28$ and $d_{\max}/d = 4/3$. By Theorem 5.2, the largest nearly-equidistant $(n{=}28, M, d{=}6, w)$ code has size $M \leq 63$, and equality is possible only when $w = 4$. For this value of w, the largest possible size M is attained when $\mathsf{E}_{\mathcal{C}} = \alpha(28, 4) = 48/7$, in which case Theorem 5.2 coincides with (25); therefore, for $w = 4$, Theorem 5.2 does not offer an improvement over the constant-weight DLP bound. However, for larger values of w, Theorem 5.2 strictly improves on that DLP bound. For example, for $w = 12$, Equations (23)–(24) allow $M = 280$ as a feasible solution, while Theorem 5.2 bounds M from above by 58.

Similarly, by combining Equations (23)–(24) with Theorem 5.2, we get that the largest $(n{=}28, M, d{=}12, w)$ code with $d_{\max} = 16$ has size $M \leq 63$, and equality is possible only when $w \in \{11, 12\}$. Equality is indeed attained by codes with $w = 12$ that are based on quasi-symmetric 2-designs [10], [11, p. 1263]. □

Table 3 is the constant-weight counterpart of Table 2 (for code size $M = 64$). The first five rows in Table 3 present tight bounds. Ratios of 4 and 3, respectively, can be achieved by the (trivial) $(8, 70, 2, 4)$ and $(9, 84, 2, 3)$ codes. A ratio of $d_{\max}/d = 2$ is attained by the $(11, 66, 4, 5)$ code that is based on the Steiner system $S(4, 5, 11)$ [9, p. 70], and a ratio of $d_{\max}/d = 5/3$ is attained by the $(15, 70, 6, 6)$ code that consists of the codewords of Hamming weight 6 in the shortened $(15, 128, 6)$ Nordstrom–Robinson code [9, p. 74]. Finally, one can obtain a $(19, 70, 8, 9)$ code with $d_{\max}/d = 3/2$ by shortening, expurgating, and augmenting the set of codewords of Hamming weight 12 in the extended binary Golay code (see the Appendix in [8]).

Range of n	$d_{\max}/d \geq$
$n = 8$	4
$9 \leq n \leq 10$	3
$11 \leq n \leq 14$	2
$15 \leq n \leq 18$	5/3
$19 \leq n \leq 23$	3/2
$24 \leq n \leq 28$	7/5
$29 \leq n \leq 32$	4/3

Table 3: Lower bounds on the ratio $d_{\max}/d$ for $(n, M{=}64)$ constant-weight codes, as a function of n.

Figure 2 depicts the bounds of Theorem 5.2 and Equation (25), superimposed on Figure 1 (Figure 2 is drawn to scale for $n = 5$ and $w = 2$).

References

[1] E. Agrell, A. Vardy, K. Zeger, *Upper bounds for constant-weight codes, IEEE Trans. Inform. Theory,* 46 (2000), 2373–2395.

[2] A. Ashikhmin, A. Barg, *Binomial moments of the distance distribution: bounds and applications, IEEE Trans. Inform. Theory,* 45 (1999), 438–452.

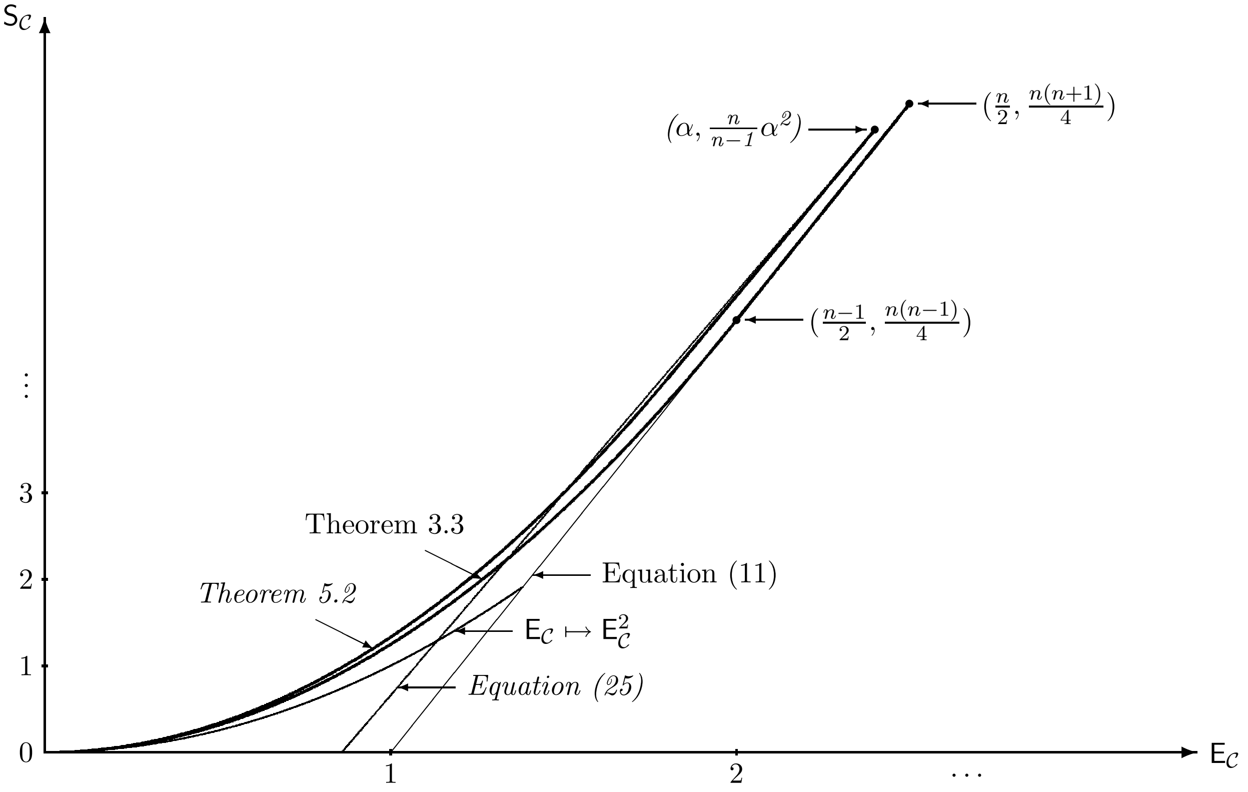

Figure 2: Bounds for the constant-weight case.

[3] A. Ashikhmin, A. Barg, S. Litsyn, *Estimates of the distance distribution of codes and designs, IEEE Trans. Inform. Theory,* 47 (2001), 1050–1061.

[4] T. Beth, D. Jungnickel, H. Lenz, *Design Theory,* Cambridge University Press, Cambridge, 1986.

[5] A. Bonisoli, *Every equidistant linear code is a sequence of dual Hamming codes, Ars Combinatoria,* 8 (1983), 181–186.

[6] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, *A new table of constant weight codes, IEEE Trans. Inform. Theory,* 36 (1990), 1334–1380.

[7] L.D. Grey, *Some bounds for error-correcting codes, IRE Trans. Inform. Theory,* 8 (1962), 200–202 and 355.

[8] P.J. Kuekes, W. Robinett, R.M. Roth, G. Seroussi, G.S. Snider, R.S. Williams, *Resistor-logic demultiplexers for nanoelectronics based on constant-weight codes, Nanotechnology,* 17 (2006), 1052–1061.

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

[10] C. Parker, E. Spence, V.D. Tonchev, *Designs with the symmetric difference property on* 64 *points and their groups, J. Comb. Theory A,* 67 (1994), 23–43.

[11] V.D. Tonchev, *Codes and designs,* in *Handbook of Coding Theory,* V.S. Pless, W.C. Huffman (Editors), Elsevier, Amsterdam, 1998, pp. 1229–1267.

[12] J.H. Wilkinson, *The Algebraic Eigenvalue Problem,* Clarendon Press, Oxford, 1988.