Linear Programming Bounds for Doubly-Even Self-Dual Codes

Ilia Krasikov and Simon Litsyn, *Member, IEEE*

***Abstract*—Using a variant of linear programming method we derive a new upper bound on the minimum distance d of doubly-even self-dual codes of length n. Asymptotically, for n growing, it gives $d/n \le 0.166315 \cdots + o(1)$, thus improving on the Mallows–Odlyzko–Sloane bound of $1/6$. To establish this, we prove that in any doubly even-self-dual code the distance distribution is asymptotically upper-bounded by the corresponding normalized binomial distribution in a certain interval.**

***Index Terms*— Distance distribution, self-dual codes, upper bounds.**

I. Introduction

A SELF-DUAL linear code C of length n and minimum distance d is doubly-even if all its weights are divisible by 4. It is known that such codes exist only for n divisible by 8 (this result is attributed to Gleason). Let d_n be the minimum distance of a doubly-even self-dual code of length n. The question is as follows: given n, how large d_n could be? We consider an asymptotical problem, namely, we want to estimate

$$\delta = n^{-1} \lim_{n\to\infty} \sup d_n.$$

We need some notations. In what follows, all logarithms are natural, and the logarithm of a negative number is understood as its real part (by this convention we avoid writing the absolute values of the expressions under logarithms). As usual

$$H(x) = -x \ln x - (1-x)\ln(1-x)$$

stands for the natural entropy function. The binomial coefficients are defined by

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

where x is arbitrary and k is a nonnegative integer. In particular, for positive x

$$\binom{-x}{k} = (-1)^k \binom{x+k-1}{k}.$$

Let $\boldsymbol{B} = (B_0, B_1, \cdots, B_n)$ stand for the distance distribution of a self-dual code C. It is invariant under the MacWilliams transform

$$|C|B_i = \sum_{j=0}^{n} B_j P_i(j) \tag{1}$$

where P_i is the corresponding Krawtchouk polynomial of degree i

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

(for properties of Krawtchouk polynomials see e.g., [5], [8], [9], [11]).

Self-dual codes attract a great deal of attention, mainly due to their intimate connections with improtant problems in algebra and number theory (see many references in [1], [2], [11], [14]). Most of the results are based on an involved machinery of invariant theory. The following are the best known upper bounds on the minimum distance of doubly-even self-dual codes.

Theorem 1 (Mallows–Sloane): In doubly-even self-dual codes

$$d \le 4\lfloor n/24 \rfloor + 4.$$

An alternative proof of this result will be given in the Appendix. For large n, a slightly stronger inequality was established in [13].

Theorem 2 (Mallows–Odlyzko–Sloane): For every constant b there exists an n_0 such that for $n \ge n_0$ in doubly-even self-dual codes

$$d \le n/6 - b.$$

Both bounds yield $\delta \le 1/6$. Despite of the general belief that actually $\delta = H^{-1}(1/2) = 0.110\ldots$, there was no progress in the last two decades in improving the upper bound of $1/6$. For unrestricted self-dual codes the best known upper bound is due to Ward [15] and it also equals $1/6$.

In this paper, we obtain an asymptotic improvement of Theorems 1 and 2.

Theorem 3:

$$\delta \le c_{\min}$$

where $c_{\min} \approx 0.166315$, is the only real root of

$$8x^5 - 24x^4 + 40x^3 - 30x^2 + 10x - 1.$$

To prove it we use a modification of the linear programming method for upper-bounding individual components of the

Manuscript received November 14, 1995; revised January 2, 1997.
I. Krasikov is with the School of Mathematical Sciences, Tel-Aviv University, Ramat-Aviv 69978 Tel-Aviv, Israel, and Beit-Berl College, Kfar-Sava, Israel.
S. Litsyn is with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel.
Publisher Item Identifier S 0018-9448(97)03447-0.

distance distribution of codes under consideration. The proof essentially employs estimates for the range of binomiality of codes, the concept introduced in [6], [7]. Roughly speaking, the binomiality means that in a certain range the components of the distance distribution are upper-bounded by the normalized binomial distribution, the same one as of a randomly chosen code. We used the MATHEMATICA package in computations; not all the transformations are straightforward, so we usually present some intermediate results.

II. Basic Relations

Let C be a doubly-even self-dual code. We start with an elementary proof to the result of Gleason.

Theorem 4: C is symmetric, that is, $B_i = B_{n-i}$, and $n = 0 \pmod 8$.

Proof: From $|C| = 2^{n/2}$ we deduce that the length n is even. Since $P_i(j) = (-1)^j P_{n-i}(j)$ and $B_j = 0$ for $j \neq 0 \pmod 4$, (1) yields that $B_i = B_{n-i}$. Hence, $n = 0 \pmod 4$. Indeed, if $n = 2 \pmod 4$, then $B_n = 0$, contradicting $B_n = B_0$ and $B_0 = 1$. Now

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

for j even, and $P_{n/2}(j) = 0$ otherwise (see, e.g., [4]). Hence, $P_{n/2}(j) > 0$ if $j = 0 \pmod 4$. Therefore, by (1)

$$2^{n/2}B_{n/2} = \sum_{j=0}^{n} B_j P_{n/2}(j) > 0.$$

So, if $n = 4 \pmod 8$ then $B_{n/2} > 0$ along with $n/2 \neq 0 \pmod 4$, a contradiction. □

Remark: The last inequality actually shows that in doubly-even self-dual codes $B_{n/2}$ is the maximal spectral component. To see this just use in (1) the inequality

$$|P_k(i)| \le |P_{n/2}(i)|$$

that is valid for n and i even (see [4, Lemma 1]). Noticing, that $P_{n/2}(j) > 0$ for $j = 0 \pmod 4$, we get

$$2^{n/2}B_i = \sum_{j=0}^{n} B_j P_i(j) \le \sum_{j=0}^{n} B_j P_{n/2}(j) = 2^{n/2}B_{n/2}.$$

Evidently, the same fact is true for the central component of any code dual to a doubly-even code of even length.

Hence, in what follows we assume everywhere that n is a multiple of 8.

Let $f(x)$ be a polynomial

$$f(x) = \sum_{i=0}^{n} A_i P_i(x)$$

then (see e.g., [9])

$$A_i = A_i(f) = 2^{-n}\sum_{j=0}^{n} f(j)P_j(i) \tag{2}$$

in particular

$$A_0(f) = 2^{-n}\sum_{j=0}^{n} f(j)\binom{n}{j}.$$

The following lemma is a special case of a proposition due to Delsarte [3].

Lemma 1: Let $f(x)$ be a polynomial of degree r

$$f(x) = \sum_{i=0}^{r} A_i P_i(x), \qquad 0 \le r \le n$$

then

$$A_0|C| + |C|\sum_{i=d}^{r} A_i B_i = f(0) + f(n) + \sum_{j=d}^{n-d} f(j)B_j. \tag{3}$$

Proof: Calculating $|C|\sum_{i=0}^{r} A_i B_i$, we get the claim from (1). □

Define polynomials

$$\beta_h^n(x,k) = \prod_{i=0}^{k-1}\left((n-2x)^2 - h^2 i^2\right) \tag{4}$$

and

$$\alpha_h^n(x,k) = x(n-x)\beta_h^n(x,k). \tag{5}$$

The zeros of $\beta_h^n(x,k)$ are $\frac{n}{2} \pm \frac{hi}{2}, i = 0, \cdots, k-1$. The polynomials $\alpha_h^n(x,k)$ have two extra zeros, 0 and n. The choice of the polynomials is motivated by the following immediate consequence of (3).

Lemma 2: Let k be odd and $2k+2 < d$. Then

$$2^{n/2}A_0\left(\alpha_8^n(x,k)\right) = 2\sum_{j=d}^{n/2-4k}\alpha_8^n(j,k)B_j. \tag{6}$$

Proof: Degree of $\alpha_8^n(x,k)$ is $2k+2$. So, $A_i(\alpha_8^n(x,k)) = 0$ for $i \ge 2k+3$. Since k is odd and d is divisible by 4, the sum in the left-hand side of (3) vanishes. Furthermore, $\alpha_8^n(x,k) = 0$ at $x = 0, n$ and all $n/2 \pm 4i$ where $i = 0, 1, \cdots, k-1$. The result follows. □

We compute $A_0(\alpha_8^n(x,k))$ using the values of $A_0(\beta_4^n(x,k))$. We start from expanding $\beta_4^n(x,k)$ in the Krawtchouk basis.

Lemma 3:

$$\beta_4^n(x,k) = (2k)!\sum_{i=0}^{k}\frac{n-4i}{n-2k-2i}\binom{n/2-k-i}{k-i}P_{2i}(x).$$

In particular

$$A_0\left(\beta_4^n(x,k)\right) = (2k)!\frac{n}{n-2k}\binom{n/2-k}{k}.$$

Proof: The proof is by induction in k. For $k = 1$ it is checked directly. Put $y = n - 2x$. The following recurrence holds (see, e.g., [9]):

$$y^2 P_i(x) = y(i+1)P_{i+1}(x) + y(n-i+1)P_{i-1}(x).$$

Substituting

$$yP_{i+1}(x) = (i+2)P_{i+2}(x) + (n-i)P_i(x)$$

and

$$yP_{i-1}(x) = iP_i(x) + (n-i+2)P_{i-2}(x)$$

we get

$$y^2P_i(x)=(i+1)(i+2)P_{i+2}(x)+(2ni+n-2i^2)P_i(x)+(n-i+1)(n-i+2)P_{i-2}(x)$$

and (replacing n by $2m$)

$$(y^2-16k^2)P_{2i}(x)=(2i+1)(2i+2)P_{2i+2}(x)+(8mi+2m-8i^2-16k^2)P_{2i}(x)+(2m-2i+1)(2m-2i+2)P_{2i-2}(x).$$

Using this equality by the induction hypothesis after shifting indices in the sums we get

$$\begin{aligned}\beta_4^n(x,k+1)/(2k)! &= (y^2-16k^2)\beta_4^n(x,k)/(2k)!\\ &= \sum_{i=1}^{k+1}\frac{m-2i+2}{m-k-i+1}\binom{m-k-i+1}{k-i+1}\times 2i(2i-1)P_{2i}(x)\\ &\quad+\sum_{i=0}^{k}\frac{m-2i}{m-k-i}\binom{m-k-i}{k-i}\times(8mi+2m-8i^2-16k^2)P_{2i}(x)\\ &\quad+\sum_{i=0}^{k-1}\frac{m-2i-2}{m-k-i-1}\binom{m-k-i-1}{k-i-1}\times(2m-2i-1)(2m-2i)P_{2i}(x).\end{aligned}$$

Routine calculations show that

$$\beta_4^n(x,k+1)/(2k)!=(2k+2)(2k+1)\sum_{i=0}^{k+1}\frac{m-2i}{m-k-i-1}\times\binom{m-k-i-1}{k-i+1}P_{2i}(x)$$

thus proving the claim. □

Now we need several combinatorial identities. The next one is a generalization of the known expression for the derivative of Chebyshev polynomials $\cos(t\arccos z)$ [10, p. 258] to noninteger values of t.

Lemma 4:

$$\left.\frac{d^k\cos(t\arccos z)}{dz^k}\right|_{z=1}=\frac{1}{(2k-1)!!}\prod_{i=0}^{k-1}(t^2-i^2).$$

Proof: The proof is by induction on k. For $k=1$ it is checked directly. Denote $F_t(z)=F_t=\cos(t\ \arccos\ z)$. Observe that $F_t(z)$ satisfies the following differential equation:

$$(1-z^2)\frac{d^2}{dz^2}F_t-z\frac{d}{dz}F_t+t^2F_t=0$$

and is holomorphic at $z=1$. Differentiating this equation k times in z using

$$\frac{d^k}{dz^k}(vu)=\sum_{i=0}^{k}\binom{k}{i}\frac{d^i}{dz^i}v\frac{d^{k-i}}{dz^{k-i}}u$$

we get

$$(1-z^2)\frac{d^{k+2}}{dz^{k+2}}F_t-2kz\frac{d^{k+1}}{dz^{k+1}}F_t-2\binom{k}{2}\frac{d^k}{dz^k}F_t-z\frac{d^{k+1}}{dz^{k+1}}F_t-k\frac{d^k}{dz^k}F_t+t^2\frac{d^k}{dz^k}F_t=0.$$

That is, for $z=1$

$$\left.\frac{d^{k+1}}{dz^{k+1}}F_t\right|_{z=1}=\frac{t^2-k^2}{2k+1}\left.\frac{d^k}{dz^k}F_t\right|_{z=1}.$$

Now the induction hypothesis yields the claim. □

Lemma 5:

$$\begin{aligned}A_0\big(\alpha_h^n(x,k)\big)&=\frac{1}{4}n(n-1)A_0\big(\beta_h^{n-2}(x,k)\big)\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{4}\left.\frac{d^k}{dz^k}\cos^{n-2}\frac{\theta}{h}\right|_{z=1}\end{aligned}$$

where $\theta=\arccos z$.

Proof: Put $s=n-2$.

$$\begin{aligned}&A_0\big(\alpha_h^n(x,k)\big)\\&=2^{-n}\sum_{x=0}^{n}x(n-x)\binom{n}{x}\prod_{i=0}^{k-1}((n-2x)^2-h^2i^2)\\&=\frac{n(n-1)}{2^n}\sum_{x=1}^{n-1}\binom{s}{x-1}\prod_{i=0}^{k-1}((n-2x)^2-h^2i^2)\\&=\frac{n(n-1)}{2^n}\sum_{x=0}^{s}\binom{s}{x}\prod_{i=0}^{k-1}((s-2x)^2-h^2i^2)\\&=\frac{n(n-1)}{4}A_0\big(\beta_h^s(x,k)\big)\\&=\frac{h^{2k}n(n-1)}{2^n}\sum_{x=0}^{s}\binom{s}{x}\prod_{i=0}^{k-1}\left(\left(\frac{s-2x}{h}\right)^2-i^2\right)\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{2^n}\sum_{x=0}^{s}\binom{s}{x}\left.\frac{d^k}{dz^k}\cos\frac{s-2x}{h}\theta\right|_{z=1}\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{2^{n+1}}\frac{d^k}{dz^k}\sum_{x=0}^{s}\binom{s}{x}\\&\quad\times\left.\left(\exp\left(i\frac{s-2x}{h}\theta\right)+\exp\left(-i\frac{s-2x}{h}\theta\right)\right)\right|_{z=1}\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{2^{n+1}}\\&\quad\times\frac{d^k}{dz^k}\left(\exp\left(\frac{is\theta}{h}\right)\left(1+\exp\left(-\frac{2i\theta}{h}\right)\right)^s\right.\\&\quad\left.\left.+\exp\left(-\frac{is\theta}{h}\right)\left(1+\exp\left(\frac{2i\theta}{h}\right)\right)^s\right)\right|_{z=1}\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{2^{n+1}}\frac{d^k}{dz^k}\left.\left(2^{s+1}\cos^s\frac{\theta}{h}\right)\right|_{z=1}\\&=\frac{h^{2k}n(n-1)(2k-1)!!}{4}\frac{d^k}{dz^k}\left.\cos^s\frac{\theta}{h}\right|_{z=1}.\end{aligned}$$ □

Comparing the expressions for $A_0(\beta_4^n(x,k))$ in the two previous lemmas we obtain the following corollary.

Corollary 1: For nonnegative integer ℓ

$$\left.\frac{d^k\cos^\ell\left(\frac{1}{4}\arccos z\right)}{dz^k}\right|_{z=1}=\frac{\ell(k-1)!}{2^{3k+1}}\binom{\frac{\ell}{2}-k-1}{k-1}.$$

Lemma 6:

$$A_0\big(\alpha_8^n(x,k)\big) = n(n-1)(2k-1)!2^{2k-n/2-1} \times \sum_{j=1}^{n/2-1} j\binom{n/2-1}{j}\binom{j/2-k-1}{k-1}.$$

Proof: From the previous lemma

$$\begin{aligned} A_0\big(\alpha_8^n(x,k)\big) &= \frac{8^{2k}n(n-1)(2k-1)!!}{4}\frac{d^k}{dz^k}\cos^{n-2}\frac{\theta}{8}\bigg|_{z=1} \\ &= \frac{8^{2k}n(n-1)(2k-1)!!}{2^{n/2+1}}\frac{d^k}{dz^k}\left(1+\cos\frac{\theta}{4}\right)^{n/2-1}\bigg|_{z=1} \\ &= \frac{8^{2k}n(n-1)(2k-1)!!}{2^{n/2+1}} \times \sum_{j=0}^{n/2-1}\binom{n/2-1}{j}\frac{d^k}{dz^k}\cos^j\frac{\theta}{4}\bigg|_{z=1} \\ &= 2^{6k-n/2-1}n(n-1)(2k-1)!! \times \sum_{j=0}^{n/2-1}\binom{n/2-1}{j}\frac{(k-1)!}{2^{3k+1}}j\binom{j/2-k-1}{k-1} \\ &= 2^{2k-n/2-1}n(n-1)(2k-1)! \times \sum_{j=0}^{n/2-1} j\binom{n/2-1}{j}\binom{j/2-k-1}{k-1}. \qquad \square \end{aligned}$$

Actually, we need only odd k's, so for the sake of simplicity we will formulate all the results below under this assumption. Since our proof of the main theorem consists of several steps and involves a great deal of algebraic manipulations, let us sketch it. First we show that under certain conditions $A_0(x,k) > 0$, and derive an asymptotic expression for it. Using it we obtain from (6) upper bounds on B_j depending on k. Optimization in k allows proving that for $\delta > c_{\min}$ the distance distribution components are upper-bounded by the normalized binomial distribution in the range $[\delta n, (1-\delta)n]$. Substituting these bounds into the right-hand side of (6) for a certain choice of k (maximal possible under the conditions of Lemma 2) we get a contradiction.

III. Bounds on the Distance Distribution

We start with asymptotical evaluation of $A_0(\alpha_8^n(x,k))$. Let $\kappa = k/n$.

Lemma 7: Let k be odd, and assume $0 \le \kappa < \frac{\sqrt{2}}{12}$. Denote

$$S(j) = j\binom{n/2-1}{j}\binom{j/2-k-1}{k-1} \tag{7}$$

and $\eta = j/n$. Then for sufficiently large n the function $|S(\eta n)|$ has two local maxima, one at

$$\eta_1 = \frac{1+8\kappa-\sqrt{1-16\kappa+128\kappa^2}}{8-16\kappa}$$

and another at

$$\eta_2 = \frac{1+8\kappa+\sqrt{1-16\kappa+128\kappa^2}}{8-16\kappa}.$$

The first maximum is the absolute maximum for $\kappa \ge 1/12$, otherwise, the second maximum is the absolute one. For $\kappa = 1/12$ they are asymptotically equal.

Proof: For k odd, $S(j)$ can be negative only for j odd, $j \in J = [2k+3, 4k-3]$. First, we show that in this interval the maximum of $|S(j)|$ is attained at either end of the interval. To see this consider

$$r_j = \frac{|S(j+2)|}{|S(j)|} = \frac{(j/2-k)(n/2-j-1)(n/2-j-2)}{j(j+1)(2k-j/2-1)}.$$

It is enough to show that there is no $j \in J$ such that $r_j > 1$ and $r_{j+2} < 1$. It is valid if

$$\frac{d}{dj}((j/2-k)(n/2-j-1)(n/2-j-2) - j(j+1)(2k-j/2-1)) > 0.$$

The last inequality holds for $\kappa < \frac{\sqrt{2}}{12}$.

Now

$$\sigma(\eta) = \frac{1}{n}\ln|S(j)| = \frac{1}{2}H(2\eta) + \left(\frac{\eta}{2}-\kappa\right)H\left(\frac{2\kappa}{\eta-2\kappa}\right). \tag{8}$$

Differentiating in j we find that there are two maxima stated above, none of them in J. Plugging the η_1 and η_2 into (8) we obtain that the corresponding extremal values are

$$\begin{aligned} \sigma(\eta_1) = (1-5\kappa)\ln 2 + \left(\frac{1}{2}-\kappa\right)\ln(1-2\kappa) - 2\kappa\ln\kappa \\ - \frac{1}{2}\ln(3-16\kappa+\sqrt{1-16\kappa+128\kappa^2}) \\ + \kappa\ln(1-12\kappa+128\kappa^2-256\kappa^3 \\ + \sqrt{1-16\kappa+128\kappa^2}) \end{aligned}$$

and

$$\begin{aligned} \sigma(\eta_2) = (1-5\kappa)\ln 2 + \left(\frac{1}{2}-\kappa\right)\ln(1-2\kappa) - 2\kappa\ln\kappa \\ - \frac{1}{2}\ln(3-16\kappa-\sqrt{1-16\kappa+128\kappa^2}) \\ + \kappa\ln(-1+12\kappa-128\kappa^2+256\kappa^3 \\ + \sqrt{1-16\kappa+128\kappa^2}). \end{aligned}$$

Now

$$\begin{aligned} \sigma(\eta_2)-\sigma(\eta_1) = \left(\frac{3}{2}-3k\right)\ln 2 + \left(\frac{1}{2}-4k\right)\ln(1-8k) \\ + \left(\frac{1}{2}-k\right)\ln(1-2k) - k\ln k \\ - \ln(3-16k-\sqrt{1-16k+128k^2}) \\ + 2k\ln(-1+12k-128k^2+256k^3 \\ + \sqrt{1-16k+128k^2}). \end{aligned}$$

Furthermore

$$\begin{aligned} \frac{d}{d\kappa}(\sigma(\eta_2)-\sigma(\eta_1)) = -3\ln 2 - 4\ln(1-8\kappa) - \ln(1-2\kappa) \\ - \ln\kappa + 2\ln(-1+12\kappa-128\kappa^2 \\ + 256\kappa^3 + \sqrt{1-16\kappa+128\kappa^2}) \end{aligned}$$

and we verify that this derivative is strictly negative in the interval $[0, \sqrt{2}/12]$. For, it is enough to check that

$$\begin{aligned}(-1+12\kappa-128\kappa^2+256\kappa^3+\sqrt{1-16\kappa+128\kappa^2})^2\\ -8(1-8\kappa)^4(1-2\kappa)\kappa\\ =2(-1+12\kappa-128\kappa^2+256\kappa^3)\\ \times(-1+12\kappa-128\kappa^2+256\kappa^3\\ +\sqrt{1-16\kappa+128\kappa^2})<0.\end{aligned}$$

Moreover, for $\kappa = 1/12$ we have $\sigma(\eta_1) = \sigma(\eta_2)$. So, $\sigma(\eta_1) < \sigma(\eta_2)$ for $\kappa < 1/12$. □

Corollary 2: For k odd and $0 \le \kappa \le 1/12$

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\ln A_0(\alpha_8^n(x,k))\\ =\left(\frac{1}{2}-\kappa\right)\ln 2+\left(\frac{1}{2}-\kappa\right)\ln(1-2\kappa)-2\kappa\\ -\frac{1}{2}\ln(3-16\kappa-\sqrt{1-16\kappa+128\kappa^2})\\ +\kappa\ln(-1+12\kappa-128\kappa^2+256\kappa^3\\ +\sqrt{1-16\kappa+128\kappa^2}).\end{aligned} \tag{9}$$

Proof: Estimating the sum in the expression for $A_0(\alpha_8^n(x,k))$ by the maximum term and using the Stirling approximation for the factorial we get the claim. □

Lemma 8:

$$\lim_{n\to\infty}\frac{1}{n}\ln\alpha_8^n(\iota n,\kappa n)=6\kappa\ln 2+2\kappa\ln(2\kappa)-2\kappa+\frac{1-2\iota+8\kappa}{8}H\left(\frac{16\kappa}{1-2\iota+8\kappa}\right). \tag{10}$$

Proof: By Stirling approximation. □

Now we can show that the distance distribution of self-dual doubly-even codes is upper-bounded in a certain range by the corresponding binomial distribution.

Theorem 5: Let $\iota = \frac{i}{n}$, and $\iota \in [c, 1-c]$, where

$$c=\frac{1}{2}-\sqrt{\frac{6\delta-1+\sqrt{1-8\delta+32\delta^2}}{8(1-\delta)}}.$$

Then in this interval

$$\lim_{n\to\infty}\sup\frac{1}{n}\ln B_i\le H(\iota)-\frac{1}{2}.$$

Proof: We will prove the theorem by varying the degree of $\alpha_8^n(x,k)$. If k is odd, $2k+2<d$, and $d \le i \le \frac{n}{2}-4k$, then by Lemma (2)

$$B_i \le 2^{n/2-1}\frac{A_0(\alpha_8^n(x,k))}{\alpha_8^n(i,k)}. \tag{11}$$

Indeed, $\alpha_8^n(i,k) > 0$ for such k's.

Choose

$$\kappa=\frac{(1-2\iota)^2(\iota^2+(1-\iota)^2)}{8(\iota^4+(1-\iota)^4)}.$$

Direct checking shows that for $\iota \in [c_1, 1-c_1]$ we have $\kappa \le \frac{1}{12}$, where c_1 is the smallest real root of the equation

$$20x^4-40x^3+30x^2-10x+1=0$$

$c_1 \approx 0.16563\ldots$. Since $c(\delta)$ is decreasing in δ, the minimum $c_{\min}$ of $c(\delta)$ under the condition $c(\delta) \ge \delta$ is determined by the equation $c(\delta)=\delta$ and thus is the only real root of the equation

$$8x^5-24x^4+40x^3-30x^2+10x-1=0.$$

Notice that for $\delta_{\min} = c_{\min}$ we have $2\kappa(\delta_{\min}) = \delta_{\min}$ since the equation $c(\delta)=\delta$ is equivalent to $2\kappa(\delta)=\delta$. Numerically, $c_{\min} = 0.166315\ldots$. Hence, $c_1 < c_{\min}$, and $\kappa < 1/12$.

Furthermore, since the κ chosen is decreasing in ι, to validate the condition $2k+2<d$ we need $2\kappa < \iota$ in the interval $[c, 1-c]$. The four roots of the equation $2\kappa = \iota$, are

$$\frac{1}{2}\pm\sqrt{\frac{6\delta-1\pm\sqrt{1-8\delta+32\delta^2}}{8(1-\delta)}}.$$

The following two

$$c_{1,2}=\frac{1}{2}\pm\sqrt{\frac{6\delta-1+\sqrt{1-8\delta+32\delta^2}}{8(1-\delta)}}$$

are real, and $c_1+c_2=1$. Therefore, for c being the smaller one we conclude that $2\kappa < \delta$ whenever $i \in [c, 1-c]$.

Now, using (11) and (10) and for the κ chosen we obtain the claim from the previous corollary. □

Theorem 6: Let $c_{\min}$ be the only real root of

$$8x^5-24x^4+40x^3-30x^2+10x-1.$$

If there exists a doubly-even self-dual code with $\delta \ge c_{\min} \approx 0.166315$, then all its spectrum is asymptotically upper-bounded by the corresponding normalized binomial distribution.

Proof: It can be checked directly that under the condition of the corollary c, defined in the previous theorem, is less than δ. □

IV. Proof of the Main Theorem

By Theorem 1 we can assume that $c_{\min} < \delta \le 1/6$. Choose in Lemma 2 the largest possible odd $k=(d-6)/2$. That is, $\kappa=\delta/2$. We have for the left-hand side of (6), by (9)

$$\begin{aligned}L=\lim_{n\to\infty}\sup\frac{1}{n}\ln\left(2^{n/2}A_0(\alpha_8^n(x,(d+2)/2))\right)\\ =-\delta+\left(1-\frac{\delta}{2}\right)\ln 2+\frac{1-\delta}{2}\ln(1-\delta)\\ -\frac{1}{2}\ln(3-8\delta-\sqrt{1-8\delta+32\delta^2})\\ +\frac{\delta}{2}\ln(-1+6\delta-32\delta^2+32\delta^3+\sqrt{1-8\delta+32\delta^2}).\end{aligned}$$

Now, by Theorem 6, to upper-bound the right-hand side of (6) we can substitute the upper binomial estimates of B_j's. This gives by virtue of (10)

$$\begin{aligned}R=\lim_{n\to\infty}\sup\frac{2}{n}\sum_{j=d}^{n/2-2d-4}\alpha_8^n(j,(d+2)/2))B_j\\ \le\max_{\eta\in[\delta,1/2-2\delta]}u(\eta)\end{aligned}$$

where

$$u(\eta) = 3\delta \ln 2 + \delta \ln \delta - 2\delta + \frac{1-2\eta+4\delta}{8} H\left(\frac{8\delta}{1-2\eta+4\delta}\right) + H(\eta) - \frac{1}{2}.$$

So, the inequality $L - R \le 0$ should hold. In what follows, we will show that for $\delta \in (c_{\min}, 1/6]$ this is not true, and thus such a code does not exist.

First we show that

$$\max_{\eta \in [\delta, 1/2-2\delta]} u(\eta) = u(\delta).$$

By differentiation, we obtain

$$u' = \frac{du(\eta)}{d\eta} = \frac{1}{4} \ln \frac{1-4\delta-2\eta}{1+4\delta-2\eta} + \ln \frac{1-\eta}{\eta}.$$

Observe that $u' < 0$ for $\delta > c_{\min}$. Indeed, this is equivalent to

$$\delta > \frac{1-6\eta+4\eta^2-16\eta^3+8\eta^4}{4(\eta^4+(1-\eta)^4)}.$$

The right-hand side of this inequality is a decreasing function in η, so we check it for $\eta = \delta$. The inequality holds precisely for $\delta > c_{\min}$. Hence

$$\begin{aligned} R &\le u(\delta) \\ &\le \left(3\delta - \frac{1}{2}\right) \ln 2 + \delta(\ln \delta - 1) \\ &\quad + \frac{1+2\delta}{8} H\left(\frac{8\delta}{1+2\delta}\right) + H(\delta) \end{aligned}$$

and

$$\begin{aligned} L - R = (&12 \ln 2 - 4\delta \ln 2 + \ln(1-6\delta) - 6\delta \ln(1-6\delta) \\ &+ 12 \ln(1-\delta) - 12\delta \ln(1-\delta) + 8\delta \ln \delta \\ &- \ln(1+2\delta) - 2\delta \ln(1+2\delta) \\ &- 4 \ln(3 - 8\delta - \sqrt{1-8\delta+32\delta^2}) \\ &+ 4\delta \ln(1 - 6\delta + 32\delta^2 \\ &- 32\delta^3 - \sqrt{1-8\delta+32\delta^2}))/8 \end{aligned}$$

$$\begin{aligned} \frac{d}{d\delta}(L-R) = (&-2\ln 2 - 3\ln(1-6\delta) - 6\ln(1-\delta) + 4\ln\delta \\ &- \ln(1+2\delta) + 2\ln(-1+6\delta-32\delta^2+32\delta^3 \\ &+ \sqrt{1-8\delta+32\delta^2}))/4. \end{aligned}$$

One can check that $c_{\min}$ is a root of $\frac{d}{d\delta}(L-R)$. This is equivalent to $c_{\min}$ being a root of

$$(-1+6\delta-32\delta^2+32\delta^3+\sqrt{1-8\delta+32\delta^2})^2\delta^4 - 4(1-6\delta)^3(1-\delta)^6(1+2\delta) = 0.$$

The equation can be transformed into

$$\begin{aligned} &16(1-\delta)^2(1-10\delta+30\delta^2-40\delta^3+24\delta^4-8\delta^5) \\ &\times (1-32\delta+415\delta^2+2714\delta^3 \\ &- 85515\delta^4 + 40452\delta^5 + 524448\delta^6 - 143768\delta^7 \\ &+ 91456\delta^8 + 208576\delta^9 - 492328\delta^{10} \\ &+ 466816\delta^{11} - 238048\delta^{12} + 59168\delta^{13}) = 0 \end{aligned}$$

giving the result.

Moreover, as it is easy to check, for $\delta \le 1/6$, that

$$\begin{aligned} &\frac{d^2}{d\delta^2}(L-R) \\ &= (12\ln 2 + \ln(1-6\delta) + 12\ln(1-\delta) - \ln(1+2\delta) \\ &\quad - 4\ln(3-8\delta-\sqrt{1-8\delta+32\delta^2}))/8 > 0. \end{aligned}$$

Thus $c_{\min}$ is the only root of $\frac{d}{d\delta}(L-R)$ in the interval under consideration. It remains to prove that $L - R = 0$ for $\delta = c_{\min}$. Indeed, consider the function

$$\begin{aligned} \rho(\delta) &= (L-R) - \delta \frac{d}{d\delta}(L-R) \\ &= (12\ln 2 + \ln(1-6\delta) + 12\ln(1-\delta) - \ln(1+2\delta) \\ &\quad - 4\ln(3-8\delta-\sqrt{1-8\delta+32\delta^2}))/8. \end{aligned}$$

Now, $\rho(\delta) = 0$ is equivalent to

$$2^{12}(1-6\delta)(1-\delta)^{12} - (1+2\delta)(3-8\delta-\sqrt{1-8\delta+32\delta^2})^4 = 0$$

or, getting rid of the square root

$$\begin{aligned} &64(1-\delta)^4(1-10\delta+30\delta^2-40\delta^3+24\delta^4-8\delta^5) \\ &\times (3825 - 86370\delta + 862866\delta^2 - 5181544\delta^3 \\ &+ 21170188\delta^4 - 62816720\delta^5 + 140812600\delta^6 \\ &- 244608448\delta^7 + 334412032\delta^8 - 362393120\delta^9 \\ &+ 311228224\delta^{10} - 210349056\delta^{11} + 110332288\delta^{12} \\ &- 43912192\delta^{13} + 12798976\delta^{14} - 2574848\delta^{15} \\ &+ 319488\delta^{16} - 18432\delta^{17}) = 0 \end{aligned}$$

proving the claim.

Hence, finally, $L - R > 0$ for $\delta \in (c_{\min}, 1/6]$, a contradiction. □

APPENDIX

Here we sketch a proof of Theorem 1. In contrast to the original proof we use only properties of the MacWilliams transform.

The following auxiliary lemma is used.

Lemma 9: If $A_0(\alpha_8^n(x,k)) \neq 0$, for some k, then $d \le \max\{2k+2, \frac{n}{2} - 4k\}$.

Proof: Note that $\alpha_8^n(x,k) = 0$ at $x = 0, n$, and all $n/2 \pm 4i$, where $i = 0, 1, \cdots, k-1$. Assume that for k chosen $A_0(\alpha_8^n(x,k)) \neq 0$. Plugging $\alpha_8^n(x,k)$ into (3), we get that either

i) $\sum_{j=d}^{n-d} \alpha_8^n(j,k) B_j = 2 \sum_{j=d}^{n/2-4k} \alpha_8^n(j,k) B_j \neq 0$

or

ii) $\sum_{i=d}^{2k+2} A_i B_i \neq 0.$

If i) holds, then $n/2 - 4k \ge d$. If ii) is true, then $2k+2 \ge d$. □

Now we are ready to prove Theorem 1.

Proof: We consider three cases, depending on n modulo 24. In all these cases we prove that $A_0(\alpha_8^n(x,k)) > 0$. Namely, referring to Lemma 9

if $n = 0 \pmod{24}$ we choose $k = n/12 + 1$, giving $d \le \frac{n}{6} + 4$;
if $n = 8 \pmod{24}$ we choose $k = (n+4)/12$, giving $d \le \frac{n+16}{6}$;
if $n = 16 \pmod{24}$ we choose $k = (n-4)/12$, giving $d \le \frac{n+8}{6}$.

Observe, that all the chosen k's are odd. Then using the same arguments as in the proof of Lemma 7 we demonstrate that in the expression for $A_0(\alpha_8^n(x,k))$ there is a positive dominating summand. To prove this for all n use the Stirling approximation

$$\frac{1}{2}\log\frac{\pi}{4} - \frac{1}{2}\log\frac{2\pi i(n-i)}{n} + nH\left(\frac{i}{n}\right) < \log\binom{n}{i} < -\frac{1}{2}\log\frac{2\pi i(n-i)}{n} + nH\left(\frac{i}{n}\right).$$

It proves the claim for $n > 100$. The small cases (there are only 12 such lengths) are checked directly. □

Acknowledgment

The authors wish to thank V. Levenshtein, P. Solé, and the anonymous referees for useful comments and suggestions.

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. Berlin, Germany: Springer-Verlag, 1988.

[2] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimum distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, Nov. 1990.

[3] P. Delsarte, *An Algebraic Approach to the Association Schemes of Coding Theory* (Philips Res. Rep. Suppl.), no. 10, 1973.

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

[5] ——, "On integral zeros of Krawtchouk polynomials," *J. Comb. Theory (Ser. A)*, vol. 74, no. 1, pp. 71–99, 1996.

[6] ——, "Bounds on spectra of codes with known dual distance," *Des., Codes Cryptogr.*, to be published.

[7] ——, "Estimates for the range of binomiality in codes' spectra," *IEEE Trans. Inform. Theory*, vol. 43, pp. 987–991, May 1997.

[8] V. I. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1303–1321, Sept. 1995.

[9] J. H. van Lint, *Introduction to Coding Theory*. Berlin, Germany: Springer-Verlag, 1992.

[10] W. Magnus, F. Oberhettinger, and R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, 3rd ed. New York/Berlin: Springer-Verlag, 1966.

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

[12] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Inform. Contr.*, vol. 22, pp. 188–200, 1973.

[13] C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, "Upper bounds for modular forms, lattices, and codes," *J. Alg.*, vol. 36, pp. 68–76, 1975.

[14] V. Pless, *Introduction to the Theory of Error-Correcting Codes*. New York: Wiley, 1982.

[15] H. N. Ward, "A bound for divisible codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 191–194, Jan. 1992.