Bounds for weight distribution of weakly self–dual codes*

Vwani P. Roychowdhury† and Farrokh Vatan‡

January 16, 2014

Abstract

Upper bounds are given for the weight distribution of binary weakly self–dual codes. To get these new bounds, we introduce a novel method of utilizing unitary operations on Hilbert spaces. This method is motivated by recent progress on quantum computing. This new approach leads to much simpler proofs for such genre of bounds on the weight distributions of certain classes of codes. Moreover, in some cases, our bounds are improvements on the earlier bounds. These improvements are achieved, either by extending the range of the weights over which the bounds apply, or by extending the class of codes subjected to these bounds.

Keywords: Weight distribution, Self–dual code, Hilbert space, Unitary operation.

1 Background

For a random linear $[n, k]$ code $\mathcal{C}$ with weight distribution $(A_0, A_1, \ldots, A_n)$ it is known that the expected value of the normalized weight distribution, i.e., $\frac{1}{2^k}A_w$, is the same as the normalized binomial distribution $\frac{1}{2^n}\binom{n}{w}$ (see, e.g., [14, p. 287]). So for such a code the expected value for the number of codewords of weight w is $\frac{1}{2^{(n-k)}}\binom{n}{w}$. The problem to determine which explicit classes of codes have binomial weight distribution has been investigated in several papers (see references). Most of these results are about the BCH codes, their extensions, or their dual codes. For example, it is shown that for these codes the number of codewords of weight w is

$$A_w = \frac{1}{2^{n-k}}\left(\binom{n}{w} + E_w\right),$$

*This work was supported in part by grants from the Revolutionary Computing group at JPL (contract #961360), and from the DARPA Ultra program (subcontract from Purdue University #530–1415–01).

†V. Roychowdhury is with the Electrical Engineering Department, UCLA, Los Angeles, CA 90095 (e-mail: vwani@ee.ucla.edu).

‡F. Vatan is with the Electrical Engineering Department, UCLA, Los Angeles, CA 90095 (e-mail: vatan@ee.ucla.edu).

for w in some range, and the error term E_w tends to zero when n tends to infinity.

There are also bounds for other classes of liner codes. Let $\mathcal{C}$ be a doubly–even self–dual $[n, n/2, d]$ code $\mathcal{C}$ with weight distribution $(A_0, A_1, \ldots, A_n)$. Let $\delta = \frac{d}{n}$, then in [11] it is shown that

$$A_w \leq 2^{\left(H_2(\frac{w}{n})-\frac{1}{2}\right)n}, \tag{1}$$

if $\frac{w}{n} \in [c, 1-c]$, where

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

This shows that for this class of codes, the weight distribution around $\frac{n}{2}$ is upper–bounded by the binomial distribution.

In [12] an upper bound for weight distribution of the *dual* of extended BCH codes is given. Let $\mathcal{C}$ of length $n = 2^m$ be the dual of the extended code of a t–error correcting BCH code. Then $\dim(\mathcal{C}) \leq mt$; i.e., $|\mathcal{C}| \leq n^t$. If $(A_0, A_1, \ldots, A_n)$ is the weight distribution of $\mathcal{C}$, then for $w > \sqrt{\frac{n}{t+1}} + 2$ we have

$$A_w \leq \frac{4\sqrt{2\pi n} n^t}{|2\sqrt{n(t+1)}-n+2w|} \cdot e^{-\frac{(n-2w)^2}{n}} \left(1 + O\left(\frac{1}{t}\right)\right). \tag{3}$$

In [18] several bounds for the weight distribution of subfield subcodes of algebraic–geometric codes is given. This class of codes contains important classes of codes, such as the binary BCH and Goppa codes. For an $[n, k]$ binary code of this type, with weight distribution $(A_0, A_1, \ldots, A_n)$, they derived the following bound

$$\left| A_w - \frac{1}{2^{n-k}} \binom{n}{w} \right| < c_1 n^{\frac{w}{2}}, \tag{4}$$

and for the special case of $w = \frac{n}{2}$, they get the following bound

$$\left| A_{\frac{n}{2}} - \frac{1}{2^{n-k}} \binom{n}{\frac{n}{2}} \right| < c_2 \binom{n}{\frac{n}{2}}^{\frac{1}{2}} n^{\frac{1}{4}}. \tag{5}$$

Here c_1 and c_2 are two constants, both much larger than $\sqrt{e}$.

In this paper, *we apply a novel approach based on unitary operations on Hilbert spaces*, and *derive bounds for the weight distribution of another class of linear codes*. In particular, we study the class of weakly self–dual codes, i.e., the class of codes $\mathcal{C}$ such that $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. We show that, for $0 < w < \frac{n}{2}$, the number A_w of codewords of weight w in $\mathcal{C}$ satisfies the following bounds

$$A_w \leq 2^{\frac{1}{2}H_2(\frac{w}{n})n}, \tag{6}$$

and

$$A_w \leq \sqrt{e}(n-w+1)^{\frac{w}{2}}. \tag{7}$$

If we compare our bounds with previously known bounds (1), (3), and (4), we realize that these new bounds, for some values of w and in the intersection of their corresponding classes of codes, give a better estimate than the old bounds. For example, (6) holds for any value of w, $0 < w < \frac{n}{2}$, and it applies also to the special case of doubly–even self–dual codes, and, hence, comparable to the bounds in [11]. The bound in (1) applies to doubly–even self–dual codes, but holds only in the interval $[c, 1-c]$, with c defined by (2). So if $\frac{d}{n} \leq {H_2}^{-1}(\frac{1}{2}) = 0.1100\cdots$ then $c > 0.27$. Hence, for this choice of $\frac{d}{n}$, (6) is a better bound than (1) for $\frac{w}{n} < 0.27$, since (1) does not even hold for these values of w; we should note, however, that (1) is a better bound if $\frac{w}{n} > 0.27$. One can also verify that (7) gives a better bound than (4), as the constant c_1 is much larger than $\sqrt{e}$.

2 Unitary operations on Hilbert spaces

We derive our bounds via actions of unitary operations on Hilbert spaces. Toward this end, we find it more comfortable to use the language of "bra–ket" of quantum mechanics (see, e.g., [3]) as it is used in the theory of quantum computation (see, e.g., [15] and [1]). We briefly describe the necessary notions and notations.

Consider the two–dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$. We denote its standard basis by $\{|0\rangle, |1\rangle\}$; i.e., $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$. We consider also the tensor product

$$\mathcal{H}^{\otimes n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$$

of n copies of $\mathbb{C}^2$. So $\mathcal{H}^{\otimes n}$ is a 2^n–dimensional Hilbert space isomorphic with $\mathbb{C}^{2^n}$. We represent the standard basis of $\mathcal{H}^{\otimes n}$ by 2^n products of the form

$$|c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle,$$

where $c_i \in \{0,1\}$. For simplicity, we write $|c_1 c_2 \cdots c_n\rangle$ instead of $|c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle$. The Euclidean length on $\mathcal{H}^{\otimes n}$ is defined in the natural way; we denote the length of the vector $|a\rangle \in \mathcal{H}^{\otimes n}$ by $\| |a\rangle \|$. For example, $\mathcal{H}^{\otimes 2} = \mathbb{C}^2 \otimes \mathbb{C}^2$ is a 4–dimensional Hilbert space with

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

as its standard basis. If

$$|a\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \in \mathcal{H}^{\otimes 2}$$

then $\| |a\rangle \| = (aa^* + bb^* + cc^* + dd^*)^{\frac{1}{2}}$, where * stands for the complex conjugate.

An $m \times m$ matrix M is *unitary* if $M^\dagger \cdot M = I_m$, where I_m is the identity matrix and $M^\dagger$ is the *adjoint* matrix of M; i.e., $M^\dagger = \left(M^{\mathrm{tr}}\right)^*$, where "tr" denotes the transpose. A linear operation on the m–dimensional Hilbert space $\mathbb{C}^m$ is called a *unitary operation* if it is represented by a unitary matrix. Note that every unitary operation is a *length–preserving* operation.

We denote the group of $m \times m$ unitary matrices by $\mathbf{U}(m)$. The general form of a matrix in $\mathbf{U}(2)$ is

$$\begin{pmatrix} e^{i(\alpha+\gamma)}\cos\theta & e^{i(\beta+\gamma)}\sin\theta \\ -e^{-i(\beta-\gamma)}\sin\theta & e^{-i(\alpha-\gamma)}\cos\theta \end{pmatrix}.$$

Suppose that $U_1, U_2 \in \mathbf{U}(2)$, then the tensor product $U_1 \otimes U_2$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is defined in the natural way. For example, if $U_1(|0\rangle) = a\,|0\rangle + b\,|1\rangle$ and $U_2(|1\rangle) = c\,|0\rangle + d\,|1\rangle$ then

$$\begin{aligned} U_1 \otimes U_2(|01\rangle) &= U_1(|0\rangle) \otimes U_2(|1\rangle) \\ &= (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) \\ &= ac\,|00\rangle + ad\,|01\rangle + bc\,|01\rangle + bd\,|11\rangle\,. \end{aligned}$$

3 Bounds for weights

For any real number θ, consider the unitary operation $R_\theta \in \mathbf{U}(2)$ defined by the following matrix

$$R_\theta = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix}.$$

Then the action of R_θ on a vector $|c\rangle$, $c \in \{0,1\}$, can be written as follows:

$$R_\theta(|c\rangle) = \sum_{a\in\{0,1\}} (-1)^{ac} (\sin\theta)^{1-c-a+2ac} (\cos\theta)^{c+a-2ac}\,|a\rangle\,.$$

Now let $\boldsymbol{S}_\theta = {R_\theta}^{\otimes n}$, i.e., the tensor product of n copies of R_θ. Thus $\boldsymbol{S}_\theta \in \mathbf{U}(2^n)$. The following lemma provides a closed form for the action of $\boldsymbol{S}_\theta$.

Lemma 3.1 *For any vector $|\boldsymbol{c}\rangle$ in the standard basis, i.e., $\boldsymbol{c} \in \{0,1\}^n$, we have*

$$\boldsymbol{S}_\theta(|\boldsymbol{c}\rangle) = \sum_{\boldsymbol{a}\in\{0,1\}^n} (-1)^{\boldsymbol{c}\cdot\boldsymbol{a}} (\sin\theta)^{n-\mathrm{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathrm{wt}(\boldsymbol{c}+\boldsymbol{a})}\,|\boldsymbol{a}\rangle\,, \tag{8}$$

where $\boldsymbol{c}\cdot\boldsymbol{a}$ is the inner product of $\boldsymbol{c}$ and $\boldsymbol{a}$ as real vectors, $\mathrm{wt}(\boldsymbol{x})$ denotes the Hamming weight of a binary vector $\boldsymbol{x}$, and the addition of binary vectors is considered over GF(2).

Proof. We first show that

$$\boldsymbol{S}_\theta(|\boldsymbol{c}\rangle) = \sum_{\boldsymbol{a}\in\{0,1\}^n} (-1)^{\boldsymbol{c}\cdot\boldsymbol{a}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c})-\mathsf{wt}(\boldsymbol{a})+2\boldsymbol{c}\cdot\boldsymbol{a}} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c})+\mathsf{wt}(\boldsymbol{a})-2\boldsymbol{c}\cdot\boldsymbol{a}} |\boldsymbol{a}\rangle\,, \tag{9}$$

We prove the identity (9) only for $n = 2$; the proof in the general case is quite similar. Let $\boldsymbol{c} = (c_1, c_2)$ and $\boldsymbol{a} = (a_1, a_2)$.

$$\begin{aligned}
\boldsymbol{S}_\theta(|\boldsymbol{c}\rangle) &= R_\theta(|c_1\rangle) \otimes R_\theta(|c_2\rangle) \\
&= \Big(\sum_{a_1\in\{0,1\}} (-1)^{a_1c_1} (\sin\theta)^{1-c_1-a_1+2a_1c_1} (\cos\theta)^{c_1+a_1-2a_1c_1} |a_1\rangle \Big) \otimes \\
&\quad \Big(\sum_{a_2\in\{0,1\}} (-1)^{a_2c_2} (\sin\theta)^{1-c_2-a_2+2a_2c_2} (\cos\theta)^{c_2+a_2-2a_2c_2} |a_2\rangle \Big) \\
&= \sum_{a_1,a_2\in\{0,1\}} (-1)^{a_1c_1+a_2c_2} (\sin\theta)^{2-(c_1+c_2)-(a_1+a_2)+2(a_1c_1+a_2c_2)} \\
&\quad (\cos\theta)^{(c_1+c_2)+(a_1+a_2)-2(a_1c_1+a_2c_2)} |a_1a_2\rangle\,,
\end{aligned}$$

which is the of form of (9). We note that

$$\mathsf{wt}(\boldsymbol{c}) + \mathsf{wt}(\boldsymbol{a}) - 2\boldsymbol{c}\cdot\boldsymbol{a} = \mathsf{wt}(\boldsymbol{c}+\boldsymbol{a}).$$

Therefore, (9) can be rewritten as (8). ∎

Now we consider a linear code $\mathcal{C} \subseteq \{0,1\}^n$ of dimension k, and the corresponding *unit* vector

$$|\mathcal{C}\rangle = \frac{1}{\sqrt{2^k}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}\rangle\,.$$

By applying the unitary operation $\boldsymbol{S}_\theta$ on the unit vector $|\mathcal{C}\rangle$ we get

$$\boldsymbol{S}_\theta(|\mathcal{C}\rangle) = \frac{1}{\sqrt{2^k}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{a}\in\{0,1\}^n} (-1)^{\boldsymbol{c}\cdot\boldsymbol{a}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} |\boldsymbol{a}\rangle\,.$$

This can be rewritten as follows

$$\boldsymbol{S}_\theta(|\mathcal{C}\rangle) = \frac{1}{\sqrt{2^k}} \sum_{\boldsymbol{a}\in\mathcal{C}^\perp} \left(\sum_{\boldsymbol{c}\in\mathcal{C}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} \right) |\boldsymbol{a}\rangle + |\mathrm{remainder}\rangle\,.$$

Since $\|\boldsymbol{S}_\theta(|\mathcal{C}\rangle)\| = 1$, the following lemma follows.

Lemma 3.2 *For any k–dimensional linear code $\mathcal{C}$ of length n, and any real number θ we have*

$$\frac{1}{2^k} \sum_{\boldsymbol{a}\in\mathcal{C}^\perp} \left(\sum_{\boldsymbol{c}\in\mathcal{C}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} \right)^2 \leq 1. \tag{10}$$

Lemma 3.3 *For any k–dimensional weakly self–dual linear code $\mathcal{C}$ of length n, i.e., $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, and any real number θ we have*

$$\left| \sum_{\boldsymbol{c} \in \mathcal{C}^{\perp}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c})} \right| \leq 2^{(n-2k)/2}. \tag{11}$$

Proof. We apply Lemma III.2 to the code $\mathcal{C}^{\perp}$. The result is

$$\frac{1}{2^{n-k}} \sum_{\boldsymbol{a} \in \mathcal{C}} \left(\sum_{\boldsymbol{c} \in \mathcal{C}^{\perp}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} \right)^2 \leq 1.$$

Since $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, for every $\boldsymbol{a} \in \mathcal{C}$ we have

$$\sum_{\boldsymbol{c} \in \mathcal{C}^{\perp}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c}+\boldsymbol{a})} = \sum_{\boldsymbol{c} \in \mathcal{C}^{\perp}} (\sin\theta)^{n-\mathsf{wt}(\boldsymbol{c})} (\cos\theta)^{\mathsf{wt}(\boldsymbol{c})},$$

and the lemma follows. ∎

Lemma 3.4 *Let $\mathcal{C}$ be a weakly self–dual code with weight distribution $(A_0, A_1, \ldots, A_n)$. Then for any $0 < \lambda < 1$ we have*

$$\sum_{j=0}^{n/2} A_{2j} \lambda^j \leq (1+\lambda)^{n/2}, \qquad 0 < \lambda < 1. \tag{12}$$

Proof. We first apply the following form of the MacWilliams identity (see [14]) to get a handier form of inequality (11):

$$\sum_{\boldsymbol{u} \in \mathcal{C}^{\perp}} x^{n-\mathsf{wt}(\boldsymbol{u})} y^{\mathsf{wt}(\boldsymbol{u})} = \frac{1}{|\mathcal{C}|} \sum_{\boldsymbol{u} \in \mathcal{C}} (x+y)^{n-\mathsf{wt}(\boldsymbol{u})} (x-y)^{\mathsf{wt}(\boldsymbol{u})}.$$

This way, from (11), we obtain the following inequality:

$$\left| \sum_{\boldsymbol{c} \in \mathcal{C}} (\sin\theta + \cos\theta)^{n-\mathsf{wt}(\boldsymbol{c})} (\sin\theta - \cos\theta)^{\mathsf{wt}(\boldsymbol{c})} \right| \leq 2^{n/2}. \tag{13}$$

Now suppose that $\frac{\pi}{4} < \theta < \frac{\pi}{2}$, $\sqrt{u} = \sin\theta + \cos\theta$, and $\sqrt{v} = \sin\theta - \cos\theta$. Thus $1 < u < 2$ and $v = 2 - u$. Then inequality (13) can be written as

$$\sum_{\boldsymbol{c} \in \mathcal{C}} \sqrt{u}^{\,n-\mathsf{wt}(\boldsymbol{c})} \sqrt{2-u}^{\,\mathsf{wt}(\boldsymbol{c})} \leq 2^{n/2}. \tag{14}$$

Since $\mathcal{C}$ is weakly self–dual then $A_j = 0$, for every odd index j. Therefore, (14) can be written as follows (assume n is even):

$$\sum_{j=0}^{n/2} A_{2j} u^{\frac{n}{2}-j} (2-u)^j \leq 2^{n/2}, \qquad 1 < u < 2. \tag{15}$$

Let $\frac{2-u}{u} = \lambda$, then $0 < \lambda < 1$ and (15) became

$$\sum_{j=0}^{n/2} A_{2j} \lambda^j \leq (1+\lambda)^{n/2}. \blacksquare$$

Theorem 3.5 *For every weakly self–dual code $\mathcal{C}$ with weight distribution $(A_0, A_1, \ldots, A_n)$ we have*

$$A_w \leq 2^{\frac{1}{2}H_2(\frac{w}{n})n}, \qquad 0 < w < \frac{n}{2}. \tag{16}$$

and

$$A_w \leq \sqrt{e}(n-w+1)^{w/2}, \qquad 0 < w < \frac{n}{2}. \tag{17}$$

Proof. For $0 < w < \frac{n}{2}$, let $\alpha = \frac{w}{n}$ and $A_w = 2^{\beta n}$. From (12) it follows

$$2^{\beta n} \lambda^{\frac{w}{2}} \leq (1+\lambda)^{\frac{n}{2}}.$$

Therefore,

$$\beta \leq -\frac{1}{2}\alpha \log_2 \lambda + \frac{1}{2}\log_2(1+\lambda), \qquad 0 < \lambda < 1. \tag{18}$$

For fixed $0 < \alpha < \frac{1}{2}$, let

$$F(\lambda) = -\frac{1}{2}\alpha \log_2 \lambda + \frac{1}{2}\log_2(1+\lambda).$$

A simple calculation shows that, on the interval $0 < \lambda < 1$, the minimum of $F(\lambda)$ is achieved for $\lambda = \frac{\alpha}{1-\alpha}$. Thus, for $0 < \alpha < \frac{1}{2}$,

$$\beta \leq \frac{1}{2}\left(-\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)\right) = \frac{1}{2}H_2(\alpha).$$

Therefore, we have proved (16).

On the other hand, from (12) we have

$$A_w \leq \left(1+\frac{1}{\lambda}\right)^{w/2} (1+\lambda)^{(n-w)/2}.$$

Let $\lambda = \frac{1}{n-w}$, and note that $\left(1+\frac{1}{t}\right)^t \leq e$. This proves (17). $\blacksquare$

References

[1] L. M. Adleman, J. Demarrais, and M. D. A. Huang, "Quantum computability," *SIAM Journal on Computing*, vol. 26, pp. 1524–1540, October 1997.

[2] T. Beth, D. E. Lazic, and V. Senk, "A family of binary codes with asymptotically good distance distribution," in *EUROCODE '90*, Heidelberg, Germany, 1990, pp. 30–41, Springer–Verlag.

[3] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Quantum Mechanics*, vol. I, John Wiley & Sons, New York, 1977, Translation of *Mécanique Quantique*, Hermann, Paris, 1973.

[4] G. Kalai and N. Linial, "On the distance distribution of codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1467–1472, September 1995.

[5] H. Kalouti, D. E. Lazic, and T. Beth, "On the relation between distance distribution of binary block codes and the binomial distribution," *Annales des Télécommun*, vol. 50, pp. 762–778, 1995.

[6] T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight distribution of binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT–31, pp. 769–780, November 1985.

[7] O. Keren and S. Litsyn, "More on the distance distribution of BCH codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 251–255, January 1999.

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

[9] I. Krasikov and S. Litsyn, "On accuracy of binomial approximation to the distance distribution of codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1472–1474, September 1995.

[10] I. Krasikov and S. Litsyn, "Estimates for the range of binomiality in codes' spectra," *IEEE Trans. Inform. Theory*, vol. 43, pp. 987–991, May 1997.

[11] I. Krasikov and S. Litsyn, "Linear programming bounds for doubly–even self–dual codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1238–1244, July 1997.

[12] I. Krasikov and S. Litsyn, "On the distance distribution of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 247–250, January 1999.

[13] D. E. Lazic, H. Kalouti, and T. Beth, "Spectra of long primitive binary BCH codes cannot approach the binomial distribution," *IEEE Trans. Inform. Theory*, vol. 44, pp. 294–295, January 1998.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North Holland, Amsterdam, The Netherlands, 1983.

[15] P. W. Shor, "Polynomial–time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, October 1997.

[16] V. M. Sidel'nikov, "Weight spectrum of binary Bose–Chaudhuri–Hoquinghem codes," *Problemy Peredachi Informatsii*, vol. 7, no. 1, pp. 14–22, 1971, English translation: *Problems of Information Transmission*, vol. 7, no. 1, pp. 11–17, 1971.

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

[18] S. G. Vladuts and A. N. Skorobogatov, "Weight distributions of subfield subcodes of algebraic–geometric codes," *Problemy Peredachi Informatsii*, vol. 27, no. 1, pp. 24–36, 1991, English translation: *Problems of Information Transmission*, vol. 27, no. 1, pp. 19–29, 1991.