Upper Bounds on the Size of Quantum Codes

Alexei Ashikhmin
Los Alamos National Laboratory
Group CIC-3, Mail Stop P990
Los Alamos, NM 87545
e-mail: alexei@c3serve.c3.lanl.gov

Simon Litsyn
Department of Electrical Engineering-Systems
Tel Aviv University
Tel Aviv 69978, Israel
e-mail: litsyn@eng.tau.ac.il

Abstract

The paper is concerned with bounds for quantum error correcting codes. Using the quantum MacWilliams identities, we generalize the linear programming approach from classical coding theory to the quantum case. Using this approach, we obtain Singleton type, Hamming type, and the first linear programming type bounds for quantum codes. Using the special structure of linear quantum codes, we derive an upper bound that is better than both Hamming and the first linear programming bounds on some subinterval of rates.

Index Terms — Quantum codes, upper bounds, linear programming

1 Introduction

Recently Shor presented a polynomial time algorithm for factoring large numbers on a quantum computer [24]. Following this the interest in quantum computations grew dramatically. A crucial problem in implementation of quantum computer appeared to be the one of eliminating errors caused by decoherence and inaccuracy. Unlike classical information, quantum information cannot be duplicated [8], [28]. Since error correcting codes appeared to protect classical information by duplicating it, their application for quantum information protection seemed impossible. However, Shor in [25] and

Steane in [26],[27] showed that quantum error correcting codes do exist and presented the first examples of one-error correcting codes. In [13] Knill and Laflamme formulated necessary and sufficient conditions for an error to be detectable by a given quantum code, and thus introduced the notion of the minimum distance of a quantum code. In [23] Shor and Laflamme showed that, similarly to classical codes, quantum codes have enumerators related by the MacWilliams identities. Properties of quantum enumerators were extensively studied by Rains [20],[21],[22]. In particular, he showed that the minimum distance of a quantum code is determined by its enumerators. In [3],[4] Calderbank, Rains, Shor and Sloane found a strong connection between a large class of quantum error-correcting codes (so-called stabilizer codes), which can be seen as an analog of classical group codes, and self-orthogonal codes over $GF(4)$. We are interested in the best possible parameters of arbitrary quantum error-correcting codes.

The parameters of a quantum code are length n, dimension K, and minimum distance w. Let δ stand for the relative distance of the code, $\delta = \frac{w}{n}$. A Gilbert-Varshamov type lower bound on the size of quantum codes was derived in [9] and [3] (for stabilizer codes).

Theorem 1 *There exist quantum codes of length n, dimension K and relative distance δ such that*

$$\frac{log K}{n} \geq 1 - \delta \log 3 - H(\delta),$$

where $H(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function.

Remark All over the paper the logarithms are base 2.

The goal of the present paper is to derive asymptotic upper bounds on the size of an arbitrary quantum code of given length and minimum distance. We use the linear programming approach and some strengthening of the bounds for stabilizer codes. For upper bounds known earlier see Laflamme and Knill [13], Rains [22] and Cleve [6].

The paper is organized as follows. In Section 2 we give a short introduction to the theory of quantum error correcting codes. The material of the section is presented in a form convenient for the readers with a coding theory background. In Section 3 we give a short survey of properties of Krawtchouk polynomials that are necessary for our purposes. In Section 4 we prove the key theorem that allows us to apply the linear programming approach to obtain bounds for quantum codes. In Sections 5.1, 5.2 and 5.3

we apply the key theorem to obtain Singleton type, Hamming type, and the first linear programming type bounds for arbitrary quantum codes. In Section 6 we strengthen the bounds for linear stabilizer codes.

2 Quantum error correcting codes

The material of this section is not new. It is mostly due to [12], [13], [20], [22], and [23]. The idea is to present the definitions and prove the known results in a style digestible for readers with a coding theory background.

We start with the notion of qubit. Information is transmitted as vectors of the Hilbert space $\mathbf{C}^t$. It is natural to ask about the minimum dimension t that is necessary for transmission of one bit of (classical) information. According to quantum mechanics, two vectors from the space $\mathbf{C}^t$ are completely distinguishable by a measurement if and only if they are orthogonal. In $\mathbf{C}^2$ there exists an orthogonal basis, say $\mathbf{v}_0$, $\mathbf{v}_1$, and we can assign logical 0 to $\mathbf{v}_0$ and logical 1 to $\mathbf{v}_1$. So the space $\mathbf{C}^2$ allows us to encode one bit of information and is called qubit (quantum bit).

Now if we want to transmit n bits of information we need the space $\mathbf{C}^{2^n} = \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \ldots \otimes \mathbf{C}^2$, where $\otimes$ is the tensor product. In $\mathbf{C}^{2^n}$ we can choose 2^n orthogonal vectors from the space that allows transmission of n bits of information. In fact, it is not necessary to restrict ourselves to use of only mutually orthogonal vectors; any vectors from $\mathbf{C}^{2^n}$ could be sent over a channel.

Remark When we say *vector* we assume *column* vector.

In the process of transmission over a channel the information can be altered by an error. There are several models of channels. We consider here the most popular one – completely depolarized channel. In this model a vector $\mathbf{v} \in \mathbf{C}^2$ can be altered by one of the following error operators

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix}, \text{ and } \iota = \sqrt{-1}. \quad (1)$$

The error operator, say E, has the following form

$$E = \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n, \quad (2)$$

where $\sigma_i \in \{I_2, \sigma_x, \sigma_z, \sigma_y\}, i = 1, \ldots, n$. The number of non-identity matrices in the tensor product (2) is called the weight of E and is denoted by $wt(E)$. If a vector $\mathbf{v}$ is affected by an error E, then the result is $\mathbf{w} = E\mathbf{v}$.

Definition 1 *A quantum code Q of length n and size K, denoted as $((n, K))$ code, is a $K-$dimensional linear subspace of the space $\mathbf{C}^{2^n}$.*

We say that an error E is detectable if any two orthogonal vectors from the code remain orthogonal (i.e. distinguishable) after one of them has been altered by E. In other words we have the following definition.

Definition 2 *E is detectable if and only if*

$$\mathbf{v}^\dagger E \mathbf{w} = 0, \tag{3}$$

for all orthogonal vectors $\mathbf{v}$ and $\mathbf{w}$ from the code Q.

Here $\dagger$ means the Hermitian conjugation.

Later in this section we will need another definition of the error detectability. Let P be the orthogonal projection operator on the code subspace.

Definition 3 *E is detectable if and only if*

$$PEP = \lambda_E P, \tag{4}$$

where λ_E is a constant that depends only on E.

As the following lemma shows, (3) and (4) are equivalent.

Lemma 1 *The criteria (3) and (4) are equivalent.*

Proof Let E be a detectable error. Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be any two orthonormal vectors from Q and $\mathbf{w}_1 = \mathbf{v}_1 + \mathbf{v}_2$ and $\mathbf{w}_2 = \mathbf{v}_1 - \mathbf{v}_2$. Clearly $\mathbf{w}_1$ and $\mathbf{w}_2$ are orthogonal and belong to the code. Hence from (3) we have

$$\mathbf{w}_1^\dagger E \mathbf{w}_2 = \mathbf{v}_1^\dagger E \mathbf{v}_1 + \mathbf{v}_2^\dagger E \mathbf{v}_1 - \mathbf{v}_1^\dagger E \mathbf{v}_2 - \mathbf{v}_2^\dagger E \mathbf{v}_2 = 0.$$

From this we get $\mathbf{v}_1^\dagger E \mathbf{v}_1 = \mathbf{v}_2^\dagger E \mathbf{v}_2 = \lambda_E$. Now let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K$ be an orthonormal basis of Q. Then the orthogonal projection operator on Q can be written as

$$P = \sum_{i=1}^{K} \mathbf{v}_i \mathbf{v}_i^\dagger.$$

So we have

$$PEP = \left(\sum_{i=1}^{K} \mathbf{v}_i \mathbf{v}_i^\dagger\right) E \left(\sum_{i=1}^{K} \mathbf{v}_i \mathbf{v}_i^\dagger\right) = \sum_{i,j} \mathbf{v}_i \mathbf{v}_i^\dagger E \mathbf{v}_j \mathbf{v}_j^\dagger = \lambda_E P.$$

In other direction, let $\mathbf{v}$ and $\mathbf{w}$ be any two orthogonal vectors from the code. Then from (4) we have the following chain of identities

$$\begin{aligned} PEP &= \lambda_E P, \\ \mathbf{v}^\dagger PEP\mathbf{w} &= \lambda_E \mathbf{v}^\dagger P\mathbf{w}, \\ \mathbf{v}^\dagger E\mathbf{w} &= \lambda_E \mathbf{v}^\dagger \mathbf{w}, \\ \mathbf{v}^\dagger E\mathbf{w} &= 0. \end{aligned}$$

□

Now we are in the position to define the minimum distance of a quantum code.

Definition 4 *The minimum distance of the code Q is the maximum integer w such that any error E, $wt(E) \leq w-1$, is detectable.*

Note that if we use these definitions for classical codes, then we get the usual definition of the minimum distance. Moreover, as in the case of classical codes one can introduce the enumerators of a quantum $((n, K))$ code. An $((n, K))$ quantum code Q has two enumerators $(B_i)_{i=0}^n$ and $(B_i^\perp)_{i=0}^n$ defined by

$$B_i = \frac{1}{K^2} \sum_{wt(E)=i} \mathrm{Tr}^2(EP),$$

$$B_i^\perp = \frac{1}{K} \sum_{wt(E)=i} \mathrm{Tr}(EPEP).$$

Note that according to the definition of the error set (1), an error operator E is hermitian. The orthogonal projection operator P is also hermitian. Trivially PEP is also hermitian. Now, using the well-known fact that $\mathrm{Tr}(AB)$ is real for any hermitian A and B (see e.g. [19, Exercise 3.34, p.73]), we convince that $\mathrm{Tr}(EP)$ and $\mathrm{Tr}(EPEP)$ are real. So the numbers B_i and $B_i^\perp$ are also real.

In the case of a quantum stabilizer code (to be defined later), say Q, the numbers B_i and $B_i^{\perp}$ are the weight spectra of codes C and $C^{\perp}$ over $GF(4)$ associated with Q. So in this case B_i and $B_i^{\perp}$ are connected by the MacWilliams identities. However, the MacWilliams identities are valid for the enumerators of general quantum codes. Moreover, as we will show later, the enumerators define the minimum distance of a quantum code.

Let $B(x,y) = \sum_{t=0}^{n} B_t x^{n-t} y^t$ and $B^{\perp}(x,y) = \sum_{t=0}^{n} B_t^{\perp} x^{n-t} y^t$. The statements of the two following theorems first appeared in [23].

Theorem 2 *The numbers B_t and $B_t^{\perp}$ are related by the quaternary MacWilliams identities. That is*

$$B(x,y) = \frac{1}{2^n K} B^{\perp}(x+3y, x-y). \tag{5}$$

Proof The following proof was suggested by A.Kitaev [12]. Denote by $e_{i,j}, p_{i,j}, 0 \leq i,j \leq 2^n - 1$, the entries of E and P. Then

$$\begin{aligned} B(x,y) &= \frac{1}{K^2} \sum_{t=0}^{n} x^{n-t} y^t \sum_{wt(E)=t} \sum_{i,j,k,l} p_{j,i} p_{l,k} e_{i,j} e_{k,l} \\ &= \frac{1}{K^2} \sum_{E} x^{n-wt(E)} y^{wt(E)} \sum_{i,j,k,l} p_{j,i} p_{l,k} e_{i,j} e_{k,l} \\ &= \frac{1}{K^2} \sum_{i,j,k,l} p_{j,i} p_{l,k} \sum_{E} e_{i,j} e_{k,l} x^{n-wt(E)} y^{wt(E)}. \end{aligned}$$

Let $i = i_0 + 2i_1 + \ldots + 2^{n-1} i_{n-1}$. Analogously we denote the binary expansions of j, k, and l. Taking into account (2), we obtain that

$$\begin{aligned} B(x,y) &= \frac{1}{K^2} \sum_{i,j,k,l} p_{j,i} p_{l,k} \prod_{t=0}^{n-1} \{ x (I_2)_{i_t,j_t} (I_2)_{k_t,l_t} \\ &\quad + y \left[(\sigma_x)_{i_t,j_t} (\sigma_x)_{k_t,l_t} + (\sigma_y)_{i_t,j_t} (\sigma_y)_{k_t,l_t} + (\sigma_z)_{i_t,j_t} (\sigma_z)_{k_t,l_t} \right] \}. \end{aligned}$$

By the same method, we have

$$\begin{aligned} B^{\perp}(x,y) &= \frac{1}{K} \sum_{i,j,k,l} p_{j,i} p_{l,k} \prod_{t=0}^{n-1} \{ x (I_2)_{i_t,l_t} (I_2)_{k_t,j_t} \\ &\quad + y \left[(\sigma_x)_{i_t,l_t} (\sigma_x)_{k_t,j_t} + (\sigma_y)_{i_t,l_t} (\sigma_y)_{k_t,j_t} + (\sigma_z)_{i_t,l_t} (\sigma_z)_{k_t,j_t} \right] \}. \end{aligned}$$

Denote

$$b_{i_t,j_t,k_t,l_t}(x,y)$$

$$= x(I_2)_{i_t,j_t}(I_2)_{k_t,l_t} + y\left[(\sigma_x)_{i_t,j_t}(\sigma_x)_{k_t,l_t} + (\sigma_y)_{i_t,j_t}(\sigma_y)_{k_t,l_t} + (\sigma_z)_{i_t,j_t}(\sigma_z)_{k_t,l_t}\right]$$

and

$$b^{\perp}_{i_t,j_t,k_t,l_t}(x,y)$$

$$= x(I_2)_{i_t,l_t}(I_2)_{k_t,j_t} + y\left[(\sigma_x)_{i_t,l_t}(\sigma_x)_{k_t,j_t} + (\sigma_y)_{i_t,l_t}(\sigma_y)_{k_t,j_t} + (\sigma_z)_{i_t,l_t}(\sigma_z)_{k_t,j_t}\right].$$

It is easy to check that

$$b_{i_t,j_t,k_t,l_t}(x,y) = b^{\perp}_{i_t,j_t,k_t,l_t}(\frac{x+3y}{2}, \frac{x-y}{2}). \tag{6}$$

In fact, all 16 possibilities for binary i_t, j_t, k_t, l_t should be checked. For instance if $i_t = 0, j_t = 0, k_t = 1$, and $l_t = 1$, we have

$$b_{i_t,j_t,k_t,l_t}(x,y) = x - y,$$

$$b^{\perp}_{i_t,j_t,k_t,l_t}(x,y) = 2y,$$

in compliance with (6). □

Theorem 3 *Let Q be a quantum code with enumerators B_i and $B_i^{\perp}$. Then*

i) $B_i^{\perp} \geq B_i \geq 0$, for $i = 0, 1, \ldots, n$, and $B_0 = B_0^{\perp} = 1$,

ii) if t is the largest integer such that $B_i = B_i^{\perp}, i \leq t$, then the minimum distance of Q equals $t + 1$.

Proof Taking into account that $P^2 = P$ and $\mathrm{Tr}(P) = K$, we get $B_0 = B_0^{\perp} = 1$. The numbers B_i are sums of squares and so are nonnegative. Using the matrix form of the Schwartz inequality,

$$\mathrm{Tr}^2(A^{\dagger}B) \leq \mathrm{Tr}(A^{\dagger}A)\mathrm{Tr}(B^{\dagger}B),$$

we get

$$\mathrm{Tr}^2(EP) = \mathrm{Tr}^2((PEP)P) \leq \mathrm{Tr}((PEP)(PEP))\mathrm{Tr}(PP) \tag{7}$$

$$= \mathrm{Tr}(PEPE)\mathrm{Tr}(P) = K\mathrm{Tr}(PEPE).$$

This yields $B_i^{\perp} \geq B_i$.

The equality holds in (7) if and only if $PEP = \lambda_E P$, for some constant λ_E. Hence, by $B_i = B_i^{\perp}$, all the errors of weight i are detectable, and from the fact that all the errors of weight i are detectable, the equality $B_i = B_i^{\perp}$ follows. Thus, by the definition of the minimum distance, $w(Q) = t + 1$. $\square$

Note that substituting $x = 1, y = 0$ into (5) and taking into account that $B_0 = B_0^{\perp} = 1$, we get

$$K = \frac{1}{2^n} \sum_{i=0}^{n} B_i^{\perp}. \tag{8}$$

Linear codes play a special role in classical coding theory. Similarly, in quantum coding theory there exist the so-called stabilizer codes [3], [4], and [10]. They can be seen as an analog of classical linear or, more precisely, group codes. The definition of quantum stabilizer codes is as follows. It is easy to check that the matrices $c_0 I_2, c_1 \sigma_x, c_2 \sigma_y, c_3 \sigma_z$ with $c_i \in \{\pm 1, \pm \iota\}$ constitute a group, say $\mathcal{E}_1$. Tensor products of n elements of $\mathcal{E}_1$ also constitute a group, say $\mathcal{E}_n$ (an extraspecial group). A quantum code Q is called a stabilizer code if there exists an Abelian subgroup $\mathcal{E}$ of the group $\mathcal{E}_n$ such that all vectors $\mathbf{v} \in \mathbf{C}^{2^n}$, satisfying $E\mathbf{v} = \mathbf{v}$ for all $E \in \mathcal{E}$, form the code Q. In other words, Q forms an eigenspace of $\mathcal{E}$ corresponding to the eigenvalue 1 of $\mathcal{E}$. If the group $\mathcal{E}$ has order 2^k then $dim(Q) = 2^{n-k}$, and so the dimension of a stabilizer code is always equal to a power of 2. A nice property of quantum stabilizer codes is that they are strongly related to classical self-orthogonal codes over $GF(4)$ [3], [4]. Namely, there exists an $[[n, k]] = ((n, 2^k))$ quantum stabilizer code Q of minimum distance w if and only if there exists a self-orthogonal group code C of length n, cardinality $|C| = 2^{n-k}$ such that $w = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^{\perp} \setminus C\}$, where $C^{\perp}$ is the code orthogonal to C with respect to the trace inner product. The trace inner product of vectors $\mathbf{v}$ and $\mathbf{u}$, denoted by $*$, is

$$\mathbf{v} * \mathbf{u} = \mathrm{tr}\left(\sum_i v_i \overline{u_i}\right) = \sum_i (v_i u_i^2 + v_i^2 u_i),$$

where the bar denotes conjugation in $GF(4)$ and the trace acts from $GF(4)$ onto $GF(2)$. If a code C associated to a quantum stabilizer code is linear over $GF(4)$, then we call Q a linear stabilizer code or simply a linear quantum code.

3 Krawtchouk polynomials

Let the $i-$th quaternary Krawtchouk polynomial be defined as follows:

$$P_i(x) = \sum_{j=0}^{i} (-1)^j 3^{i-j} \binom{x}{j} \binom{n-x}{i-j}, i \leq i \leq n. \tag{9}$$

An easy corollary of Theorem 2 and (8) is as follows.

Corollary 1 *For* $t = 0, \ldots, n$,

$$B_t = \frac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} P_t(i).$$

Here we survey some properties of the quaternary Krawtchouk polynomials, see, e.g., [15],[17].

The Krawtchouk polynomials satisfy the following orthogonality relation

$$\sum_{i=0}^{n} P_r(i) P_i(s) = 4^n \delta_{r,s}. \tag{10}$$

A symmetry relation is satisfied by the polynomials

$$3^i \binom{n}{i} P_s(i) = 3^s \binom{n}{s} P_i(s). \tag{11}$$

Every polynomial of degree at most n has the unique expansion in the basis of Krawtchouk polynomials. If a polynomial $f(x)$ has the expansion

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

then

$$f_i = 4^{-n} \sum_{j=0}^{n} f(j) P_j(i).$$

The following property (see [17, Chap. 5, Exercise 41]) holds:

$$\sum_{i=0}^{n} \binom{n-i}{n-j} P_i(x) = 4^j \binom{n-x}{j}. \tag{12}$$

The Christoffel-Darboux formula (see [15, Corollary 3.5]) is of importance:

$$P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a) \tag{13}$$
$$= \frac{4(a-x)}{t+1} 3^t \binom{n}{t} \sum_{i=0}^{t} \frac{P_i(x)P_i(a)}{3^i \binom{n}{i}}.$$

The Krawtchouk polynomials satisfy a recurrent relation,

$$(i+1)P_{i+1}(x) = (3n - 2i - 4x)P_i(x) - 3(n-i+1)P_{i-1}(x). \tag{14}$$

Some useful values of the Krawtchouk polynomials:

$$P_0(x) = 1, \quad P_1(x) = 3n - 4x, \quad 2P_2(x) = 16x^2 - 8x(3n-1) + 9n(n-1),$$

$$P_i(0) = 3^i \binom{n}{i}.$$

We will also need a result on asymptotic behavior of the smallest root r_t of $P_t(j)$. For t growing linearly in n and $\tau = t/n$ (see e.g. [15])

$$\xi_t = \frac{r_t}{n} = \frac{3}{4} - \frac{1}{2}\tau - \frac{1}{2}\sqrt{3\tau(1-\tau)} + o(1). \tag{15}$$

Remark All over the paper $o(1)$ tends to 0 as n grows.

4 The key inequality

In this section we obtain the key inequality allowing us to reduce the problem of upper bounding the size of codes to a problem of finding polynomials possessing special properties.

Theorem 4 *Let Q be an $((n, K))$ quantum code of the minimum distance w. Let*

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

be a polynomial satisfying the conditions

i) $f_i \geq 0$,

ii) $f(x) > 0$ *for* $x = 0, \ldots, w-1$, *and*

iii) $f(x) \leq 0$ *for* $x = w, \ldots, n$.

Then

$$K \leq \frac{1}{2^n} \max_{j=0,\ldots,w-1} \frac{f(j)}{f_j}.$$

Proof Let Q be an $((n, K, w))$ quantum code with enumerators B_i and $B_i^\perp$. Denote $S = \sum_{i=0}^{n} B_i^\perp$. Then using Corollary 1 and Theorem 3, we get

$$\begin{aligned} S \sum_{i=0}^{w-1} f_i B_i &\leq S \sum_{i=0}^{n} f_i B_i \\ &= S \sum_{i=0}^{n} \frac{1}{S} f_i \sum_{j=0}^{n} B_j^\perp P_i(j) = \sum_{j=0}^{n} B_j^\perp \sum_{i=0}^{n} f_i P_i(j) \\ &= \sum_{j=0}^{n} f(j) B_j^\perp \leq \sum_{j=0}^{w-1} f(j) B_j^\perp = \sum_{j=0}^{w-1} f(j) B_j. \end{aligned}$$

Thus,

$$S \leq \frac{\sum_{j=0}^{w-1} f(j) B_j}{\sum_{j=0}^{w-1} f_j B_j} \leq \max_{j=0,\ldots,w-1} \frac{f(j)}{f_j}.$$

□

5 Upper bounds

Several bounds are known for classical nonbinary error-correcting codes. In particular, Delsarte [7] demonstrated that the Singleton and Hamming bounds can be obtained using linear programming approach. Aaltonen [1] generalized the first linear programming bound obtained in [16] to the nonbinary case. For the best currently available bounds on parameters of nonbinary classical codes see Aaltonen [2], Laihonen and Litsyn [14], and Levenshtein [15].

In what follows we present quantum counterparts to the Singleton, Hamming, and the first linear programming bounds derived from Theorem 4.

5.1 A Singleton type bound

Choose in Theorem 4

$$f(x) = 4^{n-w+1} \prod_{j=w}^{n} (1 - \frac{x}{j}) = 4^{n-w+1} \frac{\binom{n-x}{n-w+1}}{\binom{n}{w-1}}.$$

Then using (12), we get

$$\begin{aligned} f_x &= 4^{-n} \sum_{j=0}^{n} f(j) P_j(x) \\ &= 4^{-w+1} \sum_{j=0}^{n} \frac{\binom{n-j}{n-w+1}}{\binom{n}{w-1}} P_j(x) \\ &= \frac{\binom{n-x}{w-1}}{\binom{n}{w-1}}. \end{aligned}$$

Now,

$$r(x) = \frac{f(x)}{f_x} = 4^{n-w+1} \frac{\binom{n-x}{n-w+1}}{\binom{n-x}{w-1}}.$$

Considering the ratio

$$\begin{aligned} \frac{r(x)}{r(x+1)} &= \frac{\binom{n-x}{n-w+1}}{\binom{n-x}{w-1}} \times \frac{\binom{n-x-1}{w-1}}{\binom{n-x-1}{n-w+1}} \\ &= \frac{n-x-w+1}{w-x-1}, \end{aligned}$$

we find that it is greater than 1 if $w \leq (n+2)/2$. Note that it is enough for our purposes, since for $w = (n+2)/2$ we have

$$K \leq \frac{f(0)}{f_0} = 1.$$

Theorem 5 *In every $((n, K))$ quantum code of the minimum distance w,*

$$K \leq 2^{n-2w+2}.$$

Note that though this bound has been already derived in [13],[22], the proof presented here is different and so could be of interest.

5.2 A Hamming type bound

Let $e = \left\lfloor \frac{w-1}{2} \right\rfloor$. Define $f_i = (P_e(i))^2$ and $f(x) = \sum_{i=0}^{n} f_i P_i(x)$.

Lemma 2

$$P_i(x)P_j(x)$$
$$= \sum_{k=0}^{n} P_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-i-j} \binom{n-k}{s} \binom{2k+2s-i-j}{k+s-j} 2^{i+j-2s-k} 3^s.$$

Proof The proof of the lemma is a straightforward generalization of the proof to a similar expression in the binary case (see e.g. [16, A.19]). □

Using the lemma, we get

$$f_x = \sum_{k=0}^{n} P_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s.$$

This yields

$$\begin{aligned} f(x) & \\ &= \textstyle\sum_{j=0}^{n} \sum_{k=0}^{n} \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s P_k(j) P_j(x) \\ &= \textstyle\sum_{k=0}^{n} \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s \sum_{j=0}^{n} P_k(j) P_j(x) \\ &= \textstyle 4^n \sum_{s=\max\{0,e-x\}}^{e-x/2} \binom{x}{2x+2s-2e} \binom{n-x}{s} \binom{2x+2s-2e}{x+s-e} 2^{2e-2s-x} 3^s, \end{aligned}$$

where on the last step we use (10). Taking into account that

$$\frac{1}{n} \log \binom{n}{k} = H\left(\frac{k}{n}\right) + O\left(\frac{1}{n}\right),$$

and denoting $\xi = x/n, \nu = s/n$, and $\tau = e/n$, we get

$$\frac{1}{n} \log \left[\binom{x}{2x+2s-2e} \binom{n-x}{s} \binom{2x+2s-2e}{x+s-e} 2^{2e-2s-x} 3^s \right]$$
$$= \xi H\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) + (1-\xi) H\left(\frac{\nu}{1-\xi}\right) + \nu \log 3 + \xi + O\left(\frac{1}{n}\right).$$

Taking derivative in ν of the last expression, we get

$$2\log\left(1 - \frac{2\xi+2\nu-2\tau}{\xi}\right) - 2\log\left(\frac{2\xi+2\nu-2\tau}{\xi}\right)$$
$$+ \log\left(1 - \frac{\nu}{1-\xi}\right) - \log\left(\frac{\nu}{1-\xi}\right) + \log 3. \qquad (16)$$

It is not difficult to check (see Appendix) that this function has only one root in the interval $\max\{0, \tau - \xi\} < \nu < \tau - \xi/2$.

Definition 5 *The function $\alpha(\tau,\xi)$ is the root of (16) in the interval* $\max\{0,\tau-\xi\} < \nu < \tau - \xi/2$.

Thus

$$\begin{aligned}\frac{1}{n}\log f(x) &= 2+\xi+\xi H\left(\frac{2\xi+2\alpha(\tau,\xi)-2\tau}{\xi}\right)\\ &\quad +(1-\xi)H\left(\frac{\alpha(\tau,\xi)}{1-\xi}\right)+\alpha(\tau,\xi)\log 3+O\left(\frac{1}{n}\right). \quad (17)\end{aligned}$$

To derive an estimate for f_x we need bounds on values of Krawtchouk polynomials. Recall that by (15),

$$\xi_e = \frac{r_e}{n} = \frac{3}{4}-\frac{1}{2}\tau-\frac{1}{2}\sqrt{3\tau(1-\tau)}+o(1).$$

The next observation is a generalization of a similar fact in the binary case [11].

Lemma 3 *For $\xi < \xi_e$,*

$$\frac{1}{n}\log P_e(x) = \frac{1}{n}\log\binom{n}{e}3^e \quad (18)$$
$$+\int_0^\xi \log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6(1-z)}\right)dz+O\left(\frac{1}{n}\right).$$

Proof Like in the binary case (see, e.g. [17, Lemma 36]), using recursion (14), one can show that for $\xi < \xi_t$

$$\frac{P_t(j+1)}{P_t(j)} = \frac{3n-2j-4t+\sqrt{(3-2j-4t)^2-12j(1-j)}}{6(1-j)}\left(1+O\left(\frac{1}{n}\right)\right).$$

Taking logarithm on both sides, applying this recursively to $P_t(0) = \binom{n}{t}3^t$, and approximating the sum by the integral, we get the claim.

□

Notice, that the integral in Lemma 3 can be expressed explicitly, namely

$$\begin{aligned}&\int \log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6-6z}\right)dz\\ =\ & -z\log 6+(1-z)\log(1-z)+z\log(\beta+\gamma)\\ &+\frac{(\alpha-1)}{4}\log(3+\alpha-8z-2\gamma)+\log(\alpha-2)-\log 2\\ &-\frac{1}{2}\log(6+2\alpha-\alpha^2-10z+2\alpha z-(\alpha-2)\gamma)+\text{const},\end{aligned}$$

where $\alpha = 3 - 4\tau, \beta = \alpha - 2z, \gamma = \sqrt{\beta^2 - 12z(1-z)}$. Hence

$$\begin{aligned}\frac{1}{n}\log f_x &= 2\tau\log 3 + 2H(\tau) \\ &+[-z\log 6 + (1-z)\log(1-z) + z\log(\beta+\gamma) \\ &+\frac{(\alpha-1)}{4}\log(3+\alpha-8z-2\gamma) + \log(\alpha-2) - \log 2 \\ &-\frac{1}{2}\log(6+2\alpha-\alpha^2-10z+2\alpha z-(\alpha-2)\gamma]\Big|_{z=0}^{\xi} + O\left(\frac{1}{n}\right).\end{aligned} \tag{19}$$

From Lemma 3,

$$\begin{aligned}\frac{1}{n}\log f_x &= 2\tau\log 3 + 2H(\tau) \\ &+2\int_0^{\xi}\log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6-6z}\right)dz \\ &+O\left(\frac{1}{n}\right),\end{aligned}$$

Using (19) and (17), we get a Hamming type bound.

Theorem 6 *Let $\tau = w/(2n)$ and $\alpha(\tau,\xi)$ is from Definition 5. Then for $((n,K))$ code with the minimum distance w we have*

$$\begin{aligned}\frac{\log K}{n} &\le \max_{0\le\xi\le 2\tau}\left\{1+\xi+\xi H\left(\frac{2\xi+2\alpha(\tau,\xi)-2\tau}{\xi}\right)\right. \\ &+ (1-\xi)H\left(\frac{\alpha(\tau,\xi)}{1-\xi}\right) + \alpha(\tau,\xi)\log 3 - 2\tau\log 3 - 2H(\tau) \\ &- \left. 2\int_0^{\xi}\log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6-6z}\right)dz\right\} + o(1).\end{aligned}$$

Computations with Maple show that this function achieves its maximum at $\xi = 0$ for any $\delta \le \xi_e$. If $0 \le \delta \le (9-3\sqrt{2})/14$ then $\delta \le \xi_e$. E. Rains showed that $\delta \le 1/3$ when $\log(K)/n \ge 0$ [22]. Since $(9-3\sqrt{2})/14 > 1/3$, the conventional Hamming bound is valid in the interval $0 \le \delta \le 1/3$.

Corollary 2 *The conventional Hamming bound is valid for quantum codes, i.e. if Q is an $((n,K))$ quantum code then*

$$\frac{\log K}{n} \le 1 - \frac{\delta}{2}\log 3 - H\left(\frac{\delta}{2}\right) + o(1).$$

5.3 The First Linear Programming Bound

Define

$$f(x) = \frac{1}{a-x}\left\{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\right\}^2.$$

This polynomial yields the first linear programming bound for classical codes over $GF(4)$ [1],[15]. To get the first linear programming bound one has to choose

$$\frac{t}{n} = \frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)} + o(1),$$

where $\delta = w/n$, and $r_{t+1} < a < r_t$, $\frac{P_t(a)}{P_{t+1}(a)} = -1$.

By the Christoffel-Darboux formula (13),

$$\begin{aligned} f(x) &= \frac{4\cdot 3^t}{t+1}\binom{n}{t}\left\{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\right\}\sum_{i=0}^{t}\frac{P_i(x)P_i(a)}{3^i\binom{n}{i}} \\ &= \frac{4\cdot 3^t}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{3^i\binom{n}{i}}\left\{P_{t+1}(x)P_i(x) + P_t(x)P_i(x)\right\}. \end{aligned}$$

Lemma 2 yields

$$\begin{aligned} & f(x) \\ &= \frac{4\cdot 3^t}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{3^i\binom{n}{i}} \\ &\quad \left\{\sum_{j=0}^{n}P_j(x)\sum_{s=0}^{n-j}\binom{j}{2j+2s-t-1-i}\binom{n-j}{s}\binom{2j+2s-t-1-i}{j+s-t-1}2^{t+1+i-2s-j}3^s\right. \\ &\quad \left.\sum_{j=0}^{n}P_j(x)\sum_{s=0}^{n-j}\binom{j}{2j+2s-t-i}\binom{n-j}{s}\binom{2j+2s-t-i}{j+s-t}2^{t+i-2s-j}3^s\right\} \\ &= \sum_{j=0}^{n}P_j(x)\frac{4\cdot 3^t}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{3^i\binom{n}{i}} \\ &\quad \sum_{s=0}^{n-j}\left\{\binom{j}{2j+2s-t-i-1}\binom{n-j}{s}\binom{2j+2s-t-1-i}{j+s-t-1}2^{t+1+i-2s-j}3^s\right. \\ &\quad \left.+\binom{j}{2j+2s-t-i}\binom{n-j}{s}\binom{2j+2s-t-i}{j+s-t}2^{t+i-2s-j}3^s\right\}. \end{aligned}$$

Estimating f_x by the term with $i = t$, we have

$$\begin{aligned} & f_x \\ &\geq \frac{4\cdot 3^t}{t+1}\binom{n}{t}\frac{P_t(a)^2}{3^t\binom{n}{t}}\sum_{s=0}^{n-x}\left\{\binom{x}{2x+2s-2t}\binom{n-x}{s}\binom{2x+2s-2t}{x+s-t}2^{2t-2s-x}3^s\right\} \\ &= \frac{4}{t+1}P_t(a)^2\sum_{s=\max\{0,t-x\}}^{t-x/2}\left\{\binom{x}{2x+2s-2t}\binom{n-x}{s}\binom{2x+2s-2t}{x+s-t}2^{2t-2s-x}3^s\right\}. \end{aligned}$$

Denote $\xi = x/n, \nu = s/n$, and $\tau = t/n$. Then, similarly to the derivation of the Hamming bound we have

$$\begin{aligned}
&\frac{1}{n}\log\left\{\binom{x}{2x+2s-2t}\binom{n-x}{s}\binom{2x+2s-2t}{x+s-t}2^{2t-2s-x}3^s\right\}\\
&= \xi H\left(\frac{2\xi+2\nu-2\tau}{\xi}\right)+(1-\xi)H\left(\frac{\nu}{1-\xi}\right)+\xi+\nu\log 3+O\left(\frac{1}{n}\right).
\end{aligned}$$

Again, like in the derivation of the Hamming bound, we differentiate the last expression in ν and find the root $\alpha(\tau,\xi)$ (see Definition 5). Then, using (11), we get

$$\begin{aligned}
&\frac{f(x)}{f_x}\\
&\le \frac{P_t(a)^2(t+1)\{P_{t+1}(x)+P_t(x)\}^2}{(a-x)\cdot 4\cdot P_t(a)^2\binom{x}{2x+2n\alpha(\tau,\xi)-2t}\binom{n-x}{n\alpha(\tau,\xi)}\binom{2x+2n\alpha(\tau,\xi)-2t}{x+n\alpha(\tau,\xi)-t}2^{2t-2n\alpha(\tau,\xi)-x}3^{n\alpha(\tau,\xi)}}\\
&= \frac{(t+1)\left\{\frac{3^{t+1}\binom{n}{t+1}P_x(t+1)}{3^x\binom{n}{x}}+\frac{3^{t+1}\binom{n}{t}P_x(t)}{3^x\binom{n}{x}}\right\}^2}{\binom{x}{2x+2n\alpha(\tau,\xi)-2t}\binom{n-x}{n\alpha(\tau,\xi)}\binom{2x+2n\alpha(\tau,\xi)-2t}{x+n\alpha(\tau,\xi)-t}2^{2t-2n\alpha(\tau,\xi)-x}3^{n\alpha(\tau,\xi)}}\\
&= \frac{(t+1)3^{2t}\binom{n}{t}^2\left\{3\frac{n-t}{t+1}P_x(t+1)+P_x(t)\right\}^2}{4(a-x)3^{2x}\binom{n}{x}^2\binom{x}{2x+2n\alpha(\tau,\xi)-2t}\binom{n-x}{n\alpha(\tau,\xi)}\binom{2x+2n\alpha(\tau,\xi)-2t}{x+n\alpha(\tau,\xi)-t}2^{2t-2n\alpha(\tau,\xi)-x}3^{n\alpha(\tau,\xi)}}.
\end{aligned}$$

Now using Lemma 3, after some efforts we get

$$\begin{aligned}
&\frac{f(x)}{f_x}\\
&\le \frac{P_t(x)^2\left\{3(n-t)^{\frac{3n-2t-4x+\sqrt{(3-2t-4x)^2-12t(1-t)}}{6-6t}}+1\right\}^2}{4(a-x)(t+1)\binom{x}{2x+2n\alpha(\tau,\xi)-2t}\binom{n-x}{n\alpha(\tau,\xi)}\binom{2x+2n\alpha(\tau,\xi)-2t}{x+n\alpha(\tau,\xi)-t}2^{2t-2n\alpha(\tau,\xi)-x}3^{n\alpha(\tau,\xi)}}.
\end{aligned}$$

Theorem 7 *Let $\delta = w/n, \tau = \frac{3}{4}-\frac{1}{2}\delta-\frac{1}{2}\sqrt{3\delta(1-\delta)}$ and $\alpha(\tau,\xi)$ be from Definition 5. Then for $((n,K))$ code with the minimum distance w, we have*

$$\begin{aligned}
&\frac{\log K}{n}\\
&\le \max_{0\le\xi\le\delta}\{2H(\tau)+2\tau\log 3\\
&+ 2\int_0^\xi \log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6-6z}\right)dz\\
&- \xi H\left(\frac{2\xi+2\alpha(\tau,\xi)-2\tau}{\xi}\right)-(1-\xi)H\left(\frac{\alpha(\tau,\xi)}{1-\xi}\right)-\xi-\alpha(\tau,\xi)\log 3\Big\}+o(1).
\end{aligned}$$

Computations with Maple show that this function achieves its minimum at $\xi = 0$ for any $\delta \leq 0.3152$.

Corollary 3 *If $0 \leq \delta \leq 0.3152$ then the conventional first linear programming bound is valid for quantum codes, i.e. if Q is an $((n, K))$ quantum code then*

$$\frac{\log K}{n} \leq H\left(\frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}\right) + \left(\frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}\right)\log 3 - 1 + o(1).$$

Note that when $\delta = 0.3152$, $\frac{\log K}{n} \approx 0.0028$. So for all $0.0028 \leq \frac{\log K}{n} \leq 1$, the conventional first linear programming bound is valid.

Notice that would the bound be valid on all the interval, it would hit the point $\frac{\log K}{n} = 0$ at $\delta \approx 0.31$.

6 Strengthening in the linear case

Let now Q be an $((n, K = 2^k))$ stabilizer quantum code with associated linear self-orthogonal code C over $GF(4)$. Recall that $|C| = 2^{n-k}$. We will call Q an $[[n, k]]$ linear quantum code.

Lemma 4 *Let Q be an $[[n, k]]$ liner quantum code. Then the minimum distance of Q is at most the minimum distance of an $[(n+k)/2, k]$ code over $GF(4)$.*

Proof Let

$$G_C = \left[\begin{array}{cc} I_{\frac{n+k}{2}} & A \end{array}\right]$$

be a generator matrix of the code C. Since $C \subseteq C^{\perp}$ we can append some rows to the matrix G_C to get a generator matrix of $C^{\perp}$. That is,

$$G_{C^{\perp}} = \begin{bmatrix} G_C \\ G' \end{bmatrix}.$$

Let us call the code C' generated by the matrix G', a complementary code of C to $C^{\perp}$. It is clear that the minimum distance of C' has to be at least $w = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^{\perp} \setminus C\}$. Using Gaussian elimination, we can force the elements of G' in the first $\frac{n+k}{2}$ positions to be 0. In this case C' is an $[(n+k)/2, k]$ code over GF(4). □

Now we can use any upper bound for the code C' to get a bound for Q. For example, denoting by $D_{lp2}\left(\frac{\log_4 |C|}{n}\right)$ the maximum possible value of

the ratio $\frac{d}{n}$ of a quaternary classical code C of length n and cardinality $|C|$ with respect to the asymptotic bound obtained in [2], we get the following bound.

Theorem 8 *Let Q be an $[[n,k]]$ linear quantum code. Then*

$$\delta \leq \frac{1}{2}\left(1+\frac{k}{n}\right) D_{lp2}\left(\frac{2\frac{k}{n}}{1+\frac{k}{n}}\right).$$

One can see (bound S on fig.1) that this bound is better than the first linear programming and Hamming bounds in the interval $[0, a \approx 0.238]$.

7 Conclusion

In the paper we have derived new upper bounds on the size of quantum codes. The graphs of the bounds are given on Figure 1. Here we label the quantum Gilbert-Varshamov bound by "GV", Singleton bound by "Sng", Hamming bound by "H", the first linear programming bound by "LP1", and the bound for linear quantum codes by "S". "R" is Rains' "threshold" bound from [22]. For the sake of comparison we also give the graph of the second linear programming bound LP2 – the best one known for the classical codes of the corresponding size and alphabet.

Acknowledgments The authors are indebted to A. Barg, A. Kitaev, E. Knill, E. Rains and the referees for their very helpful comments and suggestions.

8 Appendix

Let

$$\begin{aligned} f(\xi,\nu,\tau) &= 2\log\left(1-\frac{2\xi+2\nu-2\tau}{\xi}\right) - 2\log\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) \\ &\quad + \log\left(1-\frac{\nu}{1-\xi}\right) - \log\left(\frac{\nu}{1-\xi}\right) + \log 3, \end{aligned}$$

where $0 \leq \tau \leq 0.25, 0 \leq \xi \leq 2\tau$, and $\max\{0, \tau-\xi\} \leq \nu \leq \tau - \frac{\xi}{2}$. We shall show that this function has only one root for allowed τ, ξ, and ν.

Taking the partial derivative of the function, we get

$$g(\xi,\nu,\tau) = \frac{\partial f(\xi,\nu,\tau)}{\partial \tau} = \frac{2}{\xi+2\nu-2\tau} - \frac{2}{\xi+\nu-\tau} - \frac{1}{1-\xi-\nu} - \frac{1}{\nu}.$$

The roots of the equation $\frac{\partial g(\xi,\nu,\tau)}{\partial \tau} = 0$ are

$$\tau_{1,2} = \nu \pm \frac{\xi}{\sqrt{2}}.$$

Since τ has to be greater than $\nu + \frac{\xi}{2}$, we conclude that the function $\frac{\partial f(\xi,\nu,\tau)}{\partial \tau}$ achieves its maximum at $\tau = \nu + \frac{\xi}{\sqrt{2}}$. Substituting $\tau = \nu + \frac{\xi}{\sqrt{2}}$, we obtain that

$$\frac{\partial f(\xi,\nu,\tau)}{\partial \tau} \leq \frac{2}{\xi-\sqrt{2}\xi} - \frac{2}{\xi-\xi/\sqrt{2}} - \frac{1}{1-\xi-\nu} - \frac{1}{\nu}.$$

It is easy to check that the last expression achieves its maximum at

$$\nu = \frac{1-\xi}{2}.$$

Substitution of this value into $\frac{\partial f(\xi,\nu,\tau)}{\partial \tau}$ gives

$$\frac{\partial f(\xi,\nu,\tau)}{\partial \tau} \leq \frac{2}{\xi-\sqrt{2}\xi} - \frac{2}{\xi-\xi/\sqrt{2}} - \frac{4}{1-\xi}.$$

The last expression is negative for any $0 \leq \xi \leq 0.5$. It is also obvious that $f(\xi,\nu,\tau) > 0$ when $\nu = \max\{0, \tau-\xi\}$, and $f(\xi,\nu,\tau) < 0$ when $\nu = \tau - \frac{\xi}{2}$.

References

[1] M. J. Aaltonen, "Linear programming bounds for tree codes," *IEEE Trans. Info. Theory*, vol. 25, pp. 85–90, 1977.

[2] M. J. Aaltonen, "A new bound on nonbinary block codes," *Discrete Math.*, vol. 83, pp. 139–160, 1990.

[3] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-409, 1997.

[4] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$," *IEEE Trans. Info. Theory*, vol. 44, pp.1369 –1387, 1998.

[5] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098-1105, 1996.

[6] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A*, vol. 55, pp. 4054-4059, 1997.

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

[8] D. Dieks, "Communication by EPR devices," *Phys. Lett. A,* **92**, p. 271, 1982.

[9] A. Ekert and C. Macchiavello, "Error correction in quantum communication," *Phys. Rev. Lett.*, vol. 77, pp. 2585-2588, 1996.

[10] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862-1868, 1996.

[11] G. Kalai and N. Linial, " On the distance distribution of codes," *IEEE Trans. Inform. Theory*, vol. 42, pp.1467–1472, 1995.

[12] A. Kitaev, private communication, 1997.

[13] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900-911, 1997.

[14] T. Laihonen and S. Litsyn, "On upper bounds for minimum distance and covering radius of nonbinary codes," *Designs, Codes, and Cryptography*, **14**, no. 1, pp. 71–80, 1998.

[15] V.I. Levenshtein, "Krawtchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces," *IEEE Trans. on Inf. Theory*, **41**, no. 5, pp. 1303–1321, 1995.

[16] R. J. McEliece, E. R. Rodemich,H. C. Rumsey, Jr. and L. R. Welch, "New Upper Bounds on the Rate of a Code via the Delsarte-MacWilliams Inequalities,"*IEEE Trans. Inform. Theory*, vol. 23, pp.157–166, 1977.

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

[18] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self dual codes exist," *Discrete Math.*, **3**, pp.153–162, 1972.

[19] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer, 1995.

[20] E.M. Rains, "Quantum weight enumerators," *IEEE Trans. Info. Theory*, vol. 44, pp.1388–1394, 1998.

[21] E.M. Rains, "Nonbinary quantum codes," LANL e-print quant-ph/9703048.

[22] E.M. Rains, "Quantum shadow enumerators," LANL e-print quant-ph/961101.

[23] P.W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

[24] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S.Goldwasser, Editor, IEEE Computer Society Press, Los Alamitos, CA, p.124, 1994.

[25] P.W. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A, **52**, p. 2493, 1995.

[26] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

[27] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. London A*, vol. 452, pp. 2551-2577, 1996.

[28] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, **299**, p.802, 1982.

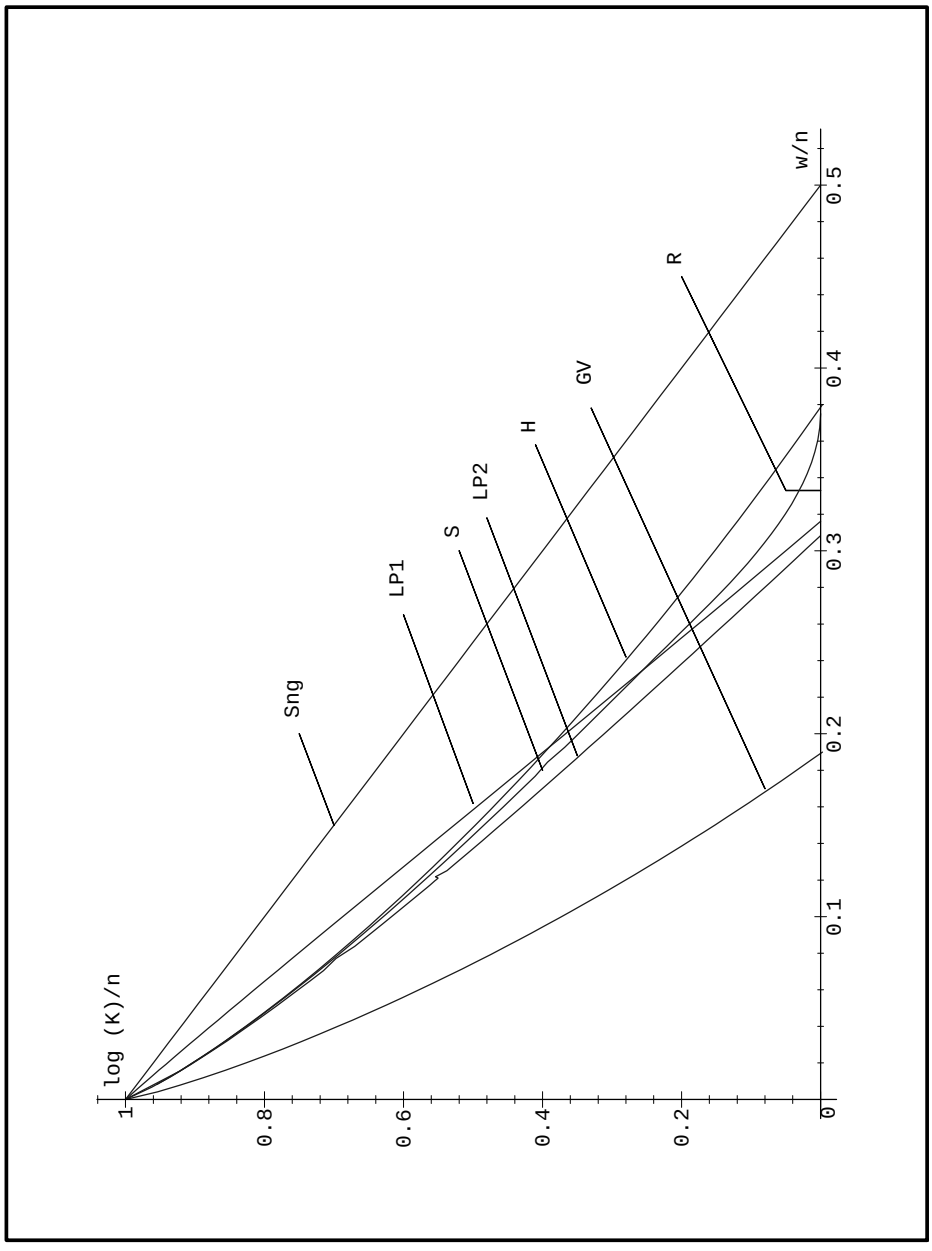


Figure 1: *VG is Varshamov-Gilbert bound; Sng is Singleton bound; LP1 and LP2 are the linear programming bounds ; H is Hamming type bound; S is strengthening for linear codes; "R" is Rains' bound* $\delta \leq 1/3$.