IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received April 13, 2019, accepted May 14, 2019, date of publication May 23, 2019, date of current version June 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2918529

Complete Weight Distributions and MacWilliams Identities for Asymmetric Quantum Codes

CHUANGQIANG HU[1], SHUDI YANG[2], AND STEPHEN S.-T. YAU[3]
[1]Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, China
[2]School of Mathematical Sciences, Qufu Normal University, Shandong 273165, China
[3]Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

Corresponding author: Stephen S.-T. Yau (yau@uic.edu)

This work was supported in part by the National Natural Science Foundation of China under Grant 11701317, Grant 11531007, Grant 11431015, Grant 61472457, and Grant 11571380, in part by the Tsinghua University Start-up Fund, in part by the Natural Science Foundation of Shandong Province of China under Grant ZR2016AM04, and in part by the Guangzhou Science and Technology Program under Grant 201607010144.

ABSTRACT In 1997, Shor and Laflamme defined the weight enumerators for quantum error-correcting codes and derived a MacWilliams identity. We extend their work by introducing our double weight enumerators and complete weight enumerators for qubit codes and then investigate the MacWilliams identities for these enumerators. Based on the generalized MacWilliams identities, we solve an open problem, namely, the Singleton-type bound for asymmetric quantum codes (AQCs). Besides, the Hamming-type and the first linear-programming-type bounds for the AQCs are deduced similarly.

INDEX TERMS MacWilliams identities, asymmetric quantum codes, quantum singleton bound.

I. INTRODUCTION

Quantum information theory is rapidly becoming a well-established discipline. It shares many of the concepts of classical information theory but involves new subtleties arising from the nature of quantum mechanics. Among the central concepts in common between classical and quantum information is that of error correction. Quantum error-correcting codes have been initially discovered by Shor [37] and Steane [39], [40] in 1995-1996 for the purpose of protecting quantum information from noise in computation or communication [5], [6], [8], [14], [21], [33]. The discovery of [37] has revolutionized the field of quantum information and leads to a new research line. In [13], [49], [50] noiseless quantum codes were built using group theoretic methods [44], [51]. In [7], [21] quantum error correction was used to broader analyses of the physical principles. The authors in [9], [15], [43] gave various new constructions of quantum error-correcting codes.

It is well known that if further information about the error process is available, more efficient codes can be designed. Indeed, in many physical systems, the noise is likely to be unbalanced between amplitude (X-type) errors and phase (Z-type) errors. Recently a lot of attention has been put into designing codes for this situation and into studying their fault tolerance properties [17], [18], [36], [43]. All these results use error models described by Kraus operators [24] that generalize Pauli operators.

In classical coding theory the famous MacWilliams identity gives a relationship between the weight distributions of a code C and its dual code $C^{\perp}$ without knowing specifically the codewords of $C^{\perp}$ or anything else about its structure [31], [32]. The same technique was adapted to the quantum case by Shor and Laflamme [38] generalizing the classical case and they derived a MacWilliams identity. Rains [34] investigated the properties of quantum enumerators. In [35], Rains extended the work of [38] to general codes by introducing quantum shadow enumerators. This idea was further developed by Lai *et al.* [26]. They considered the weight generating functions associated with convolutional codes in the viewpoint of constraint codes and obtained a simple and direct proof of this MacWilliams identity in the case of minimal encoders.

Several bounds are known for classical error-correcting codes. Delsarte [11] investigated the Singleton and Hamming bounds using linear programming approach. The first linear programming bound was generalized by Aaltonen [1] to the nonbinary case. See [2], [27], [28] for more information on available bounds for non-binary codes. Recently there has been intensive activity in the area of quantum codes.

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Xu.

In particular, Knill and Laflamme [22] introduced the notion of the minimum distance of a quantum error-correcting code and showed that the error for entangled states is bounded linearly by the error for pure states. Shor and Laflamme [38] presented a linear-programming bound for quantum error-correcting codes. Cleve [10] demonstrated connections between quantum stabilizer codes and classical codes and gave upper bounds on the best asymptotic capacity. Rains [34], [35] showed that the minimum distance of a quantum code is determined by its enumerators. Ashikhmin and Litsyn [4] attained upper asymptotic bounds on the size of quantum codes. Aly [3] established asymmetric Singleton and Hamming bounds on asymmetric pure quantum and subsystem code parameters. Sarvepalli *et al.* [41] studied asymmetric quantum codes and derived upper bounds on the code parameters using linear programming. Wang *et al.* [43] extended the characterization of non-additive symmetric quantum codes given in [15], [16] to the asymmetric case and obtained an asymptotic bound from algebraic geometry codes. Recently, Huber *et al.* [19] demonstrated some bounds on absolutely maximally entangled states from shadow inequalities with the help of the quantum MacWilliams identity.

It should be mentioned that there is another weight enumerator for a classical code that contains more detailed information about the codewords. Namely, the complete weight enumerator, which enumerates the codewords according to the number of alphabets of each kind contained in each codeword. MacWilliams [31], [32] also proved that there is an identity between the complete weight enumerators of C and its dual code $C^{\perp}$. The complete weight enumerators and weight enumerators of classical codes have been studied extensively, see [12], [29], [42], [45]–[48] and the reference therein. However, to the best of our knowledge, there is no quantum analog complete weight enumerators as in classical coding theory. Therefore the purpose of the present paper is to introduce the notions of double weight enumerators and complete weight enumerators for qubit codes, and then generalize the MacWilliams identities about complete weight enumerators from classical coding theory to the quantum case. Using the generalized MacWilliams identities, we will find new upper bounds on the minimum distance of asymmetric quantum codes (AQCs).

Here is the plan of the rest of this paper. In Section II, we introduce some basic definitions and notations on symmetric and asymmetric quantum codes. In Section III, we establish our main result on quantum MacWilliams identities by defining double weight enumerators and complete weight enumerators of quantum codes. In Section IV, we give a short survey of properties of the Krawtchouk polynomials and we prove the key inequality that allows us to get new upper bounds of the minimum distance of asymmetric quantum codes. In Section V, we apply the key inequality to obtain Singleton-type, Hamming-type and the first linear-programming-type bounds for asymmetric quantum codes.

II. SYMMETRIC AND ASYMMETRIC QUANTUM CODES

We begin with some basic definitions and notations. Let $\mathbb{C}$ be a complex number field. We regard $\mathbb{C}^2$ as a Hilbert space with orthonormal basis $|0\rangle$ and $|1\rangle$. Denote by $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ the n-th tensor of $\mathbb{C}^2$. This space enables us to transmit n qubits of information. Its coordinate basis is given by

$$|j\rangle = |j_0\rangle \otimes |j_1\rangle \otimes \cdots \otimes |j_{n-1}\rangle,$$

for each $j_r \in \{0, 1\}$. For two quantum states $|u\rangle$ and $|v\rangle$ in $\mathbb{C}^{2^n}$ with

$$|u\rangle = \sum_j u_j|j\rangle, \quad |v\rangle = \sum_j v_j|j\rangle,$$

the Hermitian inner product of $|u\rangle$ and $|v\rangle$ is defined by

$$\langle u|v\rangle = \sum_j \overline{u}_j v_j,$$

where we denote by $\overline{x}$ the complex conjugate of x.

In the process of transmission over a channel the information can be altered by errors. There are several models of channels. Perhaps the most popular one is the completely depolarized channel, among which a vector $v \in \mathbb{C}^2$ can be altered by one of the following error operators:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The error operators acting on $\mathbb{C}^{2^n}$ constitute a set

$$E := \{e = \sigma_0 \otimes \cdots \otimes \sigma_{n-1} | \sigma_r \in \{I, \sigma_x, \sigma_y, \sigma_z\}\}.$$

For $e \in E$, the number of non-identity matrices in the expression of e is called the weight of e which is denoted by $w_Q(e)$. Similarly, we denote by $N_x(e)$, $N_y(e)$ and $N_z(e)$ the number of the matrices σ_x, σ_y and σ_z occurred in the expression of e, respectively. Clearly

$$w_Q(e) = N_x(e) + N_y(e) + N_z(e). \tag{1}$$

It is well known that each $e \in E$ is the composition of two kinds of error operators, i.e. the bit flip and the phase flip. Precisely, for a fixed error operator e, there exist vectors $a = (a_0, \cdots, a_{n-1}) \in \mathbb{F}_2^n$ and $b = (b_0, \cdots, b_{n-1}) \in \mathbb{F}_2^n$ such that

$$e = i^{a \cdot b} X(a) Z(b), \tag{2}$$

where

$$X(a) = \omega_0 \otimes \cdots \otimes \omega_{n-1}, \quad Z(b) = \omega'_0 \otimes \cdots \otimes \omega'_{n-1},$$

and

$$\omega_j = \begin{cases} I & \text{if } a_j = 0, \\ \sigma_x & \text{if } a_j = 1, \end{cases} \quad \omega'_j = \begin{cases} I & \text{if } b_j = 0, \\ \sigma_z & \text{if } b_j = 1. \end{cases}$$

We define the X-weight $w_X(e)$ and the Z-weight $w_Z(e)$ to be the Hamming weights of a and b of Equation (2) respectively. In fact, they alternatively can be defined as

$$w_X(e) = N_x(e) + N_y(e), \tag{3}$$

$$w_Z(e) = N_y(e) + N_z(e). \tag{4}$$

In the following section we want to investigate some natural partitions of the set E, so we define

$$E[i,j,k] := \{e \in E | N_x(e) = i, N_y(e) = j, N_z(e) = k\},$$
$$E[i,j] := \{e \in E | w_X(e) = i, w_Z(e) = j\},$$
$$E[i] := \{e \in E | w_Q(e) = i\}.$$

Definition 1: A quantum code of length n is a linear subspace of $\mathbb{C}^{2^n}$ with dimension $K \geqslant 1$. Such a quantum code can be denoted as $((n, K))$ code or $[[n, k]]$ code, where $k = \log K$.

Remark 2: Here and thereafter, the logarithms are base 2.

The conditions for error correction are due to Knill *et al.* [23].

Definition 3 [23]: Let Q be a quantum code. An error e in E is called detectable if

$$\langle v|e|w\rangle = 0$$

for all orthogonal codewords v and w from the code Q.

Denote by P the orthogonal projection from $\mathbb{C}^{2^n}$ onto a quantum code Q. We have an alternative definition for detectable errors. It is deduced from [4] that e is detectable if and only if

$$PeP = \lambda_e P$$

for a constant λ_e depending on e.

Definition 4: Let Q be a quantum code with parameters $((n, K))$. The minimum distance of Q is the maximum integer d such that any error $e \in E[i]$ with $i < d$ is detectable. Such a quantum code is called a symmetric quantum code with parameters $((n, K, d))$ or $[[n, k, d]]$. If the integers d_x and d_z are the maximum integers such that each error $e \in E[i, j]$ with $i < d_x$ and $j < d_z$ is detectable, then we call Q an asymmetric quantum code with parameters $((n, K, d_z/d_x))$ or $[[n, k, d_z/d_x]]$.

The classical Singleton bound can be extended to quantum codes.

Theorem 5 (Theorem 5, [4]): Let Q be a quantum code with parameters $[[n, k, d]]$. We have

$$n \geqslant k + 2d - 2.$$

In [3], [43], the authors have proved the Singleton bound for stabilizer asymmetric quantum codes. That is

$$n \geqslant k + d_x + d_z - 2.$$

However, we cannot find the proof of Singleton bound for general quantum codes.

III. WEIGHT DISTRIBUTIONS AND ENUMERATORS

The weight distributions for classical codes can be generalized to the case of quantum codes. According to [38], the weight distributions for quantum codes are defined by the following two sequences of numbers

$$B_i = \frac{1}{K^2} \sum_{e \in E[i]} \mathrm{Tr}^2(eP),$$
$$B_i^{\perp} = \frac{1}{K} \sum_{e \in E[i]} \mathrm{Tr}(ePeP).$$

Moreover, the corresponding weight enumerators are defined to be the following two bivariate polynomials

$$B(X, Y) := \sum_{i=0}^{n} B_i X^{n-i} Y^i,$$
$$B^{\perp}(X, Y) := \sum_{i=0}^{n} B_i^{\perp} X^{n-i} Y^i.$$

In a similar manner, we introduce the double weight distributions

$$C_{i,j} = \frac{1}{K^2} \sum_{e \in E[i,j]} \mathrm{Tr}^2(eP),$$
$$C_{i,j}^{\perp} = \frac{1}{K} \sum_{e \in E[i,j]} \mathrm{Tr}(ePeP),$$

and the complete weight distributions

$$D_{i,j,k} = \frac{1}{K^2} \sum_{e \in E[i,j,k]} \mathrm{Tr}^2(eP),$$
$$D_{i,j,k}^{\perp} = \frac{1}{K} \sum_{e \in E[i,j,k]} \mathrm{Tr}(ePeP).$$

Then the double weight enumerators and the complete weight enumerators are defined by

$$C(X, Y, Z, W) := \sum_{i,j=0}^{n} C_{i,j} X^{n-i} Y^i Z^{n-j} W^j,$$
$$C^{\perp}(X, Y, Z, W) := \sum_{i,j=0}^{n} C_{i,j}^{\perp} X^{n-i} Y^i Z^{n-j} W^j,$$
$$D(X, Y, Z, W) := \sum_{i+j+k \leqslant n} D_{i,j,k} X^i Y^j Z^k W^{n-i-j-k},$$
$$D^{\perp}(X, Y, Z, W) := \sum_{i+j+k \leqslant n} D_{i,j,k}^{\perp} X^i Y^j Z^k W^{n-i-j-k}.$$

These enumerators are related by the following theorem.

Theorem 6: Let Q be a quantum code with enumerators $B, B^{\perp}, C, C^{\perp}, D$ and $D^{\perp}$. Then the following four identities hold:

$$B(X, Y) = D(Y, Y, Y, X), \tag{5}$$
$$B^{\perp}(X, Y) = D^{\perp}(Y, Y, Y, X), \tag{6}$$
$$C(X, Y, Z, W) = D(YZ, YW, XW, XZ), \tag{7}$$
$$C^{\perp}(X, Y, Z, W) = D^{\perp}(YZ, YW, XW, XZ). \tag{8}$$

Proof: It follows from (1), (3) and (4) that

$$B_l = \sum_{i+j+k=l} D_{i,j,k},$$
$$B_l^{\perp} = \sum_{i+j+k=l} D_{i,j,k}^{\perp},$$
$$D_{i,j,k} = C_{i+j,j+k},$$
$$D_{i,j,k}^{\perp} = C_{i+j,j+k}^{\perp}.$$

The four Equations (5), (6), (7) and (8) then follow immediately, finishing the proof of the theorem. □

The classical MacWilliams identity provides a relationship between classical linear codes and their dual codes. It is interesting to see that the MacWilliams identity also holds for quantum weight enumerators [38]. That is

$$B(X,Y)=\frac{1}{K}B^{\perp}(\frac{X+3Y}{2},\frac{X-Y}{2}). \tag{9}$$

Our main result is to show that quaternary MacWilliams identities similarly hold for the double weight enumerators and complete weight enumerators.

Theorem 7 (Quaternary MacWilliams Identities): Let Q be an ((n, K)) quantum code. With the notation introduced above, we have

$$\begin{aligned} &C(X,Y,Z,W)\\ &\quad=\frac{1}{K}C^{\perp}(Z+W,Z-W,\frac{X+Y}{2},\frac{X-Y}{2}), \end{aligned}\tag{10}$$

$$\begin{aligned} &D(X,Y,Z,W)\\ &\quad=\frac{1}{K}D^{\perp}(\frac{X-Y-Z+W}{2},\frac{-X+Y-Z+W}{2},\\ &\qquad\frac{-X-Y+Z+W}{2},\frac{X+Y+Z+W}{2}). \end{aligned}\tag{11}$$

Proof: We shall investigate the explicit expressions for these enumerators. Recall that the coordinate basis for $\mathbb{C}^{2^n}$ is given by

$$|j\rangle=|j_0\rangle\otimes\cdots\otimes|j_{n-1}\rangle,$$

where $0\leqslant j<2^n$ and $j=j_0+j_1 2+\cdots+j_{n-1}2^{n-1}$. Denote by $e_{i,j},p_{i,j}$ the entries of e and P, respectively, with respect to our coordinate basis. For $e=\sigma_0\otimes\cdots\otimes\sigma_{n-1}\in E$, the identity $e|i\rangle=\sum_j e_{i,j}|j\rangle$ implies

$$e_{i,j}=(\sigma_0)_{i_0,j_0}(\sigma_1)_{i_1,j_1}\cdots(\sigma_{n-1})_{i_{n-1},j_{n-1}}.$$

According to the definition of D, we get

$$\begin{aligned} &D(X,Y,Z,W)\\ &\quad=\sum_{i,j,k}X^iY^jZ^kW^{n-i-j-k}D_{i,j,k}\\ &\quad=\frac{1}{K^2}\sum_{i,j,k}X^iY^jZ^kW^{n-i-j-k}\\ &\qquad\times\sum_{e\in E[i,j,k]}\sum_{r,s,t,u}e_{r,s}p_{s,r}e_{t,u}p_{u,t}\\ &\quad=\frac{1}{K^2}\sum_{r,s,t,u}p_{s,r}p_{u,t}\\ &\qquad\times\sum_{e\in E}X^{N_x(e)}Y^{N_y(e)}Z^{N_z(e)}W^{n-w_Q(e)}e_{r,s}e_{t,u}\\ &\quad=\frac{1}{K^2}\sum_{r,s,t,u}p_{s,r}p_{u,t}\prod_{\lambda=0}^{n-1}d_\lambda(X,Y,Z,W), \end{aligned}$$

where

$$\begin{aligned} &d_\lambda(X,Y,Z,W)\\ &\quad=(\sigma_x)_{r_\lambda,s_\lambda}(\sigma_x)_{t_\lambda,u_\lambda}X+(\sigma_y)_{r_\lambda,s_\lambda}(\sigma_y)_{t_\lambda,u_\lambda}Y\\ &\qquad+(\sigma_z)_{r_\lambda,s_\lambda}(\sigma_z)_{t_\lambda,u_\lambda}Z+(I)_{r_\lambda,s_\lambda}(I)_{t_\lambda,u_\lambda}W. \end{aligned}\tag{12}$$

Using the same method, one can show that

$$D^{\perp}(X,Y,Z,W)=\frac{1}{K}\sum_{r,s,t,u}p_{s,r}p_{u,t}\prod_{\lambda=0}^{n-1}d_\lambda^{\perp}(X,Y,Z,W),$$

where

$$\begin{aligned} &d_\lambda^{\perp}(X,Y,Z,W)\\ &\quad=(\sigma_x)_{r_\lambda,u_\lambda}(\sigma_x)_{t_\lambda,s_\lambda}X+(\sigma_y)_{r_\lambda,u_\lambda}(\sigma_y)_{t_\lambda,s_\lambda}Y\\ &\qquad+(\sigma_z)_{r_\lambda,u_\lambda}(\sigma_z)_{t_\lambda,s_\lambda}Z+(I)_{r_\lambda,u_\lambda}(I)_{t_\lambda,s_\lambda}W. \end{aligned}\tag{13}$$

To establish Equation (11), it remains to prove that for arbitrary $r_\lambda,s_\lambda,t_\lambda,u_\lambda\in\{0,1\}$,

$$\begin{aligned} &d_\lambda(X,Y,Z,W)\\ &\quad=d_\lambda^{\perp}(\frac{X-Y-Z+W}{2},\frac{-X+Y-Z+W}{2},\\ &\qquad\frac{-X-Y+Z+W}{2},\frac{X+Y+Z+W}{2}). \end{aligned}\tag{14}$$

We can check directly that (14) is true for all of the 16 cases. Let us pick the case of $(r_\lambda,s_\lambda,t_\lambda,u_\lambda)=(0011)$ for example. It is computed from (12) and (13) that $d_\lambda(X,Y,Z,W)=-Z+W$ and $d_\lambda^{\perp}(X,Y,Z,W)=X+Y$, respectively. So (14) holds for the case of $(r_\lambda,s_\lambda,t_\lambda,u_\lambda)=(0011)$. Thus we have proved Equation (11).

Using (11) and the relationship between C and D, we get

$$\begin{aligned} &C(X,Y,Z,W)\\ &\quad=D(YZ,YW,XW,XZ)\\ &\quad=\frac{1}{K}D^{\perp}(\frac{(X+Y)(Z-W)}{2},\frac{(X-Y)(Z-W)}{2},\\ &\qquad\frac{(X-Y)(Z+W)}{2},\frac{(X+Y)(Z+W)}{2})\\ &\quad=\frac{1}{K}C^{\perp}(Z+W,Z-W,\frac{X+Y}{2},\frac{X-Y}{2}), \end{aligned}$$

where in the last step we use (8). This implies Equation (10). Thus we complete the proof of the theorem. □

The following theorem generalize Theorem 3 in [4] to the case of double weight distributions.

Theorem 8: Let $((Q,K,d_z/d_x))$ be an asymmetric quantum code with double weight distributions $C_{i,j}$ and $C_{i,j}^{\perp}$. Then

1) *$C_{i,j}^{\perp}\geqslant C_{i,j}\geqslant 0$ for $0\leqslant i,j\leqslant n$, and $C_{0,0}=C_{0,0}^{\perp}=1$.*
2) *If t_x, t_z are the two largest integers such that $C_{i,j}=C_{i,j}^{\perp}$ for $i<t_x$ and $j<t_z$, then $d_x=t_x$ and $d_z=t_z$.*

Proof: The proof is similar to that of Theorem 3 in [4] and so it is omitted here. □

Remark 9: Suppose that Q is an additive quantum code of length n constructed from a classical linear code C over $\mathbb{F}_4$. Then the weight distributions of Q are nothing but the classical distributions induced by C and its symplectic dual $C_{th}^{\perp}$. That is

$$B_i=\#\{c\in C:w_H(c)=i\},$$
$$B_i^{\perp}=\#\{c\in C_{th}^{\perp}:w_H(c)=i\},$$

where $w_H(c)$ denotes the Hamming weight of a codeword c, see [5], [35]. Let α be a fixed primitive element of $\mathbb{F}_4$, *i.e.,* $\mathbb{F}_4 = \{\alpha, \alpha^2, \alpha^3 = \alpha + \alpha^2, 0\}$. *Write*

$$\begin{aligned} c &= (c_1, c_2, \cdots, c_n) \\ &= (a_1\alpha + b_1\alpha^2, a_2\alpha + b_2\alpha^2, \cdots, a_n\alpha + b_n\alpha^2) \in \mathbb{F}_4^n, \end{aligned}$$

where $(a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n) \in \mathbb{F}_2^{2n}$. *Then the double weight distributions of* Q *are deduced from* C *and its symplectic dual* $C_{th}^{\perp}$, *i.e.,*

$$C_{i,j} = \#\{(c_1, c_2, \cdots, c_n) \in C : \sum_{s=1}^{n} a_s = i, \sum_{s=1}^{n} b_s = j\},$$
$$C_{i,j}^{\perp} = \#\{(c_1, c_2, \cdots, c_n) \in C_{th}^{\perp} : \sum_{s=1}^{n} a_s = i, \sum_{s=1}^{n} b_s = j\}.$$

For a vector $c = (c_1, c_2, \cdots, c_n) \in \mathbb{F}_4^n$, *the composition of* c, *denoted by* $\mathrm{comp}(c)$, *is defined as*

$$\mathrm{comp}(c) = (k_1, k_2, k_3, n - k_1 - k_2 - k_3),$$

where k_j $(j \neq 0)$ *is the number of components* c_s *of* c *that are equal to* α^j. *Then the complete weight distributions of* Q *are also deduced from* C *and its symplectic dual* $C_{th}^{\perp}$, *i.e.,*

$$D_{i,j,k} = \#\{c \in C : \mathrm{comp}(c) = (i, j, k, n - i - j - k)\},$$
$$D_{i,j,k}^{\perp} = \#\{c \in C_{th}^{\perp} : \mathrm{comp}(c) = (i, j, k, n - i - j - k)\}.$$

Here we provide a concrete example to illustrate our main results.

Example 10: Let $(q, m) = (4, 2)$. Consider the $[5, 3, 3]$ Hamming code $\mathcal{H}_2$ over $\mathbb{F}_4$ of length $n = (q^m - 1)/(q - 1) = 5$ with check matrix

$$\begin{bmatrix} 1 & 0 & 1 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha^2 & 1 \end{bmatrix},$$

where α is a fixed primitive element of $\mathbb{F}_4$. Its dual code $\mathcal{H}_2^{\perp}$ is a $[5, 2, 4]$ linear code over $\mathbb{F}_4$. The code $\mathcal{H}_2^{\perp}$ induces an additive quantum code Q with parameters $[[n, n - 2m, 3]] = [[5, 1, 3]]$. The weight enumerators of Q are computed from $C := \mathcal{H}_2^{\perp}$ and its symplectic dual $C_{th}^{\perp} := \mathcal{H}_2$, namely,

$$B(X, Y) = X^5 + 15XY^4,$$
$$B^{\perp}(X, Y) = X^5 + 30X^2Y^3 + 15XY^4 + 18Y^5.$$

One verifies that the MacWilliams identity (9) holds for B and $B^{\perp}$. The double weight enumerators of Q are as follows

$$\begin{aligned} &C(X, Y, Z, W) \\ &= X^5 Z^5 + 5X^3Y^2 Z^3 W^2 + 5X^3Y^2 ZW^4 + 5XY^4 Z^3 W^2, \\ &C^{\perp}(X, Y, Z, W) \\ &= X^5 Z^5 + X^5W^5 + 5X^4 YZ^3W^2 + 5X^4 YZ^2W^3 \\ &\quad + 5X^3 Y^2Z^4W + 5X^3 Y^2Z^3W^2 + 5X^3 Y^2Z^2W^3 \\ &\quad + 5X^3 Y^2ZW^4 + 5X^2 Y^3Z^4W + 5X^2 Y^3Z^3W^2 \\ &\quad + 5X^2 Y^3Z^2W^3 + 5X^2 Y^3ZW^4 + 5XY^4Z^3W^2 \\ &\quad + 5XY^4Z^2W^3 + Y^5Z^5 + Y^5W^5. \end{aligned}$$

The complete weight enumerators of Q are given below

$$\begin{aligned} &D(X, Y, Z, W) \\ &\quad = W^5 + 5\, WX^2\, Y^2 + 5\, WX^2\, Z^2 + 5\, WY^2\, Z^2, \\ &D^{\perp}(X, Y, Z, W) \\ &\quad = W^5 + X^5 + Y^5 + Z^5 + 5\, W^2\, X^2\, Y + 5\, W^2\, X^2\, Z \\ &\qquad + 5\, W^2\, XY^2 + 5\, W^2\, XZ^2 + 5\, W^2\, Y^2\, Z + 5\, W^2\, YZ^2 \\ &\qquad + 5\, WX^2\, Y^2 + 5\, WX^2\, Z^2 + 5\, WY^2\, Z^2 + 5\, X^2\, Y^2\, Z \\ &\qquad + 5\, X^2\, YZ^2 + 5\, XY^2\, Z^2. \end{aligned}$$

The above experimental results by Magma are consistent with the conclusions of Theorems 6 and 7.

IV. KRAWTCHOUK POLYNOMIALS AND THE KEY INEQUALITY

In this section, we introduce Krawtchouk polynomials and summarize their properties. This allows us to obtain the close relationship between $C_{i,j}$ and $C_{i,j}^{\perp}$ of an asymmetric quantum code. Then we propose the key inequality which enables us to reduce the problem of upper-bounding the size of asymmetric quantum codes to a problem of finding polynomials possessing special properties.

Fix an integer n. For $0 \leqslant i \leqslant n$, the polynomial

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

is called the i-th Krawtchouk polynomial. The first few polynomials are

$$P_0(x) = 1, \quad P_1(x) = n - 2x, \quad P_2(x) = 2\, x^2 - 2nx + \binom{n}{2}.$$

These polynomials have the generating function

$$(X + Y)^{n-r}(X - Y)^r = \sum_{i=0}^{n} P_i(r) X^{n-i} Y^i.$$

Now we recall several important properties of the Krawtchouk polynomials, see [32] for more information.

The Krawtchouk polynomials satisfy the reciprocity formula

$$\binom{n}{i} P_s(i) = \binom{n}{s} P_i(s). \tag{15}$$

They also have the following property

$$\sum_{i=0}^{n} \binom{n-i}{n-j} P_i(x) = 2^j \binom{n-x}{j}.$$

Besides they are orthogonal to each other, namely

$$\sum_{i=0}^{n} P_r(i) P_i(s) = 2^n \delta_{r,s}. \tag{16}$$

Many important facts follow from this orthogonality. For example, there is a three-term recurrence:

$$(i+1)P_{i+1}(x) = (n-2x)P_i(x) - (n-i+1)P_{i-1}(x). \tag{17}$$

The Christoffel-Darboux formula (see Corollary 3.5 of [28]) also holds:

$$P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a) = \frac{2(a-x)}{t+1}\binom{n}{t}\sum_{i=0}^{t}\frac{P_i(x)P_i(a)}{\binom{n}{i}}. \quad (18)$$

Using (15) and (17), the ratio $P_t(x+1)/P_t(x)$ is given by McEliece *et.al*. [30]

$$\frac{P_t(x+1)}{P_t(x)} = \frac{n-2t+\sqrt{(n-2t)^2-4j(n-x)}}{2(n-x)}\left(1+O\left(\frac{1}{n}\right)\right). \quad (19)$$

We will also need a result on asymptotic behaviour of the smallest root r_t of $P_t(x)$. For t growing linearly in n and $\tau = t/n$ (see, e.g., Eq A.20 of [30])

$$\gamma_t = \frac{r_t}{n} = \frac{1}{2} - \sqrt{\tau(1-\tau)} + o(1). \quad (20)$$

Remember that $o(1)$ tends to 0 as n grows.

The following theorem shows that the Krawtchouk polynomials have close relation to double weight distributions $C_{i,j}$ and $C^{\perp}_{i,j}$ of a quantum code.

Theorem 11: Let $((Q, K, d_z/d_x))$ be an asymmetric quantum code with double weight distributions $C_{i,j}$ and $C^{\perp}_{i,j}$. Then

$$C_{i,j} = \frac{1}{2^n K}\sum_{r,s=0}^{n} P_i(s)P_j(r)C^{\perp}_{r,s}, \quad (21)$$

$$C^{\perp}_{r,s} = \frac{K}{2^n}\sum_{i,j=0}^{n} P_r(j)P_s(i)C_{i,j}. \quad (22)$$

Proof: We have from Theorem 7 that

$$\begin{aligned}\sum_{i,j=0}^{n} C_{i,j}X^{n-i}Y^iZ^{n-j}W^j &= \frac{1}{2^nK}\sum_{r,s=0}^{n} C^{\perp}_{r,s}(Z+W)^{n-r}(Z-W)^r(X+Y)^{n-s}(X-Y)^s \\ &= \frac{1}{2^nK}\sum_{r,s=0}^{n} C^{\perp}_{r,s}\sum_{i,j=0}^{n} P_i(s)P_j(r)X^{n-i}Y^iZ^{n-j}W^j \\ &= \frac{1}{2^nK}\sum_{i,j=0}^{n}\sum_{r,s=0}^{n} C^{\perp}_{r,s}P_i(s)P_j(r)X^{n-i}Y^iZ^{n-j}W^j.\end{aligned}$$

This completes the proof of (21). Taking into account that

$$C^{\perp}(X,Y,Z,W) = K\cdot C(Z+W, Z-W, \frac{X+Y}{2}, \frac{X-Y}{2})$$

from (10), we get (22) immediately. □

The key inequality is given below, which will be needed in the sequel. Note that it is a further generalization of the inequality in Theorem 4 of [4].

Lemma 12: Let Q be an $((n, K, d_z/d_x))$ quantum code. Assume that the polynomial $f(x, y) = \sum_{i,j=0}^{n}\alpha_{i,j}P_i(y)P_j(x)$ satisfies the following conditions

1) *$\alpha_{i,j} \geqslant 0$ for $0 \leqslant i, j \leqslant n$,*
2) *$f(r, s) > 0$ for $0 \leqslant r < d_x$ and $0 \leqslant s < d_z$,*
3) *$f(r, s) \leqslant 0$ for $r \geqslant d_x$ or $s \geqslant d_z$.*

Then

$$K \leqslant \frac{1}{2^n}\max_{0\leqslant i<d_x, 0\leqslant j<d_z}\frac{f(i,j)}{\alpha_{i,j}}.$$

Proof: It follows from Theorems 8 and 11 that

$$\begin{aligned}2^nK\sum_{i=0}^{d_x-1}\sum_{j=0}^{d_z-1}\alpha_{i,j}C_{i,j} &\leqslant 2^nK\sum_{i,j=0}^{n}\alpha_{i,j}C_{i,j} \\ &= \sum_{i,j=0}^{n}\alpha_{i,j}\sum_{r,s=0}^{n}P_i(s)P_j(r)C^{\perp}_{r,s} \\ &= \sum_{r,s=0}^{n} f(r,s)C^{\perp}_{r,s} \\ &\leqslant \sum_{r=0}^{d_x-1}\sum_{s=0}^{d_z-1} f(r,s)C^{\perp}_{r,s} \\ &= \sum_{r=0}^{d_x-1}\sum_{s=0}^{d_z-1} f(r,s)C_{r,s}.\end{aligned}$$

Thus we have

$$2^nK \leqslant \frac{\sum_{i=0}^{d_x-1}\sum_{j=0}^{d_z-1} f(i,j)C_{i,j}}{\sum_{i=0}^{d_x-1}\sum_{j=0}^{d_z-1}\alpha_{i,j}C_{i,j}} \leqslant \max_{0\leqslant i<d_x, 0\leqslant j<d_z}\frac{f(i,j)}{\alpha_{i,j}},$$

completing the proof of this lemma. □

Let us mention an important consequence of Lemma 12 when $f(x, y)$ factorizes.

Lemma 13: Let Q be an $((n, K, d_z/d_x))$ quantum code. Define $f(x, y) = f_1(x)f_2(y)$ where $f_1(x) = \sum_{j=0}^{n}\beta_jP_j(x)$ and $f_2(y) = \sum_{i=0}^{n}\alpha_iP_i(y)$. Assume that the polynomial $f(x, y)$ satisfies the following conditions

1) *For even i, $\alpha_i > 0$, $\beta_i > 0$. For odd i, $\alpha_i = \beta_i = 0$.*
2) *$f(r, s) \geqslant 0$ for $0 \leqslant r < d_x$ and $0 \leqslant s < d_z$. For even r, $f_1(r) > 0$, $f_2(r) > 0$. For odd r, $f_1(r) = f_2(r) = 0$.*
3) *$f(r, s) \leqslant 0$ for $r \geqslant d_x$ or $s \geqslant d_z$.*

Then

$$K \leqslant \frac{1}{2^n}\max_{\substack{0\leqslant i<d_x \\ 2|i}}\frac{f_1(i)}{\beta_i}\max_{\substack{0\leqslant j<d_z \\ 2|j}}\frac{f_2(j)}{\alpha_j}.$$

Lemma 14: Let $A(x) = 2^{n-d+1}\prod_{r=d}^{n}\left(1-\frac{x}{r}\right)$. Then

$$A(x) = \sum_{i=0}^{n}\alpha_iP_i(x)$$

where

$$\alpha_i = \alpha_i(d) = \binom{n-i}{d-1}\Big/\binom{n}{n-d+1}. \quad (23)$$

Proof: By definition, we have

$$A(x) = 2^{n-d+1}\prod_{r=d}^{n}\left(1-\frac{x}{r}\right) = 2^{n-d+1}\binom{n-x}{n-d+1}\Big/\binom{n}{n-d+1}.$$

It is known from the book [32] (Exercise 41) that

$$\sum_{r=0}^{n}\binom{n-r}{n-d+1}P_r(i) = 2^{d-1}\binom{n-i}{d-1},$$

This implies that

$$\alpha_i = 2^{-n}\sum_{r=0}^{n}A(r)P_r(i) = \binom{n-i}{d-1}\Big/\binom{n}{n-d+1},$$

completing the proof of this lemma. □

V. UPPER BOUNDS

In this section, we extend the work of [4] and derive asymptotic upper bounds on the size of an arbitrary asymmetric quantum code of given length and minimum distance. Precisely, the Singleton bound, the Hamming bound and the first linear programming bound are determined utilizing the key inequality presented in Section IV.

A. A SINGLETON-TYPE BOUND

Theorem 15 (Quantum Singleton Bound): Let Q be an $[[n, k, d_z/d_x]]$ quantum code. Then $n \geqslant k + d_x + d_z - 2$.

Proof: Set $\alpha_{i,j} = \alpha_i(d_z)\alpha_j(d_x) \geqslant 0$ for $0 \leqslant i, j \leqslant n$, where $\alpha_i(d)$ is defined in (23). Let

$$\begin{aligned} f(x,y) &= \sum_{i,j=0}^{n}\alpha_{i,j}P_i(y)P_j(x) \\ &= \sum_{i,j=0}^{n}\alpha_i(d_z)\alpha_j(d_x)P_i(y)P_j(x) \\ &= 2^{2n-d_x-d_z+2}\prod_{r=d_x}^{n}\left(1-\frac{x}{r}\right)\prod_{s=d_z}^{n}\left(1-\frac{y}{s}\right). \end{aligned}$$

One may check that this polynomial verifies all conditions of Lemma 12. So

$$\begin{aligned} K &\leqslant \frac{1}{2^n}\max_{0\leqslant i<d_x, 0\leqslant j<d_z}\frac{f(i,j)}{\alpha_{i,j}} \\ &= 2^{n-d_x-d_z+2}\max_{0\leqslant i<d_x} g(i,d_x)\max_{0\leqslant j<d_z} g(j,d_z), \end{aligned}$$

where

$$g(i,d) = \binom{n-i}{n-d+1}\Big/\binom{n-i}{d-1}.$$

For $d \leqslant n/2+1$, we have $g(i,d)/g(i+1,d) \geqslant 1$. Therefore, we obtain

$$K \leqslant 2^{n-d_x-d_z+2}g(0,d_x)g(0,d_z) = 2^{n-d_x-d_z+2}.$$

Since $K = 2^k$, we find $n \geqslant k + d_x + d_z - 2$. □

B. A HAMMING-TYPE BOUND

Let $\phi = \left\lfloor\frac{d_x-1}{2}\right\rfloor$ and $\theta = \left\lfloor\frac{d_z-1}{2}\right\rfloor$. Define $\alpha_i(d_z) = (P_\theta(i))^2$, $\beta_j(d_x) = (P_\phi(j))^2$ and

$$f(x,y) = \sum_{i,j=0}^{n}\alpha_i(d_z)\beta_j(d_x)P_i(y)P_j(x). \tag{24}$$

Lemma 16 ([30], Eq A.19): Any product $P_i(x)P_j(x)$ can be expressed as a linear combination of the $P_k(x)$ as follows:

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

where a binomial coefficient with fractional or negative lower index is to be interpreted as zero.

Using the lemma, we get

$$\alpha_i(d_z) = \sum_{k=0}^{n}\binom{n-k}{\theta-k/2}\binom{k}{k/2}P_k(i)$$

and

$$\beta_j(d_x) = \sum_{k=0}^{n}\binom{n-k}{\phi-k/2}\binom{k}{k/2}P_k(j).$$

It then follows that

$$\begin{aligned} \sum_{i=0}^{n}\alpha_i(d_z)P_i(y) &= \sum_{i=0}^{n}\sum_{k=0}^{n}\binom{n-k}{\theta-k/2}\binom{k}{k/2}P_k(i)P_i(y) \\ &= \sum_{k=0}^{n}\binom{n-k}{\theta-k/2}\binom{k}{k/2}\sum_{i=0}^{n}P_k(i)P_i(y) \\ &= 2^n\binom{n-y}{\theta-y/2}\binom{y}{y/2}, \end{aligned}$$

where in the last step we use (16). Similarly we have

$$\sum_{j=0}^{n}\beta_j(d_x)P_j(x) = 2^n\binom{n-x}{\phi-x/2}\binom{x}{x/2},$$

Hence

$$f(x,y) = 2^{2n}\binom{n-x}{\phi-x/2}\binom{x}{x/2}\binom{n-y}{\theta-y/2}\binom{y}{y/2}.$$

For later use, we define the binary entropy function

$$H(x) = -x\log x - (1-x)\log(1-x),$$

for $0 \leqslant x \leqslant 1$. Taking into account that

$$\frac{1}{n}\log\binom{n}{k} = H\left(\frac{k}{n}\right) + O\left(\frac{1}{n}\right) \tag{25}$$

and denoting $\xi = x/n$, $\eta = y/n$, $\tau = \phi/n$ and $\sigma = \theta/n$, we get

$$\begin{aligned}
&\frac{1}{n}\log\left[\binom{n-x}{\phi-x/2}\binom{x}{x/2}\binom{n-y}{\theta-y/2}\binom{y}{y/2}\right]\\
&\quad= \frac{1}{n}\log\binom{n-x}{\phi-x/2} + \frac{1}{n}\log\binom{x}{x/2}\\
&\qquad+\frac{1}{n}\log\binom{n-y}{\theta-y/2} + \frac{1}{n}\log\binom{y}{y/2}\\
&\quad= (1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big) + \xi\\
&\qquad+(1-\eta)H\Big(\frac{\sigma-\eta/2}{1-\eta}\Big) + \eta + O\Big(\frac{1}{n}\Big).
\end{aligned}$$

This yields

$$\begin{aligned}
\frac{1}{n}\log f(x,y) &= 2+\xi+\eta+(1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big)\\
&\quad+(1-\eta)H\Big(\frac{\sigma-\eta/2}{1-\eta}\Big)+O\Big(\frac{1}{n}\Big). \quad (26)
\end{aligned}$$

To derive an estimate for $\alpha_{x,y} = \alpha_y(d_x)\alpha_x(d_z)$, we need bounds on values of Krawtchouk polynomials. Recall that by (20)

$$\gamma_\phi = \frac{r_\phi}{n} = \frac{1}{2} - \sqrt{\tau(1-\tau)} + o(1), \quad (27)$$

and

$$\gamma_\theta = \frac{r_\theta}{n} = \frac{1}{2} - \sqrt{\sigma(1-\sigma)} + o(1). \quad (28)$$

We also recall the following equations, see [20]:

$$\begin{aligned}
&\frac{1}{n}\log P_\phi(x)\\
&\quad= H(\tau)+\int_0^\xi \log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz\\
&\qquad+O\Big(\frac{1}{n}\Big), \quad (29)
\end{aligned}$$

for $\xi < \gamma_\phi$ and

$$\begin{aligned}
&\frac{1}{n}\log P_\theta(y)\\
&\quad= H(\sigma)+\int_0^\eta \log\Big(\frac{1-2\sigma+\sqrt{(1-2\sigma)^2-4z(1-z)}}{2(1-z)}\Big)dz\\
&\qquad+O\Big(\frac{1}{n}\Big), \quad (30)
\end{aligned}$$

for $\eta < \gamma_\theta$. Hence we obtain

$$\begin{aligned}
&\frac{1}{n}\log \alpha_{x,y}\\
&\quad= \frac{1}{n}\log\Big((P_\theta(x))^2(P_\phi(y))^2\Big)\\
&\quad= 2H(\tau)+2\int_0^\xi \log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz\\
&\qquad+2H(\sigma)+2\int_0^\eta \log\Big(\frac{1-2\sigma+\sqrt{(1-2\sigma)^2-4z(1-z)}}{2(1-z)}\Big)dz\\
&\qquad+O\Big(\frac{1}{n}\Big). \quad (31)
\end{aligned}$$

Now we are in a position to give the Hamming type bound.

Theorem 17 (Hamming-Type Bound): Let $\tau = \left\lfloor \frac{d_x-1}{2} \right\rfloor/n$ *and* $\sigma = \left\lfloor \frac{d_z-1}{2} \right\rfloor/n$. *Define*

$$\begin{aligned}
\Omega_\tau(\xi) &:= \xi + (1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big) - 2H(\tau)\\
&\quad -2\int_0^\xi \log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz.
\end{aligned}$$

Suppose that $2\tau < \gamma_\phi$ *and* $2\sigma < \gamma_\theta$ *where* γ_ϕ *and* γ_θ *are given in (27) and (28), respectively. Then for an* $((n, K, d_z/d_x))$ *quantum code we have*

$$\frac{\log K}{n} \leqslant 1 + \max_{0\leqslant\xi\leqslant 2\tau}\Big\{\Omega_\tau(\xi)\Big\} + \max_{0\leqslant\eta\leqslant 2\sigma}\Big\{\Omega_\sigma(\eta)\Big\} + o(1).$$

Proof: It can be easily verified that the polynomial $f(x, y)$ of (24) satisfies all the conditions of Lemma 13. So we get from (26), (31) and Lemma 13 that

$$\begin{aligned}
&\frac{\log K}{n}\\
&\leqslant -1 + \max_{\substack{0\leqslant x<d_x, 2|x\\ 0\leqslant y<d_z, 2|y}}\Big\{\frac{1}{n}\log f(x,y) - \frac{1}{n}\log \alpha_{x,y}\Big\}\\
&= -1 + \max_{\substack{0\leqslant x\leqslant 2\phi, 2|x\\ 0\leqslant y\leqslant 2\theta, 2|y}}\Big\{\frac{1}{n}\log f(x,y) - \frac{1}{n}\log \alpha_{x,y}\Big\}\\
&= 1 + \max_{0\leqslant\xi\leqslant 2\tau}\Big\{\xi + (1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big) - 2H(\tau)\\
&\quad -2\int_0^\xi \log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz\Big\}\\
&\quad + \max_{0\leqslant\eta\leqslant 2\sigma}\Big\{\eta + (1-\eta)H\Big(\frac{\sigma-\eta/2}{1-\eta}\Big) - 2\,H(\sigma)\\
&\quad -2\int_0^\eta \log\Big(\frac{1-2\sigma+\sqrt{(1-2\sigma)^2-4z(1-z)}}{2(1-z)}\Big)dz\Big\}\\
&\quad + o(1),
\end{aligned}$$

where in the third step we use the fact that $\xi = x/n \leqslant 2\phi/n = 2\tau < \gamma_\phi$ and $\eta = y/n \leqslant 2\theta/n = 2\sigma < \gamma_\theta$. This completes the proof. □

Matlab shows that the function in Theorem 17 achieves its maximum at $\xi = 0$ and $\eta = 0$ for any $2\tau < \gamma_\phi$ and $2\sigma < \gamma_\theta$. A straightforward calculation gives that

$$h(x) = 2x + \sqrt{x(1-x)} - 1/2$$

is a monotone increasing function in x if $0 \leqslant x \leqslant 1/2$. Denote $\delta_x = d_x/n$ and $\delta_z = d_z/n$. Assume that $0 \leqslant \delta_x \leqslant 1/5$. Then we have $\tau = \left\lfloor \frac{d_x-1}{2} \right\rfloor/n < d_x/2n = \delta_x/2$. Let $\Delta = h'(1/10)(\tau - 1/10) < 0$ where h' denotes the first derivative of h. Then we have

$$\frac{h(1/10) - h(\tau)}{1/10 - \tau} = h'(\vartheta) > h'(1/10),$$

where $\tau < \vartheta < 1/10$. Since $h(1/10) = 0$, then

$$h(\tau) < h'(1/10)(\tau - 1/10) = \Delta.$$

It follows that $2\tau < 1/2 - \sqrt{\tau(1-\tau)} + \Delta \leqslant \gamma_\phi$ by noting that $\Delta < o(1)$ for n sufficiently large. Therefore we conclude that if $0 \leqslant \delta_x \leqslant 1/5$ and $0 \leqslant \delta_z \leqslant 1/5$ then $2\tau < \gamma_\phi$ and $2\sigma < \gamma_\theta$. This means the conventional Hamming bound is valid when $0 \leqslant \delta_x \leqslant 1/5$ and $0 \leqslant \delta_z \leqslant 1/5$.

Corollary 18: The conventional Hamming bound is valid for quantum codes, i.e., if Q is an $((n, K, d_z/d_x))$ quantum code then

$$\frac{\log K}{n} \leqslant 1 - H\left(\frac{\delta_x}{2}\right) - H\left(\frac{\delta_z}{2}\right) + o(1),$$

where $\delta_x = d_x/n$ and $\delta_z = d_z/n$ stand for the relative distances of the code, $0 \leqslant \delta_x \leqslant 1/5$ and $0 \leqslant \delta_z \leqslant 1/5$.

Proof: Taking $\xi = 0$ and $\eta = 0$ in Theorem 17 yields that

$$\begin{aligned}\frac{\log K}{n} &\leqslant 1 - H(\tau) - H(\sigma) + o(1)\\ &= 1 - H\left(\frac{\delta_x}{2}\right) - H\left(\frac{\delta_z}{2}\right) + o(1),\end{aligned}$$

where in the last step we use the fact $H(\tau) = H(\delta_x/2) + o(1)$ and $H(\sigma) = H(\delta_z/2) + o(1)$. □

C. THE FIRST LINEAR PROGRAMMING BOUND

To get the first linear programming bound for an $((n, K, d_z/d_x))$ code, one has to choose integers s and t such that

$$\frac{t}{n} = \frac{1}{2} - \sqrt{\delta_x(1-\delta_x)} + o(1),$$
$$\frac{s}{n} = \frac{1}{2} - \sqrt{\delta_z(1-\delta_z)} + o(1),$$

where $\delta_x = d_x/n$, $\delta_z = d_z/n$. Then we choose integers a and b such that $r_{t+1} < a < r_t$, $r_{s+1} < b < r_s$, $P_t(a)/P_{t+1}(a) = -1$ and $P_s(b)/P_{s+1}(b) = -1$. Define

$$f(x, y) = F(x)F(y), \tag{32}$$

where

$$F(x) = \frac{1}{a-x}\left\{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\right\}^2,$$
$$G(y) = \frac{1}{b-y}\left\{P_{s+1}(y)P_s(b) - P_s(y)P_{s+1}(b)\right\}^2.$$

This polynomial (32) will yield the first linear programming bound for classical codes over $\mathbb{F}_4$ [1], [25], [28]. By the Christoffel-Darboux formula (18)

$$\begin{aligned}F(x) &= \frac{2}{t+1}\binom{n}{t}\left\{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\right\}\\ &\quad\times \sum_{i=0}^{t}\frac{P_i(x)P_i(a)}{\binom{n}{i}}\\ &= \frac{2}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{\binom{n}{i}}\left\{P_{t+1}(x)P_i(x)+P_t(x)P_i(x)\right\}.\end{aligned}$$

It follows from Lemma 16 that

$$\begin{aligned}F(x) &= \frac{2}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{\binom{n}{i}}\\ &\quad\times\left\{\sum_{j=0}^{n}P_j(x)\binom{n-j}{(t+1+i-j)/2}\binom{j}{(t+1-i+j)/2}\right.\\ &\quad\left.+\sum_{j=0}^{n}P_j(x)\binom{n-j}{(t+i-j)/2}\binom{j}{(t-i+j)/2}\right\}\\ &= \sum_{j=0}^{n}P_j(x)\frac{2}{t+1}\binom{n}{t}P_t(a)\sum_{i=0}^{t}\frac{P_i(a)}{\binom{n}{i}}\\ &\quad\times\left\{\binom{n-j}{(t+1+i-j)/2}\binom{j}{(t+1-i+j)/2}\right.\\ &\quad\left.+\binom{n-j}{(t+i-j)/2}\binom{j}{(t-i+j)/2}\right\}\\ &= \sum_{j=0}^{n}P_j(x)F_j,\end{aligned}$$

where we use the symbol F_j to denote the coefficient of $P_j(x)$. Taking $j = x$ and estimating F_x by the term with $i = t$, we obtain

$$\begin{aligned}F_x &\geqslant \frac{2}{t+1}\binom{n}{t}\frac{P_t(a)^2}{\binom{n}{t}}\binom{n-x}{t-x/2}\binom{x}{x/2}\\ &= \frac{2}{t+1}P_t(a)^2\binom{n-x}{t-x/2}\binom{x}{x/2}.\end{aligned}$$

Denote $\xi = x/n$, $\tau = t/n$. Similarly to the derivation of the Hamming bound, we have

$$\begin{aligned}&\frac{1}{n}\log\left\{\binom{n-x}{t-x/2}\binom{x}{x/2}\right\}\\ &\qquad= (1-\xi)H\left(\frac{\tau-\xi/2}{1-\xi}\right) + \xi + O\left(\frac{1}{n}\right).\end{aligned} \tag{33}$$

Then, using (15), we get

$$\begin{aligned}\frac{F(x)}{F_x} &\leqslant \frac{(t+1)P_t(a)^2\{P_{t+1}(x)+P_t(x)\}^2}{2(a-x)P_t(a)^2\binom{n-x}{t-x/2}\binom{x}{x/2}}\\ &= \frac{(t+1)\left\{\frac{\binom{n}{t+1}P_x(t+1)}{\binom{n}{x}} + \frac{\binom{n}{t}P_x(t)}{\binom{n}{x}}\right\}^2}{2(a-x)\binom{n-x}{t-x/2}\binom{x}{x/2}}\\ &= \frac{(t+1)\binom{n}{t}^2\left\{\frac{n-t}{t+1}P_x(t+1)+P_x(t)\right\}^2}{2(a-x)\binom{n}{x}^2\binom{n-x}{t-x/2}\binom{x}{x/2}}.\end{aligned}$$

It then follows from (15) and (19) that

$$\frac{F(x)}{F_x} \leqslant \frac{P_t(x)^2\left\{\frac{n-2x+\sqrt{(n-2x)^2-4t(n-t)}}{2}+t+1\right\}^2}{2(a-x)(t+1)\binom{n-x}{t-x/2}\binom{x}{x/2}}.$$

Taking logarithm on both sides and dividing by n, we obtain from (25), (29) and (33) that

$$\begin{aligned}&\frac{1}{n}\log\frac{F(x)}{F_x}\\&\leqslant 2\int_0^{\xi}\log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz\\&\quad+2H(\tau)-(1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big)-\xi+O\Big(\frac{1}{n}\Big),\end{aligned}\tag{34}$$

for $\xi<\gamma_\phi$, where γ_ϕ is given in (27). By a similar argument as above, we have

$$G(y)=\sum_{i=0}^{n}P_i(y)G_i,$$

where G_i is the coefficient of $P_i(y)$ defined by

$$\begin{aligned}G_i=&\frac{2}{s+1}\binom{n}{s}P_s(b)\sum_{j=0}^{s}\frac{P_j(b)}{\binom{n}{j}}\\&\times\Big\{\binom{n-i}{(s+1+j-i)/2}\binom{i}{(s+1-j+i)/2}\\&+\binom{n-i}{(s+j-i)/2}\binom{i}{(s-j+i)/2}\Big\}.\end{aligned}$$

Consequently we obtain

$$\begin{aligned}&\frac{1}{n}\log\frac{G(y)}{G_y}\\&\leqslant 2\int_0^{\eta}\log\Big(\frac{1-2\sigma+\sqrt{(1-2\sigma)^2-4z(1-z)}}{2(1-z)}\Big)dz\\&\quad+2H(\sigma)-(1-\eta)H\Big(\frac{\sigma-\eta/2}{1-\eta}\Big)-\eta+O\Big(\frac{1}{n}\Big),\end{aligned}\tag{35}$$

for $\eta<\gamma_\theta$, where $\sigma=s/n$, $\eta=y/n$ and γ_θ is given in (28).

With the above preparation, we can get the following theorem.

Theorem 19: Let $\delta_x=d_x/n$, $\delta_z=d_z/n$, $\tau=\frac{1}{2}-\sqrt{\delta_x(1-\delta_x)}$ and $\sigma=\frac{1}{2}-\sqrt{\delta_z(1-\delta_z)}$. Further let

$$\begin{aligned}\Gamma_\tau(\xi):=2\int_0^{\xi}&\log\Big(\frac{1-2\tau+\sqrt{(1-2\tau)^2-4z(1-z)}}{2(1-z)}\Big)dz\\&+2H(\tau)-(1-\xi)H\Big(\frac{\tau-\xi/2}{1-\xi}\Big)-\xi.\end{aligned}$$

Suppose that $\delta_x<\gamma_\phi$ and $\delta_z<\gamma_\theta$. Then for an $((n,K,d_z/d_x))$ code, we have

$$\frac{\log K}{n}\leqslant -1+\max_{0\leqslant\xi<\delta_x}\Big\{\Gamma_\tau(\xi)\Big\}+\max_{0\leqslant\eta<\delta_z}\Big\{\Gamma_\sigma(\eta)\Big\}+o(1).$$

Proof: One verifies that the polynomial $f(x,y)$ of (32) satisfies all the conditions of Lemma 12. Therefore applying Lemma 12, (34) and (35) gives that

$$\frac{\log K}{n}\leqslant\max_{0\leqslant x<d_x}\Big\{\frac{1}{n}\log\frac{F(x)}{F_x}\Big\}+\max_{0\leqslant y<d_z}\Big\{\frac{1}{n}\log\frac{G(y)}{G_y}\Big\}-1+O\Big(\frac{1}{n}\Big).$$

The desired assertion follows immediately by taking $\xi=x/n$ and $\eta=y/n$. This completes the proof. □

Computations with Matlab show that this function achieves its minimum at $\xi=0$ and $\eta=0$ for any $\delta_x\leqslant 0.1865$ and $\delta_z\leqslant 0.1865$.

Corollary 20 (The First Linear Programming Bound): If $0\leqslant\delta_x\leqslant 0.1865$ and $0\leqslant\delta_z\leqslant 0.1865$ then the conventional linear programming bound is valid for quantum codes, i.e., if Q is an $((n,K,d_z/d_x))$ quantum code then

$$\frac{\log K}{n}\leqslant H\Big(\frac{1}{2}-\sqrt{\delta_x(1-\delta_x)}\Big)+H\Big(\frac{1}{2}-\sqrt{\delta_z(1-\delta_z)}\Big)-1+o(1).$$

A straightforward computation gives that when $\delta_x=\delta_z=0.1865$, $\log K/n\approx 0.0028$. So for all $0.0028\leqslant\log K/n\leqslant 1$, the conventional first linear programming bound is valid.

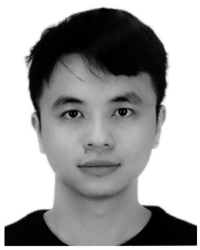
ACKNOWLEDGMENT

Prof. S. S.-T. Yau is grateful to National Center for Theoretical Sciences (NCTS) for providing excellent research environment while part of this research was done.

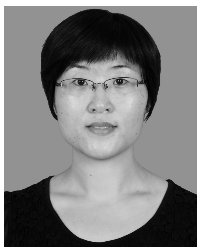
REFERENCES

[1] M. Aaltonen, "Linear programming bounds for tree codes," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 1, pp. 85–90, Jan. 1979.
[2] M. Aaltonen, "A new upper bound on nonbinary block codes," *Discrete Math.*, vol. 83, nos. 2–3, pp. 139–160, Aug. 1990.
[3] S. A. Aly, "Asymmetric and symmetric subsystem BCH codes and beyond," 2008, *arXiv:0803.0764*. [Online]. Available: https://arxiv.org/abs/0803.0764
[4] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206–1215, May 1999.
[5] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn, "Quantum error detection .I. Statement of the problem," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 778–788, May 2000.
[6] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn, "Quantum error detection .II. Bounds," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 789–800, May 2000.
[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 5, pp. 3824–3851, 1996.
[8] A. K. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett*, vol. 78, nos. 3–20, pp. 405–408, 1997.
[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[10] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 6, pp. 4054–4059, Jun. 1997.
[11] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res.Reports Supplements*, vol. 10, 1973.
[12] C. Ding, "The weight distribution of some irreducible cyclic codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 955–960, Mar. 2009.
[13] M. Durdevich, H. E. Makaruk, and R. Owczarek, "Generalized noiseless quantum codes utilizing quantum enveloping algebras," *J. Phys. A, Math. Gen.*, vol. 34, no. 7, pp. 1423–1437, Feb. 2000.
[14] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett.*, vol. 77, no. 12, pp. 2585–2588, Sep. 1996.
[15] K. Feng and C. Xing, "A new construction of quantum error-correcting codes," *Trans. Amer. Math. Soc.*, vol. 360, no. 4, pp. 2007–2019, Apr. 2008.
[16] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 986–991, Mar. 2006.
[17] A. S. Fletcher, P. W. Shor, and M. Z. Win, "Channel-adapted quantum error correction for the amplitude damping channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5705–5718, Dec. 2008.

[18] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 3, Art. no. 032345, Mar. 2007.
[19] F. Huber, C. Eltschka, J. Siewert, and O. Gühne, "Bounds on absolutely maximally entangled states from shadow inequalities, and the quantum MacWilliams identity," *J. Phys. A, Math. Theor.*, vol. 51, no. 17, 2018, Art. no. 175301.
[20] G. Kalai and N. Linial, "On the distance distribution of codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1467–1472, Sep. 1995.
[21] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, pp. 900–911, Oct. 1997.
[22] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, Feb. 1997.
[23] E. Knill, R. Laflamme, and L. Viola, "Theory of quantum error correction for general noise," *Phys. Rev. Lett.*, vol. 84, no. 11, pp. 2525–2528, Mar. 2000.
[24] K. Kraus, *States, Effects, and Operations Fundamental Notions of Quantum Theory*. Berlin, Germany: Springer-Verlag, 1983.
[25] C.-Y. Lai and A. Ashikhmin, "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 622–639, Jan. 2018.
[26] C.-Y. Lai, M.-H. Hsieh, and H.-F. Lu, "On the MacWilliams identity for classical and quantum convolutional codes," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3148–3159, Aug. 2016.
[27] T. Laihonen and S. Litsyn, "On upper bounds for minimum distance and covering radius of non-binary codes," *Des., Codes Cryptogr.*, vol. 14, no. 1, pp. 71–80, Apr. 1998.
[28] V. I. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Trans. Inf. Theory*, vol. 41, no. 5, pp. 1303–1321, Sep. 1995.
[29] C. Li, Q. Yue, and F. Li, "Weight distributions of cyclic codes with respect to pairwise coprime order elements," *Finite Fields Appl.*, vol. 28, pp. 94–114, Jul. 2014.
[30] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inf. Theory*, vol. 23, no. 2, pp. 157–166, Mar. 1977.
[31] F. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, no. 1, pp. 79–94, Jan. 1963.
[32] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York, NY, USA: North-Holland, 1977.
[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[34] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1388–1394, Jul. 1998.
[35] E. M. Rains, "Quantum shadow enumerators," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2361–2366, Nov. 1999.
[36] P. K. Sarvepalli, M. Röetteler, and A. Klappenecker, "Asymmetric quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, Jul. 2008, pp. 305–309.
[37] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. 2493–2496, Oct. 1995.
[38] P. W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, no. 8, pp. 1600–1602, Feb. 1997.
[39] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, Jul. 1996.
[40] A. Steane, "Multiple particle interference and quantum error correction," *Proc., Math., Phys. Eng. Sci.*, vol. 452, no. 1954, pp. 2551–2557, Nov. 1996.
[41] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: Constructions, bounds and performance," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 465, pp. 1645–1672, Mar. 2009.
[42] G. Vega, "The weight distribution of an extended class of reducible cyclic codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4862–4869, Jul. 2012.
[43] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: Characterization and constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2938–2945, Jun. 2010.
[44] Y. Xu, D. Wang, and J. Chen, "Analogues of quantum schubert cell algebras in PBW-deformations of quantum groups," *J. Algebra Appl.*, vol. 15, no. 10, 2015, Art. no. 1650179.
[45] S. Yang, Z.-A. Yao, and C.-A. Zhao, "The weight enumerator of the duals of a class of cyclic codes with three zeros," *Applicable Algebra Eng., Commun. Comput.*, vol. 26, no. 4, pp. 347–367, Aug. 2015.
[46] S. Yang, X. Kong, and C. Tang, "A construction of linear codes and their complete weight enumerators," *Finite Fields Appl.*, vol. 48, pp. 196–226, Nov. 2017.
[47] S. Yang and Z.-A. Yao, "Complete weight enumerators of a class of linear codes," *Discrete Math.*, vol. 340, no. 4, pp. 729–739, 2017.
[48] S. Yang, Z.-A. Yao, and C.-A. Zhao, "The weight distributions of two classes of p-ary cyclic codes with few weights," *Finite Fields Appl.*, vol. 44, pp. 76–91, Mar. 2017.
[49] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, no. 17, pp. 3306–3309, Oct. 1997.
[50] P. Zanardi and M. Rasetti, "Error avoiding quantum codes," *Mod. Phys. Lett. B*, vol. 11, no. 25, pp. 1085–1093, 1997.
[51] X. Zhang and L. Dong, "Braided mixed datums and their applications on Hom-quantum groups," *Glasgow Math. J.*, vol. 60, no. 1, pp. 231–251, Jan. 2018.



CHUANGQIANG HU was born in Guangdong, China, in 1989. He received the Ph.D. degree in mathematics from Sun Yat-sen University, Guangzhou, China, in 2017. Since 2017, he has been a Postdoctoral Researcher with the Yau Mathematical Sciences Center, Tsinghua University, Peking, China. His research fields are coding theory and algebraic geometry.



SHUDI YANG was born in Shandong, China, in 1979. She received the Ph.D. degree in mathematics from Sun Yat-sen University, Guangzhou, China, in 2016. From 2016 to 2019, she was a Postdoctoral Researcher with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. She is currently an Associate Professor with Qufu Normal University, China. Her research interests include exponential sums and coding theory.

STEPHEN S.-T. YAU received the Ph.D. degree in mathematics from the State University of New York at Stony Brook, NY, USA, in 1976. He was a member of the Institute of Advanced Study at Princeton (1976–1977) and (1981–1982), respectively, and a Benjamin Pierce Assistant Professor with Harvard University (1977–1980). After that, he joined the Department of Mathematics, Statistics and Computer Science (MSCS), University of Illinois at Chicago (UIC), and has served for over 30 years. From 2005 to 2011, he became a Joint-Professor with the Department of Electrical and Computer Engineering and MSCS, UIC. After his retirement, in 2012, he joined Tsinghua University, Beijing, China, where he is currently a Full-Time Professor with the Department of Mathematical Science. His research interests include nonlinear filtering, bioinformatics, complex algebraic geometry, CR geometry, and singularities theory. He was the General Chairman of the IEEE International Conference on Control and Information, which was held in The Chinese University of Hong Kong, in 1995. He received the Sloan Fellowship, in 1980; the Guggenheim Fellowship, in 2000; the IEEE Fellow Award, in 2003; and the AMS Fellow Award, in 2013. He is the Managing Editor and a founder of the *Journal of Algebraic Geometry*, since 1991, and the Editors-in-Chief and founder of *Communications in Information and Systems*, since 2000. In 2005, he was entitled the UIC Distinguished Professor.