On the complete weight distributions of quantum error-correcting codes

Chao Du(杜超)[1,2], Zhi Ma(马智)[1,2,†], and Maosheng Xiong(熊茂胜)[3,‡]

[1] *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhenghzhou* 450001, *China*
[2] *Henan Key Laboratory of Network Cryptography Technology, Zhenghzhou* 450001, *China*
[3] *Department of Mathematics, Hong Kong University of Science and Technology, Hong Kong, China*

(Received 7 September 2022; revised manuscript received 15 December 2022; accepted manuscript online 16 December 2022)

In a recent paper, Hu *et al.* defined the complete weight distributions of quantum codes and proved the MacWilliams identities, and as applications they showed how such weight distributions may be used to obtain the singleton-type and hamming-type bounds for asymmetric quantum codes. In this paper we extend their study much further and obtain several new results concerning the complete weight distributions of quantum codes and applications. In particular, we provide a new proof of the MacWilliams identities of the complete weight distributions of quantum codes. We obtain new information about the weight distributions of quantum MDS codes and the double weight distribution of asymmetric quantum MDS codes. We get new identities involving the complete weight distributions of two different quantum codes. We estimate the complete weight distributions of quantum codes under special conditions and show that quantum BCH codes by the Hermitian construction from primitive, narrow-sense BCH codes satisfy these conditions and hence these estimate applies.

Keywords: quantum codes, complete weight distributions, MacWilliams identities, BCH codes

PACS: 03.67.Lx, 03.67.Pp **DOI:** 10.1088/1674-1056/acac09

1. Introduction

Quantum error-correcting codes (QECCs for short) protect quantum information against noise. They play important roles in many areas of quantum information theory, but most critically, in the viability of a quantum computer. Since the pioneering work in Refs. [1–5], the theory of QECCs has been rapidly developed. It has received much attention in the past two decades and remains one of the most actively studied research areas.

In the quantum world, the common error model is the Pauli errors X, Z, and $Y = \mathrm{i}XZ$ acting on qubits. More efficient codes can be designed if further information about the error process is available. Therefrom, a lot of work on designing codes has been carried out.[6–8] In 1997, Shor and Laflamme[9] introduced the weight distributions of quantum codes and proved that they satisfy the MacWilliams identity. As in classical coding theory, the weight distributions of quantum codes are invariants and give much information about codes and errors. For example, the minimum distance can be read off from the weight distributions of quantum codes and thus the error correcting capability of the codes. Various other kinds of weight distributions of quantum codes were defined and studied in Refs. [10–13], which could be used in many other things to effectively determine whether certain good quantum codes exist. Linear programming bounds were obtained by using the quantum MacWilliams identity.[14,15] The weight distributions of quantum codes can be used to compute the probability of failure for quantum error correction in the codes,[16,17] etc.

In the classical coding theory, the complete weight distribution of linear codes contains much more detailed information than the weight distribution, and therefore it is more general and useful. The complete weight distribution of a classical code enumerates the codewords according to the number of symbols of each kind in a codeword. This was used to analyze the error performance of the code. For example, the complete weight distribution is useful in soft decision decoding,[18] and it was employed to calculate the deception probabilities of certain authentication codes.[19] Many aspects of the complete weight distributions of linear codes, including the MacWilliams identity, can be found in Ref. [20].

In a recent paper,[21] Hu *et al.* defined the quantum version of the complete and double weight distributions for the first time and proved that they satisfy the MacWilliams identity. Error operators are usually the tensor product of Pauli operators. As in the classical coding setting, the quantum complete weight distribution enumerates the error operators according to the number of Pauli symbols of each kind (X, Z, or XZ) in an operator. Moreover, noise is often unbalanced between bit-flip (X-type) and phase-flip (Z-type) errors, and there is also a difference in the number of blocks of X-type and Z-type inside an error operator on a multi-qubit system. The double weight distribution usually enumerates the error operators in terms of the number of Pauli X-symbol and Z-

†Corresponding author. E-mail: ma_zhi@163.com
‡Corresponding author. E-mail: mamsxiong@ust.hk

© 2023 Chinese Physical Society and IOP Publishing Ltd

symbol inside. In fact, in Ref. [21], the authors showed how these results imply the MacWilliams identity for the double weight distributions of quantum codes, which in turn was employed, in combination with the linear programming approach, to obtain the singleton-like and hamming-like bounds for arbitrary asymmetric quantum codes. This work was built upon their previous work[22] where similar results were obtained for binary quantum codes.

The purpose of this paper is to extend the study of the complete weight distributions of quantum codes much further. We obtain several new results concerning the complete weight distributions of quantum codes and their applications. Firstly, in Section 3, we provide a new proof of the MacWilliams identities for the complete weight distributions of quantum codes (see Theorem 4). Compared with Ref. [21], our proof is more aligned with the original paper[9] where the MacWilliams identities were first proved for the weight distributions of quantum codes, and our formulation of the MacWilliams identities closely resembles that of the classical coding setting. Given the importance of the complete weight distributions of quantum codes and the MacWilliams identities in the theory of QECC, a new proof is useful. Secondly, in Section 4, we show that a more careful analysis of the linear programming approach used in Refs. [14,21] can reveal a lot of new information about the weight distributions of quantum MDS codes and the double weight distributions of asymmetric quantum MDS codes respectively. Here we recover a recent result (see Theorem 9 and Ref. [23]) by a completely different method. Thirdly, in Section 5 we obtain new identities concerning the complete weight distributions of two distinct quantum codes (see Theorem 8). Fourthly, in Section 6 we show that the complete weight distributions of quantum codes can be effectively estimated under certain conditions (Theorem 10). These conditions look quite restrictive. However, we show in Section 7 that a large family of quantum BCH codes obtained by the Hermitian construction from primitive, narrow-sense BCH codes satisfy these conditions (Theorem 12). This can be considered as a quantum analogue of Ref. [24] where similar estimates were obtained on the complete weight distributions for a large family of subfield subcodes of algebraic geometric codes. Also in this paper, whenever possible, we obtain similar results for the double weight distributions of quantum codes.

2. Preliminaries

Classical error-correcting codes have many critical applications, especially the classical linear codes, which develop a wide variety of good QECCs. In this section, we give a brief review of quantum and classical linear coding theory. For further details, the readers can refer to Refs. [20,25–30]. In what follows, we always assume that $\mathbb{F}_q$ is a finite field of order q where $q = p^m$, p is a prime, and $m \geqslant 1$.

2.1. The classical linear error-correcting codes

Definition 1[20] Each nonzero k-dimensional linear vector subspace of $\mathbb{F}_q^n$ is a so-called $[n,k]_q$ classical linear error-correcting code, usually denoted by $\mathcal{C}$. The symbol n is the length of $\mathcal{C}$. A vector in $\mathcal{C}$ is called a codeword of $\mathcal{C}$. The number of codewords in $\mathcal{C}$ is $|\mathcal{C}|$ and satisfies $1 \leq |\mathcal{C}| \leq q^n$.

We also need a concept to measure the error correcting ability of $\mathcal{C}$. Denote $\mathrm{wt}(c)$ by the Hamming weight of the codeword $c \in \mathcal{C}$. If the integer d is the minimum Hamming weight for all codewords in $\mathcal{C}$, then d is called the minimum distance of $\mathcal{C}$, and $\mathcal{C}$ is also an $[n,k,d]_q$ code.

Theorem 1[20] If the minimum distance of $\mathcal{C}$ is d, then the code $\mathcal{C}$ can detect the errors with weight $\leq d-1$, and correct the errors with weight $\leq \lfloor \frac{d-1}{2} \rfloor$.

Denote by A_i the number of codewords in $\mathcal{C}$ with Hamming weight i. We call the numbers A_i's the weight distributions of $\mathcal{C}$, where

$$A_i = \#\{\boldsymbol{c} \in \mathcal{C} | \mathrm{wt}(\boldsymbol{c}) = i\}. \tag{1}$$

The weight distributions A_i's are important parameters of $\mathcal{C}$ because they contain much useful information. For example, the dimension can be read off from the equation $A_0 + A_1 + \cdots + A_n = q^k$, and the minimum distance is $d = \min\{i | 1 \leq i \leq n, A_i \geq 1\}$. The weight enumerator of $\mathcal{C}$ is defined by the polynomial

$$W_{\mathcal{C}}(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^n. \tag{2}$$

Moreover, if we order the elements of $\mathbb{F}_q$ explicitly as $u_0 = 0, u_1, \ldots, u_{q-1}$, then for any $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$, the complete weight of $\boldsymbol{c}$ is denoted by

$$\mathrm{Comp}(\boldsymbol{c}) = (w_0, w_1, \ldots, w_{q-1}), \tag{3}$$

where $w_i := w_i(c) = \#\{1 \leq j \leq n | c_j = u_i\}$ and $\sum_{i=0}^{q-1} w_i = n$. Denote $\Sigma^{n,q}$ by the set of all integer vectors $\boldsymbol{t} = (t_0, t_1, \ldots, t_{q-1})$ where $t_i \geq 0$ for all i and $\sum_{i=0}^{q-1} t_i = n$. Then the complete weight distribution is denoted by the sequence $(A_{\boldsymbol{t}})_{\boldsymbol{t}}$ of $\mathcal{C}$, where

$$A_{\boldsymbol{t}} := \#\{\boldsymbol{c} \in \mathcal{C} : \mathrm{Comp}(\boldsymbol{c}) = \boldsymbol{t}\}, \quad \forall \boldsymbol{t} \in \Sigma^{n,q}. \tag{4}$$

Furthermore, the complete weight enumerator of $\mathcal{C}$ is defined by the polynomial in variables $z_0, \ldots, z_{q-1}$,

$$W_{\mathcal{C}}(z_0, z_1, \ldots, z_{q-1}) := \sum_{\boldsymbol{c} \in \mathcal{C}} z_0^{w_0} z_1^{w_1} \cdots z_{q-1}^{w_{q-1}} = \sum_{\boldsymbol{t}} A_{\boldsymbol{t}} \boldsymbol{z}^{\boldsymbol{t}}, \tag{5}$$

where $\boldsymbol{t} = (t_0, t_1, \ldots, t_{q-1})$ runs over all $\boldsymbol{t} \in \Sigma^{n,q}$ and $\boldsymbol{z}^{\boldsymbol{t}} := z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}$.

For a linear code $\mathcal{C}$, it can be determined by an $(n-k) \times n$ parity-check matrix H, i.e., $\mathcal{C} = \{\boldsymbol{c} \in \mathbb{F}_q^n | H\boldsymbol{c}^{\mathrm{T}} = 0\}$. Accordingly, there exists a $k \times n$ generator matrix G satisfying $HG^{\mathrm{T}} = 0$. The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is an $[n, n-k, d]_q$ linear

code orthogonal to $\mathcal{C}$, i.e., $\mathcal{C}^{\perp}=\{\boldsymbol{c}'\in\mathbb{F}_q^n|\boldsymbol{c}'\cdot c^{\mathrm{T}}=0,\forall c\in\mathcal{C}\}$. If $\mathcal{C}\subset\mathcal{C}^{\perp}$, $\mathcal{C}$ is called a self-orthogonal code; if $\mathcal{C}=\mathcal{C}^{\perp}$, then $\mathcal{C}$ is a self-dual code. Obviously, G is the parity-check matrix of $\mathcal{C}^{\perp}$.

The weight distribution of dual code $\mathcal{C}^{\perp}$ is

$$A_i^{\perp}:=\#\{\boldsymbol{c}\in\mathcal{C}^{\perp}|\mathrm{wt}(\boldsymbol{c})=i\},\tag{6}$$

and the corresponding weight enumerator is

$$W_{\mathcal{C}^{\perp}}(x,y)=\sum_{i=0}^{n}A_i^{\perp}x^{n-i}y^n.\tag{7}$$

For any $\boldsymbol{t}\in\Sigma^{n,q}$, the complete distribution and complete weight enumerator are denoted by

$$A_{\boldsymbol{t}}^{\perp}:=\#\{\boldsymbol{c}\in\mathcal{C}^{\perp}:\mathrm{Comp}(\boldsymbol{c})=\boldsymbol{t}\},\tag{8}$$

and

$$W_{\mathcal{C}^{\perp}}(z_0,z_1,\ldots,z_{q-1})=\sum_{\boldsymbol{t}}A_{\boldsymbol{t}}^{\perp}\boldsymbol{z}^{\boldsymbol{t}}.\tag{9}$$

Let $\mathbb{C}$ be the complex field and $\mathbb{C}^*=\mathbb{C}\backslash\{0\}$. Denote by $\psi:\mathbb{F}_q\to\mathbb{C}^*$ the standard additive character. The fundamental relations between the weight enumerators of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are given by MacWilliams identities[20]

$$W_{\mathcal{C}^{\perp}}(x,y)=\frac{1}{q^k}W_{\mathcal{C}}(x+(q-1)y,x-y),\tag{10}$$

$$W_{\mathcal{C}^{\perp}}(z_0,z_1,\ldots,z_{q-1})=\frac{1}{q^k}W_{\mathcal{C}}(x_0,x_1,\ldots,x_{q-1}),\tag{11}$$

where $x_i=\sum_{s=0}^{q-1}\psi(u_iu_s)z_s$ for $0\le i\le q-1$.

In addition, the linear codes satisfy an important bound named as the singleton bound.

Theorem 2[20] If the linear code $\mathcal{C}$ is an $[n,k,d]_q$ code, then $n-k\ge d-1$.

Furthermore, the codes with $d=n-k+1$ are called the maximum distance separable (MDS) codes, which are also known to be optimal. The name of MDS codes comes from the fact that such a code has the maximum possible distance between codewords, and that the codewords may be separated into message symbols and check symbols. Thus, there is a systematic encoder.[20]

2.2. Symmetric and asymmetric quantum codes

In this subsection, we first review some basic concepts about quantum error operators and quantum codes.

2.2.1. Nice error bases

Let $\mathbb{C}$ be the complex field and $\mathbb{C}^q$ be the state space of a q-ary quantum system. Denote by $\{|x\rangle\,|\,x\in\mathbb{F}_q\}$ an orthonormal basis of $\mathbb{C}^q$. For any $a,b\in\mathbb{F}_q$, the unitary operators X_a and Z_b on $\mathbb{C}^q$ are given by

$$X_a|x\rangle=|x+a\rangle,\ Z_b|x\rangle=\zeta_p^{\mathrm{tr}(xb)}|x\rangle,\quad\forall x\in\mathbb{F}_q.$$

Here $\zeta_p=\exp(2\pi\sqrt{-1}/p)$ is reserved for a primitive p-th root of unity, and $\mathrm{tr}(\cdot)$ denotes the trace map from $\mathbb{F}_q$ to the prime subfield $\mathbb{F}_p$. The set of error operators defined by

$$\mathcal{E}=\{X_aZ_b\,|\,a,b\in\mathbb{F}_q\}$$

forms an orthogonal basis of the space of operators on $\mathbb{C}^q$ under the inner product given by $\langle A,B\rangle=\mathrm{Tr}(A^{\dagger}B)$, where Tr is the trace of linear operators and $A^{\dagger}$ is the Hermitian transpose of A. For simplicity, we may identify the operator X_aZ_b with $(a|b)$ for $a,b\in\mathbb{F}_q$, hence $\mathcal{E}$ may be identified with the set $\mathbb{F}_q^2$. Define by the symplectic inner product of $(a|b)$ and $(a'|b')$ over $\mathbb{F}_q^2$ by

$$\langle(a|b),(a'|b')\rangle_s=\mathrm{tr}(a'b-ab').\tag{12}$$

For any $e=X_aZ_b,e'=X_{a'}Z_{b'}\in\mathcal{E}$, it is easy to see that e and e' satisfy the commutation relation

$$ee'=\zeta_p^{\langle(a|b),(a'|b')\rangle_s}e'e.$$

Each $(a|b)\in\mathbb{F}_q^2$ can identify an operator of $\mathcal{E}$. For convenience, we rewrite Eq. (12) as

$$\langle e,e'\rangle_s\triangleq\langle(a|b),(a'|b')\rangle_s=\mathrm{tr}(a'b-ab').\tag{13}$$

The operator e commutes with e' if and only if $\langle e,e'\rangle_s=0$.

Denote by $(\mathbb{C}^q)^{\otimes n}=\mathbb{C}^{q^n}$ the n-fold tensor product of $\mathbb{C}^q$. Its coordinate basis is given by

$$\{|\boldsymbol{x}\rangle=|x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_n\rangle\,|\,\boldsymbol{x}=(x_1,\ldots,x_n)\in\mathbb{F}_q^n\}.$$

For any $\boldsymbol{a}=(a_1,a_2,\ldots,a_n),\boldsymbol{b}=(b_1,b_2,\ldots,b_n)\in\mathbb{F}_q^n$, $\boldsymbol{a}\cdot\boldsymbol{b}=\sum_{i=1}^{n}a_ib_i$ denotes the usual inner product. The operator $\boldsymbol{e}=X_{\boldsymbol{a}}Z_{\boldsymbol{b}}$ acts on a basis element $|\boldsymbol{x}\rangle=|x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_n\rangle$ as

$$\boldsymbol{e}|\boldsymbol{x}\rangle=X_{a_1}Z_{b_1}|x_1\rangle\otimes X_{a_2}Z_{b_2}|x_2\rangle\otimes\cdots\otimes X_{a_n}Z_{b_n}|x_n\rangle.$$

This defines a unitary operator on $\mathbb{C}^{q^n}$. Denoting $e_i=X_{a_i}Z_{b_i}$, $1\le i\le n$, we may write $\boldsymbol{e}=X_{\boldsymbol{a}}Z_{\boldsymbol{b}}=e_1\otimes e_2\otimes\cdots\otimes e_n$. Define

$$\mathcal{E}_n=\{X_{\boldsymbol{a}}Z_{\boldsymbol{b}}\,|\,\boldsymbol{a},\boldsymbol{b}\in\mathbb{F}_q^n\}.\tag{14}$$

The set $\mathcal{E}_n$ is a nice error basis on the space $\mathbb{C}^{q^n}$.[25] In other words, the set $\mathcal{E}_n$ is a finite set of q^{2n} unitary matrices that satisfy three interesting properties: (a) It contains the identity matrix I. (b) The product of two matrices in $\mathcal{E}_n$ is a scalar multiple of another element in $\mathcal{E}_n$. (c) $\mathrm{Tr}(A^{\dagger}B)=0$ for distinct elements A,B in $\mathcal{E}_n$.

We may identify $X_{\boldsymbol{a}}Z_{\boldsymbol{b}}$ with $(\boldsymbol{a}|\boldsymbol{b})$ for $\boldsymbol{a},\boldsymbol{b}\in\mathbb{F}_q^n$ and hence the set $\mathcal{E}_n$ with $\mathbb{F}_q^{2n}$. It is known that $\mathcal{E}_n$ is an orthogonal basis of the space of operators on $\mathbb{C}^{q^n}$, hence any operator $\mathcal{O}$ on $\mathbb{C}^{q^n}$ can be expressed as (see Ref. [9])

$$\mathcal{O}=\sum_{\boldsymbol{e}\in\mathcal{E}_n}\frac{\mathrm{Tr}(\boldsymbol{e}^{\dagger}\mathcal{O})}{q^n}\boldsymbol{e}.\tag{15}$$

2.2.2. The error group

The set

$$G_n = \left\{ {\zeta_p}^i X_{\boldsymbol{a}} Z_{\boldsymbol{b}} \,|\, 0 \leqslant i \leqslant p-1, \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^n \right\}$$

is a non-abelian group of order pq^{2n} and is called the error group associated with the nice error basis $\mathcal{E}_n$. Let $(\boldsymbol{a}|\boldsymbol{b})$ and $(\boldsymbol{a}'|\boldsymbol{b}')$ be the vectors in $\mathbb{F}_q^{2n}$. The symplectic inner product on $\mathbb{F}_q^{2n}$ is defined by

$$\langle (\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \rangle_s := \mathrm{tr}\left(\boldsymbol{a}' \cdot \boldsymbol{b} - \boldsymbol{a} \cdot \boldsymbol{b}'\right). \tag{16}$$

For any $\boldsymbol{e} = {\zeta_p}^i X_{\boldsymbol{a}} Z_{\boldsymbol{b}}, \boldsymbol{e}' = {\zeta_p}^{i'} X_{\boldsymbol{a}'} Z_{\boldsymbol{b}'} \in G_n$, we also have the relation

$$\boldsymbol{e}\boldsymbol{e}' = {\zeta_p}^{\langle (\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \rangle_s} \boldsymbol{e}'\boldsymbol{e}, \quad \forall \boldsymbol{e}, \boldsymbol{e}' \in G_n.$$

For convenience, we also rewrite Eq. (16) as

$$\left\langle \boldsymbol{e}, \boldsymbol{e}' \right\rangle_s \triangleq \langle (\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \rangle_s = \mathrm{tr}(\boldsymbol{a}' \cdot \boldsymbol{b} - \boldsymbol{a} \cdot \boldsymbol{b}').$$

2.2.3. Weights of error operators

We define the symplectic weight of a vector $(\boldsymbol{a}|\boldsymbol{b})$ in $\mathbb{F}_q^{2n}$ as

$$\mathrm{swt}((\boldsymbol{a}|\boldsymbol{b})) := \#\{1 \leq i \leq n : (a_i, b_i) \neq (0,0)\}.$$

Let $\boldsymbol{e} = X_{\boldsymbol{a}} Z_{\boldsymbol{b}} = e_1 \otimes \cdots \otimes e_n \in \mathcal{E}_n$ be an error operator. The weight $\mathrm{wt}(\boldsymbol{e})$ of $\boldsymbol{e}$ is the number of non-identity tensor components, i.e.,

$$\mathrm{wt}(\boldsymbol{e}) = \mathrm{swt}((\boldsymbol{a}|\boldsymbol{b})). \tag{17}$$

We also define the X-weight $\mathrm{wt}_X(\boldsymbol{e})$ and the Z-weight $\mathrm{wt}_Z(\boldsymbol{e})$ to be the Hamming weights of $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively, i.e.,

$$\begin{aligned} \mathrm{wt}_X(\boldsymbol{e}) &= \#\{1 \leq i \leq n \,|\, a_i \neq 0\}, \\ \mathrm{wt}_Z(\boldsymbol{e}) &= \#\{1 \leq i \leq n \,|\, b_i \neq 0\}. \end{aligned} \tag{18}$$

We define the complete weight of $\boldsymbol{e}$ as follows: for each error $x \in \mathcal{E}$, $r_x(\boldsymbol{e})$ denotes the number of tensor components which are equal to x, that is, $r_x(\boldsymbol{e}) = \#\{1 \leq i \leq n : e_i = x\}$. It is clear that $r_x(\boldsymbol{e}) \geq 0$ for any x and $\sum_{x \in \mathcal{E}} r_x(\boldsymbol{e}) = n$. The complete weight of $\boldsymbol{e}$ is then given by the vector

$$\mathrm{Comp}(\boldsymbol{e}) = (r_x(\boldsymbol{e}))_{x \in \mathcal{E}}. \tag{19}$$

In particular, $\mathrm{wt}(\boldsymbol{e}) = \sum_{x \in \mathcal{E} \setminus \{I\}} r_x(\boldsymbol{e})$, and if we take denotation

$$\mathcal{E}_X = \{X_a Z_b \in \mathcal{E} \,|\, a \neq 0\}, \quad \mathcal{E}_Z = \{X_a Z_b \in \mathcal{E} \,|\, b \neq 0\},$$

then

$$\mathrm{wt}_X(\boldsymbol{e}) = \sum_{x \in \mathcal{E}_X} r_x(\boldsymbol{e}), \quad \mathrm{wt}_Z(\boldsymbol{e}) = \sum_{x \in \mathcal{E}_Z} r_x(\boldsymbol{e}). \tag{20}$$

2.3. Quantum error-correcting codes

Definition 2[31] An $((n,K))_q$ quantum code Q is a K-dimensional subspace of $\mathbb{C}^{q^n}(K \geq 1)$. The symbol n is the length of the code. If the dimension K is a power of q, say $K = q^k$, we also call Q an $[[n,k]]_q$ quantum code. A vector in Q is called a codeword.

For two quantum states $u, v \in \mathbb{C}^{q^n}$, the $\langle u|v\rangle$ is the standard Hermitian inner product. If $\langle u|v\rangle = 0$, then u and v are known to be orthogonal. An error $\boldsymbol{e} \in \mathcal{E}_n$ is said to be detectable in Q if any two orthogonal codewords from Q remain orthogonal after one of them is altered by $\boldsymbol{e}$. That is,

Definition 3[28] Let Q be an $((n,K))_q$ quantum code. An error $\boldsymbol{e} \in G_n$ is said to be detectable in Q if $\langle u|\boldsymbol{e}|v\rangle = 0$ for all orthogonal codewords $u, v \in Q$.

Definition 4[28] Let Q be an $((n,K))_q$ quantum code with $K \geq 2$. The minimum distance of Q is the maximum integer d such that any error $\boldsymbol{e} \in \mathcal{E}_n$ of weight less than d is detectable. Such a quantum code is called a symmetric quantum code with parameters $((n,K,d))_q$ or $[[n,k,d]]_q$ if $K = q^k$.

In some quantum systems, phase-flips (or Z-errors) and bit-flips (or X-errors) may occur with a different probability. Asymmetric quantum codes arise to account for this effect.

Definition 5[8] Let Q be an $((n,K))_q$ quantum code with $K \geq 2$. Let d_x and d_z be positive integers. If d_x and d_z are the maximum integers such that each error $\boldsymbol{e} \in \mathcal{E}_n$ with $\mathrm{wt}_X(\boldsymbol{e}) < d_x, \mathrm{wt}_Z(\boldsymbol{e}) < d_z$ is detectable, then we call Q an asymmetric quantum code with parameters $((n,K,d_z/d_x))_q$ or $[[n,k,d_z/d_x]]_q$ if $K = q^k$.

Symmetric and asymmetric quantum codes satisfy similar singleton bounds.

Theorem 3 (Quantum singleton bounds) If Q is an $((n,K,d))_q$ symmetric quantum code, then

$$\log_q K \leq n - 2d + 2. \tag{21}$$

If Q is an $((n,K,d_z/d_x))_q$ asymmetric quantum code, then

$$\log_q K \leq n - d_x - d_z + 2. \tag{22}$$

The singleton bound (21) for symmetric quantum codes was proved in Refs. [14,32] for binary and nonbinary cases, respectively. The singleton bound (22) for arbitrary asymmetric quantum codes was proved only recently in Ref. [21], while the bound was established much earlier for stabilizer asymmetric quantum codes.[33] Quantum codes attaining the upper bounds on the right sides of inequalities (21) and (22) are called symmetric quantum MDS (maximum-distance separable) codes and asymmetric quantum MDS codes, respectively.

2.4. Quantum stabilizer codes

Nonzero quantum stabilizer codes $Q \subset \mathbb{C}^{q^n}$ are in one–one correspondence to abelian subgroups $S \leqslant G_n$, satisfying

$$S \cap Z(G_n) = \{1\}. \tag{23}$$

Here $Z(G_n)=\{\zeta_p^i I_{q^n}: 0\le i\le p-1\}$ is the center of G_n, with I_{q^n} being the identity operator on $\mathbb{C}^{q^n}$. The relations between Q and S are

$$Q=\bigcap_{E\in S}\left\{v\in\mathbb{C}^{q^n}|Ev=v\right\},\quad S=\bigcap_{v\in Q}\{E\in G_n|Ev=v\}.$$

In other words, Q forms an eigenspace of S corresponding to the eigenvalue 1 and S is the stabilizer group of Q. Thus, to describe a nonzero quantum stabilizer code $Q\subset\mathbb{C}^{q^n}$, it is equivalent to describe an abelian subgroup $S\leqslant G_n$ satisfying Eq. (23).

Quantum stabilizer codes are related to classical codes. Let S be an abelian subgroup of G_n satisfying Eq. (23). Denote by $SZ(G_n)$ the group generated by S and the center $Z(G_n)$, and define the centralizer of S in G_n by

$$C_{G_n}(S)=\{E\in G_n|EF=FE \text{ for all } F\in S\}.$$

From this, we can define

$$\begin{aligned}\mathcal{C} &= \left\{(\boldsymbol{a}|\boldsymbol{b})\in\mathbb{F}_q^{2n}\,|\,\zeta_p^i X_{\boldsymbol{a}}Z_{\boldsymbol{b}}\in SZ(G_n)\right\}\\ &\cong SZ(G_n)/Z(G_n).\end{aligned}\tag{24}$$

The symplectic dual of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_s} = \left\{\boldsymbol{c}'\in\mathbb{F}_q^{2n}|\langle\boldsymbol{c},\boldsymbol{c}'\rangle_s=0 \text{ for all } \boldsymbol{c}\in\mathcal{C}\right\}.$$

Properties of $SZ(G_n), C_{G_n}(S)$ imply that both $\mathcal{C}$ and $\mathcal{C}^{\perp_s}$ are classical codes in $\mathbb{F}_q^{2n}$ and satisfy the condition $\mathcal{C}\subset\mathcal{C}^{\perp_s}$.

On the other hand, given a classical code $\mathcal{C}$ of $\mathbb{F}_q^{2n}$ such that $\mathcal{C}\subset\mathcal{C}^{\perp_s}$, one can find an abelian subgroup $S\leqslant G_n$ satisfying Eqs. (23) and (24). Such an S gives rise to a nonzero quantum stabilizer code Q, whose many properties such as dimension and the minimal distance can be derived directly from the classical codes $\mathcal{C}$ and $\mathcal{C}^{\perp_s}$.

In fact, it is much easier to work with the usual inner product in the classical coding theory, such as the (Euclidean) inner product and the Hermitian inner product. As it turns out, these inner products can be used under special conditions. In particular, there are ways to construct stabilizer codes Q by linear codes $\mathcal{C}$ over $\mathbb{F}_q$ with (Euclidean) self-orthogonal condition $\mathcal{C}\subset\mathcal{C}^{\perp}$ (CSS construction, see corollary 21[25]) and by linear codes $\mathcal{C}$ over $\mathbb{F}_{q^2}$ with Hermitian self-orthogonal condition $\mathcal{C}\subset\mathcal{C}^{\perp_h}$ (see Ref. [25] corollary 19). Interested readers may see the review[25] for more details.

3. Complete weight distributions of quantum codes and the MacWilliams identity

In Ref. [21], the authors defined the complete weight distributions of q-ary quantum codes and derived the MacWilliams identity expressed in terms of a $q\times q$ matrix. Here we present the MacWilliams identity in a form more aligned with the classical MacWilliams identity for the complete weight distributions of linear codes over finite fields (see Ref. [20] [Chapter 5, Theorem 10]). We also present a simple and different proof, following the original idea of Shor and Laflamme[9] in their study of the weight enumerators of quantum codes.

Let Q be an $((n,K,d))_q$ quantum code and $P:\mathbb{C}^{q^n}\to Q$ be the corresponding orthogonal projection. For the complete weight distributions of Q, let us define

$$\Sigma^n=\left\{\boldsymbol{t}=(t_x)_{x\in\mathcal{E}}\mid\sum_{x\in\mathcal{E}}t_x=n,t_x\in\mathbb{Z},t_x\ge 0\right\}.$$

For any error operator $\boldsymbol{e}\in\mathcal{E}_n$, the vector $\mathrm{Comp}(\boldsymbol{e})=(r_x(\boldsymbol{e}))_{x\in\mathcal{E}}\in\Sigma^n$ [see Eq. (19)] is the complete weight of $\boldsymbol{e}$. The complete weight distributions of the quantum code Q are the numbers $D_{\boldsymbol{t}}$'s and $D_{\boldsymbol{t}}^{\perp}$'s for $\boldsymbol{t}\in\Sigma^n$, where $D_{\boldsymbol{t}},D_{\boldsymbol{t}}^{\perp}$ are given by

$$\begin{aligned}D_{\boldsymbol{t}}&=\frac{1}{K^2}\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\mathrm{Tr}(\boldsymbol{e}^{\dagger}P)\mathrm{Tr}(\boldsymbol{e}P),\\ D_{\boldsymbol{t}}^{\perp}&=\frac{1}{K}\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\mathrm{Tr}(\boldsymbol{e}^{\dagger}P\boldsymbol{e}P).\end{aligned}$$

The complete weight enumerators of Q are defined as two polynomials in the multi-variables $\boldsymbol{z}=(z_x)_{x\in\mathcal{E}}$ given by

$$D(\boldsymbol{z})=\sum_{\boldsymbol{t}}D_{\boldsymbol{t}}\boldsymbol{z}^{\boldsymbol{t}},\quad D^{\perp}(\boldsymbol{z})=\sum_{\boldsymbol{t}}D_{\boldsymbol{t}}^{\perp}\boldsymbol{z}^{\boldsymbol{t}}.$$

Here the subscript $\boldsymbol{t}=(t_x)_{x\in\mathcal{E}}$ runs over the set Σ^n and $\boldsymbol{z}^{\boldsymbol{t}}:=\prod_{x\in\mathcal{E}}z_x^{t_x}$. We remark that these enumerators are essentially the same as given in Ref. [22] for binary quantum codes and in Ref. [21] for q-ary quantum codes. This definition is also similar to that in the classical coding theory setting. We also remark that if $\{c_i|1\le i\le K\}$ is an orthonormal basis of Q, then the complete weight distributions $D_{\boldsymbol{t}}$ and $D_{\boldsymbol{t}}^{\perp}$ can be expressed as[9]

$$\begin{aligned}D_{\boldsymbol{t}}&=\frac{1}{K^2}\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\left|\sum_i\langle c_i|\boldsymbol{e}|c_i\rangle\right|^2,\\ D_{\boldsymbol{t}}^{\perp}&=\frac{1}{K}\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\sum_{ij}\left|\langle c_i|\boldsymbol{e}|c_j\rangle\right|^2.\end{aligned}\tag{25}$$

A simple application of the Cauchy–Schwartz inequality implies that $D_{\boldsymbol{t}}^{\perp}\ge D_{\boldsymbol{t}}\ge 0$ for any $\boldsymbol{t}\in\Sigma^n$.[9] In particular, for $I=X_{\boldsymbol{0}}Z_{\boldsymbol{0}}\in\mathcal{E}_n$, define $\boldsymbol{t}_0=\mathrm{Comp}(I)$, it is easy to see $D_{\boldsymbol{t}_0}=D_{\boldsymbol{t}_0}^{\perp}=1$.

Now we can describe the MacWilliams-type identities relating $D(\boldsymbol{z})$ and $D^{\perp}(\boldsymbol{z})$.

Theorem 4 Assume that Q is an $((n,K,d))_q$ quantum code. The general MacWilliams identities for the complete weight enumerators $D(\boldsymbol{z})$ and $D^{\perp}(\boldsymbol{z})$ are given by

$$D^{\perp}(\boldsymbol{z})=\frac{K}{q^n}D(\boldsymbol{u}),\quad D(\boldsymbol{z})=\frac{1}{q^nK}D^{\perp}(\boldsymbol{u}),\tag{26}$$

where $\boldsymbol{z}=(z_x)_{x\in\mathcal{E}}, \boldsymbol{u}=(u_x)_{x\in\mathcal{E}}$ are the multi-variables satisfying the relation

$$u_x=\sum_{v\in\mathcal{E}}\zeta_p^{\langle x,v\rangle_s}z_v,\quad \forall x\in\mathcal{E}. \tag{27}$$

Here for any $x,v\in\mathcal{E}$, $\langle x,v\rangle$ is the symplectic inner product defined in Eq. (12).

Proof of Theorem 4 Let P be the orthogonal projection operator from $\mathbb{C}^{q^n}$ onto the quantum code Q. From Eq. (15), we may expand P into the form

$$P=\sum_{D\in\mathcal{E}_n}\frac{\mathrm{Tr}(D^\dagger P)}{q^n}D=\frac{1}{pq^n}\sum_{D\in G_n}\mathrm{Tr}(D^\dagger P)D.$$

Hence we obtain

$$\begin{aligned}D_{\boldsymbol{t}}^{\perp} &= \frac{1}{K}\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\mathrm{Tr}\Bigg(\boldsymbol{e}^\dagger\sum_{D_1\in G_n}\frac{\mathrm{Tr}(D_1^\dagger P)}{pq^n}D_1\boldsymbol{e}\\ &\quad\times\sum_{D_2\in G_n}\frac{\mathrm{Tr}(D_2^\dagger P)}{pq^n}D_2\Bigg)\\ &= \frac{1}{p^2q^{2n}K}\sum_{D_1,D_2\in G_n}\mathrm{Tr}(D_1^\dagger P)\mathrm{Tr}(D_2^\dagger P)\\ &\quad\times\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\mathrm{Tr}(\boldsymbol{e}^\dagger D_1\boldsymbol{e}D_2).\end{aligned}$$

Since $\boldsymbol{e}D=\zeta_p^{\langle\boldsymbol{e},D\rangle_s}D\boldsymbol{e}$ and $\boldsymbol{e}^\dagger\boldsymbol{e}=I$ for any $\boldsymbol{e},D\in G_n$, we have

$$\begin{aligned}\mathrm{Tr}(\boldsymbol{e}^\dagger D_1\boldsymbol{e}D_2) &= \mathrm{Tr}(\zeta_p^{\langle D_1,\boldsymbol{e}\rangle_s}\boldsymbol{e}^\dagger\boldsymbol{e}D_1D_2)\\ &= \zeta_p^{\langle D_1,\boldsymbol{e}\rangle_s}\mathrm{Tr}(D_1D_2).\end{aligned}$$

Noting that for $D_1,D_2\in G_n$,

$$\mathrm{Tr}(D_1D_2)=\begin{cases}\zeta_p{}^i q^n & :\ \text{if } D_2=\zeta_p{}^iD_1^\dagger \text{ for some } i;\\ 0 & :\ \text{if } D_2\notin\{\zeta_p{}^iD_1^\dagger\,|\,0\le i\le p-1\},\end{cases}$$

we have

$$\begin{aligned}D_{\boldsymbol{t}}^{\perp} &= \frac{1}{p^2q^{2n}K}\sum_{\substack{D_1\in G_n\\ D_2=\zeta_p{}^iD_1^\dagger}}\mathrm{Tr}(D_1^\dagger P)\mathrm{Tr}(\zeta_p{}^{-i}D_1P)\\ &\quad\times\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\zeta_p^{\langle D_1,\boldsymbol{e}\rangle_s}\zeta_p{}^iq^n\\ &= \frac{1}{q^nK}\sum_{D\in\mathcal{E}_n}\mathrm{Tr}(D^\dagger P)\mathrm{Tr}(DP)\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\zeta_p^{\langle D,\boldsymbol{e}\rangle_s}.\end{aligned}$$

For any $D\in\mathcal{E}_n$, denoting

$$\alpha(D)=\frac{\mathrm{Tr}(D^\dagger P)\mathrm{Tr}(DP)}{q^nK},$$

we have

$$D_{\boldsymbol{t}}^{\perp}=\sum_{D\in\mathcal{E}_n}\alpha(D)\sum_{\substack{\boldsymbol{e}\in\mathcal{E}_n\\ \mathrm{Comp}(\boldsymbol{e})=\boldsymbol{t}}}\zeta_p^{\langle D,\boldsymbol{e}\rangle_s}.$$

Now we can verify the identity (26) easily. First,

$$D^\perp(\boldsymbol{z})=\sum_{\boldsymbol{t}}D_{\boldsymbol{t}}^{\perp}\boldsymbol{z}^{\boldsymbol{t}}=\sum_{D\in\mathcal{E}_n}\alpha(D)\sum_{\boldsymbol{e}\in\mathcal{E}_n}\zeta_p^{\langle D,\boldsymbol{e}\rangle_s}\boldsymbol{z}^{\mathrm{Comp}(\boldsymbol{e})}. \tag{28}$$

Next, by using $\boldsymbol{e}=e_1\otimes\ldots\otimes e_n, D=D_1\otimes\ldots\otimes D_n$ where $e_i,D_i\in\mathcal{E}$, and hence $\langle D,\boldsymbol{e}\rangle_s=\sum_{i=1}^n\langle D_i,e_i\rangle_s$ and $r_x(\boldsymbol{e})=\sum_{i=1}^n r_x(e_i)$ for any $x\in\mathcal{E}$, we obtain

$$\sum_{\boldsymbol{e}\in\mathcal{E}_n}\zeta_p^{\langle D,\boldsymbol{e}\rangle_s}\boldsymbol{z}^{\mathrm{Comp}(\boldsymbol{e})}=\prod_{i=1}^n\left(\sum_{e\in\mathcal{E}}\zeta_p^{\langle D_i,e\rangle_s}z_e\right).$$

By using the relation (27) it is easy to see that the right-hand side of the above becomes $\prod_{x\in\mathcal{E}}u_x^{r_x(D)}=\boldsymbol{u}^{\mathrm{Comp}(D)}$. Inserting this into the right side of Eq. (28), we finally conclude that

$$D^\perp(\boldsymbol{z})=\sum_{D\in\mathcal{E}_n}\alpha(D)\boldsymbol{u}^{\mathrm{Comp}(D)}=\frac{K}{q^n}D(\boldsymbol{u}),$$

which proves the first identity in Eq. (26). The second identity in Eq. (26) can be derived immediately from the first by noting that

$$z_v=q^{-2}\sum_{x\in\mathcal{E}}\zeta_p^{\langle v,x\rangle_s}u_x,\quad\forall v\in\mathcal{E}.$$

Now Theorem 4 is proved.

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

Example 1 Assume $q=p=2$. We list the elements of the error operator set $\mathcal{E}=\{X_aZ_b:a,b\in\mathbb{F}_2\}$ as $w_0=X_0Z_0$, $w_1=X_0Z_1$, $w_2=X_1Z_0$, $w_3=X_1Z_1$. Then we can obtain the following results:

$$\begin{aligned}\sum_{s=0}^3\zeta_p^{\langle w_s,w_0\rangle_s}z_s &= z_0+z_1+z_2+z_3,\\ \sum_{s=0}^3\zeta_p^{\langle w_s,w_1\rangle_s}z_s &= z_0+z_1-z_2-z_3,\\ \sum_{s=0}^3\zeta_p^{\langle w_s,w_2\rangle_s}z_s &= z_0-z_1+z_2-z_3,\\ \sum_{s=0}^3\zeta_p^{\langle w_s,w_3\rangle_s}z_s &= z_0-z_1-z_2+z_3.\end{aligned}$$

Therefore, the MacWilliams identity is given by

$$\begin{aligned}&D(z_0,z_1,z_2,z_3)\\ &=\frac{1}{2^nK}D^\perp(z_0+z_1+z_2+z_3,z_0+z_1-z_2-z_3,\\ &\quad z_0-z_1+z_2-z_3,z_0-z_1-z_2+z_3).\end{aligned} \tag{29}$$

This identity (29) is consistent with the MacWilliams identity given in by Hu *et al.* (Ref. [22] Theorem 7).

For any $\boldsymbol{t}=(t_x)_{x\in\mathcal{E}}\in\Sigma^n$, since each u_x given in Eq. (27) is a linear polynomial in the variables $\boldsymbol{z}=(z_v)_{v\in\mathcal{E}}$, we may expand $\prod_{x\in\mathcal{E}}u_x^{t_x}$ as

$$\prod_{x\in\mathcal{E}}\left(\sum_{v\in\mathcal{E}}\zeta_p^{\langle v,x\rangle_s}z_v\right)^{t_x}=\sum_{\boldsymbol{s}}P_{\boldsymbol{s}}(\boldsymbol{t};n)\boldsymbol{z}^{\boldsymbol{s}}, \tag{30}$$

where the subscript $\boldsymbol{s}=(s_x)_{x\in\mathcal{E}}$ is over all $\boldsymbol{s}\in\Sigma^n$ and $\boldsymbol{z}^{\boldsymbol{s}}:=\prod_{x\in\mathcal{E}}z_x^{s_x}$. The coefficients $P_{\boldsymbol{s}}(\boldsymbol{t};n)$ are polynomials in variables $\boldsymbol{s}$ and $\boldsymbol{t}$ and are called the generalized Krawtchouk polynomials (see Ref. [34] Definition 2.9). Using these polynomials we can write the MacWilliams identities (26) as follows.

Corollary 1 Assume that Q is an $((n,K,d))_q$ quantum code. The complete weight distributions $D_{\boldsymbol{t}},D_{\boldsymbol{t}}^{\perp}$ satisfy

$$D_{\boldsymbol{t}}=\frac{1}{q^nK}\sum_{\boldsymbol{s}}P_{\boldsymbol{t}}(\boldsymbol{s};n)D_{\boldsymbol{s}}^{\perp},$$
$$D_{\boldsymbol{t}}^{\perp}=\frac{K}{q^n}\sum_{\boldsymbol{s}}P_{\boldsymbol{t}}(\boldsymbol{s};n)D_{\boldsymbol{s}},\quad\forall\boldsymbol{t}\in\Sigma^n.$$

Remark 1 The idea of our proof follows directly from the original paper[9] where MacWilliams identity (for weight distribution of quantum codes) was proved in the first place; so essentially we extend the ideas of Ref. [9] slightly further to complete weight distribution of quantum codes. A earlier proof of the MacWilliams identity for complete weight distributions of q-ary quantum codes were given in Ref. [21]. The authors proved that $D(\boldsymbol{z})$ and $D^{\perp}(\boldsymbol{z})$ are the same by giving them concrete forms expressed in terms of a $q\times q$ matrix. By contrast, our formulation of the MacWilliams identity closely resembles that of the classical coding setting and is consistent with quantum language in general (for the classical setting, see (Ref. [20], Theorem 10 in Chapter 5). We complete the proof just using the properties of trace. With the generalized Krawtchouk polynomials, we further give the relations between $D_{\boldsymbol{t}}$ and $D_{\boldsymbol{t}}^{\perp}$ (Corollary 1, which has been proved for the weight distributions of quantum codes[28]). The proof in Ref. [21] may be translated into our language correctly, but the translation is not completely trivial.

4. Quantum MDS codes and the weight distributions

Let Q be an $((n,K))_q$ quantum code and $P:\mathbb{C}^{q^n}\to Q$ the orthogonal projection. The weight distributions $\{(B_t,B_t^{\perp})|0\le t\le n\}$ of Q and the double weight distributions $\{(C_{i,j},C_{i,j}^{\perp})|0\le i,j\le n\}$ of Q are defined by

$$B_t=\frac{1}{K^2}\sum_{\substack{e\in\mathcal{E}_n\\ \mathrm{wt}(e)=t}}\mathrm{Tr}(e^{\dagger}P)\mathrm{Tr}(eP),$$
$$B_t^{\perp}=\frac{1}{K}\sum_{\substack{e\in\mathcal{E}_n\\ \mathrm{wt}(e)=t}}\mathrm{Tr}(e^{\dagger}PeP),\tag{31}$$
$$C_{i,j}=\frac{1}{K^2}\sum_{\substack{e\in\mathcal{E}_n\\ \mathrm{wt}_X(e)=i\\ \mathrm{wt}_Z(e)=j}}\mathrm{Tr}(e^{\dagger}P)\mathrm{Tr}(eP),$$
$$C_{i,j}^{\perp}=\frac{1}{K}\sum_{\substack{e\in\mathcal{E}_n\\ \mathrm{wt}_X(e)=i\\ \mathrm{wt}_Z(e)=j}}\mathrm{Tr}(e^{\dagger}PeP).\tag{32}$$

Correspondingly, the weight enumerators $B(X,Y),B^{\perp}(X,Y)$ of Q and the double weight enumerators $C(X,Y,Z,W)$, $C^{\perp}(X,Y,Z,W)$ of Q are defined by

$$B(X,Y)=\sum_{i=0}^{n}B_iX^{n-i}Y^i,\quad B^{\perp}(X,Y)=\sum_{i=0}^{n}B_i^{\perp}X^{n-i}Y^i;$$
$$C(X,Y,Z,W)=\sum_{i,j=0}^{n}C_{i,j}X^{n-i}Y^iZ^{n-j}W^j,$$
$$C^{\perp}(X,Y,Z,W)=\sum_{i,j=0}^{n}C_{i,j}^{\perp}X^{n-i}Y^iZ^{n-j}W^j.$$

Since for any error operator $e\in\mathcal{E}_n$, the weights $\mathrm{wt}(e)$, $\mathrm{wt}_X(e)$, and $\mathrm{wt}_Z(e)$ can be expressed by the complete weight $\mathrm{Comp}(e)$ (see Eqs. (17) and (18)), the weight enumerators $B(X,Y)$, $B^{\perp}(X,Y)$, $C(X,Y,Z,W)$, and $C^{\perp}(X,Y,Z,W)$ can be expressed in terms of the complete weight enumerators $D(\boldsymbol{z})$ and $D^{\perp}(\boldsymbol{z})$. The corresponding MacWilliams identities can be derived easily from Theorem 4 (see Ref. [21]).

The quantum singleton bounds (21) and (22) can be proved by using linear programming approach, utilizing the MacWilliams identities of the weight enumerators of quantum codes described above (see Refs. [14,21,22]). The purpose of this section is to show that by a careful analysis of the linear programming approach in the proofs of the quantum singleton bounds, we can obtain a lot of information on the weight distributions $B_t,B_t^{\perp}$ of symmetric quantum MDS codes and the double weight distributions $C_{i,j},C_{i,j}^{\perp}$ of asymmetric quantum MDS codes. These quantum codes attain the quantum singleton bounds in inequalities (21) and (22), respectively.

Let us first introduce Krawtchouk polynomials and summarize their properties which play important roles in proving the quantum singleton bounds.

4.1. The Krawtchouk polynomials

For any real number $\gamma>0$, integers $0\le x\le n$, define the γ-Krawtchouk polynomial

$$P_i(x;n,\gamma)=\sum_{j=0}^{i}(-1)^j\gamma^{i-j}\binom{x}{j}\binom{n-x}{i-j}.\tag{33}$$

These polynomials have the generating function

$$(1+\gamma z)^{n-x}(1-z)^x=\sum_{i=0}^{\infty}P_i(x;n,\gamma)z^i,$$

and satisfy the following properties for any $0\le r,s\le n$:

$$\frac{P_s(r;n,\gamma)}{\gamma^s\binom{n}{s}}=\frac{P_r(s;n,\gamma)}{\gamma^r\binom{n}{r}},\tag{34}$$
$$\sum_{i=0}^{n}\gamma^i\binom{n}{i}P_r(i;n,\gamma)P_s(i;n,\gamma)=(\gamma+1)^n\gamma^r\binom{n}{r}\delta_{r,s}.\tag{35}$$

Here $\delta_{r,s}$ is the Kronecker symbol given by $\delta_{r,s}=1$ if $r=s$, and $\delta_{r,s}=0$ if $r\ne s$.

Let us also recall a property which plays important roles in proving the quantum singleton bounds.

Lemma 1 Let $1 \le d \le n$ and

$$A(x) = (1+\gamma)^{n-d+1} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right).$$

Then

$$A(x) = \sum_{i=0}^{n} \alpha_i P_i(x; n, \gamma)$$

where the coefficients are given by

$$\alpha_i = \alpha_i(d) = \binom{n-i}{d-1} \Big/ \binom{n}{n-d+1}. \tag{36}$$

4.2. Weight distributions of symmetric quantum MDS codes

We follow the approach of Ref. [14] in proving the quantum singleton bound (21) but do a much more careful analysis for quantum codes that attain the bound.

Let Q be an $((n,K,d))_q$ quantum code. Let $B_t, B_t^{\perp}$ be the weight distributions. It is known that they satisfy the following properties (see Ref. [14], Theorem 3):

(i) $B_t^{\perp} \ge B_t \ge 0$ for $0 \le t \le n$, and $B_0 = B_0^{\perp} = 1$.

(ii) The minimum distance d is the largest integer such that $B_t = B_t^{\perp}$ for any $t < d$.

Let $\gamma = q^2 - 1$. The MacWilliams identities between the weight enumerators $B(X,Y), B^{\perp}(X,Y)$ imply that[14,21]

$$B_t = \frac{1}{q^n K} \sum_{j=0}^{n} P_t(j; n, \gamma) B_j^{\perp}. \tag{37}$$

Consider the polynomial $A(x)$ given by

$$A(x) = (1+\gamma)^{n-d+1} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right).$$

It is known by Lemma 1 that

$$A(x) = \sum_{i=0}^{n} \alpha_i P_i(x; n, \gamma), \tag{38}$$

where the coefficients α_i are given by Eq. (36). It is easy to see

$$A(x) \begin{cases} > 0 : 0 \le x \le d-1; \\ = 0 : d \le x \le n, \end{cases} \tag{39}$$

$$\alpha_i \begin{cases} > 0 : 0 \le i \le n-d+1; \\ = 0 : i > n-d+1. \end{cases} \tag{40}$$

Since $B_i \ge 0$ for any i, we have

$$q^n K \sum_{i=0}^{d-1} \alpha_i B_i \le q^n K \sum_{i=0}^{n} \alpha_i B_i := T. \tag{41}$$

By using Eqs. (37) and (38), we can obtain

$$T = \sum_{i=0}^{n} \alpha_i \sum_{j=0}^{n} P_i(j; n, \gamma) B_j^{\perp} = \sum_{j=0}^{n} A(j) B_j^{\perp}.$$

Then using Eq. (39) and Property (ii) listed above, we find that T can be further simplified to

$$T = \sum_{i=0}^{d-1} A(i) B_i^{\perp} = \sum_{i=0}^{d-1} A(i) B_i.$$

Thus we have

$$q^n K \sum_{i=0}^{d-1} \alpha_i B_i \le \sum_{i=0}^{d-1} A(i) B_i,$$

and hence

$$q^n K \le \frac{\sum_{i=0}^{d-1} A(i) B_i}{\sum_{i=0}^{d-1} \alpha_i B_i} \le \max_{0 \le i \le d-1} \left\{ \frac{A(i)}{\alpha_i} : A(i)\alpha_i B_i > 0 \right\}. \tag{42}$$

Let $r_i = A(i)/\alpha_i$ for $0 \le i \le d-1$. Noting that $B_0 = 1$ and

$$\frac{r_i}{r_{i+1}} = \frac{n-i-d+1}{d-i-1} > 1 \quad \text{if} \quad n+2 > 2d,$$

we find that r_i is strictly decreasing for $0 \le i \le d-1$ and $r_0 = (1+\gamma)^{n-d+1} = q^{2n-2d+2}$, thus we have

$$q^n K \le q^{2n-2d+2} \implies \log_q K \le n - 2d + 2.$$

This is the quantum singleton bound (21).

Now suppose that Q is a symmetric quantum MDS codes, i.e., $k := \log_q K = n - 2d + 2$. Then both the inequalities (41) and (42) must become equalities. Using Eq. (40), we find that Eq. (41) becomes an identity if and only if

$$B_i = 0 \quad \text{for any } d \le i \le n-d+1,$$

and Eq. (42) becomes an identity if and only if

$$\frac{\sum_{i=0}^{d-1} A(i) B_i}{\sum_{i=0}^{d-1} \alpha_i B_i} = \frac{A(0)}{\alpha_0} = q^{2n-2d+2},$$

and this happens if and only if

$$B_i = 0 \quad \text{for any} \quad 1 \le i \le d-1.$$

Therefore, we have

Theorem 5 Let Q be an $((n,K,d))_q$ symmetric quantum MDS codes, i.e., $k = \log_q K = n - 2d + 2$. Then the weight distributions $B_t, B_t^{\perp}$ $(0 \le t \le n)$ satisfy

(1) $B_0 = B_0^{\perp} = 1$,

(2) $B_i = 0$ for $1 \le i \le n-d+1$,

(3) $B_i^{\perp} = 0$ for $1 \le i \le d-1$.

It is easy to see that Theorem 5 together with the MacWilliams identities (37) completely determines the weight distributions $B_t, B_t^{\perp}$ of the quantum MDS codes Q.

Theorem 6 Let Q be an $((n,K,d))_q$ symmetric quantum MDS codes, i.e., $k = \log_q K = n - 2d + 2$. Then the weight distributions $B_t^{\perp}$ of Q are given by $B_0^{\perp} = 1, B_i^{\perp} = 0$ for $1 \le i < d$, and

$$B_t^{\perp} = \binom{n}{t} \sum_{j=0}^{t-d} (-1)^j \binom{t}{j} \left(q^{2(t+1-d-j)} - 1\right), \quad \forall d \le t \le n. \tag{43}$$

Proof of Theorem 6 This is almost obvious, for the sake of completeness, we give a proof here. The MacWilliams identities (37) are equivalent to (see Ref. [30], Theorem 7.2.3)

$$\sum_{i=0}^{n-v}\binom{n-i}{v}B_i^{\perp}=\frac{K}{q^n}(\gamma+1)^{n-v}\sum_{i=0}^{v}\binom{n-i}{v-i}B_i,\quad \forall 0\le v\le n.$$

Using Theorem 5 and noting $\gamma=q^2-1$, we have

$$\sum_{i=d}^{n-v}\binom{n-i}{v}B_i^{\perp}=\left(q^{2(n-d-v+1)}-1\right)\binom{n}{v},$$
$$\forall 1\le v\le n-d+1.$$

The desired conclusion follows from the fact that the above system of equations has a unique solution if it is solvable (see Ref. [30], Theorem 7.3.1), and the $B_i^{\perp}$'s given in Theorem 6 is a solution.

Remark 2 We notice that Theorem 6 was recently proved (see Ref. [23], Theorem 9), based on a clever use of Rains' unitary weight distributions of the quantum codes Q and the fact that quantum MDS codes are always pure. Here we give a completely different proof based on linear programming approach and the MacWilliams identities.

Remark 3 Quantum MDS codes got a lot of attention early, including the purity of quantum MDS codes derived by Rains[32] and $[[n,n-2d+2,d]]_q$ codes by Grassl *et al.*[35] In particular, Grassl and Beth proved that these codes exist for all $3\le n\le q$ and $1\le d\le n/2+1$, and also presented quantum MDS codes with parameters $[[q^2,q^2-2d+2,d]]_q$ for $1\le d\le q$ which additionally give rise to shortened codes $[[q^2-s,q^2-2d+2-s,d]]_q$ for some s. Ketkar *et al.* showed that a nontrivial MDS stabilizer code satisfies constraints on the length and minimal distance.[25] The research on the construction of quantum MDS codes with new parameters has been quite active in the past ten years, which resulted in a large body of references in the literature. For example, Refs. [36–48] provided explicit constructions of many new families of quantum MDS codes, whose weight distribution would satisfy Theorems 5 and 6. Quantum MDS codes from constacyclic codes[49,50] and repeated-root cyclic codes[51–53] are also presented. Here Theorems 5 and 6 apply to all quantum MDS codes, including those which are not quantum stabilizer codes.

4.3. Double weight distributions of asymmetric quantum MDS codes

Similar to the above description, we follow the approach of Hu *et al.* (Ref. [21], Theorem 1) to prove the quantum singleton bound (22) but do a more careful analysis for asymmetric quantum MDS codes.

Let Q be an $((n,K,d_z/d_x))_q$ asymmetric quantum code. Let $C_{i,j},C_{i,j}^{\perp}$ be the double weight distributions of Q. It is known that they satisfy the following properties:[21]

(i) $C_{i,j}^{\perp}\ge C_{i,j}\ge 0$ for $0\le i,j\le n$, and $C_{0,0}=C_{0,0}^{\perp}=1$;

(ii) d_x,d_z are the largest integers satisfying $C_{i,j}=C_{i,j}^{\perp}$ for any $i<d_x$ and $j<d_z$.

Let $\gamma=q-1$. The MacWilliams identities between the weight enumerators $C(X,Y,Z,W),C^{\perp}(X,Y,Z,W)$ imply that[21]

$$C_{i,j}=\frac{1}{q^nK}\sum_{r,s=0}^{n}P_i(s;n,\gamma)P_j(r;n,\gamma)C_{r,s}^{\perp},\quad \forall 0\le i,j\le n. \tag{44}$$

Consider the polynomial $A(x)$ given by

$$A(x,y)=(1+\gamma)^{2n-d_x-d_z+2}\prod_{r=d_x}^{n}\left(1-\frac{x}{r}\right)\prod_{s=d_z}^{n}\left(1-\frac{y}{s}\right).$$

It is easy to find from Lemma 1 that

$$A(x,y)=\sum_{i,j=0}^{n}\alpha_i\beta_jP_i(y;n,\gamma)P_j(x;n,\gamma), \tag{45}$$

where the coefficients α_i,β_j are given by

$$\alpha_i=\binom{n-i}{d_z-1}\Big/\binom{n}{n-d_z+1},$$
$$\beta_j=\binom{n-j}{d_x-1}\Big/\binom{n}{n-d_x+1}.$$

It is easy to see that

$$A(x,y)\begin{cases}>0\ :\ 0\le x\le d_x-1 \text{ and } 0\le y\le d_z-1;\\ =0\ :\ x\ge d_x \text{ or } y\ge d_z,\end{cases} \tag{46}$$

$$\alpha_i\beta_j\begin{cases}>0\ :\ 0\le i\le n-d_z+1 \text{ and } 0\le j\le n-d_x+1;\\ =0\ :\ \text{otherwise.}\end{cases} \tag{47}$$

Since $C_{i,j}\ge 0$ and $\alpha_i\beta_j\ge 0$ for any i,j, we have

$$q^nK\sum_{i<d_x}\sum_{j<d_z}\alpha_i\beta_jC_{i,j}\le q^nK\sum_{i,j=0}^{n}\alpha_i\beta_jC_{i,j}:=T. \tag{48}$$

By using Eqs. (44) and (45), we can obtain

$$T=\sum_{i,j=0}^{n}\alpha_i\beta_j\sum_{r,s=0}^{n}P_i(s;n,\gamma)P_j(r;n,\gamma)C_{r,s}^{\perp}=\sum_{r,s=0}^{n}A(r,s)C_{r,s}^{\perp}.$$

Then using Eq. (46) and property (ii) listed above, we find that T can be further simplified to

$$T=\sum_{i=0}^{d_x-1}\sum_{j=0}^{d_z-1}A(i,j)C_{i,j}^{\perp}=\sum_{i=0}^{d_x-1}\sum_{j=0}^{d_z-1}A(i,j)C_{i,j}.$$

Thus we have

$$q^nK\sum_{i<d_x}\sum_{j<d_z}\alpha_i\beta_jC_{i,j}\le\sum_{i<d_x}\sum_{j<d_z}A(i,j)C_{i,j},$$

and hence

$$q^nK\le\frac{\sum_{i<d_x}\sum_{j<d_z}A(i,j)C_{i,j}}{\sum_{i<d_x}\sum_{j<d_z}\alpha_i\beta_jC_{i,j}}\le\max_{i<d_x,j<d_z}\left\{\frac{A(i,j)}{\alpha_i\beta_j}:A(i,j)\alpha_i\beta_jC_{i,j}>0\right\}. \tag{49}$$

Similar to the argument used in the previous subsection (see also Ref. [21], Proof of Theorem 1), the right-hand side achieves the maximum at $i=j=0$ and

$$\frac{A(0,0)}{\alpha_0\beta_0}=q^{2n-d_x-d_z+2}>\frac{A(i,j)}{\alpha_i\beta_j}$$
$$\forall (i,j)\neq(0,0) \text{ with } i<d_x, j<d_z.$$

This immediately shows that

$$q^nK\leq q^{2n-d_x-d_z+2} \implies \log_q K\leq n-d_x-d_z+2.$$

This is the quantum singleton bound (22).

Now suppose that Q is an asymmetric quantum MDS codes, i.e., $k:=\log_q K=n-d_x-d_z+2$, then both the inequalities (48) and (49) must become equalities. Using Eq. (47), we find that Eq. (47) becomes an identity if and only if

$$C_{i,j}=0 \quad \text{if} \begin{cases} i\geq d_x, & 0\leq j\leq n-d_x+1 \text{ or} \\ j\geq d_z, & 0\leq i\leq n-d_z+1, \end{cases}$$

and Eq. (19) becomes an identity if and only if

$$\frac{\sum_{i<d_x}\sum_{j<d_z}A(i,j)C_{i,j}}{\sum_{i<d_x}\sum_{j<d_z}\alpha_i\beta_jC_{i,j}}=\frac{A(0,0)}{\alpha_0\beta_0}=q^{2n-d_x-d_z+2},$$

and this happens if and only if

$$C_{i,j}=0 \quad \text{for any } 0\leq i\leq d_x-1, 0\leq j\leq d_z-1 \text{ and } (i,j)\neq(0,0).$$

Thus, we have

Theorem 7 Let Q be an $((n,K,d_z/d_x))_q$ asymmetric quantum MDS codes, i.e., $k=\log_q K=n-d_x-d_z+2$. Then the double weight distributions $C_{i,j},C^{\perp}_{i,j}$ $(0\leq i,j\leq n)$ satisfy

(1) $C_{0,0}=C^{\perp}_{0,0}=1$,

(2) $C_{i,j}=0$ for any $0\leq i\leq n-d_z+1, 0\leq j\leq n-d_x+1$ and $(i,j)\neq(0,0)$,

(3) $C^{\perp}_{i,j}=0$ for $0\leq i\leq d_x-1, 0\leq j\leq d_z-1$ and $(i,j)\neq(0,0)$.

It may be interesting to see if the values of the double weight distributions $C_{i,j},C^{\perp}_{i,j}$ for other weights of asymmetric quantum MDS codes $((n,K,d_z/d_x))_q$ may be determined.

Remark 4 The construction of asymmetric quantum MDS codes is also an interesting research problem but it is in general much more difficult than that of quantum MDS codes. There are a few references on constructions of asymmetric quantum MDS codes[54–56] whose double weight distribution would satisfy Theorem 7. It shall be noted that such quantum MDS codes are also quantum stabilizer codes.

5. New identities for the weight distributions of quantum codes

In this section we use the MacWilliams identities to derive some new identities for the weight distributions of quantum codes. We first deal with the complete weight distribution.

Theorem 8 Let Q be an $((n,K))_q$ quantum code and Q' an $((n,K'))_q$ quantum code. Let $D_{\boldsymbol{t}},D^{\perp}_{\boldsymbol{t}}$ and $D'_{\boldsymbol{t}},D'^{\perp}_{\boldsymbol{t}}$ be their complete wight distributions respectively. Then we have

$$\sum_{\boldsymbol{t}}\frac{K^2D^2_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}=\sum_{\boldsymbol{t}}\frac{\left(D^{\perp}_{\boldsymbol{t}}\right)^2}{\zeta_pga(\boldsymbol{t})}, \tag{50}$$

$$\sum_{\boldsymbol{t}}\frac{KK'D_{\boldsymbol{t}}D'_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}=\sum_{\boldsymbol{t}}\frac{D^{\perp}_{\boldsymbol{t}}D'^{\perp}_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}, \tag{51}$$

$$\sum_{\boldsymbol{t}}\frac{KD_{\boldsymbol{t}}D'^{\perp}_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}=\sum_{\boldsymbol{t}}\frac{K'D'_{\boldsymbol{t}}D^{\perp}_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}, \tag{52}$$

where the subscript $\boldsymbol{t}$ on both sides of the equations run over the set Σ^n, and $\zeta_pga(\boldsymbol{t})$ is the multinomial coefficient given by

$$\zeta_pga(\boldsymbol{t})=\binom{n}{\boldsymbol{t}}=\frac{n!}{\prod_{x\in\mathcal{E}}t_x!}, \quad \forall \boldsymbol{t}\in\Sigma^n. \tag{53}$$

Proof For $\boldsymbol{t}\in\Sigma^n$, from Corollary 1 we have

$$D_{\boldsymbol{t}}=\frac{1}{q^nK}\sum_{\boldsymbol{s}}P_{\boldsymbol{t}}(\boldsymbol{s};n)D^{\perp}_{\boldsymbol{s}}.$$

By using the relation[24]

$$\frac{P_{\boldsymbol{s}}(\boldsymbol{t};n)}{\zeta_pga(\boldsymbol{s})}=\frac{P_{\boldsymbol{t}}(\boldsymbol{s};n)}{\zeta_pga(\boldsymbol{t})}, \quad \forall \boldsymbol{s},\boldsymbol{t}\in\Sigma^n,$$

we have

$$\frac{KD_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}=\frac{1}{q^n}\sum_{\boldsymbol{s}}\frac{P_{\boldsymbol{t}}(\boldsymbol{s};n)D^{\perp}_{\boldsymbol{s}}}{\zeta_pga(\boldsymbol{t})}=\sum_{\boldsymbol{s}}\frac{P_{\boldsymbol{s}}(\boldsymbol{t};n)D^{\perp}_{\boldsymbol{s}}}{q^n\zeta_pga(\boldsymbol{s})}. \tag{54}$$

Given a vector $\boldsymbol{\alpha}=(\alpha_{\boldsymbol{s}})_{\boldsymbol{s}}$ where each $\alpha_{\boldsymbol{s}}$ is complex number for any $\boldsymbol{s}\in\Sigma^n$, define

$$P(\boldsymbol{t},\boldsymbol{\alpha})=\sum_{\boldsymbol{s}}\alpha_{\boldsymbol{s}}P_{\boldsymbol{s}}(\boldsymbol{t};n). \tag{55}$$

Thus,

$$\frac{KD_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}-P(\boldsymbol{t},\boldsymbol{\alpha})=\sum_{\boldsymbol{s}}P_{\boldsymbol{s}}(\boldsymbol{t};n)\left(\frac{D^{\perp}_{\boldsymbol{s}}}{q^n\zeta_pga(\boldsymbol{s})}-\alpha_{\boldsymbol{s}}\right).$$

Now taking the squared modulus and multiply $\zeta_pga(\boldsymbol{t})$ on both sides, and then summing over all $\boldsymbol{t}\in\Sigma^n$, and taking notice of the relation[24]

$$\sum_{\boldsymbol{t}}\zeta_pga(\boldsymbol{t})P_{\boldsymbol{s}_1}(\boldsymbol{t};n)\overline{P_{\boldsymbol{s}_2}(\boldsymbol{t};n)}=\delta_{\boldsymbol{s}_1,\boldsymbol{s}_2}q^{2n}\zeta_pga(\boldsymbol{s}_1), \ \forall \boldsymbol{s}_1,\boldsymbol{s}_2\in\Sigma^n,$$

where the subscript $\boldsymbol{t}$ runs over the set Σ^n, and $\delta_{\boldsymbol{s}_1,\boldsymbol{s}_2}=1$ if $\boldsymbol{s}_1=\boldsymbol{s}_2$ and $\delta_{\boldsymbol{s}_1,\boldsymbol{s}_2}=0$ if $\boldsymbol{s}_1\neq\boldsymbol{s}_2$, we can obtain

$$\sum_{\boldsymbol{t}}\zeta_pga(\boldsymbol{t})\left|\frac{KD_{\boldsymbol{t}}}{\zeta_pga(\boldsymbol{t})}-P(\boldsymbol{t},\boldsymbol{\alpha})\right|^2$$
$$=\sum_{\boldsymbol{s}}q^{2n}\zeta_pga(\boldsymbol{s})\left|\frac{D^{\perp}_{\boldsymbol{s}}}{q^n\zeta_pga(\boldsymbol{s})}-\alpha_{\boldsymbol{s}}\right|^2.$$

This can be rewritten as

$$\sum_{\boldsymbol{t}}\frac{1}{\zeta_pga(\boldsymbol{t})}\left|KD_{\boldsymbol{t}}-\zeta_pga(\boldsymbol{t})P(\boldsymbol{t},\boldsymbol{\alpha})\right|^2$$

$$= \sum_{\boldsymbol{s}} \frac{1}{\zeta_p g a(\boldsymbol{s})} \left| D_{\boldsymbol{s}}^{\perp} - q^n \zeta_p g a(\boldsymbol{s}) \alpha_{\boldsymbol{s}} \right|^2. \tag{56}$$

Let λ be any complex number. If we take

$$P(\boldsymbol{t}, \alpha) = \frac{\lambda K' D'_{\boldsymbol{t}}}{\zeta_p g a(\boldsymbol{t})},$$

then by Eq. (54) we have

$$\alpha_{\boldsymbol{s}} = \frac{\lambda D'^{\perp}_{\boldsymbol{s}}}{q^n \zeta_p g a(\boldsymbol{s})}.$$

Inserting these values into Eq. (56) we obtain

$$\sum_{\boldsymbol{t}} \frac{1}{\zeta_p g a(\boldsymbol{t})} \left| K D_{\boldsymbol{t}} - \lambda K' D'_{\boldsymbol{t}} \right|^2$$
$$= \sum_{\boldsymbol{s}} \frac{1}{\zeta_p g a(\boldsymbol{s})} \left| D_{\boldsymbol{s}}^{\perp} - \lambda D'^{\perp}_{\boldsymbol{s}} \right|^2, \quad \forall \lambda \in \mathbb{C}.$$

Taking $\lambda = 0$ and ± 1 respectively we obtain the desired results (50) and (51). As for Eq. (52), we take

$$P(\boldsymbol{t}, \alpha) = \frac{\lambda D'^{\perp}_{\boldsymbol{t}}}{\zeta_p g a(\boldsymbol{t})},$$

then similarly by Corollary 1 we can obtain

$$\alpha_{\boldsymbol{s}} = \frac{\lambda K' D'_{\boldsymbol{s}}}{q^n \zeta_p g a(\boldsymbol{s})}.$$

Inserting these values into Eq. (56) we obtain

$$\sum_{\boldsymbol{t}} \frac{1}{\zeta_p g a(\boldsymbol{t})} \left| K D_{\boldsymbol{t}} - \lambda D'^{\perp}_{\boldsymbol{t}} \right|^2$$
$$= \sum_{\boldsymbol{s}} \frac{1}{\zeta_p g a(\boldsymbol{s})} \left| D_{\boldsymbol{s}}^{\perp} - \lambda K' D'_{\boldsymbol{s}} \right|^2, \quad \forall \lambda \in \mathbb{C}.$$

Separately taking $\lambda = \pm 1$ yields the desired result (52). The proof of Theorem 8 is completed.

It is unsurprising that the double weight distributions $C_{i,j}, C^{\perp}_{i,j}$ of quantum code Q satisfy similar identities described in Theorem 8, which we list in the following. The proof is also similar.

Theorem 9 Let Q be an $((n,K))_q$ quantum code and Q' an $((n,K'))_q$ quantum code. Let $C_{i,j}, C^{\perp}_{i,j}$ and $C'_{i,j}, C'^{\perp}_{i,j}$ be their double weight wight distributions, respectively. Then we have

$$\sum_{i,j} \frac{K^2 C_{i,j}^2}{\zeta_p g a'(i) \zeta_p g a'(j)} = \sum_{i,j} \frac{\left(C^{\perp}_{i,j}\right)^2}{\zeta_p g a'(i) \zeta_p g a'(j)}, \tag{57}$$

$$\sum_{i,j} \frac{K K' C_{i,j} C'_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)} = \sum_{i,j} \frac{C^{\perp}_{i,j} C'^{\perp}_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)}, \tag{58}$$

$$\sum_{i,j} \frac{K C_{i,j} C'^{\perp}_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)} = \sum_{i,j} \frac{K' C'_{i,j} C^{\perp}_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)}, \tag{59}$$

where the subscripts i, j on both sides of the equations run over integers from 0 to n, and $\zeta_p g a'(i)$ is given by

$$\zeta_p g a'(i) = (q-1)^i \binom{n}{i}, \quad \forall 0 \le i \le n. \tag{60}$$

Proof Let $\gamma = q - 1$. Recall from Eq. (44) that we have

$$C_{i,j} = \frac{1}{q^n K} \sum_{r,s=0}^{n} P_i(s;n,\gamma) P_j(r;n,\gamma) C^{\perp}_{r,s}, \quad \forall 0 \le i, j \le n.$$

Here $P_i(s;n,\gamma)$ is the Krawtchouk polynomial defined in Eq. (33). By using the relation (34) we have

$$\frac{K C_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)} = \frac{1}{q^n} \sum_{r,s} \frac{P_i(s;n,\gamma) P_j(r;n,\gamma) C^{\perp}_{r,s}}{\zeta_p g a'(i) \zeta_p g a'(j)}$$
$$= \sum_{r,s} \frac{P_s(i;n,\gamma) P_r(j;n,\gamma) C^{\perp}_{r,s}}{q^n \zeta_p g a'(s) \zeta_p g a'(r)}.$$

Given a vector $\boldsymbol{\alpha} = (\alpha_{r,s})_{r,s}$ where each $\alpha_{r,s}$ is complex number for any $0 \le r, s \le n$, define

$$P(i,j,\boldsymbol{\alpha}) = \sum_{r,s} \alpha_{r,s} P_s(i;n,\gamma) P_r(j;n,\gamma). \tag{61}$$

Therefore,

$$\frac{K C_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)} - P(i,j,\alpha)$$
$$= \sum_{r,s} P_s(i;n,\gamma) P_r(j;n,\gamma) \left(\frac{C^{\perp}_{r,s}}{q^n \zeta_p g a'(r) \zeta_p g a'(s)} - \alpha_{r,s} \right).$$

Now taking the squared modulus and multiply $\zeta_p g a'(i) \zeta_p g a'(j)$ on both sides, and then summing over all i, j in integers from 0 to n, and taking notice of the identity (35), we can obtain

$$\sum_{i,j} \zeta_p g a'(i) \zeta_p g a'(j) \left| \frac{K C_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)} - P(i,j,\alpha) \right|^2$$
$$= \sum_{r,s} q^{2n} \zeta_p g a'(r) \zeta_p g a'(s) \left| \frac{C^{\perp}_{r,s}}{q^n \zeta_p g a'(r) \zeta_p g a'(s)} - \alpha_{r,s} \right|^2.$$

This can be rewritten as

$$\sum_{i,j} \frac{1}{\zeta_p g a'(i) \zeta_p g a'(j)} \left| K C_{i,j} - \zeta_p g a'(i) \zeta_p g a'(j) P(i,j,\alpha) \right|^2$$
$$= \sum_{r,s} \frac{1}{\zeta_p g a'(r) \zeta_p g a'(s)} \left| C^{\perp}_{r,s} - q^n \zeta_p g a'(r) \zeta_p g a'(s) \alpha_{r,s} \right|^2. \tag{62}$$

Let λ be any complex number. Inserting the values

$$P(i,j,\alpha) = \frac{\lambda K' C'_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)}, \quad \alpha_{r,s} = \frac{\lambda C'^{\perp}_{r,s}}{q^n \zeta_p g a'(r) \zeta_p g a'(s)};$$
$$P(i,j,\alpha) = \frac{\lambda C'^{\perp}_{i,j}}{\zeta_p g a'(i) \zeta_p g a'(j)}, \quad \alpha_{r,s} = \frac{\lambda K' C'_{r,s}}{q^n \zeta_p g a'(r) \zeta_p g a'(s)},$$

into Eq. (62) and taking $\lambda = 0, \pm 1$ respectively, we obtain the desired results (57)–(59). This completes the proof of Theorem 9.

It is conceivable that the weight distributions $B_t, B_t^{\perp}$ of quantum codes Q would satisfy similar identities. For the sake of simplicity, we do not list the identities here.

6. Bounds on the complete weight distributions of quantum codes

The weight distribution and weight enumerators of quantum codes were initially proposed by Shor and Laflamme in Ref. [9]. The quantum weight enumerators were polynomials with weight distribution as coefficients, and they relate the weight distributions B_t and $B_t^\perp$ by the MacWilliams identity. In the results of Shor and Laflamme,[9] they found a set of linear equations and inequalities of the weight distributions by the MacWilliams identity, and proved that these relationships could be used with linear programming to find bounds on how good quantum codes can be and to test whether good potential codes exist. The complete weight distributions contain information about the weight distributions. Thus the calculation of the complete weight distributions of quantum codes is a worthwhile but challenging problem, just like the classical case. Related research can be referred to Ref. [9].

However, direct calculations are often complicated. We want to narrow down the value of complete weight distribution by a special method. For the classical linear code $\mathcal{C}$, the complete weight distributions $A_{\boldsymbol{t}}$ and $A_{\boldsymbol{t}}^\perp$ count the number of codewords of pattern $\boldsymbol{t}$ from $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$, respectively. While the quantities $A_{\boldsymbol{t}}, A_{\boldsymbol{t}}^\perp$ are difficult to compute explicitly for general linear codes, estimates of these quantities were obtained in Ref. [24] showing that for a linear code $\mathcal{C}$, when the dual code $\mathcal{C}^\perp$ satisfies certain conditions, then $A_{\boldsymbol{t}}$ is close to a specified quantity with errors explicitly upper bounded in terms of parameters of the code. It is known that such behavior of $A_{\boldsymbol{t}}$ is typical of random codes. Here we prove that a similar phenomenon holds for quantum codes, which may give estimates of the complete weight distributions $D_{\boldsymbol{t}}$ and $D_{\boldsymbol{t}}^\perp$. Recall that $\boldsymbol{t}_0 = \mathrm{Comp}(I)$ where $I = X_0 Z_0 \in \mathcal{E}$.

Theorem 10 Let Q be an $((n,K,d))_q$ quantum code. Define

$$\mathcal{T}(Q) := \{\boldsymbol{t} \in \Sigma^n \setminus \{\boldsymbol{t}_0\} \,|\, D_{\boldsymbol{t}} > 0\}.$$

Let $\alpha > 0$ be a constant. Suppose that, for any $\boldsymbol{t} = (t_x)_{x\in\mathcal{E}} \in \mathcal{T}(Q)$, we have

$$\left|t_x - q^{-2}n\right| \leq \alpha\sqrt{n}, \quad \forall x \in \mathcal{E}. \tag{63}$$

If $n \geq (2\alpha q^2)^2$, then for any $\boldsymbol{s} \in \Sigma^n$, the weight distribution $D_{\boldsymbol{s}}^\perp$ satisfies

$$\begin{aligned}&\left|D_{\boldsymbol{s}}^\perp - \zeta_p ga(\boldsymbol{s}) K q^{-n}\right| \\ \leqslant\ & \frac{\zeta_p ga(\boldsymbol{s})^{1/2}(2\pi n)^{(q^2-1)/4}}{q^{q^2/2}} \\ & \times \exp\left(2\alpha^2 q^2(q^2-1) + \frac{1}{48\alpha^2} + \frac{q^4}{24n}\right).\end{aligned} \tag{64}$$

Here for any $\boldsymbol{s} \in \Sigma^n$, $\zeta_p ga(\boldsymbol{s})$ is the multinomial coefficient defined in Eq. (53).

Remark 5 When the dimension K is close to q^n, and the component s_x of the vector $\boldsymbol{s} \in \Sigma^n$ is close to $q^{-2}n$ for any $x \in \mathcal{E}$, then the term on the right side of Eq. (64) is much smaller in magnitude than the term $\zeta_p ga(\boldsymbol{s}) K q^{-n}$ on the left, hence under the assumption (63), the complete weight distribution $D_{\boldsymbol{s}}^\perp$ is close to the quantity $\zeta_p ga(\boldsymbol{s}) K q^{-n}$. Theorem 10 can be considered as a "quantum analogue" of Chan and Xiong (Ref. [24], Theorem 2) where a similar result on the complete weight distribution of classical linear codes was obtained.

Remark 6 The set $\mathcal{T}(Q)$ can be characterized easily as follows: by Eq. (25), we see that $D_{\boldsymbol{t}} > 0$ if and only if there is an $e \in \mathcal{E}_n$ with $\mathrm{Comp}(e) = \boldsymbol{t}$ such that $\mathrm{Tr}\left(e^\dagger P\right)\mathrm{Tr}\left(eP\right) \neq 0$, which is equivalent to $\mathrm{Tr}\left(eP\right) \neq 0$.

Proof Plugging the values

$$\alpha_{\boldsymbol{s}} = K q^{-2n} \ \ \forall \boldsymbol{s} \in \Sigma^n, \quad P(\boldsymbol{t}, \alpha) = K\delta_{\boldsymbol{t},\boldsymbol{t}_0},$$

into both sides of Eq. (56), and noting that $D_{\boldsymbol{t}_0} = 1$, we obtain the identity

$$\sum_{\boldsymbol{t}\neq\boldsymbol{t}_0} \frac{K^2 D_{\boldsymbol{t}}^2}{\zeta_p ga(\boldsymbol{t})} = \sum_{\boldsymbol{s}} \frac{\left(D_{\boldsymbol{s}}^\perp - \zeta_p ga(\boldsymbol{s}) K q^{-n}\right)^2}{\zeta_p ga(\boldsymbol{s})}.$$

Denoting

$$\zeta_p ga^* = \min_{\boldsymbol{t}\neq\boldsymbol{t}_0}\{\zeta_p ga(\boldsymbol{t}) : D_{\boldsymbol{t}} \neq 0\},$$

then we have

$$\begin{aligned}&\frac{1}{\zeta_p ga(\boldsymbol{s})}\left(D_{\boldsymbol{s}}^\perp - \zeta_p ga(\boldsymbol{s}) K q^{-n}\right)^2 \\ <\ & \frac{K^2}{\zeta_p ga^*}\sum_{\boldsymbol{t}} D_{\boldsymbol{t}}^2 < \frac{K^2}{\zeta_p ga^*}\left(\sum_{\boldsymbol{t}} D_{\boldsymbol{t}}\right)^2.\end{aligned}$$

Using $\sum_{\boldsymbol{t}} D_{\boldsymbol{t}} = q^n K^{-1}$ [14] and the bound of $\zeta_p ga^*$ given by (replace q by q^2 in Ref. [24], Theorem 4)

$$\frac{q^{2n}}{\zeta_p ga^*} < (2\pi n)^{\frac{q^2-1}{2}} q^{-q^2} \exp\left(4\alpha^2 q^2(q^2-1) + \frac{1}{24\alpha^2} + \frac{q^4}{12n}\right),$$

we obtain the desired result.

We can find a similar result for the double weight distribution of quantum codes.

Theorem 11 Let Q be an $((n,K,d))_q$ quantum code. For any $e \in \mathcal{E}$, define

$$\mathcal{D}(Q) := \left\{(i,j) | 0 \leq i,j \leq n, (i,j) \neq (0,0) \text{ and } C_{i,j} > 0\right\}.$$

Let $\alpha > 0$ be a constant. Suppose that, for any $(t_1,t_2) \in \mathcal{D}(Q)$, the components t_1, t_2 satisfy

$$\left|t_k - \left(1-q^{-1}\right)n\right| \leq \alpha\sqrt{n}, \quad \text{for } k = 1,2. \tag{65}$$

Then for any $0 \leq r,s \leq n$, the double weight distribution $C_{r,s}^\perp$ satisfies

$$\begin{aligned}&\left|C_{r,s}^\perp - \zeta_p ga'(r)\zeta_p ga'(s) K q^{-n}\right| \\ \leqslant\ & \zeta_p ga'(r)^{1/2}\zeta_p ga'(s)^{1/2}\left(\frac{2\pi n}{q}\right)^{1/2} \exp\left(\frac{\alpha^2 q^2}{q-1} + \frac{q}{6n}\right).\end{aligned} \tag{66}$$

Here the terms $\zeta_p ga'(r), \zeta_p ga'(s)$ are defined in Eq. (60).

Remark 7 Again in Eq. (66), when the dimension K is close to q^n, and the components r,s are not too large or both small in values so that $\zeta_p ga'(r)\zeta_p ga'(s)$ is relatively large, then the term on the right side of Eq. (66) is much smaller in magnitude than the term $\zeta_p ga'(r)\zeta_p ga'(s)Kq^{-n}$ on the left, hence under the assumption (65), the double complete weight distribution $C^{\perp}_{r,s}$ is close to the quantity $\zeta_p ga'(r)\zeta_p ga'(s)Kq^{-n}$. The set $\mathcal{D}(Q)$ can be characterized as follows: similar to Eq. (25), we see that $C_{i,j} > 0$ if and only if there is an $e \in \mathcal{E}_n$ with $\mathrm{wt}_X(e) = i, \mathrm{wt}_Z(e) = j$ such that $\mathrm{Tr}\left(e^{\dagger}P\right)\mathrm{Tr}\left(eP\right) \neq 0$, which is equivalent to $\mathrm{Tr}\left(eP\right) \neq 0$.

Proof Plugging the values

$$\alpha_{r,s} = Kq^{-2n} \ \forall 0 \leq r,s \leq n, \quad P(i,j,\alpha) = K\delta_{i,0}\delta_{j,0},$$

into both sides of Eq. (62), and noting that $C_{0,0} = 1$, we obtain the identity

$$\begin{aligned}&\sum_{i,j} \frac{K^2 C_{i,j}^2}{\zeta_p ga'(i)\zeta_p ga'(j)}\\ &= \sum_{r,s} \frac{1}{\zeta_p ga'(r)\zeta_p ga'(s)} \left(C^{\perp}_{r,s} - \zeta_p ga'(s)\zeta_p ga'(r)Kq^{-n}\right)^2.\end{aligned}$$

Denoting

$$\zeta_p ga^{**} = \min_{(i,j)\neq(0,0)} \{\zeta_p ga'(i)\zeta_p ga'(j) : C_{i,j} \neq 0\},$$

then we have

$$\begin{aligned}&\frac{1}{\zeta_p ga'(r)\zeta_p ga'(s)} \left(C^{\perp}_{r,s} - \zeta_p ga'(s)\zeta_p ga'(r)Kq^{-n}\right)^2\\ &< \frac{K^2}{\zeta_p ga^{**}} \sum_{i,j} C_{i,j}^2 < \zeta_p ga'(r)\zeta_p ga'(s) \frac{K^2}{\zeta_p ga^{**}} \left(\sum_{t} C_{i,j}\right)^2.\end{aligned}$$

Using $\sum_{i,j} C_{i,j} = q^n K^{-1}$ [21] and the bound of $\zeta_p ga^{**}$ given by (see Ref. [57], Lemma 3.2)

$$\frac{q^{2n}}{\zeta_p ga^{**}} < (2\pi n)\, q^{-1} \exp\left(\frac{2\alpha^2 q^2}{q-1} + \frac{q}{3n}\right),$$

we obtain the desired result.

We remark that, while the conditions (63) and (65) look quite restrictive for quantum codes Q, in the next section we show that a large family of quantum stabilizer codes obtained by the Hermitian construction from primitive narrow-sense BCH codes satisfy these conditions.

7. The complete weight distributions of quantum BCH codes

Classical BCH codes are one of the most important classes of cyclic codes used in practice due to their good nature. BCH codes containing their (Euclidean or Hermitian) dual codes can be used to construct a family of quantum stabilizer codes named quantum BCH codes.[58,59] In Ref. [25], Ketkar *et al.* introduced non-binary quantum BCH codes from narrow-sense primitive BCH codes, puncturing BCH codes and extending BCH codes. Some earlier studies can be seen in Refs. [1,60,61]. The construction methods were derived in Refs. [62,63] for quantum convolutional BCH codes. Lai *et al.* gave the MacWilliams identity for quantum convolutional codes, which applies to quantum convolutional BCH codes. In addition, the weight distribution of quantum BCH codes under Hermitian construction is closely related to that of classical BCH codes.[64] The weight distribution of classical BCH code has also been studied in Refs. [65,66]. In 2019, estimates of the complete weight distribution for classical linear codes were obtained in Ref. [24] and it was proved that they were satisfied by classical BCH codes. In this section, we show that the conditions (63) and (65) are satisfied by quantum BCH codes.

7.1. Hermitian construction of quantum stabilizer codes

Quantum stabilizer codes may be constructed from Hermitian self-orthogonal codes over $\mathbb{F}_{q^2}$. Interested readers may see the review[25] for more details.

For any $\boldsymbol{x} = (x_1,\ldots,x_n), \boldsymbol{y} = (y_1,\ldots,y_n) \in \mathbb{F}_{q^2}^n$, the Hermitian inner product $\langle \boldsymbol{x}, \boldsymbol{y}\rangle_h$ is defined as

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle_h = \sum_{i=1}^{n} x_i \bar{y}_i.$$

Here we denote $\bar{x} = x^q$.

Let C be an $[n,k]_{q^2}$ linear code (linear over $\mathbb{F}_{q^2}$). The Hermitian dual of C is given by

$$C^{\perp_h} = \left\{\boldsymbol{c}' \in \mathbb{F}_{q^2}^n \,|\, \langle \boldsymbol{c}, \boldsymbol{c}'\rangle_h = 0 \quad \forall \boldsymbol{c} \in C\right\}.$$

Suppose that C is Hermitian self-orthogonal, that is, $C \subset C^{\perp_h}$. The Hermitian construction[25] shows how C can be used to construct a quantum stabilizer code $Q \subset \mathbb{C}^{q^n}$. It is known that $\dim Q = 2k - n$. The complete weight distributions of Q are closely related to those of the codes C and $C^{\perp_h}$. To be more precise, we need some notations.

First, let $(\beta, \overline{\beta})$ be a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Via the 1–1 map $\phi : \mathbb{F}_q^2 \to \mathbb{F}_{q^2}$ given by $(a|b) \mapsto a\beta + b\overline{\beta}$, we identify $\mathbb{F}_{q^2}$ with the set $\mathcal{E}$.

Next, the complete weight of $\boldsymbol{c} = (c_1,\ldots,c_n) \in \mathbb{F}_{q^2}^n$ is defined in the usual way: for any $x \in \mathbb{F}_{q^2}$, $r_x(\boldsymbol{c})$ denotes the number of components of $\boldsymbol{c}$ which are equal to x, that is, $r_x(\boldsymbol{c}) = \#\{1 \leq i \leq n \,|\, c_i = x\}$. The complete weight of $\boldsymbol{c}$ is then given by the vector

$$\mathrm{Comp}(\boldsymbol{c}) = (r_x(\boldsymbol{c}))_{x\in\mathbb{F}_{q^2}}.$$

It is known that the complete weight distributions of Q are nothing but the classical complete weight distributions induced by C and $C^{\perp_h}$.[21] That is, for any $\boldsymbol{t} \in \Sigma^n$,

$$D_{\boldsymbol{t}} = \#\left\{\boldsymbol{c} \in C \,|\, \mathrm{Comp}(\boldsymbol{c}) = \boldsymbol{t}\right\},$$

$$D_{\boldsymbol{t}}^{\perp} = \#\left\{\boldsymbol{c} \in C^{\perp_h} \,|\, \mathrm{Comp}(\boldsymbol{c}) = \boldsymbol{t}\right\}.$$

The double weight distributions of Q are also related to those of C and $C^{\perp_h}$ by using the relation (20).

7.2. Primitive narrow-sense BCH codes

Classical BCH codes are one of the most important classes of cyclic codes used in practice. Recall that a cyclic code C of length n over $\mathbb{F}_q$ with q elements and $\gcd(n,q)=1$ is called a BCH code with designed distance $\delta > 0$ if its generator polynomial is of the form

$$g(x) = \prod_{z\in\mathcal{Z}}(x-\beta^z), \quad \mathcal{Z} = C_b \cup \cdots \cup C_{b+\delta-2}. \tag{67}$$

Here $C_x = \{xq^j \pmod n | j \in \mathbb{Z}\}$ denotes the q-cyclotomic coset of x modulo n, β is a primitive n-th root of unity in some extension of $\mathbb{F}_q$. It is called narrow-sense if $b=1$, and primitive if $n = q^m - 1$ for some positive integer m.

Primitive narrow-sense BCH codes over $\mathbb{F}_{q^2}$ can be used to construct quantum stabilizer codes because of the following result:[67]

Lemma 2 Let C be a primitive, narrow-sense BCH code of length $n = q^{2m}-1$ over $\mathbb{F}_{q^2}$ with $m > 2$. Then $C^{\perp_h} \subset C$ if and only if its designed distance δ satisfies

$$\delta \le \delta_{\max} = q^{m+\lambda_m} - 1 - (q^2-1)\lambda_m.$$

Here $\lambda_m = 1$ if m is even, and $\lambda_m = 0$ if m is odd.

7.3. Quantum stabilizer codes from primitive narrow-sense BCH codes

Let C be a primitive, narrow-sense BCH code of length $n = q^{2m}-1$ over $\mathbb{F}_{q^2}$ with $m > 2$. Assume that the design distance $\delta \ge 2$ satisfies

$$\delta \le \delta_{\max} = q^{m+\lambda_m} - 1 - (q^2-1)\lambda_m.$$

Lemma 2 implies that $C^{\perp_h} \subset C$. Let Q be the quantum stabilizer code obtained from C and $C^{\perp_h}$. Then the complete weight distributions of Q are given by

$$\begin{aligned} D_{\boldsymbol{t}} &= \#\left\{\boldsymbol{c} \in C^{\perp_h} \,|\, \mathrm{Comp}(\boldsymbol{c}) = \boldsymbol{t}\right\}, \\ D_{\boldsymbol{t}}^{\perp} &= \#\left\{\boldsymbol{c} \in C \,|\, \mathrm{Comp}(\boldsymbol{c}) = \boldsymbol{t}\right\}. \end{aligned}$$

Now we verify that the complete weight distribution $D_{\boldsymbol{t}}$ of the code Q satisfies the condition (63).

The generator polynomial of C is $g(x)$ given by Eq. (67) where $b=1$ and β is a primitive element of $\mathbb{F}_{q^{2m}}$. Let us assume that $g(x)$ is of the form

$$g(x) = \sum_{i=0}^{t} a_i x^i, \quad a_i \in \mathbb{F}_{q^2}\ \forall i,$$

then the parity-check polynomial of $C^{\perp_h}$ can be given explicitly as[67]

$$g^*(x) = \sum_{i=0}^{t} \overline{a}_i x^{t-i},$$

that is,

$$g^*(x) = \prod_{z\in\mathcal{Z}}\left(x - \overline{\beta}^{-z}\right).$$

Thus, the values $\overline{\beta}^{-z}$ for $z \in \mathcal{Z} = C_1 \cup \cdots \cup C_{\delta-1}$ are the nonzeros of $C^{\perp_h}$. Since each q^2-cyclotomic coset C_x corresponds to one irreducible polynomial over $\mathbb{F}_{q^2}$, by the well-known Delsartes theorem[28,68] we have

$$C^{\perp_h} = \left\{ \left(\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}\left(\sum_{i=1}^{\delta-1} a_i \overline{\beta}^{ij} \right) \right)_{j=0}^{n-1} \,\middle|\, a_i \in \mathbb{F}_{q^{2m}}\ \forall i \right\}. \tag{68}$$

Here $\mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}$ denotes the standard trace map from $\mathbb{F}_{q^{2m}}$ to $\mathbb{F}_{q^2}$.

Lemma 3 The code $C^{\perp_h}$ satisfies the following property: for any $b \in \mathbb{F}_{q^2}$ and any $\boldsymbol{c} \in C^{\perp_h} \setminus \{\boldsymbol{0}\}$, we have

$$\left| r_b(\boldsymbol{c}) - q^{-2}n \right| < \left(1 - q^{-2}\right)(\delta - 1)\sqrt{n}.$$

Proof According to Eq. (68), let $\boldsymbol{a} = (a_1, \ldots, a_{\delta-1}) \in \mathbb{F}_{q^2}^{\delta-1}$ be a nonzero vector corresponding to the codeword $\boldsymbol{c} \in C^{\perp_h}$. For any $b \in \mathbb{F}_{q^2}$, we want to count

$$r_b(\boldsymbol{c}) = \#\left\{ 0 \le j \le n-1 \,\middle|\, \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}\left(\sum_{i=1}^{\delta-1} a_i \overline{\beta}^{ij} \right) = b \right\}.$$

Since as j runs over integers from 0 to $n-1$, the elements $\overline{\beta}^j$ runs over the set $\mathbb{F}_{q^{2m}}^* := \mathbb{F}_{q^{2m}} \setminus \{0\}$, we have

$$r_b(\boldsymbol{c}) = \#\left\{ x \in \mathbb{F}_{q^{2m}} \,\middle|\, \mathrm{Tr}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}}\left(\sum_{i=1}^{\delta-1} a_i x^i \right) = b \right\} - \delta_{0,b}.$$

Let $f(x) = \sum_{i=1}^{\delta-1} a_i x^i$. We can obtain

$$r_b(\boldsymbol{c}) = \sum_{x\in\mathbb{F}_{q^{2m}}} \frac{1}{q^2} \sum_{t\in\mathbb{F}_{q^2}} \zeta_p^{\mathrm{Tr}_{q^2/p}\left\{t\left(-b+\mathrm{Tr}_{q^{2m}/q^2} f(x)\right)\right\}} - \delta_{0,b}.$$

The term corresponding to $t=0$ is $q^{2m}/q^2 = (n+1)/q^2$. Hence we have

$$r_b(\boldsymbol{c}) = \frac{1}{q^2} \sum_{t\in\mathbb{F}_{q^2}^*} \zeta_p^{\mathrm{Tr}_{q^2/p}(-tb)} \sum_{x\in\mathbb{F}_{q^{2m}}} \zeta_p^{\mathrm{Tr}_{q^{2m}/p}(tf(x))} + \frac{n+1}{q^2} - \delta_{0,b}.$$

The Weil bound yields[69]

$$\left| \sum_{x\in\mathbb{F}_{q^{2m}}} \zeta_p^{\mathrm{Tr}_{q^{2m}/p}(tf(x))} \right| \le (\delta-2)q^m = (\delta-2)\sqrt{n+1}.$$

Thus we have

$$\begin{aligned} \left| r_b(\boldsymbol{c}) - q^{-2}n \right| &\le \frac{q^2-1}{q^2}(\delta-2)\sqrt{n+1} + \left(1 - \frac{1}{q^2}\right) \\ &< \left(1-q^{-2}\right)(\delta-1)\sqrt{n}. \end{aligned}$$

This proves Lemma 3.

In conclusion, we can summarize the complete weight distributions of quantum BCH codes as follows.

Theorem 12 Let C be a primitive, narrow-sense BCH code of length $n = q^{2m} - 1$ over $\mathbb{F}_{q^2}$ with $m > 2$ and the designed distance δ satisfies $2 \leq \delta \leq \delta_{\max} = q^{m+\lambda_m} - 1 - (q^2 - 1)\lambda_m$. Then $C^{\perp_h} \subset C$. Let Q be the quantum stabilizer code obtained from C by the Hermitian construction. Then the complete weight distributions of Q satisfy Theorem 10 with the constant

$$\alpha = \left(1 - q^{-2}\right)(\delta - 1).$$

Remark 8 By using the relation (20), it is easy to see that the double weight distributions of Q also satisfy the condition (65) with the constant α given by $\alpha = \left(1 - q^{-1}\right)\left(1 - q^{-2}\right)q^2(\delta - 1)$, so Theorem 11 is also satisfied by this quantum BCH code for this value α. We omit the details.

8. Conclusion

In summary, we have extended a previous study on the complete weight distributions of quantum codes and obtained several new results: (1) We provide a new proof of the MacWilliams identities for the complete weight distributions of quantum codes. (2) We use linear programming methods to obtain new information about the weight distributions of quantum MDS codes and the double weight distributions of asymmetric quantum MDS codes. (3) We establish new identities concerning the complete weight distributions of two distinct quantum codes. (4) We provide estimates of the complete weight distributions of quantum codes under special conditions. (5) We study quantum BCH codes obtained by the Hermitian construction from primitive, narrow-sense BCH codes and show that they satisfy these special conditions.

Here we list two open questions we encountered when this paper was written.

(i) We can only partially determine the double weight distributions of asymmetric quantum MDS codes. Can these double weight distributions be determined completely in general, or to what extent they may be determined?

(ii) Quantum BCH codes can be constructed from the CSS construction by primitive, narrow-sense BCH codes of relatively small designed distance. What are the properties of their complete weight distributions? The only thing we know is that they do not satisfy the special condition (63) and hence Theorem 10 does not apply.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 61972413, 61901525, and 62002385), the National Key R&D Program of China (Grant No. 2021YFB3100100), and RGC under Grant No. N_HKUST619/17 from Hong Kong, China.

References

[1] Calderbank A, Rains E, Shor P and Sloane N 1997 *Proceedings of IEEE International Symposium on Information Theory*, June 29–July 4, 1997, Ulm, Germany, p. 292
[2] Calderbank A R and Shor P W 1996 *Phys. Rev. A* **54** 1098
[3] Shor P W 1995 *Phys. Rev. A* **52** 2493(R)
[4] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
[5] Steane A M 1996 *Proc. Roy. Soc. London A* **452** 2551
[6] Fletcher A S, Shor P W and Win M Z 2008 *IEEE Trans. Inform. Theory* **54** 5705
[7] Ioffe L and Mézard M 2007 *Phys. Rev. A* **75** 032345
[8] Wang L, Feng K, Ling S and Xing C 2010 *IEEE Trans. Inform. Theory* **56** 2938
[9] Shor P W and Laflamme R 1997 *Phys. Rev. Lett.* **78** 1600
[10] Rains E M 1999 *IEEE Trans. Inform. Theory* **45** 2361
[11] Rains E M 1998 *IEEE Trans. Inform. Theory* **44** 1388
[12] Rains E M 2000 *IEEE Trans. Inform. Theory* **46** 54
[13] Rains E M 1999 *IEEE Trans. Inform. Theory* **45** 2489
[14] Ashikhmin A and Litsyn S 1998 *IEEE Trans. Inform. Theory* **45** 1206
[15] Lai C Y and Ashikhmin A 2018 *IEEE Trans. Inform. Theory* **64** 622
[16] Ashikhmin A, Barg A, Knill E and Litsyn S 2000 *IEEE Trans. Inform. Theory* **46** 778
[17] Scott A J 2005 *Quantum Inf. Process.* **4** 399
[18] Blake I F and Kith K 1991 *SIAM J. Discret. Math.* **4** 164
[19] Ding C and Wang X 2005 *Theor. Comput. Sci.* **330** 81
[20] MacWilliams F J and Sloane N J A 1981 *The theory of error-correcting codes* Vol I and II (Holland: North-Holland Mathematical Library)
[21] Hu C, Yang S and Yau S S T 2020 *Adv. Appl. Math.* **121** 102085
[22] Hu C, Yang S and Yau S S T 2019 *IEEE Access* **7** 68404
[23] Huber F and Grassl M 2020 *Quantum* **4** 284
[24] Chan C and Xiong M 2019 *IEEE Trans. Inform. Theory* **65** 7079
[25] Ketkar A, Klappenecker A, Kumar S and Sarvepalli P K 2006 *IEEE Trans. Inform. Theory* **52** 4892
[26] Ashikhmin A and Knill E 2001 *IEEE Trans. Inform. Theory* **47** 3065
[27] Knill E 1996 *U.S. Department of Energy Office of Scientific Technical Information Technical Reports* Report No. LA-UR-96-2717 ON: DE96014435
[28] Feng K and Chen H 2010 *Quantum Error-Correcting Codes* (Beijing: Science Press) (in Chinese)
[29] Nielsen M A and Chuang I L 2011 *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge: Cambridge University Press)
[30] Huffman W C and Pless V 2003 *Fundamentals of Error-Correcting Codes* (Cambridge: Cambridge University Press)
[31] Luo L, Ma Z, Wei Z and Leng R 2017 *Sci. China Inf. Sci.* **60** 42501
[32] Rains E M 1999 *IEEE Trans. Inform. Theory* **45** 1827
[33] Aly S A 2008 arXiv: 0803.0764 [quant-ph]
[34] Sharma B D and Sookoo N 2011 *J. Discrete Math. Sci. Cryptogr.* **14** 503
[35] Grassl M, Beth T and Rötteler M 2004 *Int. J. Quantum Inf.* **2** 55
[36] Fang W and Fu F W 2018 *Finite Fields Appl.* **53** 85
[37] Fang W and Fu F W 2019 *IEEE Trans. Inform. Theory* **65** 7840
[38] Jin L, Ling S, Luo J and Xing C 2010 *IEEE Trans. Inform. Theory* **56** 4735
[39] Jin L and Xing C 2014 *IEEE Trans. Inform. Theory* **60** 2921
[40] Zhang T and Ge G 2017 *Des. Codes Cryptogr.* **83** 503
[41] Shi X, Yue Q and Zhu X 2017 *Finite Fields Appl.* **46** 347
[42] Kai X and Zhu S 2012 *IEEE Trans. Inform. Theory* **59** 1193
[43] Jin L, Kan H and Wen J 2017 *Des. Codes Cryptogr.* **84** 463
[44] Zhang G and Chen B 2014 *Int. J. Quantum Inf.* **12** 1450019
[45] Chen B, Ling S and Zhang G 2015 *IEEE Trans. Inform. Theory* **61** 1474
[46] Li S, Xiong M and Ge G 2016 *IEEE Trans. Inform. Theory* **62** 1703
[47] Grassl M and Rötteler M 2015 *IEEE International Symposium on Information Theory (ISIT)*, June 14–19, 2015, Hong Kong, China, p. 1104
[48] Ball S 2021 *Des. Codes Cryptogr.* **89** 811
[49] Zhang T and Ge G 2015 *IEEE Trans. Inform. Theory* **61** 5224
[50] Kai X, Zhu S and Li P 2014 *IEEE Trans. Inform. Theory* **60** 2080
[51] Dinh H Q, Nguyen B T and Yamaka W 2020 *IEEE Access* **8** 124608

[52] Dinh H Q, Le H T, Nguyen B T and Maneejuk P 2021 *IEEE Access* **9** 138543
[53] Dinh H Q, Nguyen B T and Yamaka W 2020 *IEEE Access* **8** 124608
[54] Chen J Z, Li J P and Lin J 2014 *Int. J. Theor. Phys.* **53** 72
[55] Chen J, Li J, Huang Y and Lin J 2015 *Linear Algebra Appl.* **475** 186
[56] Ezerman M F, Jitman S, Kiah H M and Ling S 2013 *Int. J. Quantum Inf.* **3** 1350027
[57] Vlăduts S G and Skorobogatov A N 1991 *Problems Inform. Transmission* **27** 19
[58] Aly S A, Klappenecker A and Sarvepalli P K 2007 *IEEE Trans. Inform. Theory* **53** 1183
[59] La Guardia G G 2014 *IEEE Trans. Inform. Theory* **60** 1528
[60] Cohen G, Encheva S and Litsyn S 1999 *Proceedings of the 1999 IEEE Information Theory and Communications Workshop (Cat. No. 99EX253)* June 25, 1999, Kruger National Park, South Africa, p. 127
[61] Steane A 1999 *IEEE Trans. Inform. Theory* **45** 2492
[62] Aly S A, Grassl M, Klappenecker A, Rotteler M and Sarvepalli P K 2007 10*th Canadian Workshop on Information Theory (CWIT)*, June 6–8, 2007, Edmonton, AB, Canada, p. 180
[63] La Guardia G G 2014 *IEEE Trans. Inform. Theory* **60** 304
[64] Niehage A 2006 *Quantum Inf. Process.* **6** 143
[65] Desaki Y, Fujiwara T and Kasami T 1997 *IEEE Trans. Inform. Theory* **43** 1364
[66] Fujiwara T, Desaki Y, Sugita T and Kasami T 1997 *Proceedings of IEEE International Symposium on Information Theory*, June 29–July 4, 1997, Ulm, Germany, p. 363
[67] Aly S A, Klappenecker A and Sarvepalli P K 2006 *IEEE International Symposium on Information Theory*, July 9–14, 2006, Seattle, WA, USA, p. 1114
[68] Delsarte P 1975 *IEEE Trans. Inform. Theory* **21** 575
[69] Schmidt W M 2004 *Equations over finite fields: an elementary approach* 2nd edn. (Berlin: Springer)