Quantum Weight Enumerators

Eric M. Rains

Abstract— In a recent paper, Shor and Laflamme define two "weight enumerators" for quantum error-correcting codes, connected by a MacWilliams transform, and use them to give a linear-programming bound for quantum codes. We introduce two new enumerators which, while much less powerful at producing bounds, are useful tools nonetheless. The new enumerators are connected by a much simpler duality transform, clarifying the duality between Shor and Laflamme's enumerators. We also use the new enumerators to give a simpler condition for a quantum code to have specified minimum distance, and to extend the enumerator theory to codes with block size greater than 2.

Index Terms—Weight enumerators q-ary quantum codes.

I. INTRODUCTION

ONE of the basic problems in the theory of quantum error-correcting codes (henceforth abbreviated QECC's) is that of giving good upper bounds on the minimum distance of a QECC. The strongest technique to date for this problem is the linear programming bound introduced by Shor and Laflamme [8]. Their bound involves the definition of two "weight enumerators" for a QECC; the two enumerators satisfy certain inequalities (e.g., nonnegative coefficients), and are related by MacWilliams identities. This allows linear programming to be applied, just as for classical error-correcting codes [5].

We introduce two new enumerators, called unitary enumerators, with simple definitions, manifestly invariant under equivalences of quantum codes. This leads to simpler conditions for codes to have specified minimum distance. Moreover, the duality between the unitary enumerators is much simpler than the duality between the Shor–Laflamme enumerators, hopefully helping to clarify the nature of that duality.

The final benefit of the unitary enumerators is that they generalize easily to block quantum codes (codes in which the basic unit has more than two states), allowing all of the enumerator machinery to be applied there as well.

Section II reviews the Shor–Laflamme enumerators and proves some basic results. Section III defines the unitary enumerators, shows how they are related to the Shor–Laflamme enumerators, and proves a number of results, including duality and minimum-distance criteria. Section IV extends everything to block quantum codes, first extending the unitary enumerators, then the Shor–Laflamme enumerators. Section V considers the extension of a fifth enumerator [6] to block codes. Finally, Section VI uses the new minimum-distance criteria to analyze some ways to construct new quantum codes

from old quantum codes, including, in particular, concatenation of codes.

A quick note on terminology: We will be using the terms "pure" and "impure" in place of the somewhat cumbersome terms "nondegenerate" and "degenerate"; that is, a pure code is one in which all low-weight errors act nontrivially on the codewords.

II. THE SHOR–LAFLAMME ENUMERATORS (A AND B)

Recall that a quantum code $\mathcal{C}$ is a K-dimensional subspace of a 2^n-dimensional Hilbert space V; $\mathcal{C}$ has minimum distance at least d if and only if

$$\langle v|U_{d-1}|v\rangle = \langle w|U_{d-1}|w\rangle$$

for v and w ranging over all unit vectors in $\mathcal{C}$ [4], and for U_{d-1} ranging over all $d-1$ qubit errors. We will use the notation $((n, K, d))$ to refer to such a code. Two quantum codes are equivalent if they can be mapped into each other by a permutation of the qubits combined with unitary transformations confined to each qubit.

To verify that a code has minimum distance d, it suffices [4] to restrict one's attention to errors of the form

$$\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n$$

where each σ_i ranges over the set

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

We will denote the set of such errors by $\mathcal{E}$. For an error E in $\mathcal{E}$, we define the weight $\operatorname{wt}(E)$ of E as the number of the σ_i not equal to the identity. Also, $\operatorname{supp}(E)$ is the subset of $\{1, 2, \cdots, n\}$ consisting of the indices for which $\sigma_i \neq 1$. Thus $\operatorname{wt}(E) = |\operatorname{supp}(E)|$.

We will also need the following fact:

Lemma 1: Let M be any operator on V. Then M can be written as the following linear combination of the elements of $\mathcal{E}$:

$$M = \frac{1}{2^n} \sum_{E \in \mathcal{E}} \operatorname{Tr}(ME)E.$$

Proof: Note, first, that if $E, E' \in \mathcal{E}$, then

$$\operatorname{Tr}(EE') = \begin{cases} 2^n, & E = E' \\ 0, & \text{otherwise.} \end{cases}$$

Thus $\{2^{-n/2}E | E \in \mathcal{E}\}$ gives an orthonormal basis of $\operatorname{Hom}(V, V)$, and the result follows immediately. $\square$

The Shor–Laflamme enumerators are defined (up to a normalization factor which we omit)

$$A_d(M_1, M_2) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E) = d}} \mathrm{Tr}(EM_1) \mathrm{Tr}(EM_2)$$

$$B_d(M_1, M_2) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E) = d}} \mathrm{Tr}(EM_1 EM_2)$$

where M_1 and M_2 are operators on V.

Theorem 2: Let P be the orthogonal projection onto a quantum code $\mathcal{C}$ of dimension K. Then

$$KB_i(P, P) \geq A_i(P, P) \geq 0$$

for $0 \leq i \leq n$.

Proof: (An alternate proof is given in [8].)

First, note that

$$A_d(M, M^\dagger) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E) = d}} |\mathrm{Tr}(EM)|^2$$

so, in particular, $A_d(P, P) \geq 0$.

Now, let v be a random unit vector from $\mathcal{C}$, uniformly distributed, and consider

$$E\left(A_d\left(vv^\dagger - \frac{1}{K}P, vv^\dagger - \frac{1}{K}P\right)\right) \geq 0.$$

In general, let O be any operator on V, and consider

$$E\left(\left|\mathrm{Tr}(Ovv^\dagger) - \frac{1}{K}\mathrm{Tr}(OP)\right|^2\right)$$
$$= E(|\langle v|O|v\rangle|^2) - \frac{1}{K^2}|\mathrm{Tr}(OP)|^2$$
$$= \frac{1}{K(K+1)}(|\mathrm{Tr}(OP)|^2 + \mathrm{Tr}(OPO^\dagger P))$$
$$\quad - \frac{1}{K^2}|\mathrm{Tr}(OP)|^2$$
$$= \frac{1}{K^2(K+1)}(K\mathrm{Tr}(OPO^\dagger P) - |\mathrm{Tr}(OP)|^2).$$

Consequently,

$$E\left(A_d\left(vv^\dagger - \frac{1}{K}P, vv^\dagger - \frac{1}{K}P\right)\right)$$
$$= \frac{1}{K^2(K+1)}(KB_d(P, P) - A_d(P, P))$$

and

$$KB_d(P, P) \geq A_d(P, P). \qquad \square$$

We will also have occasion to use enumerators $A_S(M_1, M_2)$ and $B_S(M_1, M_2)$, where $S \subset \{1, 2, \cdots, n\}$

$$A_S(M_1, M_2) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{supp}(E) = S}} \mathrm{Tr}(M_1 E) \mathrm{Tr}(M_2 E)$$

$$B_S(M_1, M_2) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{supp}(E) = S}} \mathrm{Tr}(M_1 E M_2 E).$$

Clearly Theorem 2 applies to these enumerators as well.

Finally, we consider two polynomials

$$A_{M_1 M_2}(x, y) = \sum_{0 \leq d \leq n} A_d(M_1, M_2) x^{n-d} y^d$$

$$B_{M_1 M_2}(x, y) = \sum_{0 \leq d \leq n} B_d(M_1, M_2) x^{n-d} y^d.$$

III. THE UNITARY ENUMERATORS (A' AND B')

One problem with the Shor–Laflamme enumerators as defined is that, while they are indeed invariants of the code under the $U(2)$ action on each qubit ([8], also see below), this is not immediately obvious from their definition. This motivates the introduction of two new enumerators A' and B'.

Definition: Let S be any subset of $\{1, 2, \cdots, n\}$, and let M_1 and M_2 be any operators on V. Then define

$$A'_S(M_1, M_2) = 2^{|S|} E_{U_S} \mathrm{Tr}(M_1 U_S) \mathrm{Tr}(M_2 U_S^\dagger)$$
$$B'_S(M_1, M_2) = 2^{|S|} E_{U_S} \mathrm{Tr}(M_1 U_S M_2 U_S^\dagger)$$

where U_S is a (uniformly) random unitary operator on the qubits indexed by S.

These are clearly invariant under any equivalence that maps qubits in S to qubits in S. Similarly, we define

$$A'_d(M_1, M_2) = \sum_{|S| = d} A'_S(M_1, M_2)$$

$$B'_d(M_1, M_2) = \sum_{|S| = d} B'_S(M_1, M_2).$$

These are clearly invariants under equivalence. We also consider polynomials $A'_{M_1 M_2}(x, y)$ and $B'_{M_1 M_2}(x, y)$, defined in the obvious way.

The new enumerators have the following simpler definitions:

Theorem 3: Let M_1 and M_2 be any operators on V. Then

$$A'_S(M_1, M_2) = \mathrm{Tr}_S(\mathrm{Tr}_{S^c}(M_1) \mathrm{Tr}_{S^c}(M_2))$$
$$B'_S(M_1, M_2) = \mathrm{Tr}_{S^c}(\mathrm{Tr}_S(M_1) \mathrm{Tr}_S(M_2))$$

where S^c denotes the complement of S. In particular,

$$A'_S(M_1, M_2) = B'_{S^c}(M_1, M_2).$$

Proof: We will use the following facts about random unitary matrices:

$$E_U(\mathrm{Tr}(AU) \mathrm{Tr}(BU^\dagger)) = \frac{1}{\dim(U)} \mathrm{Tr}(AB)$$

$$E_U(UAU^\dagger) = \frac{1}{\dim(U)} \mathrm{Tr}(A)$$

both of which follow easily from the fact that Tr is an irreducible character of the unitary group.

Now, then, we have:

$$A'_S(M_1, M_2) = 2^{|S|} E_{U_S} \mathrm{Tr}(M_1 U_S) \mathrm{Tr}(M_2 U_S^\dagger)$$
$$= 2^{|S|} E_{U_S} \mathrm{Tr}_S(\mathrm{Tr}_{S^c}(M_1) U_S)$$
$$\quad \cdot \mathrm{Tr}_S(\mathrm{Tr}_{S^c}(M_2) U_S^\dagger)$$
$$= \mathrm{Tr}(\mathrm{Tr}_{S^c}(M_1) \mathrm{Tr}_{S^c}(M_2)).$$

For B'_S, the proof is slightly more complicated. The crucial observation is that

$$
\begin{aligned}
B'_S(M_1, M_2) &= B'_S(E_{U_S}(U_S M_1 U_S^\dagger), E_{U_S}(U_S M_2 U_S^\dagger))\\
&= 2^{-2|S|} B'_S(\mathrm{Tr}_S(M_1) \otimes 1_S, \mathrm{Tr}_S(M_2) \otimes 1_S)\\
&= 2^{-|S|} \mathrm{Tr}\left((\mathrm{Tr}_S(M_1) \otimes 1_S)(\mathrm{Tr}_S(M_2) \otimes 1_S)\right)\\
&= \mathrm{Tr}_{S^c}(\mathrm{Tr}_S(M_1)\mathrm{Tr}_S(M_2)). \qquad \square
\end{aligned}
$$

These new enumerators are closely related to the Shor–Laflamme enumerators.

Theorem 4: Let M_1 and M_2 be any operators on V. Then

$$
A'_S(M_1, M_2) = 2^{-|S|} \sum_{T \subset S} A_T(M_1, M_2)
$$
$$
B'_S(M_1, M_2) = 2^{-|S|} \sum_{T \subset S} B_T(M_1, M_2).
$$

Proof: Expand U_S in terms of $\mathcal{E}$, using Lemma 1

$$
\begin{aligned}
A'_S(M_1, M_2) &= 2^{|S|} E_{U_S} \mathrm{Tr}\,(M_1 U_S)\,\mathrm{Tr}\,(M_2 U_S^\dagger)\\
&= 2^{|S|} 2^{-2n} \sum_{E_1, E_2 \in \mathcal{E}} E_{U_S}(\mathrm{Tr}\,(U_S E_1)\,\mathrm{Tr}\,(U_S^\dagger E_2))\\
&\quad \cdot \mathrm{Tr}\,(M_1 E_1)\,\mathrm{Tr}(M_2 E_2)
\end{aligned}
$$

and similarly for $B'_S(M_1, M_2)$. Thus we need to compute

$$
2^{|S|} E_{U_S}(\mathrm{Tr}\,(U_S E_1)\,\mathrm{Tr}\,(U_S^\dagger E_2)) = A_S(E_1, E_2).
$$

Now, by Theorem 3,

$$
A'_S(E_1, E_2) = \mathrm{Tr}_S(\mathrm{Tr}_{S^c}(E_1)\,\mathrm{Tr}_{S^c}(E_2)).
$$

If $\mathrm{supp}\,(E_1) \not\subset S$, then $\mathrm{Tr}_{S^c}(E_1) = 0$; otherwise, if both $\mathrm{supp}\,(E_1)$ and $\mathrm{supp}\,(E_2) \subset S$, then $A'_S(E_1, E_2) = 0$ unless $E_1 = E_2$, when

$$
A'_S(E_1, E_2) = 2^{|S|} 2^{2(n-|S|)} = 2^{2n-|S|}.
$$

Thus

$$
\begin{aligned}
A'_S(M_1, M_2) &= 2^{-|S|} \sum_{\substack{E \in \mathcal{E}\\ \mathrm{supp}\,(E) \subset S}} \mathrm{Tr}\,(M_1 E)\,\mathrm{Tr}\,(M_2 E)\\
&= 2^{-|S|} \sum_{T \subset S} A_T(M_1, M_2)
\end{aligned}
$$

and similarly for B'. $\square$

Corollary 5: Let M_1 and M_2 be operators on V. Then

$$
A'_d(M_1, M_2) = 2^{-d} \sum_{0 \leq i \leq d} \binom{n-i}{n-d} A_i(M_1, M_2)
$$
$$
B'_d(M_1, M_2) = 2^{-d} \sum_{0 \leq i \leq d} \binom{n-i}{n-d} B_i(M_1, M_2).
$$

Similarly,

$$
A'_{M_1 M_2}(x, y) = A_{M_1 M_2}(x + y/2, y/2)
$$
$$
B'_{M_1 M_2}(x, y) = B_{M_1 M_2}(x + y/2, y/2).
$$

Proof: We have

$$
\begin{aligned}
A'_d(M_1, M_2) &= \sum_{|S|=d} A'_S(M_1, M_2)\\
&= 2^{-d} \sum_{|S|=d} \sum_{T \subset S} A_T(M_1, M_2)\\
&= 2^{-d} \sum_{0 \leq i \leq d} \sum_{|T|=i} \sum_{\substack{S \supset T\\ |S|=d}} A_T(M_1, M_2)\\
&= 2^{-d} \sum_{0 \leq i \leq d} \sum_{|T|=i} \binom{n-i}{n-d} A_T(M_1, M_2)\\
&= 2^{-d} \sum_{0 \leq i \leq d} \binom{n-i}{n-d} A_i(M_1, M_2)
\end{aligned}
$$

and similarly for B'.

For the enumerator polynomials, we have

$$
\begin{aligned}
A'_{M_1 M_2}(x, y) &= \sum_{0 \leq d \leq n} A'_d(M_1, M_2) x^{n-d} y^d\\
&= \sum_{0 \leq d \leq n} 2^{-d} \sum_{0 \leq i \leq d} \binom{n-i}{n-d} A_i(M_1, M_2) x^{n-d} y^d\\
&= \sum_{0 \leq i \leq n} A_i(M_1, M_2) \sum_{i \leq d \leq n} 2^{-d} \binom{n-i}{n-d} x^{n-d} y^d\\
&= \sum_{0 \leq i \leq n} A_i(M_1, M_2) \left(\frac{y}{2}\right)^i \left(x + \frac{y}{2}\right)^{n-i},\\
&= A_{M_1 M_2}(x + y/2, y/2)
\end{aligned}
$$

and similarly for B'. $\square$

Corollary 6: The enumerators $A_{M_1 M_2}$ and $B_{M_1 M_2}$ are invariants under equivalence.

Proof: The quantities A_d and B_d are fixed linear combinations of the manifestly invariant quantities A'_i and B'_i. $\square$

Recall from Theorem 3 that $A'_S = B'_{S^c}$, and thus $A'_d = B'_{n-d}$ and $A'(x, y) = B'(y, x)$. This implies the following relationship between $A(x, y)$ and $B(x, y)$.

Theorem 7 (Quantum MacWilliams Identities): Let $A_{M_1 M_2}$ and $B_{M_1 M_2}$ be the Shor–Laflamme enumerators associated to a pair of operators M_1 and M_2. Then

$$
A_{M_1 M_2}(x, y) = B_{M_1 M_2}\left(\frac{x+3y}{2}, \frac{x-y}{2}\right).
$$

Proof: (see also [8])

$$
\begin{aligned}
A_{M_1 M_2}(x, y) &= A'_{M_1 M_2}(x - y, 2y) = B'_{M_1 M_2}(2y, x - y)\\
&= B_{M_1 M_2}\left(2y + \frac{x-y}{2}, \frac{x-y}{2}\right)\\
&= B_{M_1 M_2}\left(\frac{x+3y}{2}, \frac{x-y}{2}\right). \qquad \square
\end{aligned}
$$

Theorem 8: Let $\mathcal{C}$ be a quantum code of dimension K, with associated projection P. Then for $0 \leq i \leq n$

$$
K B'_i(P, P) \geq A'_i(P, P).
$$

Furthermore, $KB'_{d-1}(P,P) = A'_{d-1}(P,P)$ if and only if $\mathcal{C}$ has minimum distance at least d. If $K = 1$, then $B'_i(P,P) = A'_i(P,P)$ for all i.

Proof: By the same proof as for Theorem 2, we have

$$KB'_i(P,P) - A'_i(P,P)$$
$$= K^2(K+1)E_{v\in\mathcal{C}}A'_i\left(vv^\dagger - \frac{1}{K}P, vv^\dagger - \frac{1}{K}P\right).$$

Consequently,

$$KB'_i(P,P) - A'_i(P,P) \geq 0$$

with equality only when

$$E_{v\in\mathcal{C}}\left|\langle v|U_i|v\rangle - \frac{1}{K}\mathrm{Tr}(U_iP)\right|^2 = 0$$

where U_i ranges over all i-qubit errors. But this expectation is simply a variance; consequently, it is 0 precisely when

$$\langle v|U_i|v\rangle = \langle w|U_i|w\rangle$$

for v and w ranging over all unit vectors in $\mathcal{C}$. This is precisely the condition that $\mathcal{C}$ have minimum distance $i + 1$.

Finally, if $K = 1$, then we have

$$B'_i(P,P) \geq A'_i(P,P) = B'_{n-i}(P,P)$$
$$\geq A'_{n-i}(P,P) = B'_i(P,P)$$

so $B'_i(P,P) = A'_i(P,P)$. $\quad\square$

Corollary 9: Let $\mathcal{C}$ be a quantum code of dimension K, with associated projection P. Then $\mathcal{C}$ has minimum distance at least d if and only if

$$KB_i(P,P) = A_i(P,P)$$

for $0 \leq i < d$.

Proof: The quantity

$$KB'_{d-1}(P,P) - A'_{d-1}(P,P)$$

is a positive linear combination of

$$KB_i(P,P) - A_i(P,P)$$

for $0 \leq i < d$; the result follows immediately. $\quad\square$

We also have the following result:

Theorem 10: Let $\mathcal{C}$ be a quantum code of dimension K, with associated projection P. Then

$$KB'_S(P,P) = A'_S(P,P)$$

if and only if

$$\mathrm{Tr}_{S^c}(vv^\dagger)$$

is constant when v ranges over unit vectors in $\mathcal{C}$.

Proof: As before, we have

$$KB'_S(P,P) - A'_S(P,P) \propto E_{v\in\mathcal{C}}A'_S\left(vv^\dagger - \frac{1}{K}P, vv^\dagger - \frac{1}{K}P\right).$$

So equality holds if and only if

$$E_{v\in\mathcal{C}}\left|\mathrm{Tr}_{S^c}\left(vv^\dagger - \frac{1}{K}P\right)\right|^2 = 0$$

or

$$\mathrm{Tr}_{S^c}(vv^\dagger) = \frac{1}{K}\mathrm{Tr}_{S^c}(P)$$

for all unit vectors $v \in \mathcal{C}$. $\quad\square$

This result has the following physical interpretation: $KB'_S(P,P) = A'_S(P,P)$ if and only if the code $\mathcal{C}$ can correct for the erasure of the qubits in S; the qubits in S alone carry no information about the encoded state. (Such errors can occur, for instance, in photon-based implementations of quantum computers, in which occasionally a photon is lost.) Consequently, we have the following result:

Theorem 11: A quantum code $\mathcal{C}$ has minimum distance d if and only if it can correct for any erasure of size $d - 1$.

Remark: When talking about correcting for erasures, the assumption is that it is known which qubits have been erased. The point of this theorem is that it is generally easier to give an algorithm for correcting erasures than to give an algorithm for correcting ordinary errors; see, for instance, Theorem 21 below.

Remark: This theorem is the analog of a theorem for classical error-correcting codes [5]. Also, this theorem has been independently proved in [3].

IV. ENUMERATORS FOR CODES OF BLOCK SIZE GREATER THAN 2

We now wish to generalize everything to codes with block size greater than 2. That is, we replace the state space V by a tensor product of n Hilbert spaces V_1 through V_n, with $\dim(V_i) = D_i$, not necessarily equal to 2; in general, we will not even assume that the V_i all have the same dimension. A quantum code is again a subspace $\mathcal{C}$ of V.

Clearly, the unitary enumerators extend directly to this case, where we extend the simpler definitions of Theorem 3.

Definition: Let S be any subset of $\{1, 2, \cdots, n\}$, and let M_1 and M_2 be any operators on V. Then define

$$A'_S(M_1, M_2) = \mathrm{Tr}_S(\mathrm{Tr}_{S^c}(M_1)\mathrm{Tr}_{S^c}(M_2))$$
$$B'_S(M_1, M_2) = \mathrm{Tr}_{S^c}(\mathrm{Tr}_S(M_1)\mathrm{Tr}_S(M_2)).$$

We could also have defined these as we did for binary codes:

Theorem 12: For any S and operators M_1, M_2

$$A'_S(M_1, M_2) = \dim(V_S)E_{U_S}(\mathrm{Tr}(M_1U_S)\mathrm{Tr}(M_2U_S^\dagger))$$
$$B'_S(M_1, M_2) = \dim(V_S)E_{U_S}(\mathrm{Tr}(M_1U_SM_2U_S^\dagger)).$$

Proof: The proof of Theorem 3 carries over directly. $\square$

To generalize A_S and B_S, it will be convenient to introduce yet another definition of A'_S and B'_S. First, we define two operations on operators.

Definition: For an operator M on V, define new operators M'_S and M_S for all $S \subset \{1, 2, \cdots, n\}$

$$M'_S = \frac{1}{\dim(V_{S^c})}(\mathrm{Tr}_{S^c}(M) \otimes 1_{S^c})$$

$$M_S = \sum_{T \subset S} (-1)^{|S|-|T|} M'_T.$$

Theorem 13: For all operators M, N

$$A'_S(M, N) = \dim(V_{S^c})\mathrm{Tr}(M'_S N'_S)$$
$$B'_S(M, N) = \dim(V)E_{U \in U(V)}A'_S(MU, NU^\dagger).$$

Proof: We have

$$\mathrm{Tr}(M'_S N'_S)$$
$$= \frac{1}{\dim(V_{S^c})^2}\mathrm{Tr}((\mathrm{Tr}_{S^c}(M) \otimes 1_{S^c})(\mathrm{Tr}_{S^c}(N) \otimes 1_{S^c}))$$
$$= \frac{1}{\dim(V_{S^c})}\mathrm{Tr}(\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(N)).$$

The statement about B'_S follows easily from Theorem 12. $\square$

We can now define A_S and B_S.

Definition: Let S be any subset of $\{1, 2, \cdots, n\}$, and let M and N be any operators on V. Then define

$$A_S(M, N) = \dim(V)\mathrm{Tr}(M_S N_S)$$
$$B_S(M, N) = \dim(V)E_{U \in U(V)}A_S(MU, NU^\dagger).$$

It will follow from Theorem 16 below that this is consistent with our earlier definition for the binary case. To see how these relate to A' and B', we will need the following results.

Lemma 14: The map $M \mapsto M'_S$ is an orthogonal projection on $\mathrm{Hom}(V, V)$ for all S. Moreover,

$$(M'_S)'_T = M'_{S \cap T}.$$

Proof: Let us first show that

$$(M'_S)'_T = M'_{S \cap T}.$$

Now

$$(M'_S)'_T = \frac{1}{\dim(V_{T^c})}(\mathrm{Tr}_{T^c}(M'_S) \otimes 1_{T^c})$$
$$= \frac{1}{\dim(V_{T^c})\dim(V_{S^c})}$$
$$\quad \cdot (\mathrm{Tr}_{T^c}(\mathrm{Tr}_{S^c}(M) \otimes 1_{S^c}) \otimes 1_{T^c})$$
$$= \frac{\dim(V_{S^c \cap T^c})}{\dim(V_{T^c})\dim(V_{S^c})}\mathrm{Tr}_{S^c \cup T^c}(M) \otimes 1_{S^c \cup T^c}$$
$$= M'_{S \cap T}.$$

In particular, $(M'_S)'_S = M'_S$. It remains only to show that if $M'_S = M$ and $N'_S = 0$, then

$$\mathrm{Tr}(MN) = 0.$$

But $N'_S = 0$ if and only if $\mathrm{Tr}_{S^c}(N) = 0$. Thus

$$\mathrm{Tr}(MN) = \mathrm{Tr}(M'_S N)$$
$$= \mathrm{Tr}((\mathrm{Tr}_{S^c}(M) \otimes 1_{S^c})N)$$
$$= \mathrm{Tr}(\mathrm{Tr}_{S^c}(M)\,\mathrm{Tr}_{S^c}(N))$$
$$= 0. \qquad \square$$

Corollary 15: For all $S \subset \{1, 2, \cdots, n\}$, the map $M \mapsto M_S$ is an orthogonal projection. Moreover,

$$\mathrm{Tr}(M_S N_T) = 0$$

unless $S = T$, when

$$\mathrm{Tr}(M_S N_S) = \sum_{R \subset S} \mathrm{Tr}(M'_R N'_R)(-1)^{|S|-|R|}.$$

Finally,

$$M'_S = \sum_{T \subset S} M_T.$$

Proof: This follows readily from Lemma 14 and the Möbius inversion formula. $\square$

Theorem 16: Let M and N be any operators on V. Then

$$A'_S(M, N) = \frac{1}{\dim(V_S)} \sum_{T \subset S} A_T(M, N)$$
$$B'_S(M, N) = \frac{1}{\dim(V_S)} \sum_{T \subset S} B_T(M, N)$$
$$A_S(M, N) = \sum_{T \subset S} (-1)^{|S|-|T|} \dim(V_T)A'_T(M, N)$$
$$B_S(M, N) = \sum_{T \subset S} (-1)^{|S|-|T|} \dim(V_T)B'_T(M, N).$$

Proof: We have

$$A'_S(M, N) = \dim(V_{S^c})\mathrm{Tr}(M'_S N'_S)$$
$$= \dim(V_{S^c}) \sum_{T, T' \subset S} \mathrm{Tr}(M_T N_{T'})$$
$$= \dim(V_{S^c}) \sum_{T \subset S} \mathrm{Tr}(M_T N_T)$$
$$= \frac{1}{\dim(V_S)} \sum_{T \subset S} A_T(M, N).$$

The remaining results follow similarly. $\square$

Theorem 17: Let $\mathcal{C}$ be a quantum code of dimension K in V, and let P be its associated projection. Then for all $S \subset \{1, 2, \cdots, n\}$

$$KB'_S(P, P) \geq A'_S(P, P) \geq 0$$
$$KB_S(P, P) \geq A_S(P, P) \geq 0.$$

In particular, if $K = 1$, then $A'_S(P, P) = B'_S(P, P)$ and $A_S(P, P) = B_S(P, P)$.

Proof: The proof for A' and B' proceeds as in Theorem 8; it remains only to consider A and B.

First, let M be any operator on V, and observe that

$$A_S(M, M^\dagger) = \dim(V) \operatorname{Tr}(M_S M_S^\dagger) \geq 0.$$

Now, let v be a uniformly randomly chosen unit vector from $\mathcal{C}$. Then

$$E_{v \in \mathcal{C}} A_S\left(vv^\dagger - \frac{1}{K}P, vv^\dagger - \frac{1}{K}P\right)$$
$$= \frac{1}{K^2(K+1)}(KB_S(P,P) - A_S(P,P)).$$

This is just a linear combination of the corresponding equations for A' and B'. The theorem follows. $\square$

Let us now assume that $D_i = D$ for all i. Then it makes sense to consider

$$A_d = \sum_{|S|=d} A_S$$

and so on.

Theorem 18: Let $\mathcal{C}$ be a quantum code of dimension K in V, with associated projection P. Then $\mathcal{C}$ has minimum distance at least d if and only if

$$KB_i(P,P) = A_i(P,P)$$

for $0 \leq i < d$.

Proof: Clearly, $\mathcal{C}$ has minimum distance at least d if and only if

$$KB'_{d-1}(P,P) = A'_{d-1}(P,P).$$

But $KB'_{d-1}(P,P) - A'_{d-1}(P,P)$ is a positive linear combination of $KB_i(P,P) - A_i(P,P)$ for $0 \leq i \leq d-1$. $\square$

We also have a MacWilliams transform:

Theorem 19: Let $A_{M_1 M_2}$, $B_{M_1 M_2}$, $A'_{M_1 M_2}$, and $B'_{M_1 M_2}$ be the polynomial enumerators associated with a pair of operators M_1 and M_2. Then

$$A'_{M_1 M_2}(x,y) = B'_{M_1 M_2}(y,x)$$
$$A_{M_1 M_2}(x,y) = B_{M_1 M_2}\left(\frac{x+(D^2-1)y}{D}, \frac{x-y}{D}\right).$$

Proof: The first assertion follows by inspection. For the second assertion, we note that

$$A'_{M_1 M_2}(x,y) = A_{M_1 M_2}\left(x + \frac{y}{D}, \frac{y}{D}\right)$$
$$B'_{M_1 M_2}(x,y) = B_{M_1 M_2}\left(x + \frac{y}{D}, \frac{y}{D}\right)$$
$$A_{M_1 M_2}(x,y) = A'_{M_1 M_2}(x - y, Dy)$$
$$B_{M_1 M_2}(x,y) = B'_{M_1 M_2}(x - y, Dy)$$

so

$$A_{M_1 M_2}(x,y) = A'_{M_1 M_2}(x - y, Dy) = B'_{M_1 M_2}(Dy, x - y)$$
$$= B_{M_1 M_2}\left(Dy + \frac{x-y}{D}, \frac{x-y}{D}\right)$$
$$= B_{M_1 M_2}\left(\frac{x+(D^2-1)y}{D}, \frac{x-y}{D}\right). \quad \square$$

V. SHADOW ENUMERATORS

For binary codes, there is an additional enumerator to consider, namely, the shadow enumerator [6], which can be defined by

$$S_{\mathcal{C}}(x,y) = A_{\mathcal{C}}\left(\frac{x+3y}{2}, \frac{x-y}{2}\right).$$

If one writes $S_{\mathcal{C}}(x,y)$ in terms of $A'_{\mathcal{C}}(x,y)$, something rather curious happens

$$S_{\mathcal{C}}(x,y) = A'_{\mathcal{C}}(x+y, y-x).$$

This suggests the following definition for arbitrary block sizes:

Definition: Let T be any subset of $\{1, 2, \cdots, n\}$, and let M, N be operators on V. Then the shadow enumerator of M and N is defined by

$$S_T(M,N) = \sum_{R \subset \{1,2,\cdots,n\}} (-1)^{|R \cap T^c|} A'_R(M,N).$$

The conjecture is then that $S_T(M,N) \geq 0$ whenever M and N are positive semidefinite Hermitian operators (the case when $D_i = 2$ for all i was essentially proved in [6]). More explicitly

Conjecture: Let $V = V_1 \otimes V_2 \otimes \cdots \otimes V_n$, where V_1 through V_n are Hilbert spaces. Let T be any subset of $\{1, 2, \cdots, n\}$, and let M and N be positive semidefinite Hermitian operators on V. Then

$$\sum_{S \subset \{1,2,\cdots,n\}} (-1)^{|S \cap T|} \operatorname{Tr}\left(\operatorname{Tr}_{S^c}(M) \operatorname{Tr}_{S^c}(N)\right) \geq 0.$$

When $n = 1$, this becomes

$$|\operatorname{Tr}(M) \operatorname{Tr}(N)| \geq |\operatorname{Tr}(MN)|$$

which is easy to verify.

In fact, this is no longer a conjecture; a proof of a generalization appears in [7].

VI. CONSTRUCTIONS FOR QUANTUM CODES

We will now use the unitary enumerators to examine some constructions of new quantum codes from existing quantum codes. We will assume that D_i is constant ($=D$) throughout.

Theorem 20: Suppose $\mathcal{C}$ is a pure $((n, K, d))$ with $n, d \geq 2$. Then there exists a pure $((n-1, DK, d-1))$.

Proof: Let P be the projection associated with $\mathcal{C}$, and let $P' = D \operatorname{Tr}_{\{1\}}(P)$. The claim is then that P' is the projection associated with the desired code.

First, note that

$$\operatorname{Tr}(P'^2) = D^2 B'_{\{1\}}(P) = DK = \operatorname{Tr}(P').$$

This, combined with the fact that P' has at most DK distinct eigenvalues, implies that P' is a projection.

It remains to show that P' is pure of minimum distance $d-1$. Thus let S be a set of size $d-2$ in $\{2, 3, \cdots, n\}$, and

observe

$$
\begin{aligned}
B'_S(P', P') &= \operatorname{Tr}(\operatorname{Tr}_S(P')^2) \\
&= D^2 \operatorname{Tr}(\operatorname{Tr}_{S \cup \{1\}}(P)^2) \\
&= D^2 B'_{S \cup \{1\}}(P) \\
&= D^2 D^{1-d} K \\
&= D^{2-d}(DK). \qquad \square
\end{aligned}
$$

If $K = 1$, this construction is reversible.

Theorem 21: Suppose $\mathcal{C}$ is a quantum code with projection matrix P of rank D. Then there exists a code $\mathcal{C}'$ with $P = D \operatorname{Tr}_{\{1\}}(P')$; any two such codes are equivalent. The new code has unitary enumerator

$$
A'_i(\mathcal{C}') = D^{-2}(A'_i(\mathcal{C}) + B'_{i-1}(\mathcal{C})).
$$

Proof: P' clearly must have rank 1; consequently, we need a vector v' with $P' = v' v'^\dagger$.

Since $\operatorname{Tr}_{\{1\}}(v' v'^\dagger)$ is a projection, it follows that v' must be writable in the form

$$
\sum_{0 \le i < D} \frac{1}{\sqrt{D}} w_i \otimes v_i
$$

where v_i ranges over some orthonormal basis for $\mathcal{C}$, and w_i ranges over some orthonormal basis for V_1. Conversely, any such v' gives a suitable P'. Uniqueness follows from the fact that the freedom in the w_i can be absorbed into the freedom in the v_i, which in turn can be absorbed by applying an element of $U(V_1)$.

Finally, let $S \subset \{1, 2, \cdots, n\}$. If S does not contain 1, then

$$
\begin{aligned}
A'_S(P', P') &= \operatorname{Tr}_S(\operatorname{Tr}_{S^c}(P')^2) \\
&= D^{-2} \operatorname{Tr}_S(\operatorname{Tr}_{S^c}(P)^2) \\
&= D^{-2} A_S(P, P).
\end{aligned}
$$

Now, if S does contain 1, we have

$$
\begin{aligned}
A'_S(P', P') &= B'_{S^c}(P', P') \\
&= A'_{S^c}(P', P') \\
&= D^{-2} A'_{S^c}(P, P) \\
&= D^{-2} B'_{S-\{1\}}(P, P)
\end{aligned}
$$

where the second and fourth equalities follow from Theorem 16 and the fact that P' has rank 1.

The desired result follows by summing over S of size i. $\square$

Finally, let us consider concatenated codes. Let $\mathcal{C}_1$ be an $((n_1, K_1, d_1))$, on blocks of size D_1, and let $\mathcal{C}_2$ be an $((n_2, D_1, d_2))$, on blocks of size D_2. Then one can construct a new code $\mathcal{C}_2(\mathcal{C}_1)$, by encoding each block of $\mathcal{C}_1$ using $\mathcal{C}_2$. (Strictly speaking, the concatenated code also depends on the specific encoding map used for $\mathcal{C}_2$.) Clearly, the concatenated code encodes K_1 states in $n_1 n_2$ blocks of size $D_1 D_2$; it remains only to consider its minimum distance.

Theorem 22: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be as above. Let $\mathcal{C} = \mathcal{C}_2(\mathcal{C}_1)$ be any concatenation of $\mathcal{C}_1$ and $\mathcal{C}_2$. Then $\mathcal{C}$ has minimum distance at least $d_1 d_2$.

Proof: By Theorem 11 (which clearly holds for block codes as well), it suffices to give an algorithm for correcting erasures of size $d_1 d_2 - 1$. Suppose, therefore, that $d_1 d_2 - 1$ blocks of $\mathcal{C}$ have been erased. The correction algorithm is quite simple: decode the outer encoding, then decode the inner encoding.

We can decode erasures of up to size $d_2 - 1$ in $\mathcal{C}_2$. Thus the only blocks of the inner encoding that will be unrecoverable are those that suffered at least d_2 erasures. Clearly, there can be at most $d_1 - 1$ such blocks. But this can be corrected, using the decoding algorithm for $\mathcal{C}_1$. $\square$

Remark: This is an extension to general codes of the remarks after [2, Theorem 8].

VII. CONCLUSION

We have furthered the enumerator theory of Shor and Laflamme, with the help of two new manifestly invariant enumerators. Since the definition of these enumerators did not depend on the codes being binary, we could readily extend the theory to quantum codes on larger alphabets. We also used the new enumerators to clarify the nature of the relationship between the Shor–Laflamme enumerators, and to give a simpler condition for a quantum code to have specified minimum distance.

ACKNOWLEDGMENT

REFERENCES

[1] C. H. Bennett, D. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, 1996. Also, LANL e-print quant-ph/9604024.

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," this issue, pp. 1369–1387.

[3] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A*, vol. 56, no. 1, pp. 33–38, 1997. Also, LANL e-print quant-ph/9610042.

[4] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900–911, 1997. Also, LANL e-print quant-ph/9604034.

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

[6] E. M. Rains, "Quantum shadow enumerators," LANL e-print quant-ph/9611001.

[7] _____, "Polynomial invariants of quantum codes," LANL e-print quant-ph/9704042.

[8] P. W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600–1602, 1997. Also LANL e-print quant-ph/9610040.