Quantum Shadow 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 extend their work by introducing another enumerator, based on the classical theory of shadow codes, that tightens their bounds significantly. In particular, nearly all of the codes known to be optimal among additive quantum codes (codes derived from orthogonal geometry) can be shown to be optimal among all quantum codes. We also use the shadow machinery to extend a bound on additive codes to general codes, obtaining as a consequence that any code of length n can correct at most $\lfloor \frac{n+1}{6} \rfloor$ errors.**

***Index Terms*—Linear programming, quantum error-correcting codes, shadow, upper bounds.**

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 [4].

Linear programming was first applied to bounds for quantum codes in [1], which gave bounds only for codes of the type introduced in that paper (henceforth denoted "additive" codes). The linear programming bound given there essentially consists of three families of inequalities. Two of these were generalized to arbitrary quantum codes in [8]; the current paper generalizes the third. Consequently, in the table of upper bounds given in [1], all but 11 apply in general; it follows that nearly all of the codes known to be optimal among additive codes are optimal among QECC's in general.

II. Quantum Weight Enumerators

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 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 $\mathcal{C}$, and for U_{d-1} ranging over all $d-1$ qubit errors [3]. We will use the notation $((n, K, d))$ to refer to such a code. A code is *pure* if in fact

$$\langle v|U_{d-1}|v\rangle = 2^{-n}\operatorname{Tr}(U_{d-1}).$$

For self-dual codes ($K = 1$), we follow the convention of [1], in that the notation $((n, 1, d))$ will be used only for pure codes.

To verify that a code has minimum distance d, it suffices 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

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

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, as in [1], we note that $\mathcal{E}$ has the structure of a vector space $\mathbb{F}_2^{2n}$, with a symplectic bilinear form given by

$$(-1)^{\langle E_1, E_2\rangle} = 2^{-n}\operatorname{Tr}(E_1E_2E_1E_2).$$

The weight enumerators of Shor and Laflamme can be defined as follows. Let M_1 and M_2 be Hermitian operators on the state space V. Then define

$$A_i(M_1, M_2) = \sum_{\substack{E\in\mathcal{E}\\ \operatorname{wt}(E)=i}} \operatorname{Tr}(EM_1)\operatorname{Tr}(EM_2)$$

$$B_i(M_1, M_2) = \sum_{\substack{E\in\mathcal{E}\\ \operatorname{wt}(E)=i}} \operatorname{Tr}(EM_1EM_2).$$

Note that this differs from the definition in [8] by normalization factors, in order to simplify the theory. After Shor and Laflamme, we also define two polynomials $A(x, y)$ and $B(x, y)$ by

$$A(x, y) = \sum_{0\le i\le n} A_i(M_1, M_2)x^{n-i}y^i$$

$$B(x, y) = \sum_{0\le i\le n} B_i(M_1, M_2)x^{n-i}y^i.$$

We have the following theorems, from [8].

Theorem 1 (Duality): Let M_1 and M_2 be any Hermitian operators on V. Then

$$B(x, y) = A\left(\frac{x+3y}{2}, \frac{x-y}{2}\right)$$

$$A(x, y) = B\left(\frac{x+3y}{2}, \frac{x-y}{2}\right).$$

Manuscript received November 20, 1996; revised January 12, 1999.

The author is with AT&T Research, AT&T Shannon Laboratory, Florham Park, NJ 07932-0971 USA (e-mail: rains@research.att.com).

Communicated by C. Crépeau, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(99)07678-6.

Theorem 2 (Bounds): Let P be the orthogonal projection onto an $((n, K, d))$. Then

$$\begin{aligned} A_0(P) &= K \\ A_i(P) &\geq 0 \qquad (0 \leq i \leq n) \\ B_0(P) &= K^2 \\ KB_i(P) - A_i(P) &= 0 \qquad (0 \leq i < d) \\ KB_i(P) - A_i(P) &\geq 0 \qquad (d \leq i \leq n). \end{aligned}$$

If P is pure, then also

$$B_i(P) = 0 \qquad (1 \leq i < d).$$

We will also need the following result.

Lemma 3: Let M_1 and M_2 be any positive semi-definite Hermitian operators on V. Then $B_i(M_1, M_2) \geq 0$ for $0 \leq i \leq n$.

Proof: $B_i(M_1, M_2)$ is a sum of terms of the form $\mathrm{Tr}\,(M_1 E M_2 E^{-1})$. Each of these terms is the trace of the product of two positive semi-definite Hermitian operators, and is thus nonnegative. □

III. Additive Codes

Before presenting the shadow enumerator, it is instructive to examine a special case, namely, that of additive codes [1]. An additive code $\mathcal{C}$ is derived from a subspace C of $\mathbb{F}_2^{2n}$, self-orthogonal under the symplectic inner product (that is, $\mathcal{C} \subset \mathcal{C}^{\perp}$); the orthogonal projection onto $\mathcal{C}$ is then of the form

$$P = 2^{-\dim(C)} \sum_{E \in C} s(E) E$$

where $s(E)$ are appropriately chosen signs (in particular, $s(1) = 1$).

For additive codes, A_i and B_i have combinatorial interpretations. Indeed,

$$\mathrm{Tr}\,(EP)\,\mathrm{Tr}\,(EP) = \begin{cases} 2^{2(n-\dim(C))}, & E \in C \\ 0, & \text{otherwise} \end{cases}$$

and

$$\begin{aligned} \mathrm{Tr}\,(EPEP) &= 2^{-2\dim(C)} \sum_{E' \in C} \mathrm{Tr}\,(EE'EE') \\ &= 2^{n-2\dim(C)} \sum_{E' \in C} (-1)^{\langle E, E' \rangle} \\ &= \begin{cases} 2^{n-\dim(C)}, & E \in C^{\perp} \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Consequently, $2^{-2(n-\dim(C))} A_i$ counts the number of elements of C of weight i, while $2^{-(n-\dim(C))} B_i$ counts the number of elements of $C^{\perp}$ of weight i.

There is a third combinatorial object that we can count, namely, the "shadow" $S(C)$ of C. We first recall the definition of the shadow of a (classical) self-orthogonal binary code [2].

If v and w are binary vectors, then Hamming weight satisfies the congruence

$$\mathrm{wt}\,(v+w) \equiv \mathrm{wt}\,(v) + \mathrm{wt}\,(w) + 2\langle v, w \rangle \pmod 4.$$

In particular, if C is a self-orthogonal binary code, this becomes

$$\mathrm{wt}\,(v+w) \equiv \mathrm{wt}\,(v) + \mathrm{wt}\,(w) \pmod 4$$

for all v and $w \in C$. In other words, $(\frac{1}{2}\,\mathrm{wt}) \bmod 2$ is a linear functional on C; thus there exists a coset $S(C)$ of $C^{\perp}$ such that, for $v \in S(C)$ and $w \in C$

$$\langle v, w \rangle \equiv \frac{1}{2}\,\mathrm{wt}\,(w) \pmod 2.$$

To be precise, if every vector in C has weight a multiple of 4 (doubly-even), then $S(C) = C^{\perp}$; otherwise, the set of doubly-even vectors is a subcode C_0 of C, and $S(C) = C_0^{\perp} - C^{\perp}$. For more information (and generalizations), we refer the reader to [7]. The primary relevance of the shadow is that its enumerator can be computed from the ordinary enumerator (and, because it is an enumerator, has nonnegative coefficients).

Similarly, in $\mathcal{E}$

$$\mathrm{wt}\,(E_1 E_2) \equiv \mathrm{wt}\,(E_1) + \mathrm{wt}\,(E_2) + \langle E_1, E_2 \rangle \pmod 2$$

and thus $\mathrm{wt} \bmod 2$ is linear on our additive code C. So we define $S(C)$ to be the set of all $E \in \mathcal{E}$ such that

$$\langle E, E' \rangle \equiv \mathrm{wt}\,(E') \pmod 2$$

for all $E' \in C$. And as in the classical case, we can compute the enumerator of $S(C)$.

Theorem 4: Let S_i be $2^{n-\dim(C)}$ times the number of elements of $S(C)$ of weight i, and define

$$S(x, y) = \sum_{0 \leq i \leq n} S_i x^{n-i} y^i.$$

Then

$$S(x, y) = A\left(\frac{x+3y}{2}, \frac{y-x}{2}\right).$$

Proof: Let us distinguish two cases. Either C contains an element of odd weight, or it does not. In the latter case, an error E is in $S(C)$ if and only if it is in $C^{\perp}$; moreover, $A(x, y) = A(x, -y)$. So

$$\begin{aligned} S(x, y) &= B(x, y) \\ &= A\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) \\ &= A\left(\frac{x+3y}{2}, \frac{y-x}{2}\right). \end{aligned}$$

Thus assume C contains an element of odd weight. Since C is self-orthogonal, it follows that the subset C_0 of C consisting of elements of even weight is, in fact, a subspace of codimension 1; let it have weight enumerators $A^{(0)}$ and $B^{(0)}$. Then $S(C)$ can be written as $C_0^{\perp} - C^{\perp}$. In terms of the weight enumerators, we have

$$\begin{aligned} 2^{n-\dim(C)} S(x,y) &= 2^{n-\dim(C_0)} B^{(0)}(x,y) - 2^{n-\dim(C)} B(x,y) \\ &= 2^{n-\dim(C_0)} A^{(0)}\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) \\ &\quad - 2^{n-\dim(C)} A\left(\frac{x+3y}{2}, \frac{x-y}{2}\right). \end{aligned}$$

But $2A^{(0)}(x, y) = A(x, y) + A(x, -y)$, so

$$S(x, y) = A\left(\frac{x+3y}{2}, \frac{y-x}{2}\right). \qquad \square$$

Before we proceed to general codes, it will be helpful to digress momentarily, and consider the following problem: When is an additive code real? More generally, when is it *equivalent* to a real code?

To answer the first question, recall that

$$P = 2^{-\dim(C)} \sum_{E \in C} s(E)E.$$

Thus

$$\overline{P} = 2^{-\dim(C)} \sum_{E \in C} s(E)\overline{E}.$$

We need therefore to understand what happens to an error E when we take its complex conjugate. For single-qubit errors, this is fairly straightforward

$$\overline{\mathbb{1}} = 1 \qquad \overline{\sigma}_x = \sigma_x \qquad \overline{\sigma}_y = -\sigma_y \qquad \overline{\sigma}_z = \sigma_z.$$

It follows readily that

$$\overline{E} = (-1)^{\mathrm{wt}_y(E)}E$$

where $\mathrm{wt}_y(E)$ is the number of times σ_y appears in the tensor product expansion of E. Now, a fairly straightforward computation gives us the following identity:

$$\mathrm{wt}_y(E) \equiv \mathrm{wt}\,(E) + \langle \sigma_y^{\otimes n}, E\rangle \pmod 2$$

where $\sigma_y^{\otimes n}$ is the tensor product of n copies of σ_y. Thus

$$\overline{E} = (-1)^{\mathrm{wt}\,(E)+\langle \sigma_y^{\otimes n}, E\rangle}E.$$

It follows immediately that an additive code $\mathcal{C}$ is real if and only if the error $\sigma_y^{\otimes n}$ is in $S(C)$.

Theorem 5: Any additive code is equivalent to a real additive code.

Proof: It suffices to show that any additive code has an element of weight n in its shadow, since the group of equivalences is transitive on elements of a given weight. Now, the number of elements of weight n is proportional to the coefficient of y^n in $S(x, y)$, or equivalently, to $S(0, 1)$. But then, by Theorem 4, we have

$$S(0, 1) = A\left(\frac{3}{2}, \frac{1}{2}\right).$$

This is a sum of nonnegative terms, at least one of which is strictly positive. Consequently, $S(0, 1) > 0$, and the theorem is proved. $\square$

IV. The Shadow Enumerator for General Codes

The remarks leading up to Theorem 5 suggest that a natural starting point in the generalization of the shadow enumerator involves the conjugate of P. Consider, therefore, $\mathrm{Tr}\,(P\overline{P})$. For an additive code, this is

$$\begin{aligned}\mathrm{Tr}\,(P\overline{P}) &= 2^{-2\dim(C)} \sum_{E_1,\, E_2 \in C} s(E_1)s(E_2)\,\mathrm{Tr}\,(E_1\overline{E_2}) \\ &= 2^{n-2\dim(C)} \sum_{E \in C} (-1)^{\mathrm{wt}\,(E)+\langle \sigma_y^{\otimes n},\, E\rangle} \\ &= \begin{cases} 2^{n-\dim(C)}, & \sigma_y^{\otimes n} \in S(C) \\ 0, & \text{otherwise.} \end{cases}\end{aligned}$$

More generally,

$$\mathrm{Tr}\,(PE\overline{P}E) = \begin{cases} 2^{n-\dim(C)}, & \sigma_y^{\otimes n}E \in S(C) \\ 0, & \text{otherwise.} \end{cases}$$

So $E \in S(C)$ if and only if

$$\mathrm{Tr}\,(PE\sigma_y^{\otimes n}\overline{P}\sigma_y^{\otimes n}E) = 2^{n-\dim(C)}.$$

Thus the fundamental object seems to be

$$\tilde{P} = \sigma_y^{\otimes n}\overline{P}\sigma_y^{\otimes n}.$$

Theorem 6: Let M be a Hermitian operator on the state space V. Write M as a linear combination of elements of $\mathcal{E}$

$$M = \sum_{E \in \mathcal{E}} c_E E.$$

Define $\tilde{M}$ by

$$\tilde{M} = \sum_{E \in \mathcal{E}} (-1)^{\mathrm{wt}\,(E)} c_E E.$$

Then

$$\tilde{M} = \sigma_y^{\otimes n}\overline{M}\sigma_y^{\otimes n}.$$

Consequently, $\tilde{M}$ is similar to $\overline{M}$; in particular, if M is positive semidefinite, then so is $\tilde{M}$.

Proof: Since M is Hermitian, all of the coefficients c_E must be real; consequently, we may restrict our attention to the case $M = E \in \mathcal{E}$. In that case,

$$\begin{aligned}\tilde{E} &= (-1)^{\mathrm{wt}(E)}E, \\ &= (-1)^{\mathrm{wt}_y(E)+\langle \sigma_y^{\otimes n},\, E\rangle}E \\ &= (-1)^{\langle \sigma_y^{\otimes n},\, E\rangle}\overline{E} \\ &= \sigma_y^{\otimes n}\overline{E}\sigma_y^{\otimes n}. \end{aligned} \qquad \square$$

Corollary 7: Let M and N be positive semidefinite Hermitian operators on the state space V. Define

$$S_i(M, N) = B_i(M, \tilde{N}).$$

Then for $0 \le i \le n$, $S_i(M, N) \ge 0$.

Proof: This follows immediately from Theorem 6 and Lemma 3. $\square$

It remains only to see how $S_i(M, N)$ is related to $A_i(M, N)$. Define

$$S(x, y) = \sum_{0 \le d \le n} S_i(M, N)x^{n-i}y^i.$$

Then we get the following theorem.

Theorem 8:

$$S(x, y) = A\left(\frac{x+3y}{2}, \frac{y-x}{2}\right).$$

Proof: Consider the function $W(x, y)$ defined by

$$W(x, y) = \sum_{0 \le i \le n} A_i(M, \tilde{N}) x^{n-i} y^i.$$

By Theorem 1, we have

$$S(x, y) = W\left(\frac{x+3y}{2}, \frac{x-y}{2}\right).$$

Consequently, it suffices for us to show that $W(x, y) = A(x, -y)$; in other words, that

$$A_i(M, \tilde{N}) = (-1)^i A_i(M, N).$$

But

$$\begin{aligned} A_i(M, \tilde{N}) &= \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E)=i}} \mathrm{Tr}(ME)\,\mathrm{Tr}(\tilde{N}E) \\ &= \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E)=i}} \mathrm{Tr}(ME)(-1)^i\,\mathrm{Tr}(NE) \\ &= (-1)^i A_i(M, N). \end{aligned}$$

□

Corollary 9: For any Hermitian operators M, N

$$\begin{aligned} S_i(N, M) &= S_i(M, N) \\ B_i(\tilde{M}, \tilde{N}) &= B_i(M, N). \end{aligned}$$

Proof: The first statement follows immediately from the fact that $A_i(N, M) = A_i(M, N)$, and the fact that the transform in Theorem 8 is independent of M and N. The second statement is simply that

$$S_i(\tilde{N}, M) = S_i(M, \tilde{N})$$

since $\tilde{\tilde{N}} = N$. □

This gives us the following theorem (after Theorem 21 in [1]).

Theorem 10 (LP Bound for General QECC's): If an $((n, K, d))$ exists, then there is a solution to the following set of linear equations and inequalities:

$$\begin{aligned} &A_0 = K^2 \\ &A_i \ge 0 \qquad (0 \le i \le n) \\ &B_i = \frac{1}{2^n} \sum_{0 \le r \le n} P_i(r, n) A_r \\ &A_i = K B_i \qquad (0 \le i < d) \\ &A_i \le K B_i \qquad (d \le i \le n) \\ &S_i = \frac{1}{2^n} \sum_{0 \le r \le n} (-1)^r P_i(r, n) A_r \\ &S_i \ge 0 \qquad (0 \le i \le n) \end{aligned}$$

where

$$P_i(x, n) = \sum_{0 \le s \le i} (-1)^s 3^{i-s} \binom{x}{s} \binom{n-x}{i-s}$$

are the appropriate Krawtchouk polynomials.

Proof: The first five relations come from Theorems 1 and 2; the remaining relations come from Theorem 8 and Corollary 7. □

Remark: For pure codes, the additional constraint that $A_i = B_i = 0$ for $1 \le i < d$ must hold.

Using this theorem, one can produce a table of upper bounds analogous to the table in [1]. The resulting table differs in only eleven places

$$\begin{array}{cccc} ((7, 2^0)) & ((13, 2^0)) & ((15, 2^4)) & ((15, 2^7)) \\ ((16, 2^8)) & ((18, 2^{12})) & ((19, 2^0)) & ((19, 2^8)) \\ ((19, 2^{13})) & ((22, 2^{14})) & ((25, 2^0)) & \end{array}$$

(marked by a β or γ in [1]). In each case, the new bound is precisely 1 greater than the bound for additive codes. Consequently, nearly all of the codes in [1] that are optimal among additive codes are optimal among all codes; in particular, for $1 \le n \le 12$, the only place where the bound is not known to be tight is $n = 7$, $k = 0$. It is also worth noting that, just as for additive codes, the LP bound for impure codes agrees with the LP bound for pure codes for all n checked $(1 \le n \le 50)$.

V. Parity Issues; Self-Dual Codes

In the study of additive codes, one important distinction is between even codes (those that contain no element of odd weight) and odd codes (those in which half of the elements have odd weight). This distinction carries over to general codes, using shadow theory.

Definition: A code $\mathcal{C}$ with projection matrix P is even if $P = \tilde{P}$, and odd if $\mathrm{Tr}(P\tilde{P}) = 0$.

Remarks: Note that 1) the typical nonadditive code is neither even nor odd and 2) an equivalent criterion for a code to be even is $S_0(\mathcal{C}) = \mathrm{Tr}(P\tilde{P}) = K$; similarly, a code is odd if and only if $S_0(\mathcal{C}) = 0$.

If $\mathcal{C}$ is odd, we can define a new code $\mathcal{C}_0$, called the "even subcode," as the image of the projection

$$P + \tilde{P}.$$

(Note that the even subcode of a code is actually *larger*; the terminology is by analogy with the additive case.)

Theorem 11: Let $\mathcal{C}$ be an odd code, and let $\mathcal{C}_0$ be its even subcode. Then

$$\begin{aligned} A_i(\mathcal{C}_0) &= \begin{cases} 4A_i(\mathcal{C}), & i \equiv 0 \pmod 2 \\ 0, & i \equiv 1 \pmod 2 \end{cases} \\ B_i(\mathcal{C}_0) &= 2(B_i(\mathcal{C}) + S_i(\mathcal{C})). \end{aligned}$$

Proof: First A_i:

$$\begin{aligned} A_i(\mathcal{C}_0) &= A_i(P + \tilde{P}) \\ &= A_i(P) + A_i(\tilde{P}) + 2A_i(P, \tilde{P}). \end{aligned}$$

Since $A_i(P, \tilde{P}) = (-1)^i A_i(P)$, the result follows immediately. Similarly,

$$\begin{aligned} B_i(\mathcal{C}_0) &= B_i(P) + B_i(\tilde{P}) + 2B_i(P, \tilde{P}) \\ &= 2(B_i(P) + S_i(P)). \end{aligned}$$

□

An interesting thing happens with the shadow enumerator for self-dual codes (that is, codes with $K = 1$). In this case, P has rank 1, so it may be written as $vv^\dagger$, with v a unit vector. So we have

$$\begin{aligned} S_i(P) &= \sum_{\substack{E\in\mathcal{E}\\ \mathrm{wt}(E)=i}} \mathrm{Tr}\,(vv^\dagger E\sigma_y^{\otimes n}\overline{v}v^t\sigma_y^{\otimes n}) \\ &= \sum_{\substack{E\in\mathcal{E}\\ \mathrm{wt}(E)=i}} |v^t E\sigma_y^{\otimes n}v|^2. \end{aligned}$$

Now

$$\begin{aligned} (E\sigma_y^{\otimes n})^t &= (-1)^n\sigma_y^{\otimes n}E^t \\ &= (-1)^n\sigma_y^{\otimes n}\overline{E} \\ &= (-1)^{n+\langle\sigma_y^{\otimes n},E\rangle}\overline{E}\sigma_y^{\otimes n} \\ &= (-1)^{n-\mathrm{wt}(E)}E\sigma_y^{\otimes n}. \end{aligned}$$

In particular, if $n-\mathrm{wt}\,(E)$ is odd, then $E\sigma_y^{\otimes n}$ is antisymmetric, and $\mathrm{Tr}\,(PE\tilde{P}E) = 0$. Consequently

Theorem 12: Let $\mathcal{C}$ be a self-dual quantum code. Then

$$S_{n-2k-1}(\mathcal{C}) = 0$$

for $0 \le k \le \lfloor (n-1)/2 \rfloor$.

Corollary 13: A self-dual quantum code is odd whenever n is odd.

Proof: Consider $S_0(\mathcal{C})$. □

We can now give the following result:

Theorem 14: If a (pure) $((6m+l,\,1,\,d))$ exists, with $0 \le l \le 5$, then

$$d \le \begin{cases} 2m+2, & l<5 \\ 2m+3, & l=5. \end{cases}$$

If a $((6m+5,\,1,\,2m+3))$ exists (necessarily odd), then so does a $((6m+6,\,1,\,2m+4))$. Finally, any $((6m,\,1,\,2m+2))$ must be even.

Proof: The linear programming portion of the proof is outside the scope of this paper, so we merely sketch it here; see [6] for more details. The key point is that to the extent that the proof in [6] uses only linear programming, precisely the same proof carries over directly to the nonadditive case. Take $l < 5$, and assume $d > 2m+2$. Then we can write

$$\begin{aligned} A(1,y) &= \sum_{0\le j\le n} a_j y^j \\ S(1,y) &= \sum_{0\le j\le n} b_j y^{2j+t} \end{aligned}$$

where $t = (n \bmod 2)$ (from Theorem 12), and $a_j = 0$ for $1 \le j \le 2m+2$. From this fact, [6] deduces an equation of the form

$$\sum_{0\le j\le m+\lfloor l/2\rfloor-1} \beta_j b_j = \alpha$$

where each $\beta_j \ge 0$, and $\alpha < 0$. Since each $b_j > 0$, we obtain a contradiction. For $l = 0$ and $d = 2m+2$, we can combine two such equations to obtain

$$\sum_{1\le j\le m} \beta'_j b_j = 0$$

with each $\beta'_j > 0$, so $b_j = 0$ for $1 \le j \le m$. Then

$$\beta_0 b_0 = \alpha.$$

Since in this case $\beta_0 = \alpha$, we find $b_0 = 1$, and thus $\mathcal{C}$ is even.

If $l = 5$ and $d \ge 2m+3$, then the equation becomes

$$\sum_{0\le j\le m+1} \beta_j b_j = 0,$$

from which it follows that $b_j = 0$ for $0 \le j \le m+1$. If $d > 2m+3$, then there is also an equation of the form

$$0 = \sum_{0\le j\le m} \beta'_j b_j = \alpha'$$

with $\alpha' < 0$, so again we obtain a contradiction.

The only thing remaining (and the only essentially quantum portion of the proof) is to construct a $((6m+6,\,1,\,2m+4))$ when $l = 5$ and $d = 2m+3$. As we have just seen, we have $S_i(\mathcal{C}) = 0$ for $0 \le i < 2m+3$. In particular, $\mathcal{C}$ is odd, so we may consider its even subcode $\mathcal{C}_0$. By Theorem 11, we can compute the weight enumerator of $\mathcal{C}_0$; since $\mathcal{C}$ is self-dual, we have the simplification

$$\begin{aligned} A_i(\mathcal{C}_0) &= A_i(\mathcal{C}_0) = \begin{cases} 4A_i(\mathcal{C}), & i \equiv 0 \,(\mathrm{mod}\,2) \\ 0, & i \equiv 1 \,(\mathrm{mod}\,2) \end{cases} \\ B_i(\mathcal{C}_0) &= 2(A_i(\mathcal{C}) + S_i(\mathcal{C})). \end{aligned}$$

It follows that $A_i(\mathcal{C}_0) = 0$ for $1 \le i < 2m+4$, and $B_i(\mathcal{C}_0) = 0$ for $1 \le i < 2m+3$. By [5, Theorem 21], there exists a new self-dual code $\mathcal{C}'$ of length $6m+6$ with

$$A_i(\mathcal{C}') = \frac{1}{4}\left(A_i(\mathcal{C}_0) - A_{i-1}(\mathcal{C}_0)\right) + \frac{1}{2}B_{i-1}(\mathcal{C}_0).$$

But then $A_i(\mathcal{C}') = 0$ for $1 \le i < 2m+4$, and $\mathcal{C}'$ is the desired $((6m+6,\,1,\,2m+4))$. □

Also from [6], we get the following:

Theorem 15: If a $((6m-1+l,\,K,\,d))$ exists for $K > 1$, with $0 \le l \le 5$, then

$$d \le \begin{cases} 2m+1, & l<5 \\ 2m+2, & l=5. \end{cases}$$

Moreover, any $((6m-1,\,K,\,2m+1))$ is the even subcode of a $((6m-1,\,1,\,2m+1))$ (in particular, $K = 2$).

Proof: As above, the linear programming portion of the proof carries over directly. The only thing left to show is that a $((6m-1,\,K,\,2m+1))$ is the even subcode of a $((6m-1,\,1,\,2m+1))$.

Let $\mathcal{C}$ be a $((6m-1,\,K,\,2m+1))$. By the computations in [6], we find

$$S_0(\mathcal{C}) = K^2 - K.$$

But we must have $S_0(\mathcal{C}) \le K$, implying that $K = 2$ and $S_0(\mathcal{C}) = 2$, so $\mathcal{C}$ is even. Similarly, $\mathcal{C}$ must be pure.

Now consider any vector $v \in \mathcal{C}$. The subspace spanned by v is a self-dual code $\mathcal{C}'$; since $\mathcal{C}$ is pure, the minimum distance of $\mathcal{C}'$ is at least as large as that of $\mathcal{C}$. In other words, $\mathcal{C}'$ is a $((6m-1,\,1,\,2m+1))$. □

In particular, any quantum code of length n can correct at most $\lfloor (n+1)/6 \rfloor$ errors.

VI. Conclusion

We have extended the work of Shor and Laflamme by defining another nonnegative enumerator, computable in terms of their enumerators. This further strengthens their linear programming bound, to the point that the best bounds for general codes are nearly the same as the best bounds for additive codes. We also extended a bound on additive codes proved using shadow theory to general codes, obtaining as a consequence that any code of length n can correct at most $\lfloor (n+1)/6 \rfloor$ errors.

Acknowledgment

The author wish to thank P. Shor and N. Sloane for many helpful discussions.

References

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, July1998. LANL e-print quant-ph/9608006.

[2] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, Nov. 1990.

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

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The netherlands: North-Holland, 1977.

[5] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1388–1394, July 1998. LANL e-print quant-ph/9612015.

[6] ———, "Shadow bounds for self-dual codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 134–139, Jan. 1998.

[7] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[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.