Polynomial Invariants of Quantum Codes

Eric M. Rains

Abstract—The weight enumerators [8] of a quantum code are quite powerful tools for exploring its structure. As the weight enumerators are quadratic invariants of the code, this suggests the consideration of higher degree polynomial invariants. We show that the space of degree k invariants of a code of length n is spanned by a set of basic invariants in one-to-one correspondence with S_k^n . We then present a number of equations and inequalities in these invariants; in particular, we give a higher order generalization of the shadow enumerator of a code, and prove that its coefficients are nonnegative. We also prove that the quartic invariants of a $((4, 4, 2))_2$ code are uniquely determined, an important step in a proof that any $((4, 4, 2))_2$ code is additive [6].

Index Terms—Invariant, quantum code, shadow, weight enumerator.

I. INTRODUCTION

IN [8], Shor and Laflamme introduced the concept of the weight enumerator of a quantum code, in order to prove a bound on the minimum distance of a code, given its length and dimension. The weight enumerators have the following two properties: Equivalent codes have equal weight enumerators, and the coefficients of the weight enumerators are quadratic functions of the orthogonal projection associated to the code. More concisely, we can say that the coefficients of the weight enumerators are quadratic invariants of the code. In the present work, we will consider more general polynomial invariants.

The first task in the exploration is, naturally, to give a characterization of all polynomial invariants. Clearly, the invariants of any fixed degree form a vector space, so it suffices to give a set of invariants that span that space. This role is played by what we will call *basic* invariants; as we shall see, the basic invariants of order k and length n are in one-to-one correspondence with the group S_k^n . In the case of quadratic invariants, we recover the unitary weight enumerators of [7].

In [7], a conjecture is made regarding the *shadow enumerator* of a quantum code, in the case of alphabet size greater than 2. It turns out that this has a natural generalization to higher order invariants; moreover, the structure of the generalization suggests a natural proof, thus settling that conjecture, and strengthening the linear programming bound for nonbinary quantum codes.

The number of basic invariants is prohibitively large (k^n) for n and k of any size. In order to render these invariants tractable, it is thus necessary that a number of linear dependencies be found between them. In particular, it turns out that in a number of cases, an invariant of order k can be shown to be equal to

an invariant of order $k - 1$. In addition, if the order of the invariant is greater than the alphabet size, we get further relations. In some cases, this reduces the degrees of freedom to the point of tractability.

We examine how these relations can be used in the case when the quantum code has parameters $((4, 4, 2))_2$; that is, when the code encodes four states in four qubits, with minimum distance 2. In this case, the available relations allow one to reduce the 331 776 basic quartic invariants down to six degrees of freedom, which can be determined using more *ad hoc* methods. In particular, we conclude that any two $((4, 4, 2))_2$ codes must have the same quartic invariants. In [6], this fact is used to prove that any $((4, 4, 2))_2$ code is equivalent to an additive code, and similarly for any $((5, 2, 3))_2$ or $((6, 1, 4))_2$ code, proving the uniqueness of each of those codes.

II. DEFINITIONS

We begin with some preliminaries concerning operators on tensor product spaces. Let V and W be finite-dimensional complex Hilbert spaces (i.e., $V = \mathbb{C}^{\dim V}$, $W = \mathbb{C}^{\dim W}$, with the usual inner product). Given an operator M on $V \otimes W$, we associate the *partial trace* $\text{Tr}_W(M)$, defined in basis-independent terms by

$$\text{Tr}(N \text{Tr}_W(M)) = \text{Tr}((N \otimes 1)M)$$

for all operators N on V . (In other words, Tr_W is the adjoint of the map $N \rightarrow N \otimes 1$.) We define $\text{Tr}_V(M)$ analogously. If we choose orthonormal bases of V and W , we can obtain a more explicit expression

$$\begin{aligned} (\text{Tr}_W(M))_{ij} &\stackrel{\text{def}}{=} v_i^\dagger \text{Tr}_W(M) v_j \\ &= \text{Tr}(v_j v_i^\dagger \text{Tr}_W(M)) \\ &= \text{Tr}((v_j v_i^\dagger \otimes 1)M) \\ &= \sum_k \text{Tr}((v_j v_i^\dagger \otimes w_k w_k^\dagger)M) \\ &= \sum_k M_{ik, jk}. \end{aligned}$$

More generally, let V_i for $1 \leq i \leq n$ be finite-dimensional complex Hilbert spaces. For any subset S of $\{1, 2, \dots, n\}$, we associate the tensor product space

$$V_S = \bigotimes_{i \in S} V_i.$$

Note that when S is empty, we have $V_\emptyset = \mathbb{C}$; we also write V for $V_{\{1, 2, \dots, n\}}$. If S_1 and S_2 are disjoint subsets of $\{1, 2, \dots, n\}$, then there is a canonical isomorphism

$$\iota_{S_1, S_2}: V_{S_1} \otimes V_{S_2} \equiv V_{S_1 \cup S_2}$$

Manuscript received May 26, 1997; revised February 24, 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 D. Stinson, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(00)00064-X.

which simply sorts the tensor factors; that is,

$$\iota_{S_1, S_2} \left(\left(\bigotimes_{i \in S_1} v_i \right) \otimes \left(\bigotimes_{i \in S_2} v_i \right) \right) = \bigotimes_{i \in S_1 \cup S_2} v_i$$

for any set of vectors $v_i \in V_i$. In the sequel, we will not explicitly mention this isomorphism; for instance, given operators M_1 on V_{S_1} and M_2 on V_{S_2} , we will write $M_1 \otimes M_2$ for the corresponding operator on $V_{S_1 \cup S_2}$, in place of the technically more correct

$$\iota_{S_1, S_2}(M_1 \otimes M_2) \iota_{S_1, S_2}^{-1}.$$

The partial trace extends to this setting: given an operator M on $V_{S_1 \cup S_2}$, we obtain a new operator $\text{Tr}_{S_2}(M)$ on V_{S_1} . We readily verify that if S_1 , S_2 , and S_3 are disjoint, and M is an operator on $V_{S_1 \cup S_2 \cup S_3}$, then

$$\text{Tr}_{S_2}(\text{Tr}_{S_3}(M)) = \text{Tr}_{S_2 \cup S_3}(M).$$

A quantum code Q of length n and dimension K over an alphabet of size α is a subspace of dimension K of $(\mathbb{C}^\alpha)^{\otimes n}$. The *minimum distance* of Q is defined to be the largest number d such that for any subset S of $\{1, 2, \dots, n\}$ with $|S| > n - d$ and any unit vector $v \in Q$

$$\text{Tr}_S(vv^\dagger) = \frac{1}{K} \text{Tr}_S(P_Q)$$

where P_Q is the orthogonal projection onto Q . (Note that it is equivalent simply to require that $\text{Tr}_S(vv^\dagger)$ is constant as v ranges over the unit vectors of Q .) We use the notation $((n, K, d))_\alpha$ to refer to a quantum code of length n , dimension K , and minimum distance d over an alphabet of size α . The code Q is said to be *pure* if in addition

$$\frac{\alpha^{n-|S|}}{K} \text{Tr}_S(P_Q) = 1.$$

When $K = 1$, we take the convention that a $((n, 1, d))_\alpha$ must be pure (since otherwise the condition on the minimum distance is trivial). Two quantum codes Q_1 and Q_2 of the same length are *locally equivalent* if there exist unitary operators $\phi_i \in U(\alpha)$ such that

$$\left(\bigotimes_{1 \leq i \leq n} \phi_i \right) (Q_1) = Q_2.$$

Such an operator

$$\phi = \left(\bigotimes_{1 \leq i \leq n} \phi_i \right) \in U(\alpha)^{\otimes n}$$

will be said to be a *local equivalence*. The codes will be said to be *globally equivalent*, or just *equivalent*, if there is some permutation of the V_i that takes Q_1 into a code locally equivalent to Q_2 .

III. BASIC POLYNOMIAL INVARIANTS

For our purposes, it will be convenient to consider two types of polynomial invariants. Let Q be a quantum code of length

n , dimension K , and alphabet size α ; let P_Q be the associated projection operator. A local polynomial invariant of Q is defined as a polynomial function f of the coefficients of P_Q such that

$$f(\phi P_Q \phi^{-1}) = f(P_Q)$$

for any $\phi \in U(\alpha)^{\otimes n}$. A global invariant is then defined as a local invariant that is also left unchanged under arbitrary permutations of the tensor factors of V . While global invariants are the only *true* invariants of the code, the structure of local invariants is (somewhat) simpler, and determines the global structure; we will therefore begin by considering local polynomial invariants. Indeed, we will consider for the moment the more general problem of invariants of Hermitian operators on $V = (\mathbb{C}^\alpha)^{\otimes n}$ under local/global equivalence.

Any polynomial function $f(M)$ in the coefficients of an operator M can be written in the following form:

$$\sum_k \text{Tr}(F^{(k)} M^{\otimes k})$$

for a suitable set of operators $F^{(k)}$ on the domain of $M^{\otimes k}$. This can be seen by noting that a monomial of degree k in the coefficients of M can be written as

$$\prod_{1 \leq i \leq n} \text{Tr}(E_i M)$$

where each E_i has exactly one coefficient nonzero. But this is the same as

$$\text{Tr}((E_i)^{\otimes k} M^{\otimes k}).$$

Summing over monomials and over k , we get the desired expression. Now, consider how this expression changes when we conjugate M by a local equivalence ϕ

$$\begin{aligned} \sum_k \text{Tr}(F^{(k)} \phi^{\otimes k} M^{\otimes k} (\phi^{\otimes k})^{-1}) \\ = \sum_k \text{Tr}((\phi^{\otimes k})^{-1} F^{(k)} \phi^{\otimes k} M^{\otimes k}). \end{aligned}$$

In particular, we can average over all local equivalencies (since the group $U(\alpha)^{\otimes n}$ is compact) to obtain a polynomial invariant, and any polynomial invariant can be taken of that form. But this is equivalent to requiring that

$$F^{(k)} = (\phi^{\otimes k})^{-1} F^{(k)} \phi^{\otimes k} \quad (1)$$

for all $\phi \in U(\alpha)^{\otimes n}$. Thus we have reduced our classification problem to that of classifying the operators $F^{(k)}$ satisfying (1). (Following the suggestion of one of the referees, we will refer to these as “vector invariants.”) Once we have done that, we can recover the local *polynomial* invariants by further insisting upon invariance under permutation of the k outer tensor factors, and similarly for the global polynomial invariants.

Suppose, for a moment, that n is 1, so the group of local equivalencies is the entire unitary group. In this case, the classical theory of invariants of the classical groups (see, for instance, [1]) tells us that the space of vector invariants is spanned by a set of basic invariants in one-to-one correspondence with

the symmetric group S_k . To be precise, for $\pi \in S_k$, the corresponding basic invariant is

$$T(\pi) = \delta_{i_{\pi(1)}}^{i_1} \delta_{i_{\pi(2)}}^{i_2} \delta_{i_{\pi(3)}}^{i_3} \cdots \delta_{i_{\pi(k)}}^{i_k}.$$

Alternatively, $T(\pi)$ is the operator which permutes the k tensor factors according to the permutation π . For $n > 1$, we can simply remark that the space of degree k vector invariants of a tensor product of groups is equal to the tensor product of the invariant spaces associated to each group individually. In particular, this gives us basic invariants in one-to-one correspondence with S_k^n . The corresponding operators $T(\pi)$ for $\pi \in S_k^n$ act on $((\mathbb{C}^\alpha)^{\otimes n})^{\otimes k}$ by permuting the k copies of the i th tensor factor according to the i th permutation in π . We define the diagonal of S_k^n to be the subgroup consisting of elements of the form

$$(\pi, \pi, \dots, \pi)$$

for $\pi \in S_k$.

Theorem 1: Let f be a polynomial invariant of Hermitian operators on V . Then there exists a sequence of functions f_k on S_k^n , eventually zero, such that

$$f(M) = \sum_{0 \leq k} \sum_{\pi \in S_k^n} f_k(\pi) \text{Tr}(T(\pi)(M)^{\otimes k})$$

for all Hermitian operators M on V . The functions $f_k(\pi)$ can be taken to be invariant under conjugation by the diagonal. If f is a global invariant, then $f_k(\pi)$ can further be taken to be invariant under arbitrary permutations of the n subpermutations of π .

Proof: The above discussion has proved everything except for the observations about invariance of the function f , which follow easily from consideration of the effect that reordering the tensor factors has on the basic invariants. $\square$

Remarks:

1) When $n = 1$, the space of polynomial invariants is well known. Note that two Hermitian operators are locally equivalent if and only if they have the same eigenvalues (up to multiplicity), since any Hermitian operator can be unitarily diagonalized. Thus the polynomial invariants are just given by symmetric polynomial functions of the eigenvalues. In other words, any polynomial invariant can be written as a polynomial in the coefficients of the characteristic polynomial, and any such polynomial gives a polynomial invariant. Unfortunately, such a simple description does not seem to exist for $n > 1$ (see, for instance, [2], which considers the case $n = 2, \alpha = 2$).

2) Similarly, for $n = 1$, we can give an explicit basis for the space of vector invariants (which thus gives such a basis for $n > 1$). Namely, this basis is given by the invariants of the form $T(\pi)$ where π has no increasing subsequence of length $> \alpha$. To see that these span, we note that Lemma 4 below allows us to express $T(\pi)$ where π has such an increasing subsequence as a linear combination of $T(\pi')$ where each π' has strictly more inversions. That these form a basis then follows from the fact that the dimension of the space of vector invariants is equal to the number of such $T(\pi)$ [4]. A different, but related, explicit basis for $\alpha = 2$ is given in [2].

When $k = 2$, we recover the unitary weight enumerator of [7]. We recall that for any subset $S \subset \{1, 2, \dots, n\}$, and any

Hermitian operators M and N on V , the quantity $A'_S(M, N)$ is defined in [7] by

$$A'_S(M, N) \stackrel{\text{def}}{=} \text{Tr}(\text{Tr}_{S^c}(M) \text{Tr}_{S^c}(N)),$$

where $S^c \stackrel{\text{def}}{=} \{1, 2, \dots, n\} - S$. To relate this to the vector invariants, note that S_2^n is in one-to-one correspondence with the set of subsets of $\{1, 2, \dots, n\}$; to $\pi \in S_2^n$ we associate the set $S(\pi)$ of indices such that π_i is a transposition.

Theorem 2: For any $\pi \in S_2^n$, and any Hermitian operators M and N on V ,

$$\text{Tr}(T(\pi)(M \otimes N)) = A'_{S(\pi)}(M, N).$$

Proof: For all i in $S(\pi)^c$, we readily see that

$$\text{Tr}(T(\pi)(M \otimes N)) = \text{Tr}(T(\pi^{(i)})(\text{Tr}_{\{i\}}(M) \otimes \text{Tr}_{\{i\}}(N)))$$

where $\pi^{(i)}$ is the tuple of permutations obtained from π by removing the i th permutation. This follows, for example, by noting that we can conjugate M by an arbitrary unitary operation on the i th tensor factor without changing the result. But then we get

$$\begin{aligned} \text{Tr}(T(\pi)(M \otimes N)) &= \text{Tr}(T((12))(\text{Tr}_{S(\pi)^c}(M) \otimes \text{Tr}_{S(\pi)^c}(N))) \\ &= A'_{S(\pi)}(M, N). \end{aligned} \quad \square$$

This motivates the notation

$$A'_\pi(Q) = \text{Tr}(T(\pi)P_Q^{\otimes k})$$

for general k . Similarly, if we are given a k -tuple of Hermitian operators, we write

$$A'_\pi(M_1, M_2, \dots, M_k) = \text{Tr}(T(\pi)(M_1 \otimes M_2 \otimes \dots \otimes M_k)).$$

IV. GENERALIZED SHADOW INEQUALITIES

In [7], the author made the following conjecture:

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

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

In particular, when $M = N = P_Q$, this gives an inequality that the quadratic invariants of a code must satisfy. It turns out that this generalizes naturally to higher order invariants. Let us first restate this conjecture in terms of basic quadratic invariants. Define

$$\begin{aligned} \kappa_T(M, N) &\stackrel{\text{def}}{=} \sum_{\pi \in S_2^n} (-1)^{|S(\pi) \cap T|} A'_\pi(M, N) \\ &= \sum_{\pi \in S_2^n} \lambda_T(\pi) A'_\pi(M, N) \end{aligned}$$

where

$$\lambda_T(\pi) = (-1)^{|S(\pi) \cap T|}.$$

Then the conjecture states that $\kappa_T(M, N) \geq 0$. Note that $\lambda_T(\pi)$ is a Hermitian idempotent in the group algebra of S_2^n ; this suggests the following generalization:

Theorem 3: Let $V = V_1 \otimes V_2 \otimes \cdots \otimes V_n$, where V_1 through V_n are Hilbert spaces. Let $M_1, M_2, \dots, M_k$ be positive-semidefinite Hermitian operators on V . Then for any Hermitian idempotent λ in the group algebra of S_k^n

$$\sum_{\pi \in S_k^n} \lambda(\pi) A'_\pi(M_1, M_2, \dots, M_k) \geq 0.$$

Proof: The given expression is multilinear in the M_i ; consequently, it suffices to consider the case in which each M_i has rank one. Thus let v_i for each i be a vector in V such that $M_i = v_i v_i^\dagger$. This allows us to restate our question as showing that

$$\kappa \stackrel{\text{def}}{=} \sum_{\pi \in S_k^n} \lambda(\pi) A'_\pi(v_1 v_1^\dagger, \dots, v_k v_k^\dagger) \geq 0.$$

Rewriting A'_π as a trace, we have

$$\begin{aligned} \kappa &= \sum_{\pi \in S_k^n} \lambda(\pi) (v_1 \otimes v_2 \otimes \cdots \otimes v_k)^\dagger T(\pi) (v_1 \otimes v_2 \otimes \cdots \otimes v_k) \\ &= \sum_{\pi, \pi' \in S_k^n} \lambda(\pi \pi'^{-1}) \lambda(\pi') (v_1 \otimes v_2 \otimes \cdots \otimes v_k)^\dagger \\ &\quad \cdot T(\pi) (v_1 \otimes v_2 \otimes \cdots \otimes v_k) \\ &= \sum_{\pi_1, \pi_2 \in S_k^n} \lambda(\pi_1) \lambda(\pi_2) (v_1 \otimes v_2 \otimes \cdots \otimes v_k)^\dagger \\ &\quad \cdot T(\pi_1) T(\pi_2) (v_1 \otimes v_2 \otimes \cdots \otimes v_k) \\ &= \left(\sum_{\pi_1 \in S_k^n} \lambda(\pi_1) T(\pi_1) (v_1 \otimes v_2 \otimes \cdots \otimes v_k) \right)^\dagger \\ &\quad \cdot \left(\sum_{\pi_2 \in S_k^n} \lambda(\pi_2) T(\pi_2) (v_1 \otimes v_2 \otimes \cdots \otimes v_k) \right). \end{aligned}$$

But this is the norm of a vector, so must be nonnegative. $\square$

By the discussion preceding the theorem, the above conjecture follows as an immediate corollary.

V. REDUCTIONS AND RELATIONS

Although we have shown that the basic invariants span the space of polynomial invariants, we have by no means shown that they form a basis. Indeed, there are a number of linear equations relating the various basic invariants. For example, as noted in Theorem 1 above, if we conjugate every permutation in π by a fixed element of S_k , the corresponding polynomial invariant will be unchanged; this corresponds to the fact that the different copies of M appearing in the expression for the polynomial invariant can be freely interchanged. When M is the projection operator associated to a quantum code, we typically obtain a number of other relations as well.

Many of these relations take the form of a reduction, in which an invariant of degree k is expressed as an invariant of degree $k-1$. The most general of these reductions follows from the fact that P_Q is a projection operator, so $P_Q^2 = P_Q$. Suppose there is

an index $1 \leq j \leq k$ such that $\pi_i(j)$ is constant as i ranges from 1 to n . Then each tensor factor of the j th copy of P_Q is connected to the corresponding tensor factor of the $\pi_i(j)$ th copy. But then this gives us P_Q^2 , which we can replace by P_Q .

For example, consider the invariant

$$A'_{(12)(345), (123)(45), (124)(35), (125)(34)}(P_Q). \quad (2)$$

Here, each permutation maps 1 to 2; in consequence, we can merge 1 and 2, obtaining

$$A'_{(1)(345), (13)(45), (14)(35), (15)(34)}(P_Q)$$

which we can renumber as

$$A'_{(1)(234), (12)(34), (13)(24), (14)(23)}(P_Q)$$

which we are unable to reduce further.

In some cases, the information we are given concerning Q allows us to give further reductions. For example, in many cases we know a set S such that $\text{Tr}_S(P_Q)$ is proportional to the identity operator. (In particular, if Q is pure, then this holds when $|S| > n - d$.) Suppose there exists a j with $1 \leq j \leq k$ such that $\pi_i(j) = j$ for all i in S . Then we can splice j out of each permutation, resulting in a lower order invariant that is a constant multiple of the original invariant.

For instance, suppose that in the above example we knew that $\text{Tr}_S(P_Q) = (1/2)I$ for all S of cardinality 1; this is the case when Q is a $((4, 4, 2))_2$ code, for instance. Then we can reduce

$$A'_{(1)(234), (12)(34), (13)(24), (14)(23)}(P_Q)$$

by splicing out 1, obtaining

$$\frac{1}{2} A'_{(234), (2)(34), (3)(24), (4)(23)}(P_Q),$$

which reduces further to

$$\frac{1}{4} A'_{(34), (34), (3)(4), (3)(4)}(P_Q) = \frac{1}{4} A'_{\{1, 2\}}(P_Q).$$

Thus we have reduced the quintic invariant (2) to a quartic invariant. It should be apparent, therefore, that these reductions can be a powerful tool in simplifying higher order invariants.

A final important class of relations appears when the order of the invariant is greater than the alphabet size. For $n = 1$, we have the following classical result.

Lemma 4: If $k > \alpha$, then

$$\sum_{\pi \in S_k} \sigma(\pi) T(\pi) = 0.$$

Proof: Let M be a matrix of dimension k . Then one readily sees that

$$\text{Tr} \left(\left(\sum_{\pi \in S_k} \sigma(\pi) T(\pi) \right) M^{\otimes k} \right) = \det(M)$$

from the definition of determinant. Now, the basic invariants are unchanged if we enlarge each matrix by adding a row and

column of zeros. Consequently, for M of dimension less than k (i.e., α)

$$\text{Tr} \left(\left(\sum_{\pi \in S_k} \sigma(\pi) T(\pi) \right) M^{\otimes k} \right) = 0.$$

The only way this can happen for all M is if

$$\sum_{\pi \in S_k} \sigma(\pi) T(\pi) = 0. \quad \square$$

We get further relations by adding fixed points, or multiplying the sum of T 's by some fixed T . For instance, consider the invariant

$$A'_{(123), (123), (132)}(Q)$$

in the case when Q is a binary code. Then Lemma 4 tells us that

$$\begin{aligned} & A'_{(123), (123), (132)}(Q) + A'_{(123), (123), (1)(2)(3)}(Q) \\ & + A'_{(123), (123), (123)}(Q) \\ & = A'_{(123), (123), (12)(3)}(Q) + A'_{(123), (123), (13)(2)}(Q) \\ & + A'_{(123), (123), (23)(1)}(Q). \end{aligned}$$

The last four terms always reduce to quadratic invariants, while the second term sometimes admits reduction as well. We also have, for example,

$$\begin{aligned} & A'_{(12)(34), (123)(4)}(Q) + A'_{(134)(2), (123)(4)}(Q) \\ & + A'_{(234)(1), (123)(4)}(Q) \\ & = A'_{(1)(2)(34), (123)(4)}(Q) + A'_{(1342), (123)(4)}(Q) \\ & + A'_{(1234), (123)(4)}(Q) \end{aligned}$$

obtained by multiplying the relation

$$\begin{aligned} & T((1)(2)(3)(4)) + T((123)(4)) + T((132)(4)) \\ & = T((12)(3)(4)) + T((13)(2)(4)) + T((1)(23)(4)) \end{aligned}$$

by $T((12)(34))$. As we shall see in the next section, these relations derived from Lemma 4 can be extremely powerful. (See also the second remark after Theorem 1.)

VI. BINARY MDS CODES OF DISTANCE 2

Let us consider the case when Q is a binary maximum-distance separable (MDS) code of distance 2; that is, when Q is a $((2m, 4^{m-1}, 2))_2$ code; that is, Q is a quantum code of length $2m$, dimension 4^{m-1} , and minimum distance 2, over an alphabet of size 2. (The terminology ‘‘MDS’’ is by analogy with classical coding theory, as these codes meet the quantum analog of the Singleton bound [3], [5].) In this case, $\text{Tr}_{\{i\}}(P_Q) = (1/2)I$ for $1 \leq i \leq 2m$. This allows us to reduce any basic invariant containing a nonderangement (a permutation with a fixed point) to a lower order invariant, as we have just seen.

Lemma 5: For each $m \geq 2$, the local cubic invariants of a $((2m, 4^{m-1}, 2))_2$ code are uniquely determined. That is, if Q and Q' are $((2m, 4^{m-1}, 2))_2$ codes, and $\pi \in S_3^{2m}$, then $A'_\pi(Q) = A'_\pi(Q')$.

Proof: Since a $((2m, 4^{m-1}, 2))_2$ code meets the quantum Singleton bound, the proof of that bound in [5] implies that

its local quadratic invariants are uniquely determined. Therefore, it suffices to restrict our attention to those invariants corresponding to π consisting entirely of derangements; otherwise, the invariant can be reduced to a local quadratic invariant, and is thus uniquely determined.

Since we are dealing with a binary code, Lemma 4 applies

$$\begin{aligned} T((1, 3, 2)) &= -T((1)(2)(3)) - T((1, 2, 3)) \\ &+ T((1, 2)(3)) + T((1, 3)(2)) \\ &+ T((2, 3)(1)). \end{aligned}$$

In particular, this allows us to reduce any invariant involving $(1, 3, 2)$ to a sum of invariants involving only $(1, 2, 3)$ or permutations with fixed points. Thus the only remaining nonderangement invariant is $A'_{(1, 2, 3)^{2m}}(Q)$, which reduces to $\text{Tr}(P_Q^3) = 2^{m-2}$. $\square$

For a $((4, 4, 2))_2$ code, we can say more.

Theorem 6: The local quartic invariants of a $((4, 4, 2))_2$ code are uniquely determined.

Proof: Let Q be a $((4, 4, 2))_2$ code. As in Lemma 5, we may restrict our attention to derangements. For convenience, we define

$$\pi_1 = (1, 2, 3, 4) \quad \pi_2 = (1, 3, 4, 2) \quad \pi_3 = (1, 4, 2, 3).$$

Then any derangement in S_4 can be written as π_i^j for $i, j \in \{1, 2, 3\}$. Furthermore, we have the following relations in the representation T , from Lemma 4:

$$\begin{aligned} \pi_1^3 &= \pi_1 + \text{n.d.}, & \pi_2^3 &= \pi_2 + \text{n.d.}, & \pi_3^3 &= \pi_3 + \text{n.d.}, \\ \pi_1^2 &= \pi_2 + \pi_3 + \text{n.d.}, & \pi_2^2 &= \pi_1 + \pi_3 + \text{n.d.}, \\ \pi_3^2 &= \pi_1 + \pi_2 + \text{n.d.} \end{aligned} \quad (3)$$

where n.d. refers to some linear combination of nonderangements. This allows us to restrict our attention to invariants involving only π_1, π_2 , and π_3 . Now, note that $\pi_1(3) = \pi_2(3)$, $\pi_2(4) = \pi_3(4)$, and $\pi_1(2) = \pi_3(2)$. It follows that any invariant involving only two of the three can be reduced to a cubic invariant. We therefore have only six degrees of freedom remaining, corresponding to the local invariant

$$A'_{\pi_1, \pi_2, \pi_3}(Q),$$

and its six permutations. In particular, we have only one degree of freedom remaining in the global invariants.

Now, let v be any codeword in Q , and consider $\text{Tr}_{\{234\}}(vv^\dagger)$. Since Q is pure (any MDS code is pure), it follows that

$$\text{Tr}_{\{234\}}(vv^\dagger) = 2I.$$

Thus the commutator

$$[\text{Tr}_{\{234\}}(vv^\dagger) \otimes I, P_Q] = 0$$

for all $v \in Q$. But then

$$E_{v \in Q} (\text{Tr} (-[\text{Tr}_{\{234\}}(vv^\dagger) \otimes I, P_Q]^2)) = 0$$

where v may be taken to be normally distributed. This is a local quartic invariant of Q , equal to

$$\begin{aligned} & 2A'_{(1,2,3,4), (1,2)(3,4), (1,2)(3,4), (1,2)(3,4)}(Q) \\ & + 2A'_{(1,2,3,4), (1,2)(3,4), (1,2)(3,4), (1,2)(3,4)}(Q) \\ & - 2A'_{(1,3,2,4), (1,2)(3,4), (1,2)(3,4), (1,2)(3,4)}(Q) \\ & - 2A'_{(1,3,2,4), (1,2)(3,4), (1,2)(3,4), (1,2)(3,4)}(Q). \end{aligned}$$

Simplifying along fixed points, we conclude that

$$A'_{(1,3)(2,4), (1,2)(3,4), (1,2)(3,4), (1,2)(3,4)}(Q) = A'_{\pi_1^2, \pi_3^2, \pi_3^2, \pi_3^2} = 4.$$

Applying the reductions (3) to the first tensor factor, we find

$$A'_{\pi_3, \pi_3^2, \pi_3^2, \pi_3^2}(Q) = 2$$

then, reducing the second through fourth tensor factors

$$\begin{aligned} & A'_{\pi_3, \pi_1, \pi_3^2, \pi_3^2}(Q) + A'_{\pi_3, \pi_2, \pi_3^2, \pi_3^2}(Q) = 2 \\ & A'_{\pi_3, \pi_1, \pi_1, \pi_3^2}(Q) + A'_{\pi_3, \pi_2, \pi_1, \pi_3^2}(Q) \\ & + A'_{\pi_3, \pi_1, \pi_2, \pi_3^2}(Q) + A'_{\pi_3, \pi_2, \pi_2, \pi_3^2}(Q) = 2 \end{aligned}$$

and

$$A'_{\pi_3, \pi_1, \pi_1, \pi_2} + A'_{\pi_3, \pi_1, \pi_2, \pi_1} + A'_{\pi_3, \pi_2, \pi_1, \pi_1} = 3.$$

Permuting this equation gives us four more equations relating the local invariants, leaving two degrees of freedom. However, this is enough to determine the global invariants

$$(A'_{\pi_1, \pi_1, \pi_2, \pi_3})_{\text{sym}} = 1.$$

Now, consider, for $S \subset \{1, 2, 3, 4\}$ of size 2

$$\kappa_S = E_{v \in Q} (\text{Tr} (-[\text{Tr}_{S^c}(vv^\dagger) \otimes I, P_Q]^2)).$$

This is a local quartic invariant, and further must be nonnegative, since the commutator of two Hermitian operators is anti-Hermitian. On the other hand, we have, for example,

$$\begin{aligned} \kappa_{\{1,2\}} & \propto 8 - 2A'_{\pi_2, \pi_3, \pi_1, \pi_1}(Q) - 2A'_{\pi_1, \pi_1, \pi_2, \pi_3}(Q) \\ & - A'_{\pi_1, \pi_2, \pi_1, \pi_3}(Q) - A'_{\pi_1, \pi_2, \pi_3, \pi_1}(Q) \\ & - A'_{\pi_2, \pi_1, \pi_1, \pi_3}(Q) - A'_{\pi_2, \pi_1, \pi_3, \pi_1}(Q). \end{aligned}$$

Symmetrizing, we find

$$\sum_S \kappa_S = 0.$$

But then the nonnegativity of the κ_S implies $\kappa_S = 0$ for each S . This gives us three further equations on the local invariants, eliminating the two remaining degrees of freedom. $\square$

VII. FURTHER DIRECTIONS

It must be stressed that the relations and inequalities we have derived above by no means exhaust the possibilities; for instance, it should be possible to define a higher order, but still nonnegative, analog of the A_S weight enumerators [7], which would produce a number of inequalities on the higher order invariants. Furthermore, it seems clear that we are not taking full advantage of the relations that can be deduced from the minimum distance of the code. Progress needs to be made in these areas in order for the polynomial invariants to attain their full potential.

In addition, it should be noted in passing that there is some evidence (see [6, the remark after Corollary 9]) that some simple set of relations on the quartic invariants, satisfied by all additive codes, are enough to force a code to be additive. This possibility probably merits further investigation.

REFERENCES

- [1] R. Brauer, "On algebras which are connected with the semisimple continuous groups," *Ann. Math.*, vol. 38, pp. 857–972, 1937.
- [2] M. Grassl, M. Rötteler, and T. Beth, "Computing local invariants of qubit systems," *Phys. Rev. A*, vol. 58, pp. 1833–1839, 1998.
- [3] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900–911, 1997.
- [4] E. M. Rains, "Increasing subsequences and the classical groups," *Elect. J. Combin.*, vol. 5, no. 1, 1998.
- [5] —, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, to be published.
- [6] —, "Quantum codes of minimum distance two," *IEEE Trans. Inform. Theory*, vol. 45, pp. 266–271, Jan. 1999.
- [7] —, "Quantum weight enumerators," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1388–1394, July 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.