Nonbinary Quantum Codes

Eric M. Rains

***Abstract*—We present several results on quantum codes over general alphabets (that is, in which the fundamental units may have more than two states). In particular, we consider codes derived from finite symplectic geometry assumed to have additional global symmetries. From this standpoint, the analogs of Calderbank–Shor–Steane codes and of GF(4)-linear codes turn out to be special cases of the same construction. This allows us to construct families of quantum codes from certain codes over number fields; in particular, we get analogs of quadratic residue codes, including a single-error-correcting code encoding one letter in five, for any alphabet size. We also consider the problem of fault-tolerant computation through such codes, generalizing ideas of Gottesman.**

***Index Terms*—Finite fields, quantum codes, symplectic.**

I. Introduction

MOST of work to date on quantum error-correcting codes (QECC's) has concentrated on binary codes, both because this is the simplest case, and because such codes are likely to be the most useful. However, there are some applications for which nonbinary QECC's would be more useful (e.g., for proof-of-concept implementation in certain ion trap models (R. Laflamme, personal communication)). Also, codes over alphabets of size 2^l could be useful for constructing easily decodable binary codes, via concatenation. Finally, regardless of any practical interest, nonbinary codes are likely to be of considerable theoretical interest, just as in classical coding theory.

The most successful technique to date for constructing binary quantum codes is the *additive* or *stabilizer* construction [3]. This construction takes a classical binary code, self-orthogonal under a certain symplectic inner product, and produces a quantum code, with minimum distance determined from the classical code. This technique readily extends to nonbinary codes; indeed, most of the necessary machinery has already been discussed in [2]; we sketch the construction below.

The most useful and interesting classical nonbinary codes are the maximum-distance separable (MDS) codes, that is, codes that meet the Singleton bound. We, therefore, give the quantum analog of the Singleton bound (already proved for binary alphabets in [10]), allowing us to define quantum MDS codes. One interesting feature of the theory of quantum MDS codes that is absent in the classical theory is the requirement of self-orthogonality; this means, in particular, that the existence of an MDS code of length n and minimum distance d need not imply the existence of MDS codes of any smaller length with that minimum distance. Thus it no longer suffices to consider the largest possible length. Sometimes, however, one can safely shorten a quantum MDS code; indeed, associated to any such (symplectic) code, we construct a classical code, the codewords of which correspond to different valid shortenings. This construction applies to other codes as well, even those that are not self-orthogonal.

In [3], the problem of constructing symplectic-self-orthogonal binary codes was converted into a problem of constructing additive, Hermitian-self-orthogonal codes over $\mathrm{GF}(4)$; among other things, this allowed one to consider codes linear over $\mathrm{GF}(4)$. Unfortunately, the notion of additive codes does not seem to usefully extend to larger alphabets (in part since it is difficult to derive symplectic forms from symmetric forms in characteristic other than 2); it is somewhat surprising, therefore, that the concept of $\mathrm{GF}(4)$-linear codes *does* usefully extend. This extension works by considering codes having certain global symmetries; codes that are invariant under an algebra isomorphic to $\mathrm{GF}(p^2)$ give the desired extension. We also get analogs of Calderbank–Shor–Steane codes [4], [12] by asserting invariance under an algebra isomorphic to $\mathrm{GF}(p) \times \mathrm{GF}(p)$. This allows us, in principle, to define classes of codes for varying p by taking a code over a quadratic number field and reducing modulo different primes. As an example, we get quantum quadratic residue codes, including, for each p, a $((5, p, 3))_p$ code. We also consider the problem of fault-toleration operations (using the ideas in [6]); in particular, we show how the algebra under which a code is globally invariant extends the possibilities for fault-tolerant operation.

A quick comment on notation: We use the notation $((n, K, d))_\alpha$ to refer to a quantum code that encodes K states in n letters from an alphabet of size α, with minimum distance d. In particular, such a code can be used to correct $\lfloor (d-1)/2 \rfloor$ single-letter errors. The precise definition is as follows (see, e.g., [11]): An $((n, K, d))_\alpha$ code is a subspace $\mathcal{C}$ of $(\mathbb{C}^\alpha)^{\otimes n}$ such that, for any matrix M which is the identity on all but $d-1$ of the copies of $\mathcal{C}^\alpha$, the inner product

$$\langle v|M|v\rangle$$

is constant as v ranges over the unit vectors of $\mathcal{C}$. The code is said to be *pure* if that constant is $\alpha^{-n}\operatorname{Tr}(M)$. Note that just as in the binary case, the condition is linear in M, so need only be verified on a basis.

Manuscript received March 25, 1997; revised February 1, 1999.

The author is with AT&T Research, AT&T Shannon Laboratory, Florham Park, NJ 07974 USA (e-mail: rains@research.att.com).

Communicated by D. Stinson, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(99)06064-2.

0018–9448/99$10.00 © 1999 IEEE

II. Symplectic Codes

In the case $p = 2$, the framework of [3] can be used to construct quantum codes from codes over GF(2) that are self-orthogonal under a suitable symplectic inner product. This generalizes easily to the case $p > 2$.

Consider the GF(p)-vector space $V_n = (\mathrm{GF}(p) \times \mathrm{GF}(p))^n$. If we write $v \in V_n$ as

$$v = ((v_1^{(1)}, v_1^{(2)}), (v_2^{(1)}, v_2^{(2)}), \cdots)$$

we can define the weight of v as the number of i such that at least one of $v_i^{(1)}$ and $v_i^{(2)}$ is nonzero. We also have a natural symplectic inner product on V_n, given by

$$\langle v, w\rangle = \sum_{1\le i\le n} v_i^{(1)} w_i^{(2)} - v_i^{(2)} w_i^{(1)}.$$

Definition: Let C be an $(n-k)$-dimensional subspace of V_n, self-orthogonal under the symplectic inner product. If the minimum weight of $C^\perp - C$ is at least d, then we say C is an $[[n, k, d]]_p$ code. If d' is the minimum weight of the nonzero elements of C, then we say C is pure to weight d'. If $d' \ge d$, then we say C is pure.

The relevance of this definition is the following fact.

Theorem 1: If there exists an $[[n, k, d]]_p$ code, then there exists an $((n, p^k, d))_p$ code. If the $[[n, k, d]]_p$ code is pure, then so is the $((n, p^k, d))_p$ code.

Proof: This is completely analogous to the construction in [3]; see also [2] for a discussion of the connections between finite symplectic geometry and extraspecial groups for $p>2$. □

Remark: Note that the analog of the error group of [3] is the group of operations $T(\vec{v}, \chi)$

$$T(\vec{v}, \chi)|\vec{x}\rangle = \chi(\vec{x})|\vec{x} + \vec{v}\rangle$$

where $\vec{v}$ is an element of the (additive) group GF$(p)^n$ and χ is a character of that group. Some generalizations can be found in [8] and [9] (to non-Abelian groups), and in [13] (to infinite Abelian groups).

Let G_n be the natural semidirect product of S_n and $\mathrm{Sp}_2(p)^n$. Clearly, G_n acts on V_n ($\mathrm{Sp}_2(p)^n$ acts coordinate-wise, while S_n acts by permuting the coordinates), preserving the weight and the inner product. Thus G_n acts on symplectic codes; two codes are defined to be equivalent if they are in the same G_n-orbit. And the automorphism group of a code is given by the subgroup of G_n that preserves the code.

III. Quantum MDS Codes

When using the above theory to construct codes, it is useful to know what to shoot for. In classical coding theory, the most useful large-alphabet codes tend to be the MDS codes; that is, those codes that meet the Singleton bound. We thus consider the quantum analog.

The proof uses the nonbinary weight enumerators $A(x, y)$, $B(x, y)$, $A'(x, y)$, and $B'(x, y)$ [11]. Note in particular that a code has minimum distance d if and only if $B_i = K^{-1}A_i$ for $0 \le i < d$, and is pure if and only if $B_i = A_i = 0$ for $1 \le i < d$.

Theorem 2 (Quantum Singleton Bound): Let C be an $((n, K, d))_\alpha$ code with $K > 1$. Then

$$K \le \alpha^{n-2d+2}.$$

If equality holds, then C is pure to weight $n-d+2$. Similarly, a pure $((n, 1, d))_\alpha$ code satisfies $2d \le n + 2$.

Proof: We first consider the case $K > 1$. If $2d \ge n + 2$, then we would have both $A'_{n-d+1} = KA'_{d-1}$ and $A'_{d-1} = KA'_{n-d+1}$. But since $A'_{d-1} > 0$, this is a contradiction for $K > 1$. Consequently, we must have $2d < n + 2$. Now consider A'_{n-d+1}. On the one hand, this can be written as a linear combination of B_i for $0 \le i \le d-1$

$$A'_{n-d+1} = B'_{d-1} = \alpha^{-d+1} \sum_{0\le i\le d-1} \binom{n-i}{n-d+1} B_i.$$

On the other hand, it can be written as a linear combination of A_i for $0 \le i \le n-d+1$

$$A'_{n-d+1} = \alpha^{-n+d-1} \sum_{0\le i\le n-d+1} \binom{n-i}{d-1} A_i.$$

Since C has minimum distance d, it follows that $B_i = K^{-1}A_i$ for $0 \le i \le d-1$. Consequently

$$\begin{aligned} 0 &= A'_{n-d+1} - A'_{n-d+1} \\ &= \alpha^{-n+d-1} \sum_{0\le i\le n-d+1} \binom{n-i}{d-1} A_i \\ &\quad - \alpha^{-d+1}K^{-1} \sum_{0\le i\le d-1} \binom{n-i}{n-d+1} A_i. \end{aligned}$$

Consider the coefficient of A_i, for $0 \le i \le d-1$. This is

$$\alpha^{-n+d-1}\binom{n-i}{d-1} - \alpha^{-d+1}K^{-1}\binom{n-i}{d-1-i}.$$

For $K \ge \alpha^{n-2d+2}$ and $K > 1$, this is positive, except in the case $i = 0$ and $K = \alpha^{n-2d+2}$. The result for $K > 1$ follows immediately.

For $K = 1$, note that

$$\begin{aligned} A'_i &= \alpha^{-i} \sum_{0\le j\le i} \binom{n-j}{n-i} A_j \\ &= \alpha^{-i}\binom{n}{n-i} \end{aligned}$$

for $0 \le i \le d-1$, since then only $A_0 = 1$ is nonzero. Since $K = 1$ also implies $A'_{n-d+1} = A'_{d-1}$, we obtain a contradiction unless $2d \le n + 2$. □

Remark: The bound part of this result was proved for alphabet size 2, using an essentially equivalent proof, in [10]; the purity result is apparently new, however.

A quantum MDS code is defined as a $((n, K, d))_\alpha$ code for which equality holds in the quantum Singleton bound; that is, $K = \alpha^{n-2d+2}$. Two fairly trivial examples of quantum MDS codes are trivial codes (which have parameters $((n, \alpha^n, 1))_\alpha$), and certain codes of distance 2 (with some restrictions on n;

for instance, over a binary alphabet, n must be even). We will also see below that a $((5, \alpha, 3))_\alpha$ code and a $((6, 1, 4))_\alpha$ code exist over all alphabets. For binary codes, these are essentially the only examples, as remarked in [3]; however, larger alphabets typically have more examples as well. The hope is that by concatenating an MDS code over a reasonably large alphabet with a suitable binary code, we can construct good codes that are still relatively easy to decode, just as in classical coding theory.

IV. Puncture Codes

The classical theory of MDS codes is greatly simplified by the fact that if an MDS code with minimum distance d exists for length n, one can construct MDS codes with the same minimum distance for all lengths n' with $d \leq n' \leq n$. Thus in the classical setting, one may restrict one's attention to MDS codes of maximum length. The same is not true in general in the quantum case. For instance (from [3, Table III]), a $((20, 2^{20-6}, 3))_2$ code does not exist, even though many $((21, 2^{21-6}, 3))_2$ codes exist. An MDS example is given by the parameters $((4, 1, 3))_2$; no such (pure) code exists, despite the existence of a $((5, 2, 3))_2$ code.

For symplectic codes, for instance, the main difficulty is that self-orthogonality must be maintained. However, much of the time one can, indeed, shorten a symplectic quantum MDS code. To explore when this can be done, we introduce the concept of the puncture code of a symplectic code; each codeword in the puncture code specifies a construction of a self-orthogonal code (possibly shorter).

Let C be a subspace of $(\mathrm{GF}(p) \times \mathrm{GF}(p))^n$, not necessarily self-orthogonal of length n and size p^k, such that $C^\perp$ has minimum distance d. For every pair v and w of codewords of C, we define a vector in $\mathrm{GF}(p)^n$ by taking the component-wise inner product of v and w; that is, if $v = (v_1, v_2, \cdots v_n)$, and $w = (w_1, w_2, \cdots w_n)$, then the new vector is

$$\{v, w\} = (\langle v_1, w_1\rangle, \langle v_2, w_2\rangle, \cdots \langle v_n, w_n\rangle).$$

(Here we write $\langle v_i, w_i\rangle = v_i^{(1)} w_i^{(2)} - v_i^{(2)} w_i^{(1)}$.) We define the puncture code $P(C)$ of C as the dual (under the usual inner product on $\mathrm{GF}(p)^n$) of the code generated by $\{v, w\}$ for all $v, w \in C$.

Theorem 3: If there exists a codeword in $P(C)$ of weight r, then there exists a pure $[[r, r-k', d]]_p$ code, for some $k' \leq k$.

Proof: By permuting the columns of C (and thus $P(C)$), we may assume that the given codeword of $P(C)$ takes the form $\phi = (a_1, a_2, \cdots, a_r, 0^{n-r})$. If we apply a transformation of determinant a_i to column i of C, this has the effect of multiplying column i of $P(C)$ by a_i^{-1}. Thus we may assume without loss of generality that $a_i = 1$ for $1 \leq i \leq r$; that is, $\phi = (1^r, 0^{n-r})$.

Define a new code C' by removing all but the first r columns from a generator matrix for C; let π be the natural map from C to C'. Clearly, C' has length r and size at most p^k; also, C' is self-orthogonal, since for $v, w \in C$

$$\langle \pi(v), \pi(w)\rangle = \sum_{1 \leq i \leq r} \langle v_i, w_i\rangle = \phi \cdot \{v, w\}.$$

It remains only to show that $C'^\perp$ has minimum distance at least d. But for any codeword w in $C'^\perp$, the word $(w, 0^{n-r})$ must be in $C^\perp$; it follows immediately that w has weight at least d. □

Remark: If C is linear (see below), then we can define $P(C)^\perp$ much more simply as the code spanned by the component-wise norms of the vectors in C; in particular, in the case $p = 2$, C inert linear, this is the binary code generated by the supports of the vectors in C [3, Theorem 7].

One possible application of this theory would be construction of analogs for large alphabets of the binary quantum Hamming codes. Unfortunately, the naive construction gives a code that is not itself self-orthogonal. However, in all cases the author has checked, $P(C)$ contains a vector of full weight, allowing the construction of a quantum code with the desired parameters. See also the entries marked "S" in [3, Table III], for applications of puncture codes in the binary case.

V. Linear Codes

For $p = 2$, there are two special cases of particular interest; Calderbank–Shor–Steane codes [4], [12] and $\mathrm{GF}(4)$-linear codes [3]. Both of these generalize naturally to $p > 2$. Essentially, one can characterize both cases in terms of certain global symmetries.

Consider the group $\mathrm{Sp}_2(p)$. This acts on symplectic codes, by applying the same transformation to each coordinate. Then, let G be a subgroup of $\mathrm{Sp}_2(p)$; we wish to characterize those symplectic codes preserved by G. Clearly, this depends only on the algebra A spanned by G; this suggests that we should instead consider symplectic codes invariant under some subalgebra of the algebra spanned by $\mathrm{Sp}_2(p)$. In particular, since the algebra spanned by $\mathrm{Sp}_2(p)$ is $\mathrm{Mat}_2(p)$, we conclude immediately that A has dimension 1, 2, or 4. The first case is trivial: any code must be invariant under $\mathrm{GF}(p)$, simply by $\mathrm{GF}(p)$-linearity. The last case can be handled by noting that every two-dimensional subalgebra of A must preserve the code; we will thus postpone that case until later.

It remains to consider the case $\dim(A) = 2$. In this case, we can write the generic element of A as $a + bX$, for some fixed $X \in \mathrm{Mat}_2(p)$, not a multiple of the identity. Clearly, we care only about the orbit of X under conjugation by $\mathrm{Sp}_2(p) = \mathrm{SL}_2(p)$. Thus let us choose a basis for $\mathrm{GF}(p) \times \mathrm{GF}(p)$ in such a way that

$$X = \begin{pmatrix} 0 & 1 \\ -d & t \end{pmatrix}.$$

This gives us an isomorphism (of vector spaces, not of algebras) between A and $\mathrm{GF}(p) \times \mathrm{GF}(p)$, given by $a + bX \mapsto (a, b)$.

Theorem 4: A subspace of $(\mathrm{GF}(p) \times \mathrm{GF}(p))^n$ invariant under A is self-orthogonal if and only if the corresponding A-submodule of A^n is self-orthogonal under the A-valued inner product

$$\langle v, w\rangle_A = v \cdot \overline{w} = \sum_i v_i \overline{w_i}$$

where $\overline{a + bX} = a + b(t - X)$.

Proof: Let $v = a_1 + b_1X$ and $w = a_2 + b_2X$. Then

$$\begin{aligned} v \cdot \overline{w} &= (-a_1b_2 + b_1a_2)X + a_1a_2 + a_1b_2t + b_1b_2d \\ &= -\langle v, w\rangle X + \langle v, wX\rangle. \end{aligned}$$

The theorem follows. □

Remark: The A-valued inner product $\langle v, w\rangle_A$ should be distinguished from the GF(p)-valued inner product $\langle v, w\rangle$.

Corollary 5: If there exists an A-submodule C of A^n self-orthogonal under the inner product $v \cdot \overline{w}$, of size p^k, such that the minimum Hamming weight of $C^\perp - C$ is d, then there exists an $[[n, n-k, d]]_p$ code.

We will call such a symplectic code A-linear. The overall structure of A-linear codes clearly depends only on the orbit of A under conjugation by $\mathrm{Sp}_2(p)$. In particular, there are precisely three cases, depending on whether $t^2 - 4d$ is a nonsquare, a nonzero square, or 0; we will use the terminology inert linear, split linear, or ramified linear, respectively. If $t^2 - 4d$ is a nonsquare, then A is isomorphic to the finite field GF(p^2); this clearly corresponds to GF(4)-linear codes for $p = 2$.

In the split linear case, we may, without loss of generality, assume that X has characteristic polynomial $x^2 - x$, and thus $X(1-X) = 0$. It follows that C is the direct sum of CX and $C(1-X)$. But then there exist unique codes C_1 and C_2 in GF$(p)^n$ such that $CX = C_1X$ and $C(1-X) = C_2(1-X)$. This gives us the analog of Calderbank–Shor–Steane codes.

Theorem 6: Let C be a split linear code, with associated GF(p)-codes C_1 and C_2. Then $C_1 \subset C_2^\perp$, and the minimum distance of C is given by the minimum of the minimum weights of $C_2^\perp - C_1$ and $C_1^\perp - C_2$. Conversely, any pair of codes C_1 and C_2 with $C_1 \subset C_2^\perp$ give rise to a split linear code.

Proof: The generic element of C can be written as $v_1X + v_2(1-X)$. The inner product of two such elements is

$$\begin{aligned} &(v_1X + v_2(1-X)) \cdot \overline{(w_1X + w_2(1-X))} \\ &\quad = (v_1X + v_2(1-X)) \cdot (w_1(1-X) + w_2X) \\ &\quad = (v_1 \cdot w_2)X^2 + (v_2 \cdot w_1)(1-X)^2 \\ &\quad = (v_1 \cdot w_2 - v_2 \cdot w_1)X + (v_2 \cdot w_1). \end{aligned}$$

Consequently, C is self-orthogonal if and only if $v_1 \cdot v_2 = 0$ for all $v_1 \in C_1$ and $v_2 \in C_2$.

For the statement about the minimum distance, note that

$$\mathrm{wt}\,(v_1X + v_2(1-X)) \geq \max(\mathrm{wt}\,(v_1), \mathrm{wt}\,(v_2)).$$

Now, let $v = v_1X + v_2(1-X)$ be a minimal weight vector of $C^\perp - C$. Since $v \in C^\perp$, we find $v_1 \in C_2^\perp$ and $v_2 \in C_1^\perp$. On the other hand, either $v_1 \notin C_1$ or $v_2 \notin C_2$; without loss of generality, the first holds. But then $\mathrm{wt}\,(v_1) \leq \mathrm{wt}\,(v)$. Conversely, for any vector $w \in C_2^\perp - C_1$, the vector $wX \in C^\perp - C$ satisfies $\mathrm{wt}\,(wX) = \mathrm{wt}\,(w)$. The result follows. □

Finally, we have the ramified linear case; in this case, X has minimal polynomial X^2 without loss of generality. As in the split linear case, we have an associated code C_1 over GF(p), such that $C_1X = CX$. We also have an associated code C_0 given by those elements such that $vX = 0$; note that C_0 must contain C_1, since C contains C_1X. To complete the specification of C, it remains to give a map ϕ from C_1 to C/C_0; for $v_1 \in C_1$, $\phi(v_1)$ is defined by requiring that $v_1 + wX \in C$ precisely when $w \in \phi(v_1)$.

Lemma 7: Let C be a ramified linear code, with associated GF(p)-codes C_1 and C_0 and associated map ϕ. Then C_1 is orthogonal to C_0 (and is thus self-orthogonal). The minimum distance of the associated quantum code is bounded between the minimum weight of $C_0^\perp - C_1$ and the minimum weight of $C_1^\perp - C_0$. Conversely, any codes C_1, C_0, and map ϕ give rise to a quantum code in this fashion.

Proof: We compute, as before,

$$(v_1 + v_0X) \cdot \overline{(w_1 + w_0X)} = v_1 \cdot w_1 + (v_1 \cdot w_0 + v_0 \cdot w_1)X.$$

From the case $w_1 = 0$, $w_0 \in C_0$, we conclude that C_1 is orthogonal to C_0.

Clearly, changing the map ϕ to 0 can only decrease the minimum distance; in that case, $C = C_1 + C_0X$, and $C^\perp = C_0^\perp + C_1^\perp X$. On the other hand, for any element $v \in C_1^\perp - C_0$, $vX \in C^\perp - C$. □

Remark: In general, the minimum distance can depend on the map ϕ, although this does not happen in the pure case (the minimum distance of $C^\perp$ is equal to the minimum distance of the kernel of X in $C^\perp$, that is, $C_1^\perp X$).

It remains only to consider the case $\dim(A) = 4$. In this case, the code is certainly split linear; let C_1 and C_2 be its associated codes. Since $A = \mathrm{Mat}_2(p)$, the linear transformation taking $aX + b(1-X)$ to $a(1-X) + bX$ is certainly in A; consequently, we must have $C_1 = C_2$. Conversely, if C is a split linear code with $C_1 = C_2$, then C is $\mathrm{Mat}_2(p)$-linear.

For alphabets of size p^l, it makes sense to consider symplectic subalgebras of $\mathrm{Mat}_{2l}(p)$; that is, subalgebras invariant under the transformation

$$\overline{T} = J^{-1}T^tJ$$

where J is the symplectic inner product. Then we have a notion of A-linear codes as before (codes C such that $AC \subset C$). In general, it is not as clear how to work with such codes; certain special cases (codes linear over a subalgebra of $\mathrm{Mat}_2(p^l)$) can be dealt with as above, but others are not so straightforward (e.g., codes linear over a quaternion algebra). Such codes (including the quaternionic case) have been studied in [1] and [5].

VI. Codes from Number Fields

Let $\mathcal{O} = \mathbb{Z}[\alpha]$ be the integer ring of a real quadratic field. Suppose we are given an $\mathcal{O}$-submodule $\mathcal{C}$ of $\mathcal{O}^n$ such that $v \cdot \overline{w} = 0$ for all $v, w \in \mathcal{C}$. Clearly, we can embed $\mathcal{O}$ in $\mathrm{Mat}_2(\mathbb{Z})$ by mapping α to

$$\begin{pmatrix} 0 & 1 \\ -N(\alpha) & \mathrm{Tr}\,(\alpha) \end{pmatrix}.$$

Reduction $\bmod p$ then gives us a A-linear code $\mathcal{C}_p$, where A is the reduction of the image of $\mathcal{O}$ modulo p. This new code

is split (resp., inert, ramified) if and only if the prime p is split (resp., inert, ramified) in $\mathcal{O}$. One natural question is how the minimum distance of $\mathcal{C}_p$ behaves as p varies.

Theorem 8: Let d be the maximum over all p of the minimum distance of $\mathcal{C}_p^{\perp}$. Then this minimum distance is attained for all but a finite number of p.

Proof: For each $d-1$-set S of columns of $\mathcal{C}$, define an ideal I_S as the ideal generated by the determinants of all $d-1 \times d-1$ submatrices of the selected columns of the generator matrix of $\mathcal{C}$. We readily see that there exists a codeword of $\mathcal{C}_p^{\perp}$ with support contained in S if and only if I_S is not relatively prime to p. Thus if we define I_{d-1} as the least common multiple of the ideals I_S, then $\mathcal{C}_p^{\perp}$ has minimum distance d precisely when I_{d-1} is relatively prime to p. Unless $I_{d-1}=0$, this fails only a finite number of times (for those primes dividing the norm of I_{d-1}). But by assumption there exists at least one prime p' such that $\mathcal{C}_{p'}^{\perp}$ has minimum distance d, so I_{d-1} must be nontrivial. □

As an example of the use of this theory, we define quantum quadratic-residue codes. Let p' be a prime congruent to 1 modulo 4, and consider the integer ring $\mathcal{O}=\mathbb{Z}[\delta_{p'}]$, where

$$\delta_{p'}=\frac{1+\sqrt{p'}}{2}.$$

Over $\mathcal{O}$, the polynomial $x^{p'}-1$ factors as

$$(x-1)\nu(x)\overline{\nu(x)}$$

for some $\nu(x)$ of degree $(p'-1)/2$. Then the polynomial

$$(x-1)\nu(x)$$

determines a cyclic $\mathcal{O}$-module $\mathcal{C}$ of rank $(p'-1)/2$.

Theorem 9: For all $v, w \in \mathcal{C}$

$$v \cdot \overline{w}=0.$$

Proof: Let $v(x)$ and $w(x)$ be the corresponding polynomials in

$$\mathcal{O}[x]/(x^{p'}-1).$$

Then $v \cdot \overline{w}$ can be computed as the x^0 coefficient of

$$v(x)\overline{w(x^{p'-1})}.$$

In particular, since v and w are in $\mathcal{C}$, both can be written as multiples of $(x-1)\nu(x)$. But

$$\nu(x^{p'-1})=\nu(x)$$

since -1 is a quadratic residue modulo p'. It follows that $v(x)\overline{w(x^{p'-1})}$ is a multiple of $(x-1)\nu(x)\overline{\nu(x)}$, so must be 0. □

Thus for all p, $\mathcal{C}_p$ produces an $[[n, 1, d(p)]]_p$ code for some $d(p)$. The case $p=p'$ is of particular interest.

Theorem 10: $\mathcal{C}_{p'}$ is a pure $[[n, 1, \frac{1}{2}(p'+1)]]_{p'}$ code; in particular, it is MDS.

Proof: By the remark after Lemma 7, it suffices to show that $\sqrt{p'}\,\mathcal{C}_{p'}$ has minimum dual distance $\frac{1}{2}(p'+1)$; equivalently, we need to show that the code $(\mathcal{C}_{p'} \bmod \sqrt{p'})$ is MDS. But, in fact, any classical cyclic code of length equal to its characteristic is MDS. □

Corollary 11: For all but a finite number of primes p, $\mathcal{C}_p$ is MDS.

Proof: Apply Theorem 8 to $\mathcal{C}$. □

Corollary 12: For all but a finite number of primes p, $\mathcal{C}_p$ can be extended to a self-dual MDS code of length $p'+1$.

Proof: Let p be any prime such that $\mathcal{C}_p$ is MDS. By Theorem 2, $\mathcal{C}_p$ is pure to weight $(p'+3)/2$. But then [11, Theorem 20] allows us to construct the desired self-dual MDS code of length $p'+1$ and minimum distance $(p'+3)/2$. □

Consider, for example, the case $p'=5$. In this case, a direct computation readily shows that the ideal I_2 as defined in Theorem 8 is $\langle 1\rangle$; consequently

Theorem 13: For all prime integers $\alpha>1$, there exists a $((5, \alpha, 3))_\alpha$ code and a $((6, 1, 4))_\alpha$ code.

In fact, this is valid for composite α as well, using the following result.

Theorem 14: For all n, d, α, β, K and L, if there exists a $((n, K, d))_\alpha$ code and a $((n, L, d))_\beta$ code, then there also exists a $((n, KL, d))_{\alpha\beta}$ code, which is pure if the original codes are pure.

Proof: Let the two given codes be $C_1 \subset (\mathbb{C}^\alpha)^{\otimes n}$ and $C_2 \subset (\mathbb{C}^\beta)^{\otimes n}$. Then $C_1 \otimes C_2$ can be viewed as a subspace of $(\mathbb{C}^{\alpha\beta})^{\otimes n}$. It is straightforward to verify that $C_1 \otimes C_2$ is the required code. (In particular, note that we may choose a basis of the space of errors which is a tensor product of bases for the α error space and for the β error space.) □

Remarks: 1) This is essentially a quantum analog of the direct sum of classical codes and 2) in the natural extension of the symplectic construction to composite alphabets, there is a partial converse to this result; in particular, any $[[n, k, d]]_\alpha$ code is the direct sum of codes corresponding to the prime power factors of α. This is the main reason why we have largely restricted our attention to the case of prime alphabet here.

VII. Universal Fault-Tolerant Operations

In [6], Gottesman gives a method for doing fault-tolerant operations through quantum codes using automorphisms of the code and of certain related codes. In particular, he gives a quaternary operation that can be applied fault-tolerantly through any additive code. It is natural to wonder how this extends to codes over larger alphabets, and to what extent existing symmetries of the code can be used to extend the set of operations.

In particular, fix a prime p, an integer $l \geq 1$, and a symplectic subalgebra A of $\mathrm{Mat}_{2l}(\mathrm{GF}(p))$; we would like to characterize all fault-tolerant operations that are universal for A-linear codes. That is, we would like to determine all elements of $\mathrm{Sp}_{2lm}(\mathrm{GF}(p))$ that are global automorphisms of

$C^{(m)}$ for all A-linear C, where $C^{(m)}$ is the direct sum of m copies of C, viewed as a symplectic code over $\mathrm{GF}(p)^{lm}$. Clearly, it suffices to consider the corresponding subalgebra of $\mathrm{Mat}_{2lm}(\mathrm{GF}(p))$.

Theorem 15: Let C be an A-linear code. Then $C^{(m)}$ is $\mathrm{Mat}_m(A)$-linear. Conversely, if $T \in \mathrm{Mat}_{2lm}(\mathrm{GF}(p))$ is not in $\mathrm{Mat}_m(A)$, then there exists an A-linear code C such that $C^{(m)}$ is not T-invariant.

Proof: Let T be an element of $\mathrm{Mat}_{2lm}(\mathrm{GF}(p))$ such that $TC^{(m)} \subset C^{(m)}$ for all A-linear C. For all $v \in (\mathrm{GF}(p)^{2l})^k$ such that $\langle v, va\rangle = 0$ for all $a \in A$, vA is an A-linear code; consequently, we must have $T(vA)^{(m)} \subset (vA)^{(m)}$ for all such v. Conversely, if this is true, then T is universal, since any A-linear C can be written as a union of such codes. Now, it follows that $T(v, 0, 0, \cdots, 0) = (v_1, v_2, v_3, \cdots, v_m)$, where each v_i must be in vA. By choosing k sufficiently large, we may insist that the coefficients of v form a basis of $\mathrm{GF}(p)^{2lm}$; it follows that there must exist elements $a_{11}, a_{12}, \cdots, a_{1m}$ such that for all v

$$T(v, 0, 0, \cdots, 0) = (va_{11}, va_{12}, \cdots, va_{1m}).$$

It follows that T can be written as an element of $\mathrm{Mat}_m(A)$. Clearly, any such T will take $(vA)^{(m)}$ to a subspace of $(vA)^{(m)}$, so the desired algebra is $\mathrm{Mat}_m(A)$. □

It remains only to determine which of these operations preserve the inner product (and thus correspond to operations that can be physically performed). Considered as an element of $\mathrm{Mat}_{2lm}(\mathrm{GF}(p))$, T must satisfy $TJT^t = J$, where J is the symplectic inner product. Equivalently, JT^tJ^{-1} must be T^{-1}. Considering T as an element of $\mathrm{Mat}_m(A)$, this says that $T^\dagger T = 1$, where $T^\dagger$ is the conjugate of the transpose of T.

Of particular interest are those operations that cannot be decomposed as a product of unary operations and permutations; that is, those elements T which are not monomial matrices over A.

Example 1: Let $A = \mathrm{GF}(p^l)$; in particular, if $l = 1$, this includes all symplectic codes. Then for $T \in \mathrm{Mat}_m(A)$, $\overline{T} = T$, so we get the group $O_m(\mathrm{GF}(p^l))$. For $p^l = 2$, the first nonmonomial operation appears when $m = 4$. This is, for instance, given by

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

this is equivalent to [6, eq. (45)]. For $p = 2$, $l > 1$, we always have nonmonomial operations of the following form:

$$\begin{pmatrix} 1+x & x \\ x & 1+x \end{pmatrix}$$

where x is any element of $\mathrm{GF}(p^l) - \mathrm{GF}(p)$; it is not clear, however, whether these can be used to perform fault-tolerant operations.

Example 2: Let $A = \mathrm{GF}(p^{2l})$. This is readily seen to correspond to the unitary group $U_m(\mathrm{GF}(p^{2l}))$. For $p^l = 2$, we first see nonmonomial operations when $m = 3$; for instance,

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \omega \end{pmatrix}.$$

Note that the operation given as [6, eq. (40)] as fault-tolerant for the well-known [[5, 1, 3]] code is unitary, so can be applied to any $\mathrm{GF}(4)$-linear binary code.

Example 3: Let $A = \mathrm{GF}(p^l) \times \mathrm{GF}(p^l)$ (i.e., Calderbank–Shor–Steane codes). Any element of $\mathrm{Mat}_m(A)$ can be written as a pair of elements of $\mathrm{Mat}_m(\mathrm{GF}(p^l))$; conjugation switches these elements. Thus the fault-tolerant operations are those of the form (T_1, T_2), where $T_1^t T_2 = 1$. This is equivalent to the group $\mathrm{GL}_m(\mathrm{GF}(p^l))$. We first see nonmonomial operations when $m = 2$; for instance, when $p^l = 2$, we get

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

which corresponds to a controlled-not.

Further work on this subject can be found in [7].

REFERENCES

[1] C. Bachoc, "Applications of coding theory to the construction of modular lattices," *J. Combin. Theory Ser. A*, vol. 78, pp. 92–119, 1997.

[2] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.*, vol. 75, pp. 436–480, 1997.

[3] 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, July 1998, LANL e-print quant-ph/9608006.

[4] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996, LANL e-print quant-ph/9512032.

[5] P. Gaborit, "Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1222–1228, 1996.

[6] D. Gottesman, "A theory of fault-tolerant quantum computation," *Phys. Rev. A*, vol. 57, no. 1, pp. 127–137, 1998, LANL e-print quant-ph/9702029 .

[7] ——, "Fault-tolerant quantum computation with higher-dimensional systems," LANL e-print quant-ph/9802007.

[8] E. Knill, "Non-binary error bases and quantum codes," LANL e-print quant-ph/9608048.

[9] ——, "Group representations, error bases and quantum codes," LANL e-print quant-ph/9608049.

[10] 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.

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

[12] A. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996, LANL e-print quant-ph/9605021.

[13] A. Weil, "Sur certaines groupes d'opérateurs unitaires," *Acta. Arithm.*, vol. 11, pp. 143–211, 1964.