Nonbinary Stabilizer Codes Over Finite Fields

Avanti Ketkar, Andreas Klappenecker, *Member, IEEE*, Santosh Kumar, and Pradeep Kiran Sarvepalli

***Abstract*—One formidable difficulty in quantum communication and computation is to protect information-carrying quantum states against undesired interactions with the environment. To address this difficulty, many good quantum error-correcting codes have been derived as binary stabilizer codes. Fault-tolerant quantum computation prompted the study of nonbinary quantum codes, but the theory of such codes is not as advanced as that of binary quantum codes. This paper describes the basic theory of stabilizer codes over finite fields. The relation between stabilizer codes and general quantum codes is clarified by introducing a Galois theory for these objects. A characterization of nonbinary stabilizer codes over $\mathbf{F}_q$ in terms of classical codes over $\mathbf{F}_{q^2}$ is provided that generalizes the well-known notion of additive codes over $\mathbf{F}_4$ of the binary case. This paper also derives lower and upper bounds on the minimum distance of stabilizer codes, gives several code constructions, and derives numerous families of stabilizer codes, including quantum Hamming codes, quadratic residue codes, quantum Melas codes, quantum Bose–Chaudhuri–Hocquenghem (BCH) codes, and quantum character codes. The puncturing theory by Rains is generalized to additive codes that are not necessarily pure. Bounds on the maximal length of maximum distance separable stabilizer codes are given. A discussion of open problems concludes this paper.**

***Index Terms*—Bose–Chaudhuri–Hocquenghem (BCH) codes, bounds, MDS codes, nonbinary codes, puncturing, quantum codes, Reed-Muller codes, self-orthogonal codes.**

I. Introduction

RELIABLE quantum information processing requires mechanisms to reduce the effects of environmental and operational noise. Fortunately, it is possible to alleviate the detrimental effects of decoherence by employing quantum error-correcting codes, so that one can engineer more reliable quantum communication schemes and quantum computers.

The most widely studied class of quantum error-correcting codes are binary stabilizer codes, see [7], [8], [14], [18], [20], [27]–[30], [33], [37], [39], [40], [42]–[46], [49], [55], [56], [58], [69], [81], [91], [93]–[96], [98], [101] and, in particular, the seminal works [19], [38]. An appealing aspect of binary stabilizer codes is that there exist links to classical coding theory that facilitate the construction of good codes. More recently, some results were generalized to the case of nonbinary stabilizer codes [1], [3], [4], [16], [23], [24], [34], [35], [41], [48], [50], [57], [65], [71], [80], [84], [86], [87], but the theory is not nearly as complete as in the binary case.

We recall the basic principles of nonbinary stabilizer codes over finite fields in the next section. In Section III, we introduce a Galois theory for quantum error-correcting codes. The original theory developed by Evariste Galois relates field extensions to groups. Oystein Ore derived a significantly more general theory for pairs of lattices [75]. We use this framework and set up a Galois correspondence between quantum error-correcting codes and groups. This theory shows how some properties of general quantum codes, such as bounds on the minimum distance, can be deduced from results about stabilizer codes.

In Section IV, we recall that stabilizer codes over a finite field $\mathbf{F}_q$ correspond to additive codes over $\mathbf{F}_q$ that are self-orthogonal with respect to a trace-symplectic form [4]. We also establish the correspondence to additive codes over $\mathbf{F}_{q^2}$ that are self-orthogonal with respect to a trace-alternating form; remarkably, this basic construction had been missing in the literature, in spite of the fact that it is a generalization of the famous $\mathbf{F}_4$-codes [19].

The MacWilliams relations for weight enumerators of stabilizer codes are particularly easy to prove, as we show in Section V. We then derive upper and lower bounds on the minimum distance of the best possible stabilizer codes in Section VI. In Section VII, we recall basic facts about cyclic stabilizer codes.

After laying the foundation in the first seven sections, we are able to construct numerous code families in the subsequent sections. In Section VIII, we derive quantum Hamming codes; in Section IX, quantum quadratic residue codes; in Section X, quantum Melas codes; and in Section XI, quantum BCH codes. In the latter case, we show that it is possible to extend quantum BCH codes. In Section XII, we generalize the known results about puncturing pure linear stabilizer codes to arbitrary additive codes, and we illustrate this theory by puncturing quantum BCH codes.

We show in Section XIII that stabilizer codes over $\mathbf{F}_q$ attaining the quantum Singleton bound cannot exceed a length of q^2+1, except in a few sporadic cases, assuming that the classical MDS conjecture holds. We give slightly weaker bounds for the length of MDS stabilizer codes without such an assumption. In Section XIV, we derive an interesting class of quantum character codes. We give numerous code constructions in Section XV, and conclude the paper with a discussion of open questions.

We have tried to keep the prerequisites to a minimum, so that readers from the coding theory community as well as from the quantum computing community can benefit. Apart from the basics of quantum computing, we recommend [19] and [40] for background on binary stabilizer codes, in addition to books on classical coding theory, such as [53] and [68]. The general

Manuscript received August 19, 2005; revised July 26, 2006. This work was supported by the NSF under Grant CCF-0218582, NSF CAREER award CCF-0347310, a TITF grant, and a TEES Select Young Faculty Award.

A. Ketkar was with the Department of Computer Science, Texas A&M University, College Station, TX 77843 USA. She is now with Ingenio, Inc., San Francisco, CA 94111 USA.

A. Klappenecker and P. K. Sarvepalli are with the Department of Computer Science, Texas A&M University, College Station, TX 77843 USA.

S. Kumar was with the Department of Computer Science, Texas A&M University, College Station, TX 77843 USA. He is now with Microsoft Corporation, Seattle, WA 98052 USA.

Communicated by E. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2006.883612

theory of quantum codes is discussed in [62], and we assume that the reader is familiar with the notion of a detectable error, as introduced there. In general, we will omit proofs for results from our companion papers [2], [85], but otherwise we tried to make this paper reasonably self-contained.

Notations

We assume throughout this paper that $\mathbf{F}_q$ denotes a finite field of characteristic p; in particular, q always denotes a power of a prime p. The trace function from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ is defined as $\mathrm{tr}_{q^m/q}(x) = \sum_{k=0}^{m-1} x^{q^k}$; we may omit the subscripts if $\mathbf{F}_q$ is the prime field. If G is a group, then we denote by $Z(G)$ the center of G. If $S \subseteq G$, then we denote by $C_G(S)$ the centralizer of S in G. We write $H \leq G$ to express the fact that H is a subgroup of G. The trace $\mathrm{Tr}(M)$ of a square matrix M is the sum of the diagonal elements of M.

II. Stabilizer Codes

Let q a power of a prime p, and let $\mathbf{C}^q$ be a q-dimensional complex vector space representing the states of a quantum mechanical system. We denote by $|x\rangle$ the vectors of a distinguished orthonormal basis of $\mathbf{C}^q$, where the labels x range over the elements of a finite field $\mathbf{F}_q$ with q elements. A quantum error-correcting code Q is a K-dimensional subspace of $\mathbf{C}^{q^n} = \mathbf{C}^q \otimes \cdots \otimes \mathbf{C}^q$.

We need to select an appropriate error model so that we can measure the performance of a code. We simplify matters by choosing a basis $\mathcal{E}_n$ of the vector space of complex $q^n \times q^n$ matrices to represent a discrete set of errors. A stabilizer code is defined as the joint eigenspace of a subset of $\mathcal{E}_n$, so the error operators play a crucial role.

A. Error Bases

Let a and b be elements of the finite field $\mathbf{F}_q$. We define the unitary operators $X(a)$ and $Z(b)$ on $\mathbf{C}^q$ by

$$X(a)|x\rangle = |x+a\rangle, \qquad Z(b)|x\rangle = \omega^{\mathrm{tr}(bx)}|x\rangle$$

where tr denotes the trace operation from the extension field $\mathbf{F}_q$ to the prime field $\mathbf{F}_p$, and $\omega = \exp(2\pi i/p)$ is a primitive pth root of unity.

We form the set $\mathcal{E} = \{X(a)Z(b) \,|\, a,b \in \mathbf{F}_q\}$ of error operators. The set $\mathcal{E}$ has some interesting properties, namely, a) it contains the identity matrix, b) the product of two matrices in $\mathcal{E}$ is a scalar multiple of another element in $\mathcal{E}$, and c) the trace $\mathrm{Tr}(A^\dagger B) = 0$ for distinct elements A, B of $\mathcal{E}$. A finite set of q^2 unitary matrices that satisfy the properties a), b), and c) is called a nice error basis, see [61].

The set $\mathcal{E}$ of error operators forms a basis of the set of complex $q \times q$ matrices due to property c). We include a proof that $\mathcal{E}$ is a nice error basis, because parts of our argument will be of independent interest in the subsequent sections.

Lemma 1: The set $\mathcal{E} = \{X(a)Z(b) \,|\, a,b \in \mathbf{F}_q\}$ is a nice error basis on $\mathbf{C}^q$.

Proof: The matrix $X(0)Z(0)$ is the identity matrix, so property (a) holds. We have $\omega^{\mathrm{tr}(ba)}X(a)Z(b) = Z(b)X(a)$, which implies that the product of two error operators is given by

$$X(a)Z(b)\,X(a')Z(b') = \omega^{\mathrm{tr}(ba')}X(a+a')Z(b+b'). \quad (1)$$

This is a scalar multiple of an operator in $\mathcal{E}$, hence property b) holds.

Suppose that the error operators are of the form $A = X(a)Z(b)$ and $B = X(a)Z(b')$ for some $a, b, b' \in \mathbf{F}_q$. Then

$$\mathrm{Tr}(A^\dagger B) = \mathrm{Tr}(Z(b'-b)) = \sum_{x \in \mathbf{F}_q} \omega^{\mathrm{tr}((b'-b)x)}.$$

The map $x \mapsto \omega^{\mathrm{tr}((b'-b)x)}$ is an additive character of $\mathbf{F}_q$. The sum of all character values is 0 unless the character is trivial; thus, $\mathrm{Tr}(A^\dagger B) = 0$ when $b' \neq b$.

On the other hand, if $A = X(a)Z(b)$ and $B = X(a')Z(b')$ are two error operators satisfying $a \neq a'$, then the diagonal elements of the matrix $A^\dagger B = Z(-b)X(a'-a)Z(b')$ are 0, which implies $\mathrm{Tr}(A^\dagger B) = 0$. Thus, whenever A and B are distinct elements of $\mathcal{E}$, then $\mathrm{Tr}(A^\dagger B) = 0$, which proves c). □

Example 2: We give an explicit construction of a nice error basis with $q = 4$ levels. The finite field $\mathbf{F}_4$ consists of the elements $\mathbf{F}_4 = \{0, 1, \alpha, \overline{\alpha}\}$. We denote the four standard basis vectors of the complex vector space $\mathbf{C}^4$ by $|0\rangle, |1\rangle, |\alpha\rangle$, and $|\overline{\alpha}\rangle$. Let $\mathbf{1}_2$ denote the 2×2 identity matrix, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then

$$\begin{aligned} X(0) &= \mathbf{1}_2 \otimes \mathbf{1}_2, & X(1) &= \mathbf{1}_2 \otimes \sigma_x, \\ X(\alpha) &= \sigma_x \otimes \mathbf{1}_2, & X(\overline{\alpha}) &= \sigma_x \otimes \sigma_x, \\ Z(0) &= \mathbf{1}_2 \otimes \mathbf{1}_2, & Z(1) &= \sigma_z \otimes \mathbf{1}_2, \\ Z(\alpha) &= \sigma_z \otimes \sigma_z, & Z(\overline{\alpha}) &= \mathbf{1}_2 \otimes \sigma_z. \end{aligned}$$

We see that this nice error basis is obtained by tensoring the Pauli basis, a nice error basis on $\mathbf{C}^2$. The next lemma shows that this is a general design principle for nice error bases.

Lemma 3: If $\mathcal{E}_1$ and $\mathcal{E}_2$ are nice error bases, then

$$\mathcal{E} = \{E_1 \otimes E_2 \,|\, E_1 \in \mathcal{E}_1, E_2 \in \mathcal{E}_2\}$$

is a nice error basis as well.

The proof of this observation follows directly from the definitions.

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{F}_q^n$. We write $X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{a}) = Z(a_1) \otimes \cdots \otimes Z(a_n)$ for the tensor products of n error operators. Our aim is to provide an error model that conveniently represents errors acting locally on one quantum system. Using the new notations, we can easily formulate this model.

Corollary 4: The set $\mathcal{E}_n = \{X(\mathbf{a})Z(\mathbf{b}) \,|\, \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n\}$ is a nice error basis on the complex vector space $\mathbf{C}^{q^n}$.

Remark. Several authors have used an error basis that is equivalent to our definition of $\mathcal{E}_n$, see [4], [35], [57], [71]. We have defined the operator $Z(b)$ in a slightly different way, so that the properties relevant for the design of stabilizer codes

become more transparent. In particular, we can avoid an intermediate step that requires tensoring $p \times p$–matrices, and that allows us to obtain the trace-symplectic form directly, see Lemma 5.

B. Stabilizer Codes

Let G_n denote the group generated by the matrices of the nice error basis $\mathcal{E}_n$. It follows from (1) that

$$G_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \,|\, \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}.$$

Note that G_n is a finite group of order pq^{2n}. We call G_n the *error group* associated with the nice error basis $\mathcal{E}_n$.

A *stabilizer code* Q is a non-zero subspace of $\mathbf{C}^{q^n}$ that satisfies

$$Q = \bigcap_{E \in S} \{v \in \mathbf{C}^{q^n} \mid Ev = v\} \tag{2}$$

for some subgroup S of G_n. In other words, Q is the joint eigenvalue-1 eigenspace of a subgroup S of the error group G_n.

Remark. A crucial property of a stabilizer code is that it contains *all* joint eigenvectors of S with eigenvalue 1, as (2) indicates. If the code is smaller and does not exhaust all joint eigenvectors of S with eigenvalue 1, then it is not a stabilizer code for S.

C. Minimum Distance

The error correction and detection capabilities of a quantum error-correcting code Q are the most crucial aspects of the code. Recall that a quantum code Q is able to detect an error E in the unitary group $U(q^n)$ if and only if the condition $\langle c_1|E|c_2\rangle = \lambda_E \langle c_1|c_2\rangle$ holds for all $c_1, c_2 \in Q$, see [62].

It turns out that a stabilizer code Q with stabilizer S can detect all errors in G_n that are scalar multiples of elements in S or that do not commute with some element of S, see Lemma 11. In particular, an error in G_n that is not detectable has to commute with all elements of the stabilizer. Commuting elements in G_n are characterized as follows:

Lemma 5: Two elements $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ and $E' = \omega^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ of the error group G_n satisfy the relation

$$EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a})} E'E.$$

In particular, the elements E and E' commute if and only if the trace symplectic form $\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a})$ vanishes.

Proof: It follows from (1) that

$$EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}')} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$$

and

$$E'E = \omega^{\mathrm{tr}(\mathbf{b}'\cdot\mathbf{a})} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}').$$

Therefore, multiplying $E'E$ by the scalar $\omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a})}$ yields EE', as claimed. □

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

$$\mathrm{swt}((\mathbf{a}|\mathbf{b})) = |\{\, k \,|\, (a_k, b_k) \neq (0,0)\}|.$$

The weight $\mathrm{w}(E)$ of an element $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ in the error group G_n is defined to be the number of nonidentity tensor components, $\mathrm{w}(E) = \mathrm{swt}((\mathbf{a}|\mathbf{b}))$. In particular, the weight of a scalar multiple of the identity matrix is by definition zero.

A quantum code Q has *minimum distance* d if and only if it can detect all errors in G_n of weight less than d, but cannot detect some error of weight d. We say that Q is an $((n, K, d))_q$ code if and only if Q is a K-dimensional subspace of $\mathbf{C}^{q^n}$ that has minimum distance d. An $((n, q^k, d))_q$ code is also called an $[[n, k, d]]_q$ code. We remark that some authors are more restrictive and use the bracket notation just for stabilizer codes.

We say that a quantum code Q is *pure to* t if and only if its stabilizer group S does not contain non-scalar matrices of weight less than t. A quantum code is called pure if and only if it is pure to its minimum distance. As in [19], we always assume that an $[[n, 0, d]]_q$ code has to be pure.

Remarks. a) If a quantum error-correcting code can detect a set $\mathcal{D}$ of errors, then it can detect all errors in the linear span of $\mathcal{D}$. b) A code of minimum distance d can correct all errors of weight $t = \lfloor (d-1)/2 \rfloor$ or less.

III. Galois Connection

We want to clarify the relation between stabilizer codes and more general quantum codes before we proceed further. Let us denote by $\mathcal{Q}$ the set of all subspaces of $\mathbf{C}^{q^n}$. The set $\mathcal{Q}$ is partially ordered by the inclusion relation. Any two elements of $\mathcal{Q}$ have a least upper bound and a greatest lower bound with respect to the inclusion relation, namely

$$\sup\{Q, Q'\} = Q + Q' \quad \text{and} \quad \inf\{Q, Q'\} = Q \cap Q'.$$

Therefore, $\mathcal{Q}$ is a complete (order) lattice. An element of this lattice is a quantum error-correcting code or is equal to the vector space $\{0\}$.

Let $\mathcal{G}$ denote the lattice of subgroups of the error group G_n. We will introduce two order-reversing maps between $\mathcal{G}$ and $\mathcal{Q}$ that establish a Galois connection. We will see that stabilizer codes are distinguished elements of $\mathcal{Q}$ that remain the same when mapped to the lattice $\mathcal{G}$ and back.

Let us define a map Fix from the lattice $\mathcal{G}$ of subgroups to the lattice $\mathcal{Q}$ of subspaces that associates to a group S its joint eigenspace with eigenvalue 1

$$\mathrm{Fix}(S) = \bigcap_{E \in S} \{v \in \mathbf{C}^{q^n} \,|\, Ev = v\}. \tag{3}$$

We define for the reverse direction a map Stab from the lattice $\mathcal{Q}$ to the lattice $\mathcal{G}$ that associates to a quantum code Q its stabilizer group $\mathrm{Stab}(Q)$,

$$\mathrm{Stab}(Q) = \{E \in G_n \,|\, Ev = v \text{ for all } v \in Q\}. \tag{4}$$

We obtain four direct consequences of the definitions (3) and (4):

- G1) If $Q_1 \subseteq Q_2$ are subspaces of $\mathbf{C}^{q^n}$, then $\mathrm{Stab}(Q_2) \leq \mathrm{Stab}(Q_1)$.
- G2) If $S_1 \leq S_2$ are subgroups of G_n, then $\mathrm{Fix}(S_2) \leq \mathrm{Fix}(S_1)$.
- G3) A subspace Q of $\mathbf{C}^{q^n}$ satisfies $Q \subseteq \mathrm{Fix}(\mathrm{Stab}(Q))$.
- G4) A subgroup S of G_n satisfies $S \leq \mathrm{Stab}(\mathrm{Fix}(S))$.

The first two properties establish that Fix and Stab are order-reversing maps. The extension properties G3 and G4 establish that Fix and Stab form a Galois connection, see [17, p. 56]. The general theory of Galois connections establishes, among

other results, that $\mathrm{Fix}(S) = \mathrm{Fix}(\mathrm{Stab}(\mathrm{Fix}(S)))$ and $\mathrm{Stab}(Q) = \mathrm{Stab}(\mathrm{Fix}(\mathrm{Stab}(Q)))$ holds for all S in $\mathcal{G}$ and all Q in $\mathcal{Q}$.

A subspace Q of the vector space $\mathbf{C}^{q^n}$ satisfying G3 with equality is called a *closed subspace*, and a subgroup S of the error group G_n satisfying G4 with equality is called a *closed subgroup*. We record the main result of abstract Galois theory in the following proposition.

Proposition 6: The closed subspaces of the vector space $\mathbf{C}^{q^n}$ form a complete sublattice $\mathcal{Q}_c$ of the lattice $\mathcal{Q}$. The closed subgroups of G_n form a complete sublattice $\mathcal{G}_c$ of the lattice $\mathcal{G}$ that is dual isomorphic to the lattice $\mathcal{Q}_c$.

Proof: This result holds for any Galois connection, see Theorem 10 in the book by Birkhoff [17, p. 56]. □

We need to characterize the closed subspaces and subgroups to make this proposition useful. We begin with the closed subspaces because this is easier.

Lemma 7: A closed subspace is a stabilizer code or is 0-dimensional.

Proof: By definition, a closed subspace Q satisfies

$$Q = \mathrm{Fix}(\mathrm{Stab}(Q)) = \bigcap_{E \in \mathrm{Stab}(Q)} \{v \in \mathbf{C}^{q^n} \mid Ev = v\};$$

hence, it is a stabilizer code or $\{0\}$. □

Lemma 8: If Q is a nonzero subspace of $\mathbf{C}^{q^n}$, then its stabilizer $S = \mathrm{Stab}(Q)$ is an abelian group satisfying $S \cap Z(G_n) = \{1\}$.

Proof: Suppose that E and E' are noncommuting elements of $S = \mathrm{Stab}(Q)$. By Lemma 5, we have $EE' = \omega^k E'E$ for some $\omega^k \neq 1$. A nonzero vector v in Q would have to satisfy $v = EE'v = \omega^k E'Ev = \omega^k v$, contradiction. Therefore, S is an abelian group. The stabilizer cannot contain any element $\omega^k \mathbf{1}$, unless $k = 0$, which proves the second assertion. □

Lemma 9: Suppose that S is the stabilizer of a vector space Q. An orthogonal projector onto the joint eigenspace $\mathrm{Fix}(S)$ is given by

$$P = \frac{1}{|S|} \sum_{E \in S} E.$$

Proof: A vector v in $\mathrm{Fix}(S)$ satisfies $Pv = v$, hence $\mathrm{Fix}(S)$ is contained in the image of P. Conversely, note that $EP = P$ holds for all E in S, hence any vector in the image of P is an eigenvector with eigenvalue 1 of all error operators E in S. Therefore, $\mathrm{Fix}(S) =$ image P. The operator P is idempotent, because

$$P^2 = \frac{1}{|S|} \sum_{E \in S} EP = \frac{1}{|S|} \sum_{E \in S} P = P$$

holds. The inverse $E^\dagger$ of E is contained in the group S, hence $P^\dagger = P$. Therefore, P is an orthogonal projector onto $\mathrm{Fix}(S)$. □

Remark: If S is a nonabelian subgroup of the group G_n, then it necessarily contains the center $Z(G_n)$ of G_n; it follows that P is equal to the all-zero matrix. Note that the image of P has dimension $\mathrm{Tr}(P) = q^n/|S|$.

Lemma 10: A subgroup S of G_n is closed if and only if S is an abelian subgroup that satisfies $S \cap Z(G_n) = \{1\}$ or if S is equal to G_n.

Proof: Suppose that S is a closed subgroup of G_n. The vector space $Q = \mathrm{Fix}(S)$ is, by definition, either a stabilizer code or a 0-dimensional vector space. We have $\mathrm{Stab}(\{0\}) = G_n$. Furthermore, if $Q \neq \{0\}$, then $\mathrm{Stab}(Q) = S$ is an abelian group satisfying $S \cap Z(G_n) = \{\mathbf{1}\}$, by Lemma 8.

Conversely, suppose that S is an Abelian subgroup of G_n such that S trivially intersects the center $Z(G_n)$. Let $S^* = \mathrm{Stab}(\mathrm{Fix}(S))$. We have $\mathrm{Fix}(S^*) = \mathrm{Fix}(\mathrm{Stab}(\mathrm{Fix}(S))) = \mathrm{Fix}(S)$, because this holds for any pair of maps that form a Galois connection. It follows from Lemma 9 that

$$q^n/|S^*| = \mathrm{Tr}\left(\frac{1}{|S^*|} \sum_{E \in S^*} E\right) = \mathrm{Tr}\left(\frac{1}{|S|} \sum_{E \in S} E\right) = q^n/|S|.$$

Since $S \leq S^*$, this shows that $S = S^* = \mathrm{Stab}(\mathrm{Fix}(S))$; hence, S is a closed subgroup of G_n. We note that $\mathrm{Fix}(G_n) = \{0\}$, so that $G_n = \mathrm{Stab}(\mathrm{Fix}(G_n))$ is closed. □

The stabilizer codes are easier to study than arbitrary quantum codes, as we will see in the subsequent sections. If we know the error correction capabilities of stabilizer codes, then we sometimes get a lower bound on the minimum distance of an arbitrary code by the following simple observation:

Fact: An arbitrary quantum code Q is contained in the larger stabilizer code $Q^* = \mathrm{Fix}(\mathrm{Stab}(Q))$. If an error E can be detected by Q^*, then it can be detected by Q as well. Therefore, if the stabilizer code Q^* has minimum distance d, then the quantum code Q has at least minimum distance d.

IV. Additive Codes

The previous section explored the relation between stabilizer codes and other quantum codes. We show next how stabilizer codes are related to classical codes (namely, additive codes over $\mathbf{F}_q$ or $\mathbf{F}_{q^2}$). The classical codes allow us to characterize the errors in G_n that are detectable by the stabilizer code.

In the binary case, the problem of finding stabilizer codes of length n had been translated into a) finding binary classical codes of length $2n$ that are self-orthogonal with respect to a symplectic inner product or b) finding classical codes of length n over $\mathbf{F}_4$ that are self-orthogonal with respect to a trace-inner product, see [19]. The approach a) was generalized to prime alphabets by Rains [80] and to prime-power alphabets by Ashikhmin and Knill [4]. We simplify the arguments and include a full proof of this connection. There were many attempts to generalize the approach b) to nonbinary alphabets, but without complete success (but see, for instance, [57], [71], [80] for notable partial solutions). We fill this gap and introduce a natural generalization of b). Furthermore, we discuss simpler constructions for linear codes. Before exploring these connections to classical codes, we first recall some facts about detectable errors.

If S is a subgroup of G_n, then $C_{G_n}(S)$ denotes centralizer of S in G_n

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

and $SZ(G_n)$ denotes the group generated by S and the center $Z(G_n)$. We first recall the following characterization of detectable errors (see also [4]; the interested reader can find a more general approach in [59], [60]).

Lemma 11: Suppose that $S \leq G_n$ is the stabilizer group of a stabilizer code Q of dimension $\dim Q > 1$. An error E in G_n is detectable by the quantum code Q if and only if either E is an element of $SZ(G_n)$ or E does not belong to the centralizer $C_{G_n}(S)$.

Proof: An element E in $SZ(G_n)$ is a scalar multiple of a stabilizer; thus, it acts by multiplication with a scalar λ_E on Q. It follows that E is a detectable error.

Suppose now that E is an error in G_n that does not commute with some element F of the stabilizer S; it follows that $EF = \lambda FE$ for some complex number $\lambda \neq 1$, see Lemma 5. All vectors u and v in Q satisfy the condition

$$\langle u|E|v\rangle = \langle u|EF|v\rangle = \lambda\langle u|FE|v\rangle = \lambda\langle u|E|v\rangle; \quad (5)$$

hence, $\langle u|E|v\rangle = 0$. It follows that the error E is detectable.

Finally, suppose that E is an element of $C_{G_n}(S) \setminus SZ(G_n)$. Seeking a contradiction, we assume that E is detectable; this implies that there exists a complex scalar λ_E such that $Ev = \lambda_E v$ for all v in Q. The scalar λ_E cannot be zero because E commutes with the elements of S, so $EP = PEP = \lambda_E P$ and clearly $EP \neq 0$. Let S^* denote the abelian group generated by $\lambda_E^{-1}E$ and by the elements of S. The joint eigenspace of S^* with eigenvalue 1 has dimension $q^n/|S^*| < \dim Q = q^n/|S|$. This implies that not all vectors in Q remain invariant under $\lambda_E^{-1}E$, in contradiction to the detectability of E. □

Corollary 12: If a stabilizer code Q has minimum distance d and is pure to t, then all errors $E \in G_n$ with $1 \leq \mathrm{wt}(E) < \min\{t, d\}$ satisfy $\langle u|E|v\rangle = 0$ for all u and v in Q.

Proof: By assumption, the weight of E is less than the minimum distance, so the error is detectable. However, E is not an element of $Z(G_n)S$, since the code is pure to $t > \mathrm{wt}(E)$. Therefore, E does not belong to $C_{G_n}(S)$, and the claim follows from (5). □

A. Codes Over $\mathbf{F}_q$

Lemma 11 characterizes the error detection capabilities of a stabilizer code with stabilizer group S in terms of the groups $SZ(G_n)$ and $C_{G_n}(S)$. The phase information of an element in G_n is not relevant for questions concerning the detectability, since an element E of G_n is detectable if and only if ωE is detectable. Thus, if we associate with an element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ of G_n an element $(\mathbf{a}|\mathbf{b})$ of $\mathbf{F}_q^{2n}$, then the group $SZ(G_n)$ is mapped to the additive code

$$C = \{(\mathbf{a}|\mathbf{b}) \,|\, \omega^c X(\mathbf{a})Z(\mathbf{b}) \in SZ(G_n)\} = SZ(G_n)/Z(G_n).$$

To describe the image of the centralizer, we need the notion of a trace-symplectic form of two vectors $(\mathbf{a}|\mathbf{b})$ and $(\mathbf{a}'|\mathbf{b}')$ in $\mathbf{F}_q^{2n}$

$$\langle(\mathbf{a}|\mathbf{b}) \,|\, (\mathbf{a}'|\mathbf{b}')\rangle_s = \mathrm{tr}_{q/p}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a}).$$

The centralizer $C_{G_n}(S)$ contains all elements of G_n that commute with each element of S; thus, by Lemma 5, $C_{G_n}(S)$ is mapped onto the trace-symplectic dual code $C^{\perp_s}$ of the code C,

$$C^{\perp_s} = \{(\mathbf{a}|\mathbf{b}) \,|\, \omega^c X(\mathbf{a})Z(\mathbf{b}) \in C_{G_n}(S)\}.$$

The connection between these classical codes and the stabilizer code is made precise in the next theorem. This theorem is essentially contained in [4] and generalizes the well-known connection to symplectic codes [19], [38] of the binary case.

Theorem 13: An $((n, K, d))_q$ stabilizer code exists if and only if there exists an additive code $C \leq \mathbf{F}_q^{2n}$ of size $|C| = q^n/K$ such that $C \leq C^{\perp_s}$ and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$).

Proof: Suppose that an $((n, K, d))_q$ stabilizer code Q exists. This implies that there exists a closed subgroup S of G_n of order $|S| = q^n/K$ such that $Q = \mathrm{Fix}(S)$. The group S is abelian and satisfies $S \cap Z(G_n) = 1$, by Lemma 10. The quotient $C \cong SZ(G_n)/Z(G_n)$ is an additive subgroup of $\mathbf{F}_q^{2n}$ such that $|C| = |S| = q^n/K$. We have $C^{\perp_s} = C_{G_n}(S)/Z(G_n)$ by Lemma 5. Since S is an Abelian group, $SZ(G_n) \leq C_{G_n}(S)$, hence $C \leq C^{\perp_s}$. Recall that the weight of an element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ in G_n is equal to $\mathrm{swt}(\mathbf{a}|\mathbf{b})$. If $K = 1$, then Q is a pure quantum code, thus $\mathrm{wt}(C_{G_n}(S)) = \mathrm{swt}(C^{\perp_s}) = d$. If $K > 1$, then the elements of $C_{G_n}(S) \setminus SZ(G_n)$ have at least weight d by Lemma 11, so that $\mathrm{swt}(C^{\perp_s} \setminus C) = d$.

Conversely, suppose that C is an additive subcode of $\mathbf{F}_q^{2n}$ such that $|C| = q^n/K$, $C \leq C^{\perp_s}$, and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$). Let

$$N = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \,|\, c \in \mathbf{F}_p \text{ and } (\mathbf{a}|\mathbf{b}) \in C\}.$$

Notice that N is an Abelian normal subgroup of G_n, because it is the pre-image of $C = N/Z(G_n)$. Choose a character χ of N such that $\chi(\omega^c\mathbf{1}) = \omega^c$. Then

$$P_N = \frac{1}{|N|}\sum_{E\in N}\chi(E^{-1})E$$

is an orthogonal projector onto a vector space Q, because P_N is an idempotent in the group ring $\mathbf{C}[G_n]$, see [59, Theorem 1]. We have

$$\dim Q = \mathrm{Tr}\, P_N = |Z(G_n)|q^n/|N| = q^n/|C| = K.$$

Each coset of N modulo $Z(G_n)$ contains exactly one matrix E such that $Ev = v$ for all v in Q. Set $S = \{E \in N \,|\, Ev = v \text{ for all } v \in Q\}$. Then S is an abelian subgroup of G_n of order $|S| = |C| = q^n/K$. We have $Q = \mathrm{Fix}(S)$, because Q is clearly a subspace of $\mathrm{Fix}(S)$, but $\dim Q = q^n/|S| = K$. An element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ in $C_{G_n}(S) \setminus SZ(G_n)$ cannot have weight less than d, because this would imply that $(\mathbf{a}|\mathbf{b}) \in C^{\perp_s} \setminus C$ has weight less than d, which is impossible. By the same token, if $K = 1$, then all nonidentity elements of the centralizer $C_{G_n}(S)$ must have weight d or higher. Therefore, Q is an $((n, K, d))_q$ stabilizer code. □

The results of this paragraph were established by Ashikhmin and Knill [4]. It is instructive to compare the two approaches, since their definition of the error basis is different (but equivalent).

B. Codes Over $\mathbf{F}_{q^2}$

A drawback of the codes in the previous paragraph is that the symplectic weight is somewhat unusual. In the binary case, [19] provided a remedy by relating binary stabilizer codes to additive codes over $\mathbf{F}_4$, allowing the use of the familiar Hamming weight. Somewhat surprisingly, the corresponding concept was not completely generalized to $\mathbf{F}_{q^2}$, although [57], [71] and [80]

paved the way to our approach. After circulating a first version of this manuscript, Gottesman drew our attention to another interesting approach that was initiated by Barnum, see [12], [13], where a sufficient condition for the existence of stabilizer codes is established using a symplectic form.

Let (β, β^q) denote a normal basis of $\mathbf{F}_{q^2}$ over $\mathbf{F}_q$. We define a trace-alternating form of two vectors v and w in $\mathbf{F}_{q^2}^n$ by

$$\langle v|w\rangle_a = \mathrm{tr}_{q/p}\left(\frac{v\cdot w^q - v^q\cdot w}{\beta^{2q}-\beta^2}\right). \tag{6}$$

We note that the argument of the trace is invariant under the Galois automorphism $x \mapsto x^q$, so it is indeed an element of $\mathbf{F}_q$, which shows that (6) is well defined.

The trace-alternating form is bi-additive, that is, $\langle u+v|w\rangle_a = \langle u|w\rangle_a + \langle v|w\rangle_a$ and $\langle u|v+w\rangle_a = \langle u|v\rangle_a + \langle u|w\rangle_a$ holds for all $u, v, w \in \mathbf{F}_{q^2}^n$. It is $\mathbf{F}_p$-linear, but not $\mathbf{F}_q$-linear unless $q = p$ and it is alternating in the sense that $\langle u|u\rangle_a = 0$ holds for all $u \in \mathbf{F}_{q^2}^n$. We write $u \perp_a w$ if and only if $\langle u|w\rangle_a = 0$ holds.

We define a bijective map ϕ that takes an element $(\mathbf{a}|\mathbf{b})$ of the vector space $\mathbf{F}_q^{2n}$ to a vector in $\mathbf{F}_{q^2}$ by setting $\phi((\mathbf{a}|\mathbf{b})) = \beta\mathbf{a} + \beta^q\mathbf{b}$. The map ϕ is isometric in the sense that the symplectic weight of $(\mathbf{a}|\mathbf{b})$ is equal to the Hamming weight of $\phi((\mathbf{a}|\mathbf{b}))$.

Lemma 14: Suppose that c and d are two vectors of $\mathbf{F}_q^{2n}$. Then

$$\langle c\,|\,d\rangle_s = \langle \phi(c)\,|\,\phi(d)\rangle_a.$$

In particular, c and d are orthogonal with respect to the trace-symplectic form if and only if $\phi(c)$ and $\phi(d)$ are orthogonal with respect to the trace-alternating form.

Proof: Let $c = (\mathbf{a}|\mathbf{b})$ and $d = (\mathbf{a}'|\mathbf{b}')$. We calculate

$$\begin{aligned}\phi(c)\cdot\phi(d)^q &= \beta^{q+1}\,\mathbf{a}\cdot\mathbf{a}' + \beta^2\,\mathbf{a}\cdot\mathbf{b}' + \beta^{2q}\,\mathbf{b}\cdot\mathbf{a}' \\ &\quad + \beta^{q+1}\,\mathbf{b}\cdot\mathbf{b}' \\ \phi(c)^q\cdot\phi(d) &= \beta^{q+1}\,\mathbf{a}\cdot\mathbf{a}' + \beta^{2q}\,\mathbf{a}\cdot\mathbf{b}' + \beta^2\,\mathbf{b}\cdot\mathbf{a}' \\ &\quad + \beta^{q+1}\,\mathbf{b}\cdot\mathbf{b}'.\end{aligned}$$

Therefore, the trace-alternating form of $\phi(c)$ and $\phi(d)$ is given by

$$\begin{aligned}\langle\phi(c)|\phi(d)\rangle_a &= \mathrm{tr}_{q/p}\left(\frac{\phi(c)\cdot\phi(d)^q - \phi(c)^q\cdot\phi(d)}{\beta^{2q}-\beta^2}\right), \\ &= \mathrm{tr}_{q/p}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{a}\cdot\mathbf{b}'),\end{aligned}$$

which is precisely the trace-symplectic form $\langle c\,|\,d\rangle_s$. □

Theorem 15: An $((n, K, d))_q$ stabilizer code exists if and only if there exists an additive subcode D of $\mathbf{F}_{q^2}^n$ of cardinality $|D| = q^n/K$ such that $D \le D^{\perp_a}$ and $\mathrm{wt}(D^{\perp_a} \setminus D) = d$ if $K > 1$ (and $\mathrm{wt}(D^{\perp_a}) = d$ if $K = 1$).

Proof: Theorem 13 shows that an $((n, K, d))_q$ stabilizer code exists if and only if there exists a code $C \le \mathbf{F}_q^{2n}$ with $|C| = q^n/K$, $C \le C^{\perp_s}$, and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$). We obtain the statement of the theorem by applying the isometry ϕ. □

We obtain the following convenient condition for the existence of a stabilizer code as a direct consequence of the previous theorem.

Corollary 16: If there exists a classical $[n, k]_{q^2}$ additive code $D \le \mathbf{F}_{q^2}$ such that $D \le D^{\perp_a}$ and $d^{\perp_a} = \mathrm{wt}(D^{\perp_a})$, then there exists an $[[n, n-2k, \ge d^{\perp_a}]]_q$ stabilizer code that is pure to $d^{\perp_a}$.

Remark. It is not necessary to use a normal basis in the definition of the isometry ϕ and the trace-alternating form. Alternatively, we could have used a polynomial basis $(1, \gamma)$ of $\mathbf{F}_q^2/\mathbf{F}_q$. In that case, one can define the isometry ϕ by $\phi((\mathbf{a}|\mathbf{b})) = \mathbf{a} + \gamma\mathbf{b}$, and a compatible trace-alternating form by

$$\langle v\,|\,w\rangle_{a'} = \mathrm{tr}_{q/p}\left(\frac{v\cdot w^q - v^q\cdot w}{\gamma-\gamma^q}\right).$$

One can check that the statement of Lemma 14 is satisfied for this choice as well. Other variations on this theme are possible.

C. Classical Codes

Self-orthogonal codes with respect to the trace-alternating form are not often studied in classical coding theory; more common are codes which are self-orthogonal with respect to a Euclidean or Hermitian inner product. We relate these concepts of orthogonality as follows. Consider the Hermitian inner product $\mathbf{x}^q\cdot\mathbf{y}$ of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_{q^2}^n$; we write $\mathbf{x}\perp_h\mathbf{y}$ if and only if $\mathbf{x}^q\cdot\mathbf{y} = 0$ holds.

Lemma 17: If two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_{q^2}^n$ satisfy $\mathbf{x}\perp_h\mathbf{y}$, then they satisfy $\mathbf{x}\perp_a\mathbf{y}$. In particular, if $D \le \mathbf{F}_{q^2}^n$, then $D^{\perp_h} \le D^{\perp_a}$.

Proof: It follows from $\mathbf{x}^q\cdot\mathbf{y} = 0$ that $\mathbf{x}\cdot\mathbf{y}^q = 0$ holds, whence

$$\langle\mathbf{x}|\mathbf{y}\rangle_a = \mathrm{tr}_{q/p}\left(\frac{\mathbf{x}\cdot\mathbf{y}^q - \mathbf{x}^q\cdot\mathbf{y}}{\beta^{2q}-\beta^2}\right) = 0$$

as claimed. □

Therefore, any self-orthogonal code with respect to the Hermitian inner product is self-orthogonal with respect to the trace-alternating form. In general, the two dual spaces $D^{\perp_h}$ and $D^{\perp_a}$ are not the same. However, if D happens to be $\mathbf{F}_{q^2}$-linear, then the two dual spaces coincide.

Lemma 18: Suppose that $D \le \mathbf{F}_{q^2}^n$ is $\mathbf{F}_{q^2}$-linear, then $D^{\perp_h} = D^{\perp_a}$.

Proof: Let $q = p^m$, p prime. If D is a k-dimensional subspace of $\mathbf{F}_{q^2}^n$, then $D^{\perp_h}$ is an $(n-k)$-dimensional subspace of $\mathbf{F}_{q^2}^n$. We can also view D as a $2mk$-dimensional subspace of $\mathbf{F}_p^{2mn}$, and $D^{\perp_a}$ as a $2m(n-k)$-dimensional subspace of $\mathbf{F}_p^{2mn}$. Since $D^{\perp_h} \subseteq D^{\perp_a}$ and the cardinalities of $D^{\perp_a}$ and $D^{\perp_h}$ are the same, we can conclude that $D^{\perp_a} = D^{\perp_h}$. □

Corollary 19: If there exists an $\mathbf{F}_{q^2}$-linear $[n, k, d]_{q^2}$ code B such that $B^{\perp_h} \le B$, then there exists an $[[n, 2k-n, \ge d]]_q$ quantum code that is pure to d.

Proof: The Hermitian inner product is nondegenerate, so the hermitian dual of the code $D := B^{\perp_h}$ is B. The $[n, n-k]_{q^2}$ code D is $\mathbf{F}_{q^2}$-linear, so $D^{\perp_h} = D^{\perp_a}$ by Lemma 18, and the claim follows from Corollary 16. □

So it suffices to consider hermitian forms in the case of $\mathbf{F}_{q^2}$-linear codes. We have to use the slightly more cumbersome trace-alternating form in the case of additive codes that are not linear over $\mathbf{F}_{q^2}$.

An elegant and surprisingly simple construction of quantum codes was introduced in 1996 by Calderbank and Shor [20] and by Steane [95]. The CSS code construction provides perhaps the most direct link to classical coding theory.

Lemma 20 (CSS Code Construction): Let C_1 and C_2 denote two classical linear codes with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ such that $C_2^\perp \leq C_1$. Then there exists an $[[n,k_1+k_2-n,d]]_q$ stabilizer code with minimum distance $d=\min\{\mathrm{wt}(c) \mid c\in(C_1\setminus C_2^\perp)\cup(C_2\setminus C_1^\perp)\}$ that is pure to $\min\{d_1,d_2\}$.

Proof: Let $C=C_1^\perp\times C_2^\perp\leq \mathbf{F}_q^{2n}$. If $(c_1\mid c_2)$ and $(c_1'\mid c_2')$ are two elements of C, then we observe that

$$\mathrm{tr}(c_2\cdot c_1'-c_2'\cdot c_1)=\mathrm{tr}(0-0)=0.$$

Therefore, $C\leq C^{\perp_s}$. Furthermore, the trace-symplectic dual of C contains $C_2\times C_1$, and a dimensionality argument shows that $C^{\perp_s}=C_2\times C_1$. Since the cartesian product $C_1^\perp\times C_2^\perp$ has $q^{2n-(k_1+k_2)}$ elements, the stabilizer code has dimension $q^{k_1+k_2-n}$ by Theorem 13. The claim about the minimum distance and purity of the code is obvious from the construction. □

Corollary 21: If C is a classical linear $[n,k,d]_q$ code containing its dual, $C^\perp\leq C$, then there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code that is pure to d.

V. Weight Enumerators

The Shor–Laflamme weight enumerators of an arbitrary $((n,K))_q$ quantum code Q with orthogonal projector P are defined by the polynomials

$$\sum_{i=0}^n A_i^{\mathrm{SL}} z^i \quad\text{with}\quad A_i^{\mathrm{SL}}=\frac{1}{K^2}\sum_{\substack{E\in G_n\\ \mathrm{wt}(E)=i}}\mathrm{Tr}(E^\dagger P)\mathrm{Tr}(EP)$$

and

$$\sum_{i=0}^n B_i^{\mathrm{SL}} z^i \quad\text{with}\quad B_i^{\mathrm{SL}}=\frac{1}{K}\sum_{\substack{E\in G_n\\ \mathrm{wt}(E)=i}}\mathrm{Tr}(E^\dagger PEP),$$

see [92] for the binary case. The definition given here differs from the original definition by Shor and Laflamme by a normalization factor p, which is due to the sums running over the full error group G_n. The theory of Shor–Laflamme weight enumerators [92] was considerably extended by Rains in [78], [79], [82], [83]. In this section, we give a simple proof for the relation between these weight enumerators and the symplectic weight enumerators of the additive codes associated with the stabilizer code.

The weights A_i^{SL} and B_i^{SL} have a nice combinatorial interpretation in the case of stabilizer codes. Indeed, let $C\leq\mathbf{F}_q^{2n}$ denote the additive code associated with the stabilizer code Q. Define the symplectic weights of C and $C^{\perp_s}$, respectively, by $A_i=|\{c\in C\,|\,\mathrm{swt}(c)=i\}|$ and $B_i=|\{c\in C^{\perp_s}\,|\,\mathrm{swt}(c)=i\}|$.

The next lemma belongs to the folklore of stabilizer codes.

Lemma 22: The Shor-Laflamme weights of an $((n,K))_q$ stabilizer code Q are multiples of the symplectic weights of the associated additive codes C and $C^{\perp_s}$; more precisely

$$A_i^{\mathrm{SL}}=pA_i \quad\text{and}\quad B_i^{\mathrm{SL}}=pB_i \quad\text{for}\quad 0\leq i\leq n$$

where p is the characteristic of the field $\mathbf{F}_q$.

Proof: Recall that

$$P=\frac{1}{|S|}\sum_{E\in S}E$$

for the stabilizer group S of Q. The trace $\mathrm{Tr}(EP)$ is nonzero if and only if $E^\dagger$ is an element of $SZ(G_n)$. If $E^\dagger\in SZ(G_n)$, then $\mathrm{Tr}(E^\dagger P)\mathrm{Tr}(EP)=(q^n/|S|)^2=K^2$. Therefore, A_i^{SL} counts the elements in $SZ(G_n)$ of weight i, so $A_i^{\mathrm{SL}}=|Z(G_n)|\times|\{c\in C\,|\,\mathrm{swt}(c)=i\}|=pA_i$.

If E commutes with all elements in S, then $\mathrm{Tr}(E^\dagger PEP)=\mathrm{Tr}(P^2)=\mathrm{Tr}(P)=K$. If E does not commute with some element of S, then E is detectable; more precisely, the proof of Lemma 11 shows that $PEP=0P$, hence $\mathrm{Tr}(E^\dagger PEP)=0$. Therefore, B_i^{SL} counts the elements in $C_{G_n}(S)$ of weight i, hence $B_i^{\mathrm{SL}}=|Z(G_n)|\times|\{c\in C^{\perp_s}\,|\,\mathrm{swt}(c)=i\}|=pB_i$. □

Shor and Laflamme had been aware of the stabilizer case when they introduced their weight enumerators, so the combinatorial interpretation of the weights does not appear to be a coincidence. Recall that the Shor–Laflamme enumerators of arbitrary quantum codes are related by a MacWilliams identity, see [78], [92]. For stabilizer codes, we can directly relate the symplectic weight enumerators of C and $C^{\perp_s}$

$$A(z)=\sum_{i=0}^n A_i z^i \quad\text{and}\quad B(z)=\sum_{i=0}^n B_i z^i,$$

using a simple argument that is very much in the spirit of Jessie MacWilliams' original proof for euclidean dual codes [67].

Theorem 23: Let C be an additive subcode of $\mathbf{F}_q^{2n}$ with symplectic weight enumerator $A(z)$. Then the symplectic weight enumerator of $C^{\perp_s}$ is given by

$$B(z)=\frac{(1+(q^2-1)z)^n}{|C|}A\left(\frac{1-z}{1+(q^2-1)z}\right).$$

Proof: Let χ be a nontrivial additive character of $\mathbf{F}_p$. We define for $b\in\mathbf{F}_q^{2n}$ a character χ_b of the additive group C by substituting the trace-symplectic form for the argument of the character χ, such that

$$\chi_b(c)=\chi(\langle c|b\rangle_s).$$

The character χ_b is trivial if and only if b is an element of $C^{\perp_s}$. Therefore, we obtain from the orthogonality relations of characters that

$$\sum_{c\in C}\chi_b(c)=\begin{cases}|C|, & \text{for } b\in C^{\perp_s}\\ 0, & \text{otherwise.}\end{cases}$$

The following relation for polynomials is an immediate consequence

$$\sum_{c\in C}\sum_{b\in\mathbf{F}_q^{2n}}\chi_b(c)z^{\mathrm{swt}(b)}=\sum_{b\in\mathbf{F}_q^{2n}}z^{\mathrm{swt}(b)}\sum_{c\in C}\chi_b(c)=|C|B(z). \tag{7}$$

The right-hand side is a multiple of the weight enumerator of the code $C^{\perp_s}$. Let us have a closer look at the inner sum of

the left-hand side. If we express the vector $c \in C$ in the form $c = (c_1, \ldots, c_n | d_1, \ldots, d_n)$, and expand the character and its trace-symplectic form, then we obtain

$$\sum_{b \in \mathbf{F}_q^{2n}} \chi_b(c) z^{\mathrm{swt}(b)} =$$

$$\sum_{(a_1,\ldots,a_n|b_1,\ldots,b_n) \in \mathbf{F}_q^{2n}} z^{\sum_{k=1}^n \mathrm{swt}(a_k|b_k)} \chi\left(\sum_{k=1}^n \mathrm{tr}(d_k a_k - b_k c_k)\right)$$

$$= \sum_{(a_1,\ldots,a_n|b_1,\ldots,b_n) \in \mathbf{F}_q^{2n}} \prod_{k=1}^n z^{\mathrm{swt}(a_k|b_k)} \chi\left(\mathrm{tr}(d_k a_k - b_k c_k)\right)$$

$$= \prod_{k=1}^n \sum_{(a_k|b_k) \in \mathbf{F}_q^2} z^{\mathrm{swt}(a_k|b_k)} \chi\left(\mathrm{tr}(d_k a_k - b_k c_k)\right).$$

Recall that χ is a nontrivial character of $\mathbf{F}_p$, hence the map $(a_k|b_k) \mapsto \chi(\mathrm{tr}(d_k a_k - b_k c_k))$ is a nontrivial character of $\mathbf{F}_q^2$ for all $(c_k|d_k) \neq (0|0)$. Therefore, we can simplify the inner sum to

$$\sum_{(a_k|b_k) \in \mathbf{F}_q^2} z^{\mathrm{swt}(a_k|b_k)} \chi\left(\mathrm{tr}(d_k a_k - b_k c_k)\right) = \begin{cases} 1 + (q^2-1)z & \text{if } (c_k|d_k) = (0,0) \\ 1 - z & \text{if } (c_k|d_k) \neq (0,0). \end{cases}$$

It follows that

$$\sum_{b \in \mathbf{F}_q^{2n}} \chi_b(c) z^{\mathrm{swt}(b)} = (1-z)^{\mathrm{swt}(c)} (1 + (q^2-1)z)^{n - \mathrm{swt}(c)}.$$

Substituting this expression into (7), we find that

$$\begin{aligned} B(z) &= |C|^{-1} \sum_{c \in C} \sum_{b \in \mathbf{F}_q^{2n}} \chi_b(c) z^{\mathrm{swt}(b)} \\ &= \frac{(1 + (q^2-1)z)^n}{|C|} \sum_{c \in C} \left(\frac{1-z}{1+(q^2-1)z}\right)^{\mathrm{swt}(c)} \\ &= \frac{(1 + (q^2-1)z)^n}{|C|} A\left(\frac{1-z}{1+(q^2-1)z}\right) \end{aligned}$$

which proves the claim. □

The coefficient of z^j in $(1 + (q^2-1)z)^{n-x}(1-z)^x$ is given by the Krawtchouk polynomial of degree j in the variable x,

$$K_j(x) = \sum_{s=0}^{j} (-1)^s (q^2-1)^{j-s} \binom{x}{s} \binom{n-x}{j-s}.$$

Corollary 24: Keeping the notation of the previous theorem, we have

$$B_j = \frac{1}{|C|} \sum_{x=0}^{n} K_j(x) A_x.$$

Proof: According to the previous theorem, we have

$$\begin{aligned} B(z) &= \frac{(1 + (q^2-1)z)^n}{|C|} A\left(\frac{1-z}{1+(q^2-1)z}\right) \\ &= \frac{1}{|C|} \sum_{x=0}^{n} A_x (1-z)^x (1 + (q^2-1)z)^{n-x}. \end{aligned}$$

We obtain the result by comparing the coefficients of z^j on both sides. □

The weight enumerators turn out to be very useful in establishing the bounds on quantum codes, as we will see in the next section.

VI. Bounds

We need some bounds on the achievable minimum distance of a quantum stabilizer code. The main results in this section are the generalization of the linear programming bounds [19], alternative proofs for the nonbinary quantum Singleton bound using a generalization of the methods given in [5], a proof of the validity of the quantum Hamming bound for single error-correcting (degenerate) quantum codes (which generalizes an earlier result by Gottesman [40, Ch. 7]), a simpler nonconstructive proof for lower bounds on quantum codes, and an existence proof of a class of optimal quantum codes.

The first theorem yields a bound that is well-suited for computer search.

Theorem 25: If an $((n, K, d))_q$ stabilizer code with $K > 1$ exists, then there exists a solution to the optimization problem: minimize $\sum_{j=1}^{d-1} A_j$ subject to the constraints

1) $A_0 = 1$ and $A_j \geq 0$ for all $1 \leq j \leq n$;
2) $\sum_{j=0}^{n} A_j = q^n / K$;
3) $B_j = \frac{K}{q^n} \sum_{r=0}^{n} K_j(r) A_r$ holds for all j in the range $0 \leq j \leq n$;
4) $A_j = B_j$ for all j in $0 \leq j < d$ and $A_j \leq B_j$ for all $d \leq j \leq n$;
5) $(p-1)$ divides A_j for all j in the range $1 \leq j \leq n$.

Proof: If an $((n, K, d))_q$ stabilizer code exists, then the symplectic weight distribution of the associated additive code C satisfies conditions 1) and 2). For each nonzero codeword c in C, αc is again in C for all α in $\mathbf{F}_p^*$, so 5) holds. Corollary 24 shows that 3) holds. Since the quantum code has minimum distance d, it follows that 4) holds. □

Remark 26: If we are interested in bounds for $\mathbf{F}_{q^2}$ linear codes, then we can replace condition 5) in the previous theorem by $q^2 - 1$ divides A_j for $1 \leq j \leq n$. This will even help in characteristic 2.

The next bound is more convenient when one wants to find bounds by hand. In particular, any function f satisfying the constraints of the next theorem will yield a useful bound on the dimension of a stabilizer code. This approach was introduced by Delsarte for classical codes [31]. Binary versions of Theorem 27 and Corollary 28 were proved by Ashikhmin and Litsyn [5], see also [8].

Theorem 27: Let Q be an $((n, K, d))_q$ stabilizer code of dimension $K > 1$. Suppose that S is a nonempty subset of $\{0, \ldots, d-1\}$ and $N = \{0, \ldots, n\}$. Let

$$f(x) = \sum_{i=0}^{n} f_i K_i(x)$$

be a polynomial satisfying the conditions

1) $f_x > 0$ for all x in S, and $f_x \geq 0$ otherwise;
2) $f(x) \leq 0$ for all x in $N \setminus S$.

Then

$$K \leq \frac{1}{q^n} \max_{x \in S} \frac{f(x)}{f_x}.$$

Proof: Suppose that $C \leq \mathbf{F}_q^{2n}$ is the additive code associated with the stabilizer code Q. If we apply Corollary 24 to the trace-symplectic dual code $C^{\perp_s}$ of the code C, then we obtain

$$A_i = \frac{1}{|C^{\perp_s}|} \sum_{x=0}^{n} K_i(x) B_x.$$

Using this relation, we find that

$$\begin{aligned} |C^{\perp_s}| \sum_{i \in S} f_i A_i &\leq |C^{\perp_s}| \sum_{i=0}^{n} f_i A_i \\ &= |C^{\perp_s}| \sum_{i=0}^{n} f_i \left(\frac{1}{|C^{\perp_s}|} \sum_{x=0}^{n} K_i(x) B_x \right) \\ &= \sum_{x=0}^{n} B_x \sum_{i=0}^{n} f_i K_i(x). \end{aligned}$$

By assumption, $f(x) = \sum_{i=0}^{n} f_i K_i(x)$; thus, we can simplify the latter inequality and obtain

$$|C^{\perp_s}| \sum_{i \in S} f_i A_i \leq \sum_{x=0}^{n} B_x f(x) \leq \sum_{x \in S} B_x f(x) = \sum_{x \in S} A_x f(x)$$

where the last equality follows from the fact that the stabilizer code has minimum distance d, meaning that $A_x = B_x$ holds for all x in the range $0 \leq x < d$. We can conclude that

$$|C^{\perp_s}| \leq \left(\sum_{x \in S} A_x f(x) \right) \Big/ \left(\sum_{x \in S} f_x A_x \right) \leq \max_{x \in S} \frac{f(x)}{f_x}$$

which proves the theorem, since $|C^{\perp_s}| = q^n K$. □

As an example, we demonstrate that the previous theorem implies the quantum Singleton bound. In general, linear programming yields better bounds, but for short lengths one can actually find codes meeting the quantum Singleton bound.

Corollary 28 (Quantum Singleton Bound): An $((n, K, d))_q$ stabilizer code with $K > 1$ satisfies

$$K \leq q^{n-2d+2}.$$

Proof: Let $S = \{0, \ldots, d-1\}$. If we choose the polynomial

$$f(x) = q^{n-d+1} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right),$$

then $f(x) = 0$ for all x in $\{0, \ldots, n\} \setminus S$. We can express $f(x)$ in the form

$$f(x) = q^{n-d+1} \binom{n-x}{n-d+1} \Big/ \binom{n}{n-d+1}.$$

We can express this polynomial as $f(x) = \sum_{i=0}^{n} f_i K_i(x)$, where

$$\begin{aligned} f_i &= q^{-2n} \sum_{x=0}^{n} f(x) K_x(i) \\ &= q^{1-d-n} \sum_{x=0}^{n} K_x(i) \binom{n-x}{n-d+1} \Big/ \binom{n}{n-d+1}. \end{aligned}$$

Notice that $\sum_{x=0}^{n} K_x(i) \binom{n-x}{n-d+1} = \binom{n-i}{d-1} q^{2(d-1)}$, see [64]; hence

$$f_i = q^{d-1-n} \binom{n-i}{d-1} \Big/ \binom{n}{n-d+1} > 0.$$

We obtain for the fraction $r(x) := f(x)/f_x$ the value

$$r(x) = \frac{f(x)}{f_x} = q^{2n-2d+2} \binom{n-x}{n-d+1} \Big/ \binom{n-x}{d-1}.$$

An easy calculation shows that

$$\frac{r(x)}{r(x+1)} = \frac{n-x-d+1}{d-x-1}.$$

Seeking a contradiction, we assume that there exists an $((n, K, d))_q$ stabilizer code with $2d \geq n+2$. In this case $r(x)/r(x+1) \leq 1$, so that $r(d-1)$ is the maximum of the values $r(x)$ with $x \in \{0, \ldots, d-1\}$. By Theorem 27, we have $K \leq r(d-1)/q^n = q^{n-2d+2} / \binom{n-d+1}{d-1}$. This yields a contradiction, since $\binom{n-d+1}{d-1} K$ cannot be less than $q^{n-2d+2} \leq 1$ for dimension $K > 1$.

If $2d < n+2$, then $r(x)/r(x+1) > 1$, so $r(0) = f(0)/f_0$ is the largest among the values $r(x)$ with $x \in \{0, \ldots, d-1\}$. We have $r(0) = q^{2n-2d+2}$; whence, it follows from Theorem 27 that the dimension K of the code is bounded by

$$K \leq q^{-n} \max_{0 \leq x < d} \frac{f(x)}{f_x} = q^{n-2d+2}$$

which proves the claim. □

The binary version of the quantum Singleton bound was first proved by Knill and Laflamme in [62], see also [5], [8], and later generalized by Rains using weight enumerators in [80].

The quantum Hamming bound states that any pure $((n, K, d))_q$ stabilizer code satisfies

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q^2 - 1)^i \leq q^n / K$$

see [36], [38]. Several researchers have tried to find impure stabilizer codes that beat the quantum Hamming bound. However, Gottesman has shown that impure single and double error-correcting binary quantum codes cannot beat the quantum Hamming bound [40]. In the same vein, Theorem 27 allows us to derive the Hamming bound for arbitrary stabilizer codes, at least when the minimum distance is small. We illustrate the method for single error-correcting codes, and note that the same approach works for double error-correcting codes as well.

Corollary 29 (Quantum Hamming Bound): An $((n,K,3))_q$ stabilizer code with $K>1$ satisfies

$$K \le q^n/(n(q^2-1)+1).$$

Proof: Recall that the intersection number p_{ij}^k of the Hamming association scheme $H(n,q^2)$ is the integer $p_{ij}^k = |\{z \in \mathbf{F}_{q^2}^n \,|\, d(x,z)=i, d(y,z)=j\}|$, where x and y are two vectors in $\mathbf{F}_q^n$ of Hamming distance $d(x,y)=k$. The intersection numbers are related to Krawtchouk polynomials by the expression

$$p_{ij}^k = q^{-2n}\sum_{u=0}^{n} K_i^n(u)K_j^n(u)K_u^n(k),$$

see [11].

After this preparation, we can proceed to derive the Hamming bound as a consequence of Theorem 27. Let

$$\begin{aligned} f(x) &= \sum_{j,k=0}^{1}\sum_{i=0}^{n} K_j^n(i)K_k^n(i)K_i^n(x) \\ &= q^{2n}(p_{00}^x + p_{10}^x + p_{01}^x + p_{11}^x). \end{aligned}$$

The triangle inequality implies that $p_{ij}^k = 0$ if one of the three arguments exceeds the sum of the other two; hence, $f(x)=0$ for $x>2$. The coefficients of the Krawtchouk expansion $f(x) = \sum_{i=0}^{n} f_i K_i(x)$ obviously satisfy $f_i = (K_0(i)+K_1(i))^2 \ge 0$. A straightforward calculation gives

$$\begin{array}{ll} f(0) = q^{2n}(n(q^2-1)+1), & f_0 = (n(q^2-1)+1)^2, \\ f(1) = q^{2n+2}, & f_1 = ((n-1)(q^2-1))^2, \\ f(2) = 2q^{2n}, & f_2 = ((n-2)(q^2-1)-1)^2. \end{array}$$

It follows that

$$\max\{f(0)/f_0, f(1)/f_1, f(2)/f_2\} \le q^{2n}/(n(q^2-1)+1)$$

holds for all $n \ge 5$. Using Theorem 27, we obtain the claim for all $n \ge 5$. For the lengths $n<5$, we obtain the claim from the quantum Singleton bound. □

One real disadvantage of Theorem 27 is that the number of terms increase with the minimum distance and this can lead to cumbersome calculations. However, one can derive more consequences from Theorem 27; see, for instance, [5], [8], [64], [72].

A. Lower Bounds

Feng and Ma have recently shown a quantum version of the classical lower bounds by Gilbert and Varshamov [36]. We conclude this section by giving a simple proof for a weaker version of this result based on a counting argument. It must be remembered that these lower bounds are nonconstructive.

Our first lemma generalizes an idea used by Gottesman in his proof of the binary case.

Lemma 30: An $((n,K,\ge d))_q$ stabilizer code with $K>1$ exists provided that

$$(q^nK - q^n/K)\sum_{j=1}^{d-1}\binom{n}{j}(q^2-1)^j < (q^{2n}-1)(p-1) \quad (8)$$

holds.

Proof: Let L denote the multiset

$$L = \{C^{\perp_s} \setminus C \,|\, C \le C^{\perp_s} \le \mathbf{F}_q^{2n} \text{ with } |C| = q^n/K\}.$$

The elements of this multiset correspond to stabilizer codes of dimension K. Note that L is nonempty, since there exists a code C of size q^n/K that is generated by elements of the form $(a|0)$; the form of the generators ensures that $C \le C^{\perp_s}$.

All nonzero vectors in $\mathbf{F}_q^{2n}$ appear in the same number of sets in L. Indeed, the symplectic group $\mathrm{Sp}(2n,\mathbf{F}_q)$ acts transitively on the set $\mathbf{F}_q^{2n}\setminus\{0\}$, see [51, Prop. 3.2], which means that for any nonzero vectors u and v in $\mathbf{F}_q^{2n}$ there exists $\tau \in \mathrm{Sp}(2n,\mathbf{F}_q)$ such that $v=\tau u$. Therefore, u is contained in $C^{\perp_s}\setminus C$ if and only if v is contained in the element $(\tau C)^{\perp_s}\setminus \tau C$ of L.

The transitivity argument shows that any nonzero vector in $\mathbf{F}_q^{2n}$ occurs in $|L|(q^nK-q^n/K)/(q^{2n}-1)$ elements of L. Furthermore, a nonzero vector and its $\mathbf{F}_p^\times$-multiples are contained in the exact same sets of L. Thus, if we delete all sets from L that contain a nonzero vector with symplectic weight less than d, then we remove at most

$$\frac{\sum_{j=1}^{d-1}\binom{n}{j}(q^2-1)^j}{p-1}|L|\frac{(q^nK-q^n/K)}{q^{2n}-1}$$

sets from L. By assumption, this number is less than $|L|$; hence, there exists an $((n,K,\ge d))_q$ stabilizer code. □

The Gilbert–Varshamov bound shows the existence of surprisingly good codes, even for smaller lengths, when the characteristic of the field is not too small. If $n \equiv k \bmod 2$, then we can significantly strengthen the bound.

Lemma 31: If $k \ge 1$, $n \equiv k \bmod 2$ and

$$(q^{n+k}-q^{n-k})\sum_{j=1}^{d-1}\binom{n}{j}(q^2-1)^{j-1} < (q^{2n}-1) \quad (9)$$

holds, then there exists an $\mathbf{F}_{q^2}$-linear $[[n,k,d]]_q$ stabilizer code.

Proof: The proof is almost the same as in the previous lemma, except that we list only codes C such that $\phi(C)$ is linear, meaning that $\phi(C)$ is a vector space over $\mathbf{F}_{q^2}$. We repeat the previous argument with the multiset

$$L = \left\{ C^{\perp_s}\setminus C \;\middle|\; \begin{array}{l} C \le C^{\perp_s} \le F_q^{2n}, |C| = q^{n-k} \\ \phi(C) \text{ is } \mathbf{F}_{q^2}\text{-linear} \end{array} \right\}.$$

It is easy to see that L is not empty. Note that each set $C^{\perp_s}\setminus C$ in L contains now all $\mathbf{F}_{q^2}^\times$-multiples of a nonzero vector, not just the $\mathbf{F}_p^\times$-multiples, which proves the statement. □

Feng and Ma show that one can extend the previous result to even prove the existence of pure stabilizer codes, but much more delicate counting arguments are needed in that case, see [36]. We are not aware of short proofs for this stronger result.

The previous lemma allows us to show the existence of good quantum codes, especially for larger alphabets. We illustrate this fact by proving the existence of MDS stabilizer codes, see Section XIII for more details on such codes.

Corollary 32: If $2 \le d \le \lceil n/2\rceil$ and $q^2-1 \ge \binom{n}{d}$, then there exists a linear $[[n,n-2d+2,d]]_q$ stabilizer code.

Proof: The assumption $d \le \lceil n/2\rceil$ implies that $\binom{n}{1} \le \binom{n}{2} \le \cdots \le \binom{n}{d}$, so the maximum value of these binomial

coefficients is at most q^2-1. Let $k=n-2d+2$. It follows from the assumption that $k\geq 1$ and $n\equiv k \bmod 2$. It remains to show that (9) holds. For the choice $k=n-2d+2$, the left-hand side of (9) equals

$$\begin{aligned}(q^{2n-2d+2}-q^{2d-2})&\sum_{j=1}^{d-1}\binom{n}{j}(q^2-1)^{j-1}\\ &\leq (q^{2n-2d+2}-q^{2d-2})\sum_{j=1}^{d-1}(q^2-1)^j\\ &=(q^{2n-2d+2}-q^{2d-2})\frac{(q^2-1)^d-(q^2-1)}{q^2-2}.\end{aligned}$$

We claim that the latter term is less than $q^{2n}-1$. To prove this, it suffices to show that

$$q^{2n-2d+2}\frac{(q^2-1)^d-(q^2-1)}{q^2-2}\leq q^{2n} \tag{10}$$

holds. The latter inequality is equivalent to $(q^2-1)^d\leq q^{2d}-2q^{2d-2}+q^2-1$, and it is not hard to see that this inequality holds. Indeed, note that

$$q^{2d}=((q^2-1)+1)^d=(q^2-1)^d+\sum_{j=0}^{d-1}\binom{d}{j}(q^2-1)^j.$$

Recall that $\binom{d}{j}=\binom{d-1}{j-1}+\binom{d-1}{j}$; hence

$$\begin{aligned}&q^{2d}-2q^{2d-2}-(q^2-1)^d\\ &=\sum_{j=0}^{d-1}\left(\binom{d}{j}-2\binom{d-1}{j}\right)(q^2-1)^j\\ &=\sum_{j=0}^{d-1}\Big(\underbrace{\binom{d-1}{j-1}-\binom{d-1}{j}}_{\alpha(j):=}\Big)(q^2-1)^j.\end{aligned}$$

We have $\alpha(j)=-\alpha(d-j)$ for $0\leq j\leq d-1$, and $\alpha(j)\geq 0$ for $j\geq d/2$. This shows that all negative terms get canceled by larger positive terms and we can conclude that $q^{2d}-2q^{2d-2}-(q^2-1)^d\geq 0$ for $d\geq 2$; this implies inequality (10) and consequently shows that (9) holds. □

Example 33: Recall that there does not exist a $[[7,1,4]]_2$ code, see [19]. In contrast, the existence of a $[[7,1,4]]_q$ code for all prime powers $q\geq 7$ is guaranteed by the preceding corollary. It also shows that there exist $[[6,2,3]]_q$ for all prime powers $q\geq 5$ and $[[7,3,3]]_q$ for all prime powers $q\geq 7$, which slightly generalizes [34].

VII. Quantum Cyclic Codes

We will now restrict our attention to linear quantum codes and derive several families of quantum codes from classical linear codes. In essence we make use of the Hermitian and CSS constructions (Lemmas 19–21). Hence, we need to look for classical codes that are self-orthogonal with respect to the Hermitian or the Euclidean product or families of nested codes like the BCH codes.

In this section, we give conditions for identifying cyclic codes that contain their duals. These criteria belong to the folklore of quantum error-correcting codes. We have not been able to trace the references that first proved these results, but we note that these conditions have been established in various forms earlier, especially for codes over $\mathbf{F}_2$ and $\mathbf{F}_4$; see [53, Ch. 4] for general results concerning classical codes and [19], [47] for results concerning binary quantum codes. We provide a convenient and unified treatment while giving the nonbinary equivalents.

A. Cyclic Codes

Recall that a classical cyclic code with parameters $[n,k]_q$ is a principal ideal in the ring $\mathbf{F}_q[x]/(x^n-1)$ and can be succinctly described by its generator polynomial or its defining set. The polynomial x^n-1 of $\mathbf{F}_q[x]$ has simple roots if and only if n and q are coprime. If the latter condition is satisfied, then there exists a positive integer m such that the field $\mathbf{F}_{q^m}$ contains a primitive nth root of unity β. In that case, one can describe a cyclic code with generator polynomial $g(x)$ in terms of its defining set $Z=\{k\,|\,g(\beta^k)=0 \text{ for } 0\leq k<n\}$. Further details on cyclic codes can be found in any standard textbook on coding theory, see [53] or [68].

In the case of cyclic codes, identifying the self-orthogonal codes can be translated into equivalent conditions on the generator polynomial of the code or its defining set. First, we will consider codes over $\mathbf{F}_{q^2}$. Let σ denote the automorphism of the field $\mathbf{F}_{q^2}$ given by $\sigma(x)=x^q$. We can define an action of σ on the polynomial ring $\mathbf{F}_{q^2}[x]$ by

$$h(x)=\sum_{k=0}^{n}h_kx^k\longmapsto h^\sigma(x)=\sum_{k=0}^{n}\sigma(h_k)x^k.$$

Lemma 34: Suppose that B is a classical cyclic $[n,k,d]_{q^2}$ code with generator polynomial $g(x)$ and check polynomial $h(x)=(x^n-1)/g(x)$. If $g(x)$ divides $\sigma(h_0)^{-1}x^kh^\sigma(1/x)$, then $B^{\perp_h}\subseteq B$, and there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code that is pure to d.

Proof: If $h(x)$ is the check polynomial of B, then $h^\sigma(x)$ is the check polynomial of $\sigma(B)$. The generator polynomial of the dual code $\sigma(B)^\perp=B^{\perp_h}$ is given by $\sigma(h_0)^{-1}x^kh^\sigma(1/x)$, the normalized reciprocal polynomial of $h^\sigma(x)$. Therefore, the condition that the polynomial $g(x)$ divides $\sigma(h_0)^{-1}x^kh^\sigma(1/x)$ is equivalent to the condition $B^{\perp_h}\subseteq B$. The stabilizer code follows from Corollary 19. □

The following Lemma summarizes various equivalent conditions on dual containing codes in terms of the generator polynomial $g(x)$ and the defining set Z.

Lemma 35: Let $\gcd(n,q^2)=1$ and C be a classical cyclic $[n,k,d]_{q^2}$ code whose generator polynomial is $g(x)$ and defining set is Z. Suppose that any of the following equivalent conditions are satisfied

1) $x^n-1\equiv 0 \bmod g(x)g^*(x)$ where $g^*(x)=x^{n-k}g^\sigma(1/x)$;
2) $Z\subseteq\{-qz\,|\,z\in N\setminus Z\}$;
3) $Z\cap Z^{-q}=\emptyset$, where $Z^{-q}=\{-qz\mid z\in Z\}$.

Then $C^{\perp_h}\subseteq C$ and there exists an $[[n,2k-n,\geq d]]_q$ stabilizer code that is pure to d.

Proof: Let $h(x) = (x^n - 1)/g(x)$ be the check polynomial of C. Then $h^\sigma(x) = \sigma((x^n - 1)/g(x)) = (x^n - 1)/g^\sigma(x)$. From Lemma 34, we know that C contains its Hermitian dual if g(x) divides $\sigma(h_0)^{-1}x^k h^\sigma(1/x)$ viz. $g(x)|\sigma(h_0)^{-1}(1 - x^n)/(x^{n-k}g^\sigma(1/x))$, which implies $x^n - 1 \equiv 0 \bmod g(x)g^*(x)$ which proves 1).

The generator polynomial $g(x)$ of C is given by $g(x) = \prod_{z\in Z}(x - \beta^z)$, hence, its check polynomial is of the form

$$h(x) = (x^n - 1)/g(x) = \prod_{z\in N\setminus Z}(x - \beta^z).$$

Applying the automorphism σ yields $h^\sigma(x) = \prod_{z\in N\setminus Z}(x - \beta^{qz})$. Therefore, the generator polynomial of $C^{\perp_h}$ is given by

$$\begin{aligned} h^\sigma(0)^{-1}x^k h^\sigma(1/x) &= h^\sigma(0)^{-1}\prod_{z\in N\setminus Z}(1 - \beta^{qz}x) \\ &= \prod_{z\in N\setminus Z}(x - \beta^{-qz}) \end{aligned}$$

in the last equality, we have used the fact that $h^\sigma(0)^{-1} = \prod_{z\in N\setminus Z}(-\beta^{-qz})$. By Lemma 34, $B^{\perp_h} \subseteq B$ if and only if the generator polynomial $g(x)$ divides $h^\sigma(0)^{-1}x^k h^\sigma(1/x)$. The latter condition is equivalent to the fact that Z is a subset of $\{-qz \mid z \in N \setminus Z\}$ and 2) follows. From 2) we know that $C^{\perp_h} \subseteq C$ if and only if $Z \subseteq \{-qz \mid z \in N \setminus Z\}$. In other words $Z^{-q} \subseteq N \setminus Z$. Hence $Z \cap Z^{-q} = \emptyset$. An $[[n, 2k-n, \geq d]]_q$ stabilizer code follows from Corollary 19. □

Cyclic codes that contain their Euclidean duals can also be nicely characterized in terms of their generator polynomials and defining sets. The following Lemma is a very straight forward extension of the binary case and summarizes some of the known results in the nonbinary case as well, but we include it because of its usefulness in constructing cyclic quantum codes.

Lemma 36: Let C be an $[n, k, d]_q$ cyclic code such that $\gcd(n, q) = 1$. Let its defining set Z and generator polynomial $g(x)$ be such that any of the following equivalent conditions are satisfied:

1) $x^n - 1 \equiv 0 \bmod g(x)g^\dagger(x)$, where $g^\dagger(x) = x^{n-k}g(1/x)$;
2) $Z \subseteq \{-z \mid z \in N \setminus Z\}$;
3) $Z \cap Z^{-1} = \emptyset$ where $Z^{-1} = \{-z \bmod n \mid z \in Z\}$.

Then $C^\perp \subseteq C$ and there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d.

Proof: The check polynomial of C is given by $h(x) = (x^n - 1)/g(x)$, from which we obtain the (un-normalized) generator polynomial of $C^\perp$ as $h^\dagger(x) = x^k h(x^{-1}) = (1-x^n)/(x^{n-k}g(x^{-1})) = -(x^n-1)/g^\dagger(x)$. If $C^\perp \subseteq C$, then $g(x) \mid h^\dagger(x)$; this means that $g(x)$ divides $(x^n - 1)/g^\dagger(x)$. In other words, $x^n - 1 \equiv 0 \bmod g(x)g^\dagger(x)$.

The defining set of $C^\perp$ is given by $\{-z \bmod n \mid z \in N \setminus Z\}$, where $N = \{0, 1, \ldots, n - 1\}$. Thus $C^\perp \subseteq C$ implies $Z \subseteq \{-z \bmod n \mid N \setminus Z\}$. Since this means that the inverses of elements in Z are present in $N \setminus Z$, this condition can also be written as $Z \cap Z^{-1} = \emptyset$. The existence of quantum code $[[n, 2k - n, \geq d]]_q$ follows from Corollary 21. □

Although we have considered purely cyclic codes, a larger class of cyclic quantum codes can be derived by considering constacyclic or conjucyclic codes as in [19] and [101].

VIII. Cyclic Hamming Codes

Binary quantum Hamming codes have been studied by various authors; see for instance [19], [38], [35]. We now derive stabilizer codes from nonbinary classical cyclic Hamming codes. Let $m > 1$ be an integer such that $\gcd(q-1, m) = 1$. A classical cyclic Hamming code $H_q(m)$ has parameters $[n, n-m, 3]_q$ with length $n = (q^m - 1)/(q - 1)$. Let β denote a primitive nth root of unity in $\mathbf{F}_{q^m}$. The generator polynomial of $H_q(m)$ is given by

$$g(x) = \prod_{i=0}^{m-1}\left(x - \beta^{q^i}\right) \tag{11}$$

an element of $\mathbf{F}_q[x]$. Thus, the code $H_q(m)$ is defined by the cyclotomic coset $C_1 = \{q^i \bmod n \,|\, i \in \mathbf{Z}\}$.

Lemma 37: The Hamming code $H_{q^2}(m)$ contains its hermitian dual, that is, $H_{q^2}(m)^{\perp_h} \leq H_{q^2}(m)$.

Proof: The statement $H_{q^2}(m)^{\perp_h} \leq H_{q^2}(m)$ is equivalent to the fact that the cyclotomic coset C_1 satisfies $C_1 \subseteq N_1 = \{-qz \bmod n \,|\, z \in N \setminus C_1\}$, where $N = \{0, \ldots, n - 1\}$ and $n = (q^{2m} - 1)/(q^2 - 1)$. We note that C_1 can be expressed in the form

$$\begin{aligned} C_1 &= \left\{(1 - n)q^{2k} \bmod n \,\middle|\, k \in \mathbf{Z}\right\} \\ &= \left\{-qzq^{2k} \bmod n \,\middle|\, k \in \mathbf{Z}\right\} \end{aligned} \tag{12}$$

where $z = q(q^{2m-2} - 1)/(q^2 - 1)$. Therefore, the condition $C_1 \subseteq N_1$ holds if and only if $C_z \subseteq N \setminus C_1$ holds, where $C_z = \{zq^{2j} \bmod n \,|\, j \in \mathbf{Z}\}$.

Seeking a contradiction, we assume that the two cyclotomic cosets C_1 and C_z have an element in common, hence are the same. This means that there must exist a positive integer k such that $q^{2k} = q(q^{2m-2} - 1)/(q^2 - 1)$. This implies that q^{2k-1} divides $q^{2m-2} - 1$, which is absurd. Thus, the sets C_1 and C_z are disjoint, hence $C_z \subseteq N \setminus C_1$, which proves the claim. □

Theorem 38: For each integer $m \geq 2$ such that $\gcd(m, q^2 - 1) = 1$, there exists a pure $[[n, n - 2m, 3]]_q$ stabilizer code of length $n = (q^{2m} - 1)/(q^2 - 1)$.

Proof: If $\gcd(m, q^2 - 1) = 1$, then there exists a classical $[n, n-m, 3]_{q^2}$ Hamming code $H_{q^2}(m)$. By Lemma 37, we have $H_{q^2}(m)^{\perp_h} \leq H_{q^2}(m)$, hence there exists a pure $[[n, n - 2m, 3]]_q$ stabilizer code by Corollary 19. The purity is due to the fact that the $H_{q^2}(m)^{\perp_h}$ has minimum distance $q^{2m-2} \geq 3$ for $m \geq 2$ [53, Theorem 1.8.3]. □

These quantum Hamming codes are optimal since they attain the quantum Hamming bound, see Corollary 29. A different approach that allows construction of noncyclic perfect quantum codes can be found in [16]. It is also possible to construct quantum codes from Hamming codes that contain their euclidean duals, however these codes do not meet the quantum Hamming bound.

Lemma 39: If $\gcd(m, q - 1) = 1$ and $m \geq 2$, then there exists a pure $[[n, n-2m, 3]]_q$ quantum code, where $n = (q^m - 1)/(q - 1)$.

Proof: The generating polynomial of an $[n, n - m, 3]_q$ Hamming code, with $n = (q^m - 1)/(q - 1)$ is given by (11) where β is an element of order n. The code exists only if $\gcd(m, q-1) = 1$. By Lemma 36 a cyclic code contains its dual

if $x^n - 1 \equiv 0 \bmod g(x)g^\dagger(x)$, where $g^\dagger(x) = x^{n-k}g(x^{-1})$. If $g(x)$ is not self-reciprocal then $g(x)g^\dagger(x)$ divides $x^n - 1$ [100]. Since the generating polynomial of the Hamming code is not self-reciprocal, the code contains its euclidean dual. By Lemma 36, we can construct a quantum code with the parameters $[[n, n-2m, 3]]_q$. Once again the purity follows due to the fact the duals of Hamming codes are simplex codes with weight $q^{m-1} \geq 3$ for $m \geq 2$ [53, Theorem 1.8.3]. □

IX. Quantum Quadratic Residue Codes

Another well known family of classical codes are the quadratic residue codes. Rains constructed quadratic residue codes for prime alphabet in [80]. In this section we will construct two series of quantum codes based on the classical quadratic residue codes over an arbitrary field using elementary methods.

A. Quadratic Residue Codes

Let α denote a primitive nth root of unity from some extension field of $\mathbf{F}_q$. We denote by $R = \{r^2 \bmod n \mid r \in \mathbf{Z} \text{ such that } 1 \leq r \leq (n-1)/2\}$ the set of quadratic residues modulo n and by $N = \{1, \ldots, n-1\} \setminus R$ the set of quadratic non-residues modulo n.

Let C_R and C_N denote the cyclic codes of length n that are respectively generated by the polynomials $q_R(x)$ and $q_N(x)$, where

$$q_R(x) = \prod_{r \in R}(x - \alpha^r) \quad \text{and} \quad q_N(x) = \prod_{r \in N}(x - \alpha^r).$$

Both codes have parameters $[n, (n+1)/2, d]_q$ with $d^2 \geq n$, see [15, pp. 114-119]. The codes with generator polynomials $(x-1)q_R(x)$ and $(x-1)q_N(x)$ are the even-like subcodes of C_R and C_N, respectively, and have the parameters $[n, (n-1)/2, d']_q$ with $d' \geq d$. The relevance of these codes will become apparent in the following theorems.

Theorem 40: Let n be a prime of the form $n \equiv 3 \bmod 4$, and let q be a power of a prime that is not divisible by n. If q is a quadratic residue modulo n, then there exists a pure $[[n, 1, d]]_q$ stabilizer code with minimum distance d satisfying $d^2 - d + 1 \geq n$.

Proof: The code C_R has parameters $[n, (n+1)/2, d]_q$ and if $n \equiv 3 \bmod 4$, the dual code $C_R^\perp$ of C_R is given by the cyclic code generated by $(x-1)q_R(x)$, the even-like subcode of C_R. The minimum distance d is bounded by $d^2 - d + 1 \geq n$, see, for instance, [15, pp. 114-119]. Further $\mathrm{wt}(C_R \setminus C_R^\perp) = \mathrm{wt}(C_R) = d$ by [53, Theorem 6.6.22]. We can deduce from Corollary 21 that there exists a pure $[[n, (n+1) - n, d]]_q$ stabilizer code. □

For example, the prime $p = 3$ is a quadratic residue modulo $n = 23$. The previous proposition guarantees the existence of a $[[23, 1, d]]_3$ stabilizer code with minimum distance $d \geq 6$.

If n is an odd prime of the form $n \equiv 1 \bmod 4$, then we can also construct quadratic residue codes, but now we need to employ Lemma 20, because C_R does not contain its dual.

Theorem 41: Let n be a prime of the form $n \equiv 1 \bmod 4$. Let q be a power of a prime that is not divisible by n. If q is a quadratic residue modulo n, then there exists a pure $[[n, 1, d]]_q$ stabilizer code with minimum distance d bounded from below by $d \geq \sqrt{n}$.

Proof: The dual code of C_R is given by the even-like subcode of C_N; in other words, $C_R^\perp$ is a cyclic code of length n over $\mathbf{F}_q$ that is generated by the polynomial $(x-1)q_N(x)$; in particular, $C_R^\perp \leq C_N$. Moreover $\mathrm{wt}(C_R \setminus C_N^\perp) = \mathrm{wt}(C_N \setminus C_R^\perp) = \mathrm{wt}(C_R) = \mathrm{wt}(C_N) = d$ by [53, Theorem 6.6.22]. Therefore, we obtain a pure $[[n, (n+1)/2 + (n+1)/2 - n, d]]_q$ code by Lemma 20. □

X. Quantum Melas Codes

One of the earliest family of codes that were constructed with a view to correcting burst errors are the Melas codes. While not as well known as the Hamming codes or the quadratic residue codes, they are nonetheless interesting. These codes have been well investigated, especially in the mathematical community, because of their connections to algebraic geometry [63], [88], [89], [99]. See [52] for an interesting read on the connections to number theory.

A. Melas Codes

The Melas code[1] $\mathcal{M}_q(m)$ is a cyclic $[n, n-2m, \geq 3]_q$ code with $n = q^m - 1$. The generator polynomial of $\mathcal{M}_q(m)$ is given by

$$g(x) = \prod_{i=0}^{m-1}(x - \alpha^{q^i})(x - \alpha^{-q^i}) \tag{13}$$

where α is a primitive element in $\mathbf{F}_{q^m}$. Alternatively, the defining set of the code is given by $Z = C_1 \cup C_{-1} = \{\pm q^i \bmod n \mid 0 \leq i < m\}$.

Lemma 42: The Melas code $\mathcal{M}_{q^2}(m)$ contains its hermitian dual.

Proof: By Lemma 35, it suffices to show that $Z \cap Z^{-q} = \emptyset$. Seeking a contradiction, we assume that $Z \cap Z^{-q} \neq \emptyset$. Since $\gcd(q^2, q^{2m} - 1) = 1$, this implies that there must exist some integer i in the range $0 \leq i < m$ such that $q^{2i} \equiv \pm q \bmod n$, but that is impossible; so $Z \cap Z^{-q} = \emptyset$. □

Lemma 43: If q is even, then the minimum distance of the Melas code $\mathcal{M}_{q^2}(m)$ is at least 3.

Proof: The parity check matrix of $\mathcal{M}_{q^2}(m)$ is given by

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \end{bmatrix}.$$

This matrix has rank 2 only if no two columns are scalar multiples of each other. Seeking a contradiction, we suppose that

$$\begin{bmatrix} \alpha^x \\ \alpha^{-x} \end{bmatrix} = \alpha^t \begin{bmatrix} \alpha^y \\ \alpha^{-y} \end{bmatrix}$$

holds for distinct x and y. This yields $\alpha^{2t} = 1$, which implies $t \in \{0, n/2\}$. If q is even, then n is odd, and so t cannot equal $n/2$. If $t = 0$, then $x = y$ contradicting the distinctness of x and y. Therefore, we can conclude that H has rank $r = 2$; thus, the minimum distance is at least 3. □

Theorem 44 (Quantum Melas Codes): If q is even and $n = q^{2m} - 1$, then there exist quantum Melas codes with parameters $[[n, n-4m, \geq 3]]_q$ that are pure to 3.

[1]The classical Melas codes are defined over a prime field $\mathbf{F}_p$ and have the parameters $[p^m - 1, p^m - m - 1, \geq 3]_p$ (cf. [97]); here, we consider a generalization to arbitrary finite fields.

Proof: By Lemma 42 we have $\mathcal{M}_{q^2}(m)^{\perp_h} \subseteq \mathcal{M}_{q^2}(m)$ and by Lemma 43 we have the distance ≥ 3. So by Corollary 19 there exists an $[[n, n-4m, \geq 3]]_q$ quantum code. □

XI. Quantum BCH Codes

In this section we consider a popular family of classical codes, the BCH codes, and construct the associated nonbinary quantum stabilizer codes. Binary quantum BCH codes were studied in [19], [29], [45], [96]. The CSS construction turns out to be especially useful, because BCH codes form a naturally nested family of codes. In case of primitive BCH codes over prime fields, the distance of the dual is lower bounded by the generalized Carlitz–Uchiyama bound, and this allows us to derive bounds on the minimum distance of the resulting quantum codes.

A. BCH Codes

Let q be a power of a prime and n a positive integer that is coprime to q. Recall that a BCH code C of length n and designed distance δ over $\mathbf{F}_q$ is a cyclic code whose defining set Z is given by a union of $\delta-1$ subsequent cyclotomic cosets

$$Z = \bigcup_{x=b}^{b+\delta-2} C_x \quad \text{where} \quad C_x = \{xq^r \bmod n \mid r \in \mathbf{Z}, r \geq 0\}.$$

The generator polynomial of the code is of the form

$$g(x) = \prod_{z \in Z} (x - \beta^z),$$

where β is a primitive nth root of unity of some extension field of $\mathbf{F}_q$. The definition ensures that $g(x)$ generates a cyclic $[n, k, d]_q$ code of dimension $k = n - |Z|$ and minimum distance $d \geq \delta$. If $b = 1$, then the code C is called a narrow-sense BCH code, and if $n = q^m - 1$ for some $m \geq 1$, then the code is called primitive. More precise statements can be made about the structure of primitive, narrow-sense codes than the other classes of BCH codes and we will restrict our attention to these in this paper. More details on BCH codes can be found in [53], [68].

B. Generalized Carlitz-Uchiyama Bound

Our first construction derives stabilizer codes from BCH codes over prime fields. We use the Knuth-Iverson bracket [*statement*] in the formulation of the Carlitz-Uchiyama bound that evaluates to 1 if *statement* is true and 0 otherwise.

Lemma 45 (Generalized Carlitz-Uchiyama Bound): Let p be a prime. Let C denote a narrow-sense BCH code of length $n = p^m - 1$ over $\mathbf{F}_p$, of designed distance $\delta = 2t+1$. Then the minimum distance $d^\perp$ of its euclidean dual code $C^\perp$ is bounded by

$$d^\perp \geq \left(1 - \frac{1}{p}\right)\left(p^m - \frac{\delta - 2 - [\delta - 1 \equiv 0 \bmod p]}{2} \lfloor 2p^{m/2} \rfloor\right). \tag{14}$$

Proof: See [97, Theorem 7]; for further background, see [68, p. 280]. □

Theorem 46: Let p be a prime. Let C be a $[p^m - 1, k, \geq \delta]_p$ narrow-sense BCH code of designed distance $\delta = 2t+1$ and C^* a $[p^m - 1, k^*, d^*]_p$ BCH code such that $C \subseteq C^*$. Then there exists a $[[p^m - 1, k^* - k, \geq \min\{d^*, d^\perp\}]]_p$ stabilizer code, where $d^\perp$ is given by (14).

Proof: The result follows from applying Lemma 45 to C and Lemma 20 to the codes C and C^*. □

Remark 47: 1) The Carlitz-Uchiyama bound becomes trivial for larger design distances. 2) In [73, Corollary 2] it was shown that for binary BCH codes of design distance d, the lower bound in (14) is attained when $n = 2^{2ab} - 1$, where a is the smallest integer such that $d - 2 \mid 2^a + 1$ and b is odd. 3) For a further tightening of the Carlitz-Uchiyama bound see [74, Theorem 2].

C. Primitive BCH Codes Containing Their Duals

We can extend the results of the previous section to BCH codes over finite fields that are not necessarily prime. In fact, if we restrict ourselves to smaller designed distances, then we can even achieve significantly sharper results. We will just review the results and refer the reader to our companion paper [2] for the proofs.

In the BCH code construction, it is in general not obvious how large the cyclotomic cosets will be. However, if the designed distance is small, then one can show that the cyclotomic cosets all have maximal size.

Lemma 48: A narrow-sense, primitive BCH code with design distance $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$ has parameters $[q^m - 1, q^m - 1 - m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]_q$.

Proof: See [2, Theorem 7]; the binary case was already established by Steane [96]. □

In the case of small designed distances, primitive, narrow-sense BCH codes contain their euclidean duals.

Lemma 49: A narrow-sense, primitive BCH code over $\mathbf{F}_q^n$ contains its euclidean dual if and only if its design distance satisfies $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$, where $n = q^m - 1$ and $m \geq 2$.

Proof: See [2, Theorem 2]. □

A simple consequence is the following theorem.

Theorem 50: If C is a narrow-sense primitive BCH code over $\mathbf{F}_q$ with design distance $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$ and $m \geq 2$, then there exists an $[[q^m - 1, q^m - 1 - 2m\lceil(\delta - 1)(1-1/q)\rceil, \geq \delta]]_q$ stabilizer code that is pure to δ.

Proof: If we combine Lemmas 48 and 49 and apply the CSS construction, then we obtain the claim. See [2] for details about purity. □

One can argue in a similar way for hermitian duals of primitive, narrow-sense BCH codes.

Theorem 51: If C is a narrow-sense primitive BCH code over $\mathbf{F}_{q^2}^n$ with design distance $2 \leq \delta \leq q^m - 1$, then there exists an $[[q^{2m} - 1, q^{2m} - 1 - 2m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]]_q$ stabilizer code that is pure to δ.

Proof: See [2] for details. □

When $m = 1$, the BCH codes are the same as the Reed Solomon codes and this case has been dealt with in [48]. An alternate perspective using Reed–Muller codes is considered in [85].

D. Extending Quantum BCH Codes

It is not always possible to extend a stabilizer code, because the corresponding classical codes are required to be self-orthogonal. We now show that it is possible to extend narrow-sense BCH codes of certain lengths.

Lemma 52: Let $\mathbf{F}_{q^2}$ be a finite field of characteristic p. If C is a narrow-sense $[n, k, \geq d]_{q^2}$ BCH code such that $C^{\perp_h} \subseteq C$ and $n \equiv -1 \bmod p$, then there exists an $[[n, 2k-n, \geq d]]_q$ stabilizer code that is pure to d which can be extended to an $[[n+1, 2k-n-1, \geq d+1]]_q$ stabilizer code that is pure to $d+1$.

Proof: Since $C^{\perp_h} \subseteq C$, Corollary 19 implies the existence of an $[[n, 2k-n, \geq d]]_q$ quantum code that is pure to d and being narrow-sense the parity check matrix of C has the form

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^{2(2)} & \cdots & \alpha^{2(n-1)} \\ \vdots & \ddots & \ddots & \ddots & \ddots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \cdots & \alpha^{(n-1)(d-1)} \end{bmatrix}$$

where α is a primitive nth root of unity. This can be extended to give an $[n+1, k, d+1]$ code C_e, whose parity check matrix is given as

$$H_e = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{(n-1)} & 0 \\ 1 & \alpha^2 & \alpha^{2(2)} & \cdots & \alpha^{2(n-1)} & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \cdots & \alpha^{(n-1)(d-1)} & 0 \end{bmatrix}.$$

We show that $C_e^{\perp_h}$ is self-orthogonal. Let R_i be the i^{th} row in H_e. For $2 \leq i \leq d$ the self-orthogonality of H implies that $\langle R_i | R_j \rangle_h = 0$. We need to show that $\langle R_i | \mathbf{1} \rangle_h = 0$, $1 \leq i \leq d$. For $2 \leq i \leq d$ we have $\langle R_i | \mathbf{1} \rangle_h = \sum_{j=0}^{n-1} \alpha^{ij} = (\alpha^{in} - 1)/(\alpha^i - 1) = 0$, as $\alpha^n = 1$ and $\alpha^i \neq 1$. For $i = 1$ we have $\langle \mathbf{1} | \mathbf{1} \rangle_h = n + 1 \bmod p$, which vanishes because of the assumption $n \equiv -1 \bmod p$.

Now we show that the rank of H_e is d, thus C_e has a minimum distance of at least $d+1$. Any d columns of H_e excluding the last column form a $d \times d$ vandermonde matrix which is nonsingular, indicating that the d columns are linearly independent. If we consider any set of d columns that includes the last column, we can find the determinant of the corresponding matrix by expanding by the last column. This gives us a $d-1 \times d-1$ vandermonde matrix with nonzero determinant. Thus any d columns of H_e are independent and the minimum distance of C_e is at least $d+1$. Therefore C_e is an $[n+1, k, \geq d+1]_{q^2}$ extended cyclic code such that $C_e^{\perp_h} \subseteq C_e$. By Corollary 19 it defines an $[[n+1, 2k-n-1, \geq d+1]]_q$ quantum code pure to $d+1$. □

Corollary 53: For all prime powers q, integers $m \geq 1$ and all δ in the range $2 \leq \delta \leq q^m - 1$ there exists an

$$[[q^{2m}, q^{2m} - 2 - 2m\lceil (\delta-1)(1-1/q^2) \rceil, \geq \delta + 1]]_q$$

stabilizer code pure to $\delta + 1$.

Proof: The stabilizer codes from Theorem 51 are derived from primitive, narrow-sense BCH codes. If p denotes the characteristic of $\mathbf{F}_{q^2}$, then $q^{2m} - 1 \equiv -1 \bmod p$, so the stabilizer codes given in Theorem 51 can be extended by Lemma 52. □

A result similar to Lemma 52 can be developed for BCH codes that contain their euclidean duals.

XII. Puncturing Stabilizer Codes

If we delete one coordinate in all codewords of a classical code, then we obtain a shorter code that is called the punctured code. In general, we cannot proceed in the same way with stabilizer codes, since the resulting matrices might not commute if we delete one or more tensor components.

Rains [80] invented an interesting approach that solves the puncturing problem for linear stabilizer codes and, even better, gives a way to construct stabilizer codes from arbitrary linear codes. The idea is to associate with a classical linear code a so-called puncture code; if the puncture code contains a codeword of weight r, then a self-orthogonal code of length r exists and the minimum distance is the same or higher than that of the initial classical code. Further convenient criteria for puncture codes are given in [48].

In this section, we generalize puncturing to arbitrary stabilizer codes and review some known facts. Determining a puncture code is a challenging task, and we conclude this section by showing how to puncture quantum BCH codes.

A. The Puncture Code

It will be convenient to denote the the pointwise product of two vectors u and v in $\mathbf{F}_q^n$ by uv, that is, $uv = (u_i v_i)_{i=1}^n$.

Suppose that $C \leq \mathbf{F}_q^{2n}$ is an arbitrary additive code. The associated puncture code $\mathrm{P}_s(C) \subseteq \mathbf{F}_q^n$ is defined as

$$\mathrm{P}_s(C) = \{(b_k a'_k - b'_k a_k)_{k=1}^n \mid (a|b), (a'|b') \in C\}^{\perp}.$$

Theorem 54: Suppose that C is an arbitrary additive subcode of $\mathbf{F}_q^{2n}$ of size $|C| = q^n/K$ such that $\mathrm{swt}(C^{\perp_s} \setminus C) = d$. If the puncture code $\mathrm{P}_s(C)$ contains a codeword of Hamming weight r, then there exists an $((r, K^*, d^*))_q$ stabilizer code with $K^* \geq K/q^{n-r}$ that has minimum distance $d^* \geq d$ when $K^* > 1$. If $\mathrm{swt}(C^{\perp_s}) = d$, then the resulting punctured stabilizer code is pure to d.

Proof: Let x be a codeword of weight r in the $\mathrm{P}_s(C)$. Define an additive code $C_x \leq \mathbf{F}_q^{2n}$ by

$$C_x = \{(a|bx) \mid (a|b) \in C\}.$$

If $(a|bx)$ and $(a'|b'x)$ are arbitrary elements of C_x, then

$$\langle (a|bx) \mid (a'|b'x) \rangle_s = \mathrm{tr}\left(\sum_{k=1}^n (b_k a'_k - b'_k a_k) x_k \right) = 0 \quad (15)$$

by definition of $\mathrm{P}_s(C)$; thus, $C_x \leq (C_x)^{\perp_s}$.

Let $C_x^R = \{(a_k|b_k)_{k \in S} | (a|b) \in C_x\}$ denote the restriction of C_x to the support S of the vector x. Since (15) depends only on the nonzero coefficients of the vector x, it follows that $C_x^R \leq (C_x^R)^{\perp_s}$ holds.

We note that $|C| \geq |C_x^R|$; hence, the dimension K^* of the punctured quantum code is bounded by

$$K^* \geq q^r/|C_x^R| \geq q^r/|C| = q^r/(q^n/K) = K/q^{n-r}.$$

It remains to show that $\mathrm{swt}((C_x^R)^{\perp_s} \setminus C_x^R) \geq d$. Seeking a contradiction, we suppose that u_x^R is a vector in $(C_x^R)^{\perp_s} \setminus C_x^R$ such that $\mathrm{swt}(u_x^R) < d$. Let $u_x = (a|b)$ denote the vector in $(C_x)^{\perp_s}$ that is zero outside the support of x and coincides with u_x^R when restricted to the support of x. It follows that $(ax|b)$ is contained in $C^{\perp_s}$. However $\mathrm{swt}(ax|b) < d$, so $(ax|b)$ must be an element of C, since $\mathrm{swt}(C^{\perp_s} \setminus C) = d$. This implies that $(ax|bx)$ is an element of $C_x \leq (C_x)^{\perp_s}$. Arguing as before, it follows that $(ax^2|bx)$ is in C and $(ax^2|bx^2)$ is in C_x. Repeating the process, we obtain that $v_x = (ax^{q-1}|bx^{q-1})$ is in C_x, and we note that x^{q-1} is the characteristic vector of the support of x. Restricting v_x in C_x to the support of x yields $u_x^R \in C_x^R$, contradicting the assumption that $u_x^R \in (C_x^R)^{\perp_s} \setminus C_x^R$.

Finally, the last statement concerning the purity is easy to prove (a direct generalization of the argument given in [48] for pure linear codes). □

If the code C is a direct product, as in the case of CSS codes, then the expression for the puncture code simplifies somewhat.

Lemma 55: If C_1 and C_2 are two additive subcodes of $\mathbf{F}_q^n$, then

$$\mathrm{P}_s(C_1 \times C_2) = \{ab \mid a \in C_1, b \in C_2\}^{\perp} \leq \mathbf{F}_q^n.$$

Proof: Since $\langle ab \mid a \in C_1, b \in C_2\rangle = \langle (ba' - b'a) \mid a, a' \in C_1, b, b' \in C_2\rangle$, the claim about the orthogonal complements of these sets is obvious. □

Since many quantum codes are constructed from self-orthogonal codes $C \leq C^{\perp}$, we write

$$\mathrm{P}_e(C) = \mathrm{P}_s(C \times C) = \{ab \mid a, b \in C\}^{\perp}. \tag{16}$$

B. Puncturing BCH Codes

In this section, let $\mathrm{BCH}_q^m(\delta)$ denote a primitive, narrow-sense q-ary BCH code of length $n = q^m - 1$ and designed distance δ. We illustrate the previous result by puncturing such BCH codes. Some knowledge about the puncture code is necessary for this task, and we show in Theorem 57 that a cyclic generalized Reed–Muller code is contained in the puncture code.

First, let us recall some basic facts about cyclic generalized Reed–Muller codes, see [9], [10], [54], [76] for details. Let $L_m(\nu)$ denote the subspace of $\mathbf{F}_q[x_1, \ldots, x_m]$ consisting of polynomials of degree $\leq \nu$, and let $(P_0, \ldots, P_{n-1})$ be an enumeration of the points in $\mathbf{F}_q^m$ where $P_0 = \mathbf{0}$. The q-ary cyclic generalized Reed-Muller code $\mathcal{R}_q^*(\nu, m)$ of order ν and length $n = q^m - 1$ is defined as

$$\mathcal{R}_q^*(\nu, m) = \{ev\, f \mid f \in L_m(\nu)\},$$

where the codewords are evaluations of the polynomials in all but P_0 defined by $ev\, f = (f(P_1), \ldots, f(P_{n-1}))$. The dimension $k^*(\nu)$ of the code $\mathcal{R}_q^*(\nu, m)$ is given by the formula $k^*(\nu) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{m+\nu-jq}{\nu-jq}$ and its minimum distance $d^*(\nu) = (R+1)q^Q - 1$, where $m(q-1) - \nu = (q-1)Q + R$ with $0 \leq R < q-1$. The dual code of $\mathcal{R}_q^*(\nu, m)$ can be characterized by

$$\mathcal{R}_q^*(\nu, m)^{\perp} = \{evf \mid f \in L_m^*(\nu^{\perp})\} \tag{17}$$

where $\nu^{\perp} = m(q-1) - \nu - 1$ and $L_m^*(\nu)$ is the subspace of all nonconstant polynomials in $L_m(\nu)$;

It is well-known that a primitive, narrow-sense BCH code contains a cyclic generalized Reed-Muller code, see [54, Theorem 5], and we determine the largest such subcode in our next lemma.

Lemma 56: Let $\nu = (m-Q)(q-1) - R$, with $Q = \lfloor \log_q(\delta + 1) \rfloor$ and $R = \lceil (\delta+1)/q^Q \rceil - 1$, then $\mathcal{R}_q^*(\nu, m) \subseteq \mathrm{BCH}_q^m(\delta)$. Also for all orders $\nu' > \nu$, we have $\mathcal{R}_q^*(\nu', m) \not\subseteq \mathrm{BCH}_q^m(\delta)$.

Proof: First, we show that $\mathcal{R}_q^*(\nu, m) \subseteq \mathrm{BCH}_q^m(\delta)$. Recall that the minimum distance $d^*(\nu) = (R+1)q^Q - 1$, where $m(q-1) - \nu = (q-1)Q + R$ with $0 \leq R < q-1$. By [54, Theorem 5], we have $\mathcal{R}_q^*(\nu, m) \subseteq \mathrm{BCH}_q^m((R+1)q^Q - 1)$. Notice that $(R+1)q^Q - 1 = \lceil (\delta+1)/q^Q \rceil q^Q - 1 \geq \delta$, so $\mathrm{BCH}_q^m((R+1)q^Q - 1) \subseteq \mathrm{BCH}_q^m(\delta)$. Therefore, $\mathcal{R}_q^*(\nu, m) \subseteq \mathrm{BCH}_q^m(\delta)$, as claimed.

For the second claim, it suffices to show that $\mathcal{R}_q^*(\nu+1, m)$ is not a subcode of $\mathrm{BCH}_q^m(\delta)$. We prove this by showing that the minimum distance $d^*(\nu+1) < \delta$. Notice that

$$m(q-1) - (\nu+1) = \begin{cases} (q-1)Q + R - 1, & R \geq 1 \\ (q-1)(Q-1) + q - 2, & R = 0 \end{cases}$$

with R and Q as given in the hypothesis. Therefore, the distance $d^*(\nu+1)$ of $\mathcal{R}_q^*(\nu+1, m)$ is given by

$$d^*(\nu+1) = \begin{cases} (\lceil (\delta+1)/q^Q \rceil - 1)q^Q - 1, & \text{for } R \geq 1 \\ (q-1)q^{Q-1} - 1, & \text{for } R = 0. \end{cases}$$

In both cases, it is straightforward to verify that $d^*(\nu+1) < \delta$. □

Explicitly determining the puncture code is a challenging task. For the duals of BCH codes, we are able to determine large subcodes of the puncture code.

Theorem 57: If $\delta < q^{\lfloor m/2 \rfloor} - 1$, then $\mathcal{R}_q^*(\mu, m) \subseteq \mathrm{P}_e(\mathrm{BCH}_q^m(\delta)^{\perp})$ for all orders μ in the range $0 \leq \mu \leq m(q-1) - 2(R + (q-1)Q) + 1$ with $Q = \lfloor \log_q(\delta+1) \rfloor$ and $R = \lceil (\delta+1)/q^Q \rceil - 1$.

Proof: By Lemma 56, we have $\mathcal{R}_q^*(\nu, m) \subseteq \mathrm{BCH}_q^m(\delta)$ for $\nu = (m-Q)(q-1) - R$; hence, $\mathrm{BCH}_q^m(\delta)^{\perp} \subseteq \mathcal{R}_q^*(\nu, m)^{\perp}$. It follows from the definition of the puncture code that $\mathrm{P}_e(\mathrm{BCH}_q^m(\delta)^{\perp}) \supseteq \mathrm{P}_e(\mathcal{R}_q^*(\nu, m)^{\perp})$. However,

$$\begin{aligned} \mathrm{P}_e(\mathcal{R}_q^*(\nu, m)^{\perp}) &= \{evf \cdot ev\, g \mid f, g \in L_m^*(\nu^{\perp})\}^{\perp} \\ &\supseteq \{evf \mid f \in L_m^*(2\nu^{\perp})\}^{\perp} \\ &= \mathcal{R}_q^*((2\nu^{\perp})^{\perp}, m) \end{aligned}$$

where the last equality follows from (17). This is meaningful only if $(2\nu^{\perp})^{\perp} \geq 0$ or, equivalently, if $\nu \geq (m(q-1) - 1)/2$. Since $\delta < q^{\lfloor m/2 \rfloor} - 1$, it follows that $Q \leq \lfloor m/2 \rfloor - 1$, and the order ν satisfies

$$\begin{aligned} \nu &= (m-Q)(q-1) - R \geq \lceil m/2 + 1 \rceil (q-1) - R \\ &\geq \lceil m/2 \rceil (q-1) + 1 \geq (m(q-1) - 1)/2 \end{aligned}$$

as required. Since $\mathcal{R}_q^*(\mu, m) \subseteq \mathcal{R}_q^*((2\nu^{\perp})^{\perp}, m)$ for $0 \leq \mu \leq (2\nu^{\perp})^{\perp}$, we have $\mathcal{R}_q^*(\mu, m) \subseteq \mathrm{P}_e(\mathrm{BCH}_q^m(\delta)^{\perp})$. □

Unfortunately, the weight distribution of generalized cyclic Reed–Muller codes is not known, see [22]. However, we know that the puncture code of $\mathrm{BCH}_q^m(\delta)^\perp$ contains the codes

$$\mathcal{R}_q^*(0,m) \subseteq \mathcal{R}_q^*(1,m) \subseteq \cdots \subseteq \mathcal{R}_q^*(m(q-1) - 2(R+(q-1)Q)+1, m),$$

so it must contain codewords of the respective minimum distances.

Corollary 58: If δ and μ are integers in the range $2 \leq \delta < q^{\lfloor m/2 \rfloor} - 1$ and $0 \leq \mu \leq m(q-1) - 2(R+(q-1)Q)+1$, where $Q = \lfloor \log_q(\delta+1) \rfloor$ and $R = \lceil (\delta+1)/q^Q \rceil - 1$, then there exists a

$$[[d^*(\mu), \geq d^*(\mu) - 2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$$

stabilizer code of length $d^*(\mu) = (\rho+1)q^\sigma - 1$, where σ and ρ satisfy the relations $m(q-1) - \mu = (q-1)\sigma + \rho$ and $0 \leq \rho < q-1$.

Proof: If $2 \leq \delta < q^{\lfloor m/2 \rfloor} - 1$, then from Theorem 50 we know that there exists an $[[q^m-1, q^m-1-2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$ quantum code. From Lemma 57 we know that $\mathrm{P}_e(\mathrm{BCH}_q^m(\delta)^\perp) \supseteq \mathcal{R}_q^*(\mu, m)$, where $0 \leq \mu \leq m(q-1) - 2(q-1)Q - 2R + 1$. By Theorem 54, if there exists a vector of weight r in $\mathrm{P}_e(\mathrm{BCH}_q^m(\delta)^\perp)$, the corresponding quantum code can be punctured to give $[[r, \geq r - 2m\lceil(\delta-1)(1-1/q)\rceil), d \geq \delta]]_q$. The minimum distance of $\mathcal{R}_q^*(\mu, m)$ is $d^*(\mu) = (\rho+1)q^\sigma - 1$, where $0 \leq \rho < q-1$ [54, Theorem 5]. Hence, it is always possible to puncture the quantum code to $[[d^*(\mu), \geq d^*(\mu) - 2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$. □

It is also possible to puncture quantum codes constructed via classical codes self-orthogonal with respect to the hermitian inner product. Examples of such puncturing can be found in [48] and [85].

XIII. MDS Codes

A quantum code that attains the quantum Singleton bound is called a quantum Maximum Distance Separable code or quantum MDS code for short. These codes have received much attention, but many aspects have not yet been explored in the quantum case (but see [48], [80]). In this section we study the maximal length of MDS stabilizer codes.

An interesting result concerning the purity of quantum MDS codes was derived by Rains [80, Theorem 2]:

Lemma 59 (Rains): An $[[n,k,d]]_q$ quantum MDS code with $k \geq 1$ is pure up to $n-d+2$.

Corollary 60: All quantum MDS codes are pure.

Proof: An $[[n,k,d]]_q$ quantum MDS code with $k=0$ is pure by definition; if $k \geq 1$ then it is pure up to $n-d+2$. By the quantum Singleton bound $n-2d+2 = k \geq 0$; thus, $n-d+2 \geq d$, which means that the code is pure. □

Lemma 61: For any $[[n, n-2d+2, d]]_q$ quantum MDS stabilizer code with $n-2d+2 > 0$, the corresponding classical codes $C \subseteq C^{\perp_a}$ are also MDS.

Proof: If an $[[n, n-2d+2, d]]_q$ stabilizer code exists, then Theorem 15 implies the existence of an additive $[n, d-1]_{q^2}$ code C such that $C \subseteq C^{\perp_a}$. Corollary 60 shows that $C^{\perp_a}$ has minimum distance d, so $C^{\perp_a}$ is an $[n, n-d+1, d]_{q^2}$ MDS code. By Lemma 59, the minimum distance of C is $\geq n-d+2$, so C is an $[n, d-1, n-d+2]_{q^2}$ MDS code. □

A classical $[n,k,d]_q$ MDS code is said to be trivial if $k \leq 1$ or $k \geq n-1$. A trivial MDS code can have arbitrary length, but a nontrivial one cannot. The next lemma is a straightforward generalization from linear to additive MDS codes.

Lemma 62: Assume that there exists a classical additive $(n, q^k, d)_q$ MDS code C:

1) if the code is trivial, then it can have arbitrary length;
2) if the code is nontrivial, then its code parameters must be in the range $2 \leq k \leq \min\{n-2, q-1\}$ and $n \leq q+k-1 \leq 2q-2$.

Proof: The first statement is obvious. For 2), we note that the weight distribution of the code C and its dual are related by the MacWilliams relations. The proof given in [68, pp. 320-321] for linear codes applies without change, and one finds that the number of codewords of weight $n-k+2$ in C is given by

$$A_{n-k+2} = \binom{n}{k-2}(q-1)(q-n+k-1).$$

Since A_{n-k+2} must be a nonnegative number, we obtain the claim. □

We say that a quantum $[[n,k,d]]_q$ MDS code is trivial if and only if its minimum distance $d \leq 2$. The length of trivial quantum MDS codes is not bounded, but the length of nontrivial ones is, as the next lemma shows.

Theorem 63 (Maximal Length of MDS Stabilizer Codes): A nontrivial $[[n,k,d]]_q$ MDS stabilizer code satisfies the following constraints:

1) its length n is in the range $4 \leq n \leq q^2+d-2 \leq 2q^2-2$;
2) its minimum distance satisfies $\max\{3, n-q^2+2\} \leq d \leq \min\{n-1, q^2\}$.

Proof: By definition, a quantum MDS code attains the Singleton bound, so $n-2d+2 = k \geq 0$; hence, $n \geq 2d-2$. Therefore, a nontrivial quantum MDS code satisfies $n \geq 2d-2 \geq 4$.

By Lemma 61, the existence of an $[[n, n-2d+2, d]]_q$ stabilizer code implies the existence of classical MDS codes C and $C^{\perp_a}$ with parameters $[n, d-1, n-d+2]_{q^2}$ and $[n, n-d+1, d]_{q^2}$, respectively. If the quantum code is a nontrivial MDS code, then the associated classical codes are nontrivial classical MDS codes. Indeed, for $n \geq 4$ the quantum Singleton bound implies $d \leq (n+2)/2 \leq (2n-2)/2 = n-1$, so C is a nontrivial classical MDS code.

By Lemma 62, the dimension of C satisfies the constraints $2 \leq d-1 \leq \min\{n-2, q^2-1\}$, or equivalently $3 \leq d \leq \min\{n-1, q^2\}$. Similarly, the length n of C satisfies $n \leq q^2 + (d-1) - 1 \leq 2q^2 - 2$. If we combine these inequalities then we get our claim. □

Example 64: The length of a nontrivial binary MDS stabilizer code cannot exceed $2q^2 - 2 = 6$. In [19] the nontrivial MDS stabilizer codes for $q=2$ were found to be $[[5,1,3]]_2$ and $[[6,0,4]]_2$, so there cannot exist further nontrivial MDS stabilizer codes.

In [48], the question of the maximal length of MDS codes was raised. All MDS stabilizer codes provided in that reference had a length of q^2 or less; this prompted us to look at the following famous conjecture for classical codes (cf. [53, Theorem 7.4.5] or [68, pp. 327-328]).

MDS Conjecture: If there is a nontrivial $[n,k]_q$ MDS code, then $n \leq q+1$ except when q is even and $k=3$ or $k=q-1$ in which case $n \leq q+2$.

If the MDS conjecture is true (and much supporting evidence is known), then we can improve upon the result of Theorem 63.

Corollary 65: If the classical MDS conjecture holds, then there are no nontrivial MDS stabilizer codes of lengths exceeding q^2+1 except when q is even and $d=4$ or $d=q^2$ in which case $n \leq q^2+2$.

XIV. Quantum Character Codes

A new family of codes was introduced in [32]. The codes of this family are defined using group characters. These codes are in many ways remarkably similar to binary Reed-Muller codes, but they are defined over nonbinary fields. Since these codes were introduced only recently and are not yet well-known, we will provide a little more background. In this section we derive quantum codes from group character codes using the CSS construction.

A. Group Character Codes

Let G be an additive abelian group of order n and exponent m. Let $\mathbf{F}_q$ be a finite field such that $\gcd(n,q)=1$ and $m \mid q-1$.

The set $\mathrm{Hom}(G,\mathbf{F}_q^*)$ of $\mathbf{F}_q$-valued characters of G consists of the homomorphisms from G into the multiplicative group $\mathbf{F}_q^*$. Our assumptions ensure that the set of characters forms a group that is isomorphic to G. We can index the characters by elements of the group G,

$$\mathrm{Hom}(G,\mathbf{F}_q^*) = \{\chi_x \,|\, x \in G\}$$

such that χ_0 denotes the trivial character, and χ_{-x} denotes the inverse of χ_x.

For any subset X of the group G, the character code C_X is defined as

$$C_X = \left\{ c \in \mathbf{F}_q^n \,\middle|\, \sum_{i=0}^{n-1} c_i \chi_{x_i}(y) = 0 \text{ for all } y \in X \right\}. \quad (18)$$

The code C_X is an $[n,k]_q$ code with $n = |G|$ and $k = n - |X|$. The parity check matrix H_X of C_X, with $X = \{x_0,\ldots,x_{n-k+1}\}$, is given by

$$H_X = \begin{bmatrix} \chi_{x_0}(x_0) & \cdots & \chi_{x_{n-1}}(x_0) \\ \chi_{x_0}(x_1) & \cdots & \chi_{x_{n-1}}(x_1) \\ \vdots & \ddots & \vdots \\ \chi_{x_0}(x_{n-k-1}) & \cdots & \chi_{x_{n-1}}(x_{n-k-1}) \end{bmatrix}$$

and its generator matrix G_X by

$$G_X = \begin{bmatrix} \chi_{x_0}(-x_{n-k}) & \cdots & \chi_{x_{n-1}}(-x_{n-k}) \\ \chi_{x_0}(-x_{n-k+1}) & \cdots & \chi_{x_{n-1}}(-x_{n-k+1}) \\ \vdots & \ddots & \vdots \\ \chi_{x_0}(-x_{n-1}) & \cdots & \chi_{x_{n-1}}(-x_{n-1}) \end{bmatrix}. \quad (19)$$

Indeed, the characters satisfy the well-known orthogonality relation

$$\sum_{x \in G} \chi_x(y)\chi_x(z) = \begin{cases} n, & \text{if } y+z = \mathbf{0} \\ 0, & \text{if } y+z \neq \mathbf{0} \end{cases}$$

which implies $G_X H_X^T = 0$.

B. Elementary Abelian 2-Groups

We now specialize to the case of a finite elementary abelian 2-group $G = \mathbf{Z}_2^m$, $m \geq 1$. Let $\mathbf{F}_q$ be a finite field of odd characteristic; this choice ensures that $2 \mid q-1$ and $\gcd(2^m,q)=1$. Recall that the characters of G are given by $\chi_x(y) = (-1)^{x\cdot y}$ for x,y in G.

We define a 2-group character code $\mathcal{C}_q(r,m)$ by

$$\mathcal{C}_q(r,m) = C_X \quad \text{with} \quad X = \{x \in \mathbf{Z}_2^m \mid \mathrm{wt}(x) > r\}.$$

It can be shown that $C_q(r,m)$ is an $[n,k(r),d(r)]_q$ code, with

$$k(r) = \sum_{j=0}^{r} \binom{m}{j} \quad \text{and} \quad d(r) = 2^{m-r}, \quad (20)$$

see [32, Lemma 4 and Theorem 6]. We need the following result about 2-group character codes which is not explicitly proved in [32].

Lemma 66: If $r_1 \leq r_2$, then $\mathcal{C}_q(r_1,m) \subseteq \mathcal{C}_q(r_2,m)$.

Proof: By (19) the generator matrix of $\mathcal{C}_q(r,m)$ consists of vectors of the form

$$(\chi_{x_0}(x_i), \chi_{x_1}(x_i), \ldots, \chi_{x_{n-1}}(x_i)) = (\chi_{x_0}(-x_i), \chi_{x_1}(-x_i), \ldots, \chi_{x_{n-1}}(-x_i))$$

where x_i is an element of $\mathbf{Z}_2^m$ of Hamming weight $\mathrm{wt}(x_i) \leq r$. Thus, the generator matrix of $C_q(r_1,m)$ is a submatrix of the generator matrix of $C_q(r_2,m)$, which shows that $\mathcal{C}_q(r_1,m) \subseteq \mathcal{C}_q(r_2,m)$. □

Lemma 67: The dual code $\mathcal{C}_q(r,m)^\perp$ is equivalent to $\mathcal{C}_q(m-r-1,m)$.

Proof: See [32, Theorem 8]. □

Now we construct a family of codes based on the CSS construction.

Theorem 68: If $0 \leq r_1 < r_2 \leq m$ and q is the power of an odd prime, then there exists an $[[n, k(r_2) - k(r_1), \min\{2^{m-r_2}, 2^{r_1+1}\}]]_q$ quantum code, where $n = 2^m$ and $k(r)$ is given by (20).

Proof: If $r_1 < r_2$, then $C_1 = \mathcal{C}_q(r_1,m) \subseteq \mathcal{C}_q(r_2,m) = C_2$ by Lemma 66. From the equations for the minimum distances given in (20), we can see that $\mathrm{wt}(C_2 \setminus C_1) = 2^{m-r_2}$. Similarly, it follows from Lemma 67 that $\mathrm{wt}(C_1^\perp \setminus C_2^\perp) = \mathrm{wt}(\mathcal{C}_q(m-r_1-1) \setminus \mathcal{C}_q(m-r_2-1)) = 2^{r_1+1}$. By Lemma 20, there exists an $[[n, k(r_2)-k(r_1), \min\{2^{m-r_2}, 2^{r_1+1}\}]]_q$ stabilizer code, where the dimensions $k(r_1)$ and $k(r_2)$ are given by (20). □

We can get more quantum codes by puncturing, as we did in the case of BCH codes. However, only the weight distribution of $\mathcal{C}_q(1,m)$ is known, so at the moment we do not have enough information as to what codes might exist.

XV. Code Constructions

Constructing good quantum codes is a difficult task. We need a quantum code for each parameter n and k in our tables. In this section we collect some simple facts about the construction of codes. Lemmas 69–71 show how to lengthen, shorten or reduce the dimension of the stabilizer code. These generalize and extend the constructions for binary quantum codes [19, Theorem 6].

Lemma 69: If an $[[n,k,d]]_q$ stabilizer code exists for $k>0$, then there exists an impure $[[n+1,k,d]]_q$ stabilizer code.

Proof: If an $[[n,k,d]]_q$ stabilizer code exists, then there exists an additive subcode $C \leq \mathbf{F}_q^{2n}$ such that $|C| = q^{n-k}$, $C \leq C^{\perp_s}$, and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$. Define the additive code

$$C' = \{(a\alpha|b0) \,|\, \alpha \in \mathbf{F}_q, (a|b) \in C\}.$$

We have $|C'| = q^{n-k+1}$. The definition ensures that C' is self-orthogonal with respect to the trace-symplectic inner product. Indeed, two arbitrary elements $(a\alpha|b0)$ and $(a'\alpha'|b'0)$ of C' satisfy the orthogonality condition

$$\langle (a\alpha|b0)|(a'\alpha'|b'0)\rangle_s = \langle (a|b)|(a'|b')\rangle_s + \mathrm{tr}(\alpha\cdot 0 - \alpha'\cdot 0) = 0.$$

A vector in the trace-symplectic dual of C' has to be of the form $(a\alpha|b0)$ with $(a|b) \in C^{\perp_s}$ and $\alpha \in \mathbf{F}_q$. Furthermore,

$$\mathrm{swt}(C'^{\perp_s} \setminus C') = \min\{\mathrm{swt}(a\alpha|b0) \,|\, \alpha \in \mathbf{F}_q, a, b \in C^{\perp_s} \setminus C\},$$

which coincides with $\mathrm{swt}(C^{\perp_s} \setminus C)$. Therefore, an $[[n+1,k,d]]_q$ stabilizer code exists by Theorem 13. If $d>1$, then the code is impure, because $C'^{\perp_s}$ contains the vector $(\mathbf{0}\alpha|\mathbf{0}0)$ of symplectic weight 1. □

Lemma 70: If a pure $[[n,k,d]]_q$ stabilizer code exists with $n \geq 2$ and $d \geq 2$, then there exists a pure $[[n-1,k+1,d-1]]_q$ stabilizer code.

Proof: If a pure $[[n,k,d]]_q$ stabilizer code exists, then there exists an additive code $D \leq \mathbf{F}_{q^2}^n$ that is self-orthogonal with respect to the trace-alternating form, so that $|D| = q^{n-k}$ and $\mathrm{wt}(D^{\perp_a}) = d$. Let $D_0^{\perp_a}$ denote the code obtained by puncturing the first coordinate of $D^{\perp_a}$. Since the minimum distance of $D^{\perp_a}$ is at least 2, we know that $|D_0^{\perp_a}| = |D^{\perp_a}| = q^{n+k}$, and we note that the minimum distance of $D_0^{\perp_a}$ is $d-1$. The dual of $D_0^{\perp_a}$ consists of all vectors u in $\mathbf{F}_{q^2}^{n-1}$ such that $0u$ is contained in D. Furthermore, if u is an element of D_0, then $0u$ is contained in D; hence, D_0 is a self-orthogonal additive code. The code D_0 is of size $q^{(n-1)-(k+1)}$, because

$$\dim D_0 + \dim D_0^{\perp_a} = \dim \mathbf{F}_{q^2}^{n-1}$$

when we view D_0 and its dual as $\mathbf{F}_p$–vector spaces. It follows that there exists a pure $[[n-1,k+1,d-1]]_q$ stabilizer code. □

Lemma 71: If a (pure) $[[n,k,d]]_q$ stabilizer code exists, with $k \geq 2$ ($k \geq 1$), then there exists an $[[n,k-1,d^*]]_q$ stabilizer code (pure to d) such that $d^* \geq d$.

Proof: If an $[[n,k,d]]_q$ stabilizer code exists, then there exists an additive code $D \leq \mathbf{F}_{q^2}^n$ such that $D \leq D^{\perp_a}$ with $\mathrm{wt}(D^{\perp_a} \setminus D) = d$ and $|D| = q^{n-k}$. Choose an additive code D_b of size $|D_b| = q^{n-k+1}$ such that $D \leq D_b \leq D_b^{\perp_a} \leq D^{\perp_a}$. Since $D \leq D_b$, we have $D_b^{\perp_a} \leq D^{\perp_a}$. The set $\Sigma_b = D_b^{\perp_a} \setminus D_b$ is a subset of $D^{\perp_a} \setminus D$, hence the minimum weight d^* of Σ_b is at least d. This proves the existence of an $[[n,k-1,d^*]]$ code.

If the code is pure, then $\mathrm{wt}(D^{\perp_a}) = d$; it follows from $D_b^{\perp_a} \leq D^{\perp_a}$ that $\mathrm{wt}(D_b^{\perp_a}) \geq d$, so the smaller code is pure as well. □

TABLE I
The Existence of a Pure $[[n,k,d]]_q$ Stabilizer Code Implies the Existence of Codes With Other Parameters

n/k	$k-1$	k	$k+1$
$n-1$	$\geq d-1$ pure (Lemma 71)	$\geq d-1$ pure (Lemma 71)	$d-1$ pure (Lemma 70)
n	$\geq d$ pure (Lemma 71)	d pure	$d-1$ impure (Lemma 69)
$n+1$	$\geq d$ impure (Lemma 69)	d impure (Lemma 69)	

Corollary 72: If a pure $[[n,k,d]]_q$ stabilizer code with $n \geq 2$ and $d \geq 2$ exists, then there exists a pure $[[n-1,k,\geq d-1]]_q$ stabilizer code.

Proof: Combine Lemmas 70 and 71. □

Lemma 73: Suppose that an $((n,K,d))_q$ and an $((n',K',d'))_q$ stabilizer code exist. Then there exists an $((n+n',KK',\min(d,d'))_q$ stabilizer code.

Proof: Suppose that P and P' are the orthogonal projectors onto the stabilizer codes for the $((n,K,d))_q$ and $((n',K',d'))_q$ stabilizer codes, respectively. Then $P \otimes P'$ is an orthogonal projector onto a KK'-dimensional subspace Q^* of $\mathbf{C}^d$, where $d = q^{n+n'}$. Let S and S', respectively, denote the stabilizer groups of the images of P and P'. Then $S^* = \{E \otimes E' \,|\, E \in S, E' \in S'\}$ is the stabilizer group of Q^*.

If an element $F \otimes F^*$ of $G_n \otimes G_{n'} = G_{n+n'}$ is not detectable, then F has to commute with all elements in S, and F' has to commute with all elements in S'. It is not possible that both $F \in Z(G_n)S$ and $F' \in Z(G_{n'})S'$ hold, because this would imply that $F \otimes F'$ is detectable. Therefore, either F or F' is not detectable, which shows that the weight of $F \otimes F'$ is at least $\min(d,d')$. □

Lemma 74: Let Q_1 and Q_2 be pure stabilizer codes that, respectively, have parameters $[[n,k_1,d_1]]_q$ and $[[n,k_2,d_2]]$. If $Q_2 \subseteq Q_1$, then there exists a $[[2n,k_1+k_2,d]]_q$ pure stabilizer code with minimum distance $d \geq \min\{2d_2,d_1\}$.

Proof: The hypothesis implies that there exist additive subcodes $D_1 \leq D_2$ of $\mathbf{F}_{q^2}^n$ such that $D_m \leq D_m^{\perp_a}$, $|D_m| = q^{n-k_m}$, and $\mathrm{wt}(D_m^{\perp_a}) = d_m$ for $m = 1,2$. The additive code

$$D = \{(u, u+v) \,|\, u \in D_1, v \in D_2\} \leq \mathbf{F}_{q^2}^{2n}$$

is of size $|D| = q^{2n-(k_1+k_2)}$. The trace-alternating dual of the code D is $D^{\perp_a} = \{(u'+v', v') \,|\, u' \in D_1^{\perp_a}, v' \in D_2^{\perp_a}\}$. Indeed, the vectors on the right hand side are perpendicular to the vectors in D, because

$$\langle (u, u+v) \,|\, (u'+v', v')\rangle_a = \langle u|u'+v'\rangle_a + \langle u+v|v'\rangle_a = 0$$

holds for all $u \in D_1, v \in D_2$ and $u' \in D_1^{\perp_a}, v' \in D_2^{\perp_a}$. We observe that D is self-orthogonal, $D \leq D^{\perp_a}$. The weight of a vector $(u'+v', v') \in D^{\perp_a} \setminus D$ is at least $\min\{2d_2, d_1\}$; the claim follows. □

Lemma 75: Let q be a power of two. If a pure $[[n,k_1,d_1]]_q$ stabilizer code Q_1 exists that has a pure subcode $Q_2 \subseteq Q_1$ (see Table I) with parameters $[[n,k_2,d_2]]_q$ such that $k_1 > k_2$, then

TABLE II
A COMPILATION OF KNOWN FAMILIES OF QUANTUM CODES

Family	$[[n,k,d]]_q$	Purity	Parameter Ranges and References
Short MDS	$[[n, n-2d+2, d]]_q$	pure	$2 \le d \le \lceil n/2 \rceil$, $q^2-1 \ge \binom{n}{d}$
Hermitian Hamming	$[[n, n-2m, 3]]_q$	pure	$m \ge 2$, $\gcd(m, q^2-1)=1$, $n=(q^{2m}-1)/(q^2-1)$
Euclidean Hamming	$[[n, n-2m, 3]]_q$	pure	$m \ge 2$, $\gcd(m, q-1)=1$, $n=(q^m-1)/(q-1)$
Quadratic Residue I	$[[n,1,d]]_q$	pure	n prime, $n \equiv 3 \mod 4$, $q \not\equiv 0 \mod n$ q is a quadratic residue modulo n, $d^2-d+1 \ge n$
Quadratic Residue II	$[[n,1,d]]_q$	pure	n prime, $n \equiv 1 \mod 4$, $q \not\equiv 0 \mod n$ q is a quadratic residue modulo n, $d \ge \sqrt{n}$
Melas	$[[n, n-4m, \ge 3]]_q$	pure	q even, $n=q^{2m}-1$, Pure to 3
Euclidean BCH	$[[n, n-2m\lceil(\delta-1)(1-1q\ )\rceil, \ge \delta]]_q$	pure to δ	$2 \le \delta \le q^{\lceil m/2 \rceil}-1-(q-2)[m \text{ odd}]$ $n=q^m-1$ and $m \ge 2$
Punctured BCH	$[[d^*(\mu), \ge d^*(\mu)-2m\lceil(\delta-1)(1-1/q)\rfloor, \ge \delta]]_q$	pure?	$\delta < q^{\lfloor m/2 \rceil}-1$, See Corollary 58
Hermitian BCH	$[[n, n-2m\lceil(\delta-1)(1-1/q^2)\rceil, \ge \delta]]_q$	pure	$2 \le \delta \le q^m-1$, $n=q^{2m}-1$, Pure to δ
Extended BCH	$[[n+1, n-2m\lceil(\delta-1)(1-1/q^2)\rceil-1, \ge \delta+1]]_q$	pure	Pure to $\delta+1$
Trivial MDS	$[[n, n-2, 2]]_q$	pure	$n \equiv 0 \mod p$
	$[[n,n,1]]_q$	pure	$n \ge 1$
Character	$[[n, k(r_2)-k(r_1), \min\{2^{m-r_2}, 2^{r_1+1}\}]]_q$	pure	$n=2^m$, q odd, $0 \le r_1 < r_2 \le m$, $k(r)=\sum_{j=0}^{r}\binom{m}{j}$
CSS GRM	$[[q^m, k(\nu_2)-k(\nu_1), \min\{d(\nu_2), d(\nu_1^\perp)\}]]_q$ $0 \le \nu_1 \le \nu_2 \le m(q-1)-1$	pure	$k(\nu)=\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{m+\nu-jq}{\nu-jq}$, $\nu^\perp=m(q-1)-\nu-1$ $\nu^\perp+1=(q-1)Q+R$, $d(\nu)=(R+1)q^Q$
Punctured GRM	$[[d(\mu), \ge k(\nu_2)-k(\nu_1)-(n-d(\mu)), \ge d]]_q$	pure?	$d \ge \min\{d(\nu_2), d(\nu_1^\perp)\}$, $0 \le \mu \le \nu_2-\nu_1$; [85]
Hermitian GRM	$[[q^{2m}, q^{2m}-2k(\nu), d(\nu^\perp)]]_q$ $0 \le \nu \le m(q-1)-1$	pure	$k(\nu)=\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{m+\nu-jq^2}{\nu-jq^2}$, $\nu^\perp=m(q^2-1)-\nu-1$ $\nu^\perp+1=(q^2-1)Q+R$, $d(\nu)=(R+1)q^{2Q}$
Punctured GRM	$[[d(\mu^\perp), \ge d(\mu^\perp)-2k(\nu), \ge d(\nu^\perp)]]_q$	pure?	$(\nu+1)q \le \mu \le m(q^2-1)-1$; [85]
Punctured MDS	$[[q^2-q\alpha, q^2-q\alpha-2\nu-2, \nu+2]]_q$	pure	$0 \le \nu \le q-2$, $0 \le \alpha \le q-\nu-1$; [85]
Euclidean MDS	$[[n, n-2d+2, d]]_q$	pure	$3 \le n \le q$, $1 \le d \le n/2+1$; [50]
Hermitian MDS	$[[q^2-s, q^2-s-2d+2, d]]_q$	pure	$1 \le d \le q$, $s=0,1$; [50]
Twisted	$[[q^2+1, q^2-3, 3]]_q$	pure?	[16]
Extended Twisted	$[[q^r, q^r-r-2, 3]]_q$	pure	$r \ge 2$; [16]
	$[[n, n-r-2, 3]]_q$	pure	$n=(q^{r+2}-q^3)/(q^2-1)$, $r \ge 1$, r odd; [16]
Perfect	$[[n, n-r-2, 3]]_q$	pure	$n=(q^{r+2}-1)/(q^2-1)$, $r \ge 2$, r even; [16]

a pure $[[2n, k_1-k_2, d]]_q$ stabilizer code exists such that $d \ge \min\{2d_1, d_2\}$.

Proof: If an $[[n_m, k_m, d_m]]_q$ stabilizer code exists, then there exists an additive code $D_m \le \mathbf{F}_{q^2}^n$ such that $D_m \le D_m^{\perp_a}$, $\mathrm{wt}(D_m^{\perp_a})=d$, and $|D_m|=q^{n-k_m}$ for $m=1,2$. The inclusion $Q_2 \subseteq Q_1$ implies that $D_1 \le D_2$. Let D denote the additive code consisting of vectors of the form $(u, u+v)$ such that $u \in D_2^{\perp_a}$ and $v \in D_1$.

We claim that $D^{\perp_a}$ consists of vectors of the form $(u', u'+v')$ such that $u' \in D_1^{\perp_a}$ and $v' \in D_2$. Indeed, let $v_1=(u, u+v)$ denote a vector in D, and let $v_2=(u', u'+v')$ be a vector with $u' \in D_1^{\perp_a}$ and $v' \in D_2$. We have

$$\langle v_1|v_2\rangle_a = \langle u|u'\rangle_a + \langle u|u'\rangle_a + \langle u|v'\rangle_a + \langle v|u'\rangle_a + \langle v|v'\rangle_a.$$

The first two terms on the right hand side cancel because the characteristic of the field is even; the next two terms vanish since the vectors belong to dual spaces; the last term vanishes because v and v' are both contained in D_2, and D_2 is self-orthogonal. Therefore, v_1 and v_2 are orthogonal. The set $\{(u', u'+v') \mid u' \in D_1^{\perp_a}, v' \in D_2\} \subseteq D^{\perp_a}$ has cardinality $q^{2n+k_1-k_2}$, so it must be equal to $D^{\perp_a}$ by a dimension argument.

The Hamming weight of a vector $(u', u'+v')$ in $D^{\perp_a}$ is at least $\min\{2d_1, d_2\}$, because $u' \in D_1^{\perp_a}$ and $v' \in D_2 \le D_2^{\perp_a}$. □

Lemma 76: Let q be a power of a prime. If an $((n, K, d))_{q^m}$ stabilizer code exists, then an $((nm, K, \ge d))_q$ stabilizer code exists. Conversely, if an $((nm, K, d))_q$ stabilizer code exists, then there exists an $((n, K, \ge \lfloor d/m \rfloor))_{q^m}$ stabilizer code.

This lemma is implicitly contained in the paper by Ashikhmin and Knill [4].

Proof: Let $B=\{\beta_1, \ldots, \beta_m\}$ denote a basis of $\mathbf{F}_{q^m}/\mathbf{F}_q$. If a is an element of $\mathbf{F}_{q^m}$, then we denote by $e_{\mathrm{B}}(a)$ the coordinate vector in $\mathbf{F}_q^m$ given by $e_{\mathrm{B}}(a)=(a_1, \ldots, a_m)$, where $a=\sum_{i=1}^{m} a_i\beta_i$.

A nondegenerate symmetric form on the $\mathbf{F}_q$-vector space $\mathbf{F}_{q^m}$ is given by $\mathrm{tr}_{q^m/q}(xy)$. It follows that the Gram matrix $M=(\mathrm{tr}_{q^m/q}(\beta_i\beta_j))_{1 \le i,j \le m}$ is nonsingular. We have $\mathrm{tr}_{q^m/q}(xy)=e_{\mathrm{B}}(x)^t M e_{\mathrm{B}}(y)$ for all x, y in $\mathbf{F}_{q^m}$. We define an $\mathbf{F}_p$–vector space isomorphism φ_{B} from $\mathbf{F}_{q^m}^{2n}$ onto $\mathbf{F}_q^{2nm}$ by

$$\varphi_{\mathrm{B}}((a|b)) = ((e_{\mathrm{B}}(a_1), \ldots, e_{\mathrm{B}}(a_n))|(Me_{\mathrm{B}}(b_1), \ldots, Me_{\mathrm{B}}(b_n))).$$

It follows from the fact that $\mathrm{tr}_{q/p}(\mathrm{tr}_{q^m/q}(x))=\mathrm{tr}_{q^m/p}(x)$ holds for all x in $\mathbf{F}_{q^m}$ and the definition of the isomorphism φ_{B} that $(a|b) \perp_s (c|d)$ holds in $\mathbf{F}_{q^m}^{2n}$ if and only if $\varphi_{\mathrm{B}}((a|b)) \perp_s \varphi_{\mathrm{B}}((c|d))$ holds in $\mathbf{F}_{q^{2nm}}$.

If an $((n, K, d))_{q^m}$ exists, then there exists an additive code $C \le \mathbf{F}_{q^m}^{2n}$ of size $|C|=q^{nm}/K$ such that $C \le C^{\perp_s}$, $\mathrm{swt}(C^{\perp_s} \setminus C)=d$ if $K>1$, and $\mathrm{swt}(C^{\perp_s})=d$ if $K=1$. Therefore, the code $\varphi_{\mathrm{B}}(C)$ over the alphabet $\mathbf{F}_q$ is of size q^{nm}/K, satisfies $\varphi_{\mathrm{B}}(C) \le \varphi_{\mathrm{B}}(C)^{\perp_s} \le \mathbf{F}_q^{2nm}$, and $\mathrm{swt}(\varphi_{\mathrm{B}}(C)^{\perp_s} \setminus \varphi_{\mathrm{B}}(C))=d$ if $K>1$ and $\mathrm{swt}(\varphi_{\mathrm{B}}(C)^{\perp_s})=d$ if $K=1$. Thus, an $((nm, K, d))_q$ stabilizer code exists.

The existence of an $((nm, K, d))_q$ stabilizer code implies the existence of an $((n, K))_{q^m}$ stabilizer code; the claim about the minimum distance follows from the fact that $\varphi_{\mathrm{B}}^{-1}$ maps each nonzero block of m symbols to a nonzero symbol in $\mathbf{F}_{q^m}$. □

We notice that there exists a basis B such that M is the identity matrix if and only if either q is even or both q and m are

odd, see [90]. In that case, φ_{B} simply expands each symbol into coordinates with respect to B.

XVI. Conclusions and Open Problems

We have further developed the theory of nonbinary stabilizer codes. In the first seven sections, we studied the basic theory of nonbinary stabilizer codes over finite fields, and introduced Galois-theoretic methods to clarify the relation between these and more general quantum codes. In the remaining sections, we derived numerous families of quantum codes. Table II gives an overview and summarizes the main parameters of these families.

We should emphasize that it is possible to start with a different choice of error basis [61], and one can develop a similar theory for such stabilizer codes. For example, one choice leads to self-orthogonal additive subcodes of $\mathbf{Z}_q^n \times \mathbf{Z}_q^n$ instead of subcodes of $\mathbf{F}_q^n \times \mathbf{F}_q^n$. It would be interesting to know how the stabilizer codes with respect to different error bases compare.

One central theme in quantum error-correction is the construction of codes that have a large minimum distance. We were able to show that the length of an MDS stabilizer code over $\mathbf{F}_q$ cannot exceed q^2+1, except in a few sporadic cases, assuming that the classical MDS conjecture holds. An open problem is whether the length n of a q-ary quantum MDS code is bounded by q^2+1 for all but finitely many n.

A number of researchers have raised the question whether there exist degenerate quantum codes that can exceed the quantum Hamming bound. Following Gottesman's lead [40], we were able to show that single and double error-correcting nonbinary stabilizer codes cannot beat the quantum Hamming bound. We conjecture that no quantum error-correcting code can exceed the quantum Hamming bound, but a proof is still elusive.

Finally, we briefly mention some of the topics that we have deliberately omitted. We decided not to include tables of the best known stabilizer codes, but rather make such tables available on the home page of the second author. We selected code families that are easily accessible by elementary methods; the interested reader can find examples of more intricate algebro-geometric constructions in [6], [25], [26], [57], [70] and of binary quantum LDPC codes in [21], [66], [77]. We did not include constructive aspects of encoding and decoding circuits, since encoding circuits are discussed in [50] and little is known about the decoding of stabilizer codes. We did not include combinatorial aspects, but Kim pointed out that there is a forthcoming book by Glynn, Gulliver, Maks, and Gupta that explores the relation between binary stabilizer codes and finite geometry.

Acknowledgment

This paper is dedicated to the memory of Prof. Thomas Beth. The authors would like to thank the referees for very helpful comments that improved the presentation of the paper. They also received numerous comments and suggestions during the preparation of this manuscript that are much appreciated. In particular, many thanks to Markus Grassl and Martin Rötteler for sending us corrections and suggestions, to Daniel Gottesman, Jon-Lark Kim and Simon Litsyn for sending us helpful comments and references, and to Raymond Laflamme and Peter Shor for providing us with historical background. They are grateful to Neil Sloane for very fruitful discussions on MDS codes, and to Gordon Chen, Phil Hemmer, and Suhail Zubairy for helpful discussions in our quantum computing seminar.

References

[1] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," in *Proc. 29th Annu. ACM Symp. Theory of Comput. (STOC)*, New York, 1997, pp. 176–188.

[2] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "Primitive quantum BCH codes over finite fields," in *Proc. 2006 IEEE Int. Symp. Inf. Theory*, Seattle, WA, 2006, pp. 1105–1108.

[3] V. Arvind and K. R. Parthasarathy, "A family of quantum stabilizer codes based on the Weyl commutation relations over a finite field," in *A Tribute to C. S. Seshadri (Chennai, 2002)*. Cambridge, MA: Birkhäuser, 2003, Trends Math., pp. 133–153.

[4] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 3065–3072, 2001.

[5] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1206–1215, 1999.

[6] A. Ashikhmin, M. A. Tsfasman, and S. Litsyn, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, p. 032311, 2001.

[7] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn, "Quantum error detection I: Statement of the problem," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 778–788, 2000.

[8] ——, "Quantum error detection II: Bounds," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 789–800, 2000.

[9] A. R. Assmus Jr. and J. D. Key, *Designs and Their Codes*. Cambridge, MA: Cambridge University Press, 1992.

[10] E. F. Assmus Jr. and J. D. Key, "Polynomial codes and finite geometries," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. II, pp. 1269–1343.

[11] A. Barg, S. Guritman, and J. Simonis, "Strengthening the Gilbert-Varshamov bound," *Linear Algebra Its Appl.*, vol. 307, pp. 119–129, 2000.

[12] H. Barnum, Quantum Message Authentication Codes quant-ph/0103123, 2001.

[13] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *Proc. 43rd Annu. IEEE Symp. Found. Comput. Sci. (FOCS '02)*, 2002, pp. 449–458.

[14] T. Beth and M. Grassl, "The quantum Hamming and hexacodes," *Fortschr. Phys.*, vol. 46, no. 4-5, pp. 459–491, 1998.

[15] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann, *Codierungstheorie – Konstruktion und Anwendung Linearer Codes*. Berlin, Germany: Springer-Verlag, 1998.

[16] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Comb. Designs*, vol. 8, pp. 174–188, 2000.

[17] G. Birkhoff, *Lattice Theory*, 2nd ed. Providence, RI: Amer. Math. Soc., 1961.

[18] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 76, pp. 405–409, 1997.

[19] ——, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1369–1387, 1998.

[20] A. R. Calderbank and P. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[21] T. Camara, H. Ollivier, and J.-P. Tillich, Constructions and Performance of Classes of Quantum LDPC Codes eprint: quant-ph/0502086, 2005.

[22] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, V. S. Pless and C. W. Huffman, Eds. New York: Elsevier, 1998, pp. 963–1063.

[23] H. F. Chau, "Correcting quantum errors in higher spin systems," *Phys. Rev. A*, vol. 55, pp. R839–R841, 1997.

[24] ——, "Five quantum register error correction code for higher spin systems," *Phys. Rev. A*, vol. 56, pp. R1–R4, 1997.

[25] H. Chen, "Some good quantum error-correcting codes from algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2059–2061, 2001.

[26] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2055–2058, 2001.

[27] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A*, vol. 55, no. 6, pp. 4054–4059, 1997.

[28] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A*, vol. 56, no. 1, pp. 76–82, 1997.

[29] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2495–2498, 1999.

[30] L. E. Danielsen and M. G. Parker, On the Classification of all Self-Dual Additive Codes over GF(4) of Length up to 12 arXiv:math.CO/0504522, 2005.

[31] P. Delsarte, "Bounds for unrestricted codes by linear programming," *Phil. Res. Reports*, vol. 27, pp. 272–289, 1972.

[32] C. Ding, D. Kohel, and S. Ling, "Elementary 2-group character codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 280–284, 2000.

[33] A. Ekert and C. Macchiavello, "Error correction in quantum communication," *Phys. Rev. Lett.*, vol. 76, pp. 2585–2588, 1996.

[34] K. Feng, "Quantum codes $[[6,2,3]]_p$, $[[7,3,3]]_p$ $(p \geq 3)$ exist," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2384–2391, 2002.

[35] ——, "Quantum error-correcting codes," in *Coding Theory and Cryptology*. Singapore: World Scientific, 2002, pp. 91–142.

[36] K. Feng and Z. Ma, "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3323–3325, 2004.

[37] M. H. Freedman and D. A. Meyer, "Projective plane and planar quantum codes," *Found. Comput. Math.*, vol. 1, no. 3, pp. 325–332, 2001.

[38] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[39] ——, Pasting Quantum Codes eprint: quant-ph/9607027, 1996.

[40] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," Ph.D. dissertation, California Inst. of Technol., Pasadena, CA, 1997.

[41] ——, "Fault-tolerant quantum computation with higher-dimensional systems," *Chaos, Solitons, Fractals*, vol. 10, no. 10, pp. 1749–1758, 1999.

[42] ——, "An introduction to quantum error correction," in *Proc. Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, Providence, RI, 2002, pp. 221–235, eprint: quant-ph/0004072.

[43] ——, Quantum Error Correction and Fault-Tolerance eprint: quant-ph/0507174, 2005.

[44] M. Grassl, "Algorithmic aspects of error-correcting codes," in *The Mathematics of Quantum Computing*, R. Brylinski and G. Chen, Eds. Boca Raton, FL: CRC Press, 2001, pp. 223–252.

[45] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. X. Int. Symp. Theoretic. Elec. Eng.,*, Magdeburg, Germany, 1999, pp. 207–212.

[46] ——, "Cyclic quantum error-correcting codes and quantum shift registers," *Proc. Royal Soc. London Series A*, vol. 456, no. 2003, pp. 2689–2706, 2000.

[47] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. Lett. A*, vol. 56, no. 1, pp. 33–38, 1997.

[48] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 1, pp. 757–775, 2004.

[49] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed-Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Honolulu, HI, 1999)*. Berlin, Germany: Springer, 1999, vol. 1719, Lecture Notes in Comput. Sci., pp. 231–244.

[50] M. Grassl, M. Rötteler, and T. Beth, "Efficient quantum circuits for non-qubit quantum error-correcting codes," *Int. J. Found. Comput. Sci.*, vol. 14, no. 5, pp. 757–775, 2003.

[51] L. C. Grove, *Classical Groups and Geometric Algebra*, ser. Graduate Studies in Mathematics. Providence, RI: Amer. Math. Soc., 2001.

[52] T. Hiramatsu and G. Köhler, *Coding Theory and Number Theory*. London, U.K.: Kluwer Academic, 2003.

[53] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, MA: University Press, 2003.

[54] T. Kasami, S. Lin, and W. W. Peterson, "New generalizations of the Reed-Muller codes part I : Primitive codes," *IEEE Trans. Inf. Theory*, vol. 14, pp. 189–199, 1968.

[55] J.-L. Kim, "New quantum-error-correcting codes from Hermitian self-orthogonal codes over GF(4)," in *Proc. Sixth Int. Conf. Finite Fields Appl.*, Oaxaca, Mexico, May 21–25, 2002, pp. 209–213.

[56] J.-L. Kim and V. Pless, "Designs in additive codes over GF(4)," *Designs, Codes, Crypt.*, vol. 30, pp. 187–199, 2003.

[57] J.-L. Kim and J. Walker, "Nonbinary quantum error-correcting codes from algebraic curves," in *Special Issue of* $\mathrm{Com}^2\mathrm{MaC}$ *Conf. Assoc. Schemes, Codes and Designs in Discr. Math.*, 2004.

[58] A. Y. Kitaev, "Quantum computations: Algorithms and error correction," *Russian Math. Surv.*, vol. 52, no. 6, pp. 1191–1249, 1997.

[59] A. Klappenecker and M. Rötteler, "Beyond stabilizer codes II: Clifford codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2396–2399, 2002.

[60] E. Knill, Group Representations, Error Bases and Quantum Codes Los Alamos National Laboratory, LAUR-96-2807, 1996.

[61] ——, Non-Binary Unitary Error Bases and Quantum Codes Los Alamos National Laboratory, LAUR-96-2717, 1996.

[62] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, 1997.

[63] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inf. Theory*, vol. 36, pp. 686–692, 1990.

[64] V. I. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Trans. Inf. Theory*, vol. 41, pp. 1303–1321, 1995.

[65] R. Li and X. Li, "Binary construction of quantum codes of minimum distance three and four," *IEEE Trans. Inf. Theory*, vol. 50, pp. 1331–1336, 2004.

[66] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2315–2330, 2004.

[67] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, 1963.

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

[69] W. J. Martin, "A physics-free introduction to quantum error correcting codes," *Util. Math.*, pp. 133–158, 2004.

[70] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2122–2124, 2002.

[71] R. Matsumoto and T. Uyematsu, "Constructing quantum error correcting codes for p^m-state systems from classical error correcting codes," *IEICE Trans. Fund.*, vol. E83-A, no. 10, pp. 1878–1883, 2000.

[72] R. J. McEliece, E. R. Rodemich jr., H. Rumsey, and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inf. Theory*, vol. 23, p. 157, 1977.

[73] O. Moreno and C. J. Moreno, "The Macwilliams-sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of the duals of BCH codes," *IEEE Trans. Inf. Theory*, vol. 40, pp. 1894–1907, 1994.

[74] O. Moreno, J. P. Pederson, and D. Polemi, "An improved Serre bound for elementary abelian extensions of $\mathbf{F}_q(x)$ and the generalized Hamming weights of duals of BCH codes," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1291–1293, 1998.

[75] O. Ore, "Galois connexions," *Trans. Amer. Math. Soc.*, vol. 55, pp. 493–513, 1944.

[76] R. Pellikaan and X.-W. Wu, "List decoding of q–ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 50, pp. 679–682, 2004.

[77] M. S. Postol, A Proposed Quantum Low Density Parity Check Code eprint: quant-ph/0108131, 2001.

[78] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1388–1394, 1998.

[79] ——, "Monotonicity of the quantum linear programming bound," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2489–2492, 1999.

[80] ——, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1827–1832, 1999.

[81] ——, "Quantum codes of minimum distance two," *IEEE Trans. Inf. Theory*, vol. 45, pp. 266–271, 1999.

[82] ——, "Quantum shadow enumerators," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2361–2366, 1999.

[83] ——, "Polynomial invariants of quantum codes," *IEEE Trans. Inf. Theory*, vol. 46, pp. 54–59, 2000.

[84] M. Rötteler, M. Grassl, and T. Beth, "On quantum MDS codes," in *Proc. 2004 IEEE Int. Symp. Inf. Theory*, Chicago, USA, 2004, p. 355.

[85] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes," in *Proc. 2005 IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, 2005, pp. 1023–1027.

[86] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *Quantum Inf. Comput.*, vol. 2, no. 4, pp. 307–323, 2002.

[87] D. Schlingemann and R. F. Werner, Quantum Error-Correcting Codes Associated with Graphs eprint: quant-ph/00012111, 2000.

[88] R. Schoof, "Families of curves and weight distributions of codes," *Bull. Amer. Math. Soc.*, vol. 32, no. 2, pp. 171–183, 1995.

[89] R. Schoof, G. van der Geer, and M. van der Vlugt, "Weight formulas for ternary Melas codes," *Math. Comp.*, vol. 58, pp. 781–792, 1992.

[90] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, pp. 758–767, 1980.

[91] P. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 2, pp. 2493–2496, 1995.
[92] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600–1603, 1997.
[93] A. Steane, "Quantum Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1701–1703, 1999.
[94] A. M. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. London A*, vol. 452, pp. 2551–2577, 1996.
[95] ——, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996.
[96] ——, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2492–2495, 1999.
[97] H. Stichtenoth and C. Voß, "Generalized Hamming weights of trace codes," *IEEE Trans. Inf. Theory*, vol. 40, pp. 554–558, 1994.
[98] A. Thangaraj and S. W. McLaughlin, "Quantum codes from cyclic codes over $\mathrm{GF}(4^m)$," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1176–1178, 2001.
[99] G. van der Geer and M. van der Vlugt, "Generalized Hamming weights of Melas codes and dual Melas codes," *SIAM J. Disc. Math.*, vol. 7, no. 4, pp. 554–559, 1980.
[100] F. Vatan, V. P. Roychowdhury, and M. P. Anantram, "Spatially correlated qubit errors and burst-correcting quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1703–1708, 1999.
[101] L. Xiaoyan, "Quantum cyclic and constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, pp. 547–549, 2004.