Nonbinary Quantum Stabilizer Codes

Alexei Ashikhmin * Emanuel Knill †

Abstract

We define and show how to construct nonbinary quantum stabilizer codes. Our approach is based on nonbinary error bases. It generalizes the relationship between selforthogonal codes over $\mathbf{F}_4$ and binary quantum codes to one between selforthogonal codes over $\mathbf{F}_{q^2}$ and q-ary quantum codes for any prime power q.

Index Terms — quantum stabilizer codes, nonbinary quantum codes, selforthogonal codes.

1 Introduction

Probably the most important class of binary quantum codes are quantum stabilizer codes. They play a role similar to the linear codes in classical coding theory. Quantum stabilizer codes have simple encoding algorithms, can be analyzed using classical coding theory, and yield methods for fault tolerant quantum computation. The first examples of quantum codes found by Shor [18], and Steane [21, 22] were quantum stabilizer codes. General quantum stabilizer codes were introduced by Gottesman [9] and Calderbank *et. al.* [6]. Later Calderbank *et. al.* [7] gave the now standard connection between quantum stabilizer codes and classical selforthogonal codes, which was used to construct a number of new good quantum codes.

While the theory of binary quantum stabilizer codes is now well developed, nonbinary codes have been relatively ignored. A connection between classical codes over $\mathbf{Z}_n$ and quantum codes is given in [11, 12]. The connection is based on a stabilizer construction derived from so-called nice error bases. Raines [16] obtained a number of results for p-ary (p prime) quantum stabilizer codes generalizing the $\mathbf{F}_4$ constructions for binary quantum codes.

Here we consider the problem of constructing p^m-ary quantum codes from classical selforthogonal codes over $\mathbf{F}_{p^{2m}}$. The notion of selforthogonality arises naturally from the error bases of [11, 12] and can be identified with that arising from a field-theoretically defined simplectic form. Good self-orthogonal codes with respect to this form have already been found by Bierbrauer and Edel [5], and our construction can be used to obtain associated quantum codes. We conclude the paper by showing that codes meeting the non-binary quantum-Gilbert-Varshamov bound exist.

2 Basic Definitions

We start with the basic notions of classical and quantum coding theory. Denote by $\mathbf{F}_{p^m}$ the Galois field of p^m elements, where p is a prime number and m is an integer. Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ denote the elements of a basis of $\mathbf{F}_{p^m}$ over $\mathbf{F}_p$. We fix a non-zero $\mathbf{F}_p$-linear functional $\mathrm{tr} : \mathbf{F}_{p^m} \to \mathbf{F}_p$ (called a *trace function*). Thus tr satisfies

$$\begin{aligned} \mathrm{tr}(a+b) &= \mathrm{tr}(a) + \mathrm{tr}(b), \\ \mathrm{tr}(\alpha a) &= \alpha\, \mathrm{tr}(a), \end{aligned}$$

for all $a, b \in \mathbf{F}_{p^m}, \alpha \in \mathbf{F}_p$. Note that for $x \in \mathbf{F}_{p^m}$, $\mathrm{tr}_x(a) = \mathrm{tr}(xa)$ defines another trace function, and that all such functions can be obtained this way. The standard trace function is the one defined by viewing $\mathbf{F}_{p^m}$ as an extension of $\mathbf{F}_p$ and letting $\mathrm{tr}(a) = \sum_{i=0}^{m-1} a^{p^i}$, [15, Chapter 2.3].

Let t divide m.

Definition 1 *A classical $\mathbf{F}_{p^t}$-linear code C over a field $\mathbf{F}_{p^m}$ of length n and size $(p^t)^k$, is a k dimensional $\mathbf{F}_{p^t}$-linear subspace of the space $\mathbf{F}_{p^m}^n$.*

*Bell Laboratories, Lucent Technologies, 600 Mountain Ave., Rm.: 2C-180, Murray Hill, NJ 07974.

†Los Alamos National Laboratory Group CIC-3, Mail Stop K987, Los Alamos, NM 87545.

In other words, for any $\mathbf{a}, \mathbf{b}$ from C and any $\alpha, \beta \in \mathbf{F}_{p^t}$ the vector $\alpha\mathbf{a} + \beta\mathbf{b}$ is also from C. (If C is p^m-linear we shall call it just linear.) We shall say that C is an $[n,k]_{p^t}$ code and denote by $d(C) = d$, $\delta(C) = \delta = \frac{d}{n}$, and $R_C = R = \frac{1}{n}\log_r |C|$ its minimum distance, relative minimum distance, and rate respectively.

Let $*$ be a $\mathbf{F}_{p^t}$-bilinear form (an *inner product*). A code C is *selforthogonal* for $*$ if for all vectors $\mathbf{a}$ and $\mathbf{b}$ from C the following property holds

$$\mathbf{a} * \mathbf{b} = 0. \tag{1}$$

The code $C^\perp = \{\mathbf{v} : \mathbf{v} * \mathbf{a} = 0 \text{ for } \forall \mathbf{a} \in C\}$ is called the dual code of C with respect to (1).

Remark For an introduction to the theory of Galois Fields and classical codes see e.g. [15].

Definition 2 *A q-ary quantum code Q of length n and size K is a K-dimensional subspace of a q^n-dimensional Hilbert space.*

The rate of Q is given by $R_Q = \frac{1}{n}\log_q K$.

A q^n-dimensional Hilbert space is identified with the n-fold tensor product of q-dimensional Hilbert spaces. The q-dimensional spaces are thought of as the state spaces of *q-ary systems* in the same way as the values 0 and 1 can be thought of as the possible states of a bit in a bit string. We identify the state spaces with the q-dimensional complex linear space $\mathbf{C}_q$. An important characteristic of a quantum code is its *minimum distance*. If a code has minimum distance d then it can detect any $d-1$ and correct any $\lfloor \frac{d-1}{2} \rfloor$ errors. As a result it is desirable to keep d as large as possible. A strict definition of the minimum distance is given in the next section after introducing error bases.

Remark For introductions to the theory of quantum error correcting codes see e.g. [13, 10, 14]. For a reader with a background in classical coding theory the papers [1, 2] have brief introductions to the field.

3 Error Bases

A general quantum error of a p^m-ary quantum system, is a linear operator, say e, acting on the space $\mathbf{C}_{p^m}$. If $\mathbf{v}$ is a state (a unit vector in the space) of the system, then the effect of error e is to transform it to the state $e\mathbf{v}$. It is well known from the general theory of quantum codes that if a code can correct a given set $\mathcal{E}$ of error operators, then it can correct the linear span of $\mathcal{E}$. For this reason it is enough confine ourselves to errors that form a basis of the vector space of linear operators acting on $\mathbf{C}_{p^m}$. Let linear operators $e_1, e_2, \ldots, e_{p^{2m}}$ form such a basis.

Let $\mathbf{v}$ represent a state of n p^m-ary systems. A general error operator that can alter $\mathbf{v}$ is a linear operator acting on the n-fold tensor product of $\mathbf{C}_{p^m}$. Let us consider error operators of the form

$$E = \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n, \tag{2}$$

where $\sigma_i \in \{e_1, e_2, \ldots, e_{p^{2m}}\}$. Since they form a basis we can again confine ourselves to them.

It is always possible to determine operators e_1, $e_2, \ldots, e_{p^{2m}}$ in such a way that one of them, say e_1, is the identity operator I_{p^m}. Define the *weight* of E in (2) as

$$\mathrm{wt}(E) = |\{\sigma_i \neq I_{p^m}\}|. \tag{3}$$

In the depolarizing channel model of errors [4], the operators $e_2, e_3, \ldots$ satisfy $\mathrm{Tr}(e_i^\dagger e_j) = p^m \delta_{i,j}$, where Tr is the trace of linear operators. When transmitting a qubit through a depolarizing channel, the probability that it is untouched (i.e. affected by the identity operator) is $1-r$ and the probability that it is affected by $e_i, i > 1$, is $r/(p^{2m}-1)$. The standard assumption is that $1-r > r/(p^{2m}-1)$. Thus, the probability of an error operator decreases exponentially with weight, a feature common to most realistic error models [14]. This explains why it is desirable to correct or detect all error operators up to some given weight.

Let P be the orthogonal projection operator onto Q. It can be shown that (see e.g. [11]) an error operator E is *detectable* by Q iff

$$PEP = c_E P, \tag{4}$$

where c_E is a constant depending on E.

Definition 3 *The largest integer d such that every error of weight $d-1$ or less can be detected by a code is called its minimum distance.*

We now define an explicit error basis for p^m-ary quantum codes. Let T and R be linear operators

acting on the space $\mathbf{C}_p$ defined by the matrices with entries

$$T_{i,j} = \delta_{i,j-1 \bmod p} \text{ and } R_{i,j} = \xi^i \delta_{i,j},$$

where $\xi = e^{\iota 2\pi/p}, \iota = \sqrt{-1}$, and the indices range from 0 to $p-1$ [11]. Let us define an inner product for operators as follows

$$\langle A, B \rangle = \mathrm{Tr}(A^\dagger B). \tag{5}$$

Proposition 1 *Operators $T^i R^j$ form an orthogonal basis under inner product (5).*

Proof. It is easy to check that

$$TR = \xi RT$$

and therefore

$$\begin{aligned} T^i R^j &= \xi^{ij} R^j T^i, & (6)\\ \left(T^i R^j\right)\left(T^k R^l\right) &= \xi^{il-jk}\left(T^k R^l\right)\left(T^i R^j\right), & (7)\\ \left(T^i R^j\right)\left(T^k R^l\right) &= \xi^{-jk} T^{i+k} R^{j+l}. & (8) \end{aligned}$$

The Hermitian transposes of T^i and R^i are obtained by raising to the power $p-1$:

$$(T^i)^\dagger = (T^i)^{p-1}, (R^i)^\dagger = (R^i)^{p-1}, \tag{9}$$

and

$$T^p = R^p = I_p. \tag{10}$$

Now using the above expressions we obtain

$$\mathrm{Tr}((T^i R^j)^\dagger (T^k R^l)) = \mathrm{Tr}(\xi^{-(k-i)(l-j)} T^{(k-i)} R^{(l-j)}).$$

Noting that $\mathrm{Tr}(T^i R^j) = p\delta_{i,0}\delta_{j,0}$, we finish the proof. □

From (8) and (10) it follows that for $p > 2$

$$(T^i R^j)^p = \xi^{-ij(1+2+\ldots+(p-1))} = I_p. \tag{11}$$

Let $a, b \in \mathbf{F}_{p^m}$. Using a basis of $\mathbf{F}_{p^m}$ over $\mathbf{F}_p$, we can write uniquely

$$\begin{aligned} a &= a_1\alpha_1 + a_2\alpha_2 + \ldots + a_m\alpha_m,\\ b &= b_1\alpha_1 + b_2\alpha_2 + \ldots + b_m\alpha_m, \end{aligned}$$

with the a_i and b_i in $\mathbf{F}_p$. Define

$$T_a R_b = (T^{a_1} \otimes T^{a_2} \otimes \ldots \otimes T^{a_m})(R^{b_1} \otimes R^{b_2} \otimes \ldots \otimes R^{b_m}).$$

The multiplication rules given in the proof of Proposition 1 can be generalized. Define

$$\langle a, b \rangle = \sum_{i=1}^{m} a_i b_i \in \mathbf{F}_p. \tag{12}$$

From (8) and the identity $(A \otimes B)(C \otimes D) = AC \otimes BD$ it follows that

$$(T_a R_b)(T_c R_d) = \xi^{-\langle b,c \rangle} T_{a+c} R_{b+d}. \tag{13}$$

(7) and (12) yield

$$(T_a R_b)(T_c R_d) = \xi^{\langle a,d \rangle - \langle b,c \rangle} (T_c R_d)(T_a R_b). \tag{14}$$

Now, using the same arguments as in Proposition 1, one can see that the operators $T_a R_b$ form an orthonormal basis of operators acting on $\mathbf{C}_{p^m}$.

4 Nonbinary Stabilizer Codes

Let $\mathbf{a}^\dagger = (a^{(1)}, a^{(2)}, \ldots, a^{(n)}), \mathbf{b}^\dagger = (b^{(1)}, b^{(2)}, \ldots, b^{(n)})$ be vectors from the space $\mathbf{F}_{p^m}^n$. (Throughout this section we use superscripts to label the systems.) As discussed in the previous section, it is enough to consider the error operators given by

$$E_{\mathbf{a},\mathbf{b}} = T_{a^{(1)}} R_{b^{(1)}} \otimes T_{a^{(2)}} R_{b^{(2)}} \otimes \ldots \otimes T_{a^{(n)}} R_{b^{(n)}}. \tag{15}$$

The set of operators $\mathcal{E} = \{\xi^i E_{\mathbf{a},\mathbf{b}} | 0 \le i \le p-1\}$ form a group of order p^{2mn+1}. The center $\mathcal{Z}$ of $\mathcal{E}$ is generated by ξI and therefore has order p. For vectors $\mathbf{a}, \mathbf{d} \in \mathbf{F}_{p^m}^n$ define an inner product by

$$\langle \mathbf{a}, \mathbf{d} \rangle = \sum_{i=1}^{n} \langle a^{(i)}, d^{(i)} \rangle, \tag{16}$$

where $\langle a^{(i)}, d^{(i)} \rangle$ is defined in (12). It follows from (14) that

$$E_{\mathbf{a},\mathbf{b}} E_{\mathbf{c},\mathbf{d}} = \xi^{\langle \mathbf{a},\mathbf{d} \rangle - \langle \mathbf{b},\mathbf{c} \rangle} E_{\mathbf{c},\mathbf{d}} E_{\mathbf{a},\mathbf{b}}. \tag{17}$$

From (13) we have

$$E_{\mathbf{a},\mathbf{b}} E_{\mathbf{c},\mathbf{d}} = \xi^{-\langle \mathbf{b},\mathbf{c} \rangle} E_{\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{d}}. \tag{18}$$

From (15) and (11) it follows that for any $\mathbf{a}$ and $\mathbf{b}$ and $p > 2$,

$$E_{\mathbf{a},\mathbf{b}}^p = I_{p^{mn}}. \tag{19}$$

Quantum *stabilizer codes* are defined as joint eigenspaces of the operators of a commutative subgroup S of $\mathcal{E}$. Without loss of generality, assume that $\mathcal{Z} \subseteq S$. If this is not the case, extend S by $\mathcal{Z}$. The order of S is a power of p, $|S| = p^{r+1}$. Let μ be a linear character that satisfies the constraint

$$\mu(\xi I) = \xi. \tag{20}$$

Definition 4 *A quantum stabilizer code $Q_{S,\mu}$ is the eigenspace of S associated with μ, i.e.*

$$Q_{S,\mu} = \{\mathbf{v} \in \mathbf{C}_{p^m}^n : E\mathbf{v} = \mu(E)\mathbf{v} \text{ for all } E \in S\}.$$

Theorem 2 *The size of $Q_{S,\mu}$ equals p^{mn-r}.*

PROOF. Let γ be a linear character of S. Let us define a linear operator

$$P_\gamma = \frac{1}{|S|} \sum_{E \in S} \bar{\gamma}(E) E.$$

P_γ is an orthogonal projection and

$$P_\gamma P_\mu = P_\gamma \delta_{\gamma,\mu} \tag{21}$$

(For a proof of this fact see, for instance, [20, Capter 2.6].) From the definition of $Q_{S,\mu}$ and (21) it follows that $P_\gamma \mathbf{v} = \mathbf{v}\delta_{\gamma,\mu}, \mathbf{v} \in Q_{S,\mu}$. Hence $\dim(Q_{S,\mu}) \geq \mathrm{Tr}(P_\mu)$. Since for $E \in \mathcal{E} \setminus \mathcal{Z}$, $\mathrm{Tr}\, E = 0$, we have

$$\begin{aligned} \mathrm{Tr}\, P_\mu &= \frac{1}{|S|} \sum_{i=0}^{p-1} \bar{\mu}(\xi^i I)\, \mathrm{Tr}(\xi^i I) \\ &= \frac{1}{p^{r+1}} \sum_{i=0}^{p-1} p^{mn} \\ &= p^{mn-r}. \end{aligned}$$

Noting that the total number of linear characters satisfying (20) equals p^r and that the dimension of the whole space is p^{mn}, we obtain $\dim(Q_{S,\mu}) \leq p^{mn-r}$. □

We shall say that $Q_{S,\mu}$ is an $[[n, mn-r]]_q$ quantum stabilizer code.

5 Connection with Classical Codes

Let us establish a connection between quantum stabilizer and classical selforthogonal codes. Note that since the error basis is obtained as a tensor product of p-ary error bases, stabilizer codes can be viewed as p-ary stabilizer codes. This situation is essentially the same as for classical linear codes over $\mathbf{F}_{p^m}$. However, since the goal is to protect against errors on p^m-ary systems, we wish to usefully relate p^m-ary stabilizer codes to classical codes over $\mathbf{F}_{p^{2m}}$.

First we show how to construct a classical code from a quantum code. Let φ be an isomorphism of the vector space $\mathbf{F}_p^m$. Clearly the set $C = \{(\mathbf{a}, \varphi^{-1}\mathbf{b}) | E_{\mathbf{a},\mathbf{b}} \in S\}$ is an $\mathbf{F}_p$-linear code of length $2n$ and size p^r. Moreover, since all operators from S commute and because of (17) the following property holds (17) for any two vectors $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{a}', \mathbf{b}')$ from C

$$\langle \mathbf{a}, \varphi(\mathbf{b}') \rangle - \langle \mathbf{a}', \varphi(\mathbf{b}) \rangle = 0. \tag{22}$$

Thus C is selforthogonal with respect to the inner product defined by $(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \langle \mathbf{a}, \varphi(\mathbf{b}') \rangle - \langle \mathbf{a}', \varphi(\mathbf{b}) \rangle$. Later we will choose φ to relate the inner product to the structure of $\mathbf{F}_{p^m}$.

The minimum distance of a stabilizer code defined by S is related to the classical minimum distance of $C^\perp \setminus C$, where $C^\perp$ is the dual code of C with respect to (22). Define the weight of $\mathbf{v} = (\mathbf{a}, \mathbf{b}) \in \mathbf{F}_{p^m}^{2n}$ as

$$\mathrm{wt}(\mathbf{v}) = |\{i : a^{(i)} \neq 0 \text{ or } b^{(i)} \neq 0\}|.$$

Theorem 3 *The minimum distance of a stabilizer code of S equals* $\min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$.

PROOF. Our proof generalizes the arguments of [6].

Denote by $S^\perp$ the group of operators in $\mathcal{E}$ that commute with all operators from S. Thus $S^\perp$ is given by $S^\perp = \{\xi^i E_{\mathbf{a},\mathbf{a}} | (\mathbf{a}, \varphi^{-1}\mathbf{b}) \in C^\perp\}$. The desired fact follows from the observation that $E' \in \mathcal{E}$ is detectable iff $E' \notin S^\perp \setminus S$. Let P be as defined earlier. We consider three cases.

1. Let $E' \in S$. Then

$$\begin{aligned} E'P &= \frac{1}{|S|} \sum_{E \in S} \bar{\mu}(E) E'E \\ &= \frac{1}{|S|} \sum_{E \in S} \bar{\mu}((E')^\dagger E) E \\ &= \mu(E')P, \end{aligned} \tag{23}$$

   where the last equality follows from linearity of μ. Thus

$$PE'P = \mu(E')P$$

   and hence E' is detectable.

2. Let $E' \notin S^\perp$. Let S_i, $0 \le i < p$, be defined by $S_i = \{E \in S : E'E = \xi^i EE'\}$. Then from (17) and the assumption, it follows that $|S_i| = |S|/p$. Thus

$$\begin{aligned} |S|PE'P &= \sum_{E\in S} \bar{\mu}(E)EE'P \\ &= E'\sum_{i=0}^{p-1}\sum_{E\in S_i} \xi^i \bar{\mu}(E)EP \\ &= E'\sum_{i=0}^{p-1}\sum_{E\in S_i} \xi^i P \\ &= E'\sum_{i=0}^{p-1} \xi^i P|S|/p \qquad (24) \\ &= 0, \qquad (25) \end{aligned}$$

where we used (23) in the third to last step. Again, E' is detectable.

3. Let $E' \in S^\perp \setminus S$. By taking T to be the commutative subgroup generated by S and E' and extending the character μ to T, a subcode Q' of Q is obtained corresponding to the extended character. The dimension of Q' is smaller by a factor of p, which implies that Q is not an eigenspace of E'. Since E' commutes with S, E' preserves Q. All of this implies that $PE'P$ is not proportional to P. □

The inner product defined in (22) depends on the isomorphism φ. Clearly, the set of codes obtained does not depend on φ, so the choice of φ is primarily one of convenience. We now standardize this choice to simplify the construction of large minimum distance codes. With respect to our distinguished basis of $\mathbf{F}_{p^m}$, φ is given by an $m \times m$ matrix M over $\mathbf{F}_p$. Choose M by defining

$$M_{i,j} = \mathrm{tr}(\alpha_i \alpha_j).$$

With $a^T = (a_1, a_2, \ldots, a_m), b^T = (b_1, b_2, \ldots, b_m) \in \mathbf{F}_{p^m}$, we compute

$$\begin{aligned} a^T M b &= \sum_{i=1}^m \sum_{j=1}^m a_i b_j \,\mathrm{tr}(\alpha_i \alpha_j) \\ &= \sum_{i=1}^m \sum_{j=1}^m \mathrm{tr}(a_i b_j \alpha_i \alpha_j) \\ &= \mathrm{tr}\left(\left(\sum_{i=1}^m a_i \alpha_i\right)\left(\sum_{i=1}^m b_i \alpha_i\right)\right) \\ &= \mathrm{tr}(ab), \end{aligned}$$

where the product in the trace is multiplication in $\mathbf{F}_{p^m}$. For vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbf{F}_{p^m}^n$, let $\langle \mathbf{a}, \mathbf{b}\rangle_* = \sum_i a^{(i)} b^{(i)}$. With this choice of φ, C is therefore self-orthogonal with respect to the inner product defined by

$$(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \mathrm{tr}(\langle \mathbf{a}, \mathbf{b}'\rangle_* - \langle \mathbf{a}', \mathbf{b}\rangle_*). \qquad (26)$$

We can now construct a quantum stabilizer code from a classical selforthogonal code $C, |C| = p^r$. Let vectors $\mathbf{v}_i = (\mathbf{a}_i, \mathbf{b}_i), 0 \le i \le r-1$ form a basis of C over $\mathbf{F}_p$. Then the p^r operators $E_{\mathbf{a}_i, \varphi\mathbf{b}_i}$ together with $\xi I_{p^{mn}}$ generate a group of commuting operators of order p^{r+1}, which defines $[[n, mn-r]]_{p^m}$ stabilizer codes with minimum distance $d = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$.

In [5] a number of families of good classical codes that are selforthogonal with respect to the inner product

$$(\mathbf{a}, \mathbf{b}) * (\mathbf{a}', \mathbf{b}') = \langle \mathbf{a}, \mathbf{b}'\rangle_* - \langle \mathbf{a}', \mathbf{b}\rangle_* \qquad (27)$$

were constructed. Since a code that is selforthogonal with respect to (27) is also selforthogonal with respect to (26), our results establish a previously missing connection between the classical codes defined in [5] and quantum codes. Thus we already have many good nonbinary stabilizer codes. For instance from [5] we can obtain quantum stabilizer codes with parameters $[[q^r, q^r - (r+2), 3]]_q$, $[[q^2+1, q^2-3, 3]]_q$, $[[(q^{r+2}-1)/(q^2-1), (q^{r+2}-1)/(q^2-1) - (r+2), 3]]_q$ (r is even), $[[q^3(q^{r-1}-1)/(q^2-1), q^3(q^{r-1}-1)/(q^2-1) - (r+2), 3]]_q$ (r is odd), and others.

We also would like to note that if a code is $\mathbf{F}_{p^m}$-linear and is selforthogonal with respect to (26) then it is automatically selforthogonal with respect to (27). Since this does not hold for general $\mathbf{F}_p$-linear codes, one expects to find better codes selforthogonal with respect to (26) in this class.

To explicitly construct a family of good quantum codes we give a specific form of the relationship which takes us from classical to quantum codes. Let $\gamma \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ satisfy $\gamma^q = -\gamma + \gamma_0$, with $\gamma_0 \in \mathbf{F}_q$. Such γ exist, and $\{1, \gamma\}$ is a $\mathbf{F}_q$-linear basis of $\mathbf{F}_{q^2}$. D be a linear code of length n over $\mathbf{F}_{q^2}$ and $D^\perp$ be its dual code with respect to the inner product

$$\mathbf{vw} = \sum_{i=1}^n v_i w_i^q; \quad \mathbf{v}, \mathbf{w} \in \mathbf{F}_{q^2}^n. \qquad (28)$$

Note that w_i^q is the conjugate of w_i, so this is the generalization of the inner product used in [7]. Let C and $C^\perp$ be codes of length $2n$ over $\mathbf{F}_q$ obtained by expanding each symbol of D and $D^\perp$ (respectively) in the basis $\{1, \gamma\}$.

Theorem 4 *If $D \subseteq D^\perp$ then $C \subseteq C^\perp$ and $C^\perp$ is the dual code of C with respect to inner product (26).*

PROOF. The first statement is obvious. Let us prove the second statement.

Let $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in D, \mathbf{w} = (w_1, w_2, \ldots, w_n) \in D^\perp$. Let $v_i = v_i^{(1)} + \gamma v_i^{(2)}$ and $w_i = w_i^{(1)} + \gamma w_i^{(2)}$. Then

$$\begin{aligned} & \mathbf{vw} \\ = & \sum_{i=1}^{n} v_i w_i^q \\ = & \sum_{i=1}^{n} (v_i^{(1)} + \gamma v_i^{(2)})(w_i^{(1)} + (\gamma_0 - \gamma) w_i^{(2)}) \\ = & \sum_{i=1}^{n} v_i^{(1)} w_i^{(1)} + \gamma (v_i^{(2)} w_i^{(1)} - v_i^{(1)} w_i^{(2)}) \\ & + \gamma_0 v_i^{(1)} w_i^{(2)} + \gamma(\gamma_0 - \gamma) v_i^{(2)} w_i^{(2)}. \end{aligned} \quad (29)$$

Since this expression is 0 and $\gamma(\gamma_0 - \gamma) = \gamma\gamma^q \in \mathbf{F}_q$, it follows that

$$\sum_{i=1}^{n} v_i^{(2)} w_i^{(1)} - v_i^{(1)} w_i^{(2)} = 0$$

and the assertion follows. □

From this theorem the next corollary follows.

Corollary 1 *Let D be an $[n, (n-k)/2]_{q^2}$ selforthogonal code over $\mathbf{F}_{q^2}$ and let $d = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in D^\perp \setminus D\}$. Then there exists an $[[n, k]]_q$ quantum stabilizer code with minimum distance d.*

6 Good Nonbinary Codes Exists

In this section we prove that there exist p-ary quantum stabilizer codes that meet the Gilbert-Varshamov (GV) bound. One of the fundamental results of classical coding theory is the Gilbert-Varshamov bound. The classical bound asserts that for any δ, there exist r-ary codes, with relative minimum distance δ and rate R such that

$$R \geq 1 - H_r(\delta), \quad (30)$$

where $H_r(x) = -x \log_r(x) - (1-x) \log_r(1-x) + x \log_r(r-1)$.

Let Q be an $[[n, k_Q]]_q$ quantum stabilizer code associated with linear codes D and $D^\perp$ over $\mathbf{F}_{q^2}$. Recall that $R_Q = \frac{k_Q}{n}$ is the rate of Q and $R_{D^\perp}$ is the rate of $D^\perp$. It is easy to see that $R_Q = 2R_{D^\perp} - 1$. We shall say that Q meets the GV bound if $D^\perp$ does this, i.e., if

$$R_Q \geq 1 - 2H_{q^2}(\delta), \quad (31)$$

where $\delta = \frac{d}{n}$ is the relative minimum distance of Q.

Let $\mathcal{T}$ be the set of $[[n, k_Q]]_p$ quantum stabilizer codes associated with all $[n, (n-k_Q)/2]_{p^2}$ linear selforthogonal codes over $\mathbf{F}_{p^2}$.

Theorem 5 *In $\mathcal{T}$ there exists a code that meets GV bound (31).*

Remark The proof given here can be generalized to obtain the q-ary GV.

To prove the theorem one can use mostly the same arguments that have been used in the proof of its binary version, see Lemmata 2,3,4, and Theorem 5 from [3]. The sketch of the proof is following.

First we prove that the number of selforthogonal vectors in any code $D^\perp, D \subseteq D^\perp$, depends only on the length and dimension of $D^\perp$. Next, using this fact, we show that any nonzero selforthogonal vector occurs in one and the same number of codes $D^\perp$. Finally, this allows us to use averaging arguments to show the existence of a code $D^\perp$ that attains the GV bound (30), from which existence of corresponding quantum code immediately follows.

Remark In fact we prove even stronger result. Namely, we show the existence of a code $D^\perp$ with binomial distance distribution

$$A_i(D^\perp) \leq n^2 \binom{n}{i} (p-1)(p^2)^{n(R_{D^\perp} - 1)}.$$

One can look at [3] for details.

The only missing part of this proof is the first statement (Lemma 2 in [3]). We shall formulate and prove this missing part.

Lemma 6 *Let $D^\perp$ be an $[n,k]_{p^2}$ code such that $D \subseteq D^\perp$. Then the number of selforthogonal vectors in $D^\perp$ equals*

$$\frac{1}{p}\left((p^2)^k + (p-1)(-p)^n\right).$$

PROOF. Let $\mu \in \mathbf{F}_{p^2}$, and $\xi = e^{2\pi i/p}$. Then $\chi(\mu) = \xi^{\mathrm{tr}(\mu)}$ is an additive character of $\mathbf{F}_{p^2}$.

Let α be a primitive element of $\mathbf{F}_{p^2}$. We define $\alpha^\infty = 0$. Let us denote by $\mathbf{t_u} = \mathbf{t} = (t_\infty, t_0, \ldots, t_{p^2-2})$ the composition of a vector $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbf{F}_{p^2}^n$, that is, t_i is the number of components u_j equal to α^i. We denote by $A_\mathbf{t}$ and $A_\mathbf{t}^\perp$ the number of codewords of D and $D^\perp$ respectively with the composition $\mathbf{t}$. From the standard arguments of the proof of MacWilliams identities and from the definition of duality (28) it follows that

$$\sum_{\mathbf{t}} A_\mathbf{t}^\perp z_\infty^{t_\infty} z_0^{t_0} \ldots z_{p^2-2}^{t_{p^2-2}} = \frac{1}{|D|}\sum_{\mathbf{t}} A_\mathbf{t} \prod_{s=\infty}^{p^2-2}\left[\sum_{i=\infty}^{p^2-2}\chi(\alpha^{sp}\alpha^i) z_i\right]^{t_s}. \quad (32)$$

We can rewrite the rhs of (32) as follows

$$\frac{1}{|D|}\sum_{\mathbf{t}} A_\mathbf{t}\left[\sum_{i=\infty}^{p^2-2} z_i\right]^{t_\infty} \prod_{s=0}^{p^2-2}\left[\sum_{j=0}^{p-2}\sum_{i=0}^{p}\chi(\alpha^{sp}\alpha^{j+i(p-1)}) z_{j+i(p-1)}\right]^{t_s}.$$

Let us put $z_{j+i(p-1)} = y_j, 0 \le i \le p; 0 \le j \le p-2$, $y_\infty = z_\infty, r_j = \sum_{i=0}^{p} t_{j+i(p-1)}$, and $r_\infty = t_\infty$. Then we have

$$\sum_{\mathbf{r}} A_\mathbf{r}^\perp y_\infty^{r_\infty} y_0^{r_0} \ldots y_{p-2}^{r_{p-2}} = \frac{1}{|D|}\sum_{\mathbf{r}} A_\mathbf{r}\left[y_\infty + \sum_{j=0}^{p-2} y_j(p+1)\right]^{r_\infty} \prod_{s=0}^{p-2}\left[y_\infty + \sum_{j=0}^{p-2} y_j \sum_{i=0}^{p}\chi(\alpha^s\alpha^{j+i(p-1)})\right]^{r_s} \quad (33)$$

Now for $l = \infty, 0, \ldots, p-2$ let us put $y_j = \xi^{\alpha^{(j-l)(p+1)}}$. Then for lhs of (33) we have

$$\sum_{l=\infty}^{p-2}\sum_{\mathbf{r}} A_\mathbf{r}^\perp y^\infty y^0 \ldots y^{r_{p-2}} = \sum_{\mathbf{r}} A_\mathbf{r}^\perp\left(1 + \sum_{l=0}^{p-2}\xi^{f(l)}\right), \quad (34)$$

where

$$f(l) = \alpha^{-l(p+1)}\sum_{j=0}^{p-2} r_j \alpha^{j(p+1)}.$$

It is obvious that for a selforthogonal vector

$$\sum_{j=0}^{p-2} r_j \alpha^{j(p+1)} = 0. \quad (35)$$

From this it follows that (34) equals $p\sum A_\mathbf{r}^\perp$, where the sum runs over compositions of all selforthogonal vectors from $D^\perp$.

Now let us estimate the sum

$$\sum_{l=\infty}^{p-2} \text{rhs of (33)}. \quad (36)$$

The first term in the sum, i.e. when $l = \infty$, equals

$$\frac{1}{|D|}\sum_{\mathbf{r}} A_\mathbf{r}(p^2)^{r_\infty} 0^{r_0} \ldots 0^{r_{p-2}} = \frac{1}{|D|}(p^2)^n. \quad (37)$$

For any $l \ge 0$ we have

$$y_\infty + \sum_{j=0}^{p-2} y_j(p+1) = -p. \quad (38)$$

Further, for any $l \ge 0$ and any $s \ge 0$ we have

$$\begin{aligned} & y_\infty + \sum_{j=0}^{p-2} y_j \sum_{i=0}^{p}\chi(\alpha^{s+j+i(p-1)}) \\ = \; & 1 + \sum_{j=0}^{p-2}\sum_{i=0}^{p}\xi^{\mathrm{tr}\left(\alpha^{s+j+i(p-1)}\right)+\alpha^{(j-l)(p+1)}} \\ = \; & 1 + \sum_{j=0}^{p-2}\sum_{i=0}^{p}\xi^{\mathrm{tr}\left(\alpha^{s+j+i(p-1)}+\frac{p+1}{2}\alpha^{(j-l)(p+1)}\right)} \\ = \; & 1 + \sum_{j=0}^{p-2}\sum_{i=0}^{p}\xi^{\mathrm{tr}\left(\alpha^{j+i(p-1)}+\frac{p+1}{2}\frac{\alpha^{(j+i(p-1))(p+1)}}{\alpha^{(l+s)(p+1)}}\right)} \\ = \; & \sum_{\mu\in\mathbf{F}_{p^2}}\xi^{\mathrm{tr}\left(\mu+\frac{p+1}{2}\frac{1}{\alpha^{(l+s)(p+1)}}\mu^{p+1}\right)}. \end{aligned}$$

From Theorem 3 of [8] it follows that the last sum equals

$$(-p) \cdot \xi^{(p-1)\alpha^{(l+s)(p+1)}} \tag{39}$$

Substituting (38), (37), and (39) into (36) and using the fact that D is selforthogonal, we obtain

$$\begin{aligned}
&\sum_{l=\infty}^{p-2} \text{rhs of (33)} \\
&= \frac{1}{|D|}\left[(p^2)^n + \sum_{l=0}^{p-2}\sum_{\mathbf{r}} A_{\mathbf{r}}(-p)^{\sum_{s=\infty}^{p-2} r_s}\xi^{h(l)}\right] \\
&\quad (\text{were } h(l) = (p-1)\alpha^{l(p+1)}\sum_{s=0}^{p-2} r_s\alpha^{s(p+1)}) \\
&= \frac{1}{|D|}\left[(p^2)^n + \sum_{l=0}^{p-2}\sum_{\mathbf{r}} A_{\mathbf{r}}(-p)^n\right] \\
&= \frac{1}{|D|}(p^2)^n + (p-1)(-p)^n
\end{aligned}$$

and the assertion of the lemma follows. □

Acknowledgments. E. K. was supported by funding from NSA and DOE.

References

[1] A. Ashikhmin and S. Litsyn, "Upper bounds of the size of quantum codes," *IEEE Trans. Info. Theory*, vol 45, no. 4, pp.1205-1215, 1999.

[2] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum Error Detection I: Statement of the Problem ," *IEEE Trans. Info. Theory*, no. 3, pp. 778–789, 2000.

[3] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum Error Detection I: Statement of the Problem ," *IEEE Trans. Info. Theory*, no. 3, pp. 778–789, 2000.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error-correcting codes," *Phys. Rev. A*, vol. 54, pp. 3824–, 1996.

[5] J. Bierbrauer and Y. Edel, "Quantum Twisted Codes," *preprint*, 1998. (The paper is available at "http://www.math.mtu.edu/ jbierbra/".)

[6] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-409, 1997.

[7] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$,"*IEEE Trans. Info. Theory*, vol. 44, pp.1369 –1387, 1998.

[8] L. Carlitz, "Evaluation of some exponential sums over a finite field," *Math. Nachr.*, vol. 96, pp. 13–20, 1980.

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

[10] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," *Ph.D. Thesis,* California Institute of Technology, Pasadena, California, 1997.

[11] E. Knill, "Non-binary Unitary Error Bases and Quantum Codes," *LANL Preprint*, quant-ph/9608048, 1996.

[12] E. Knill, "Group Representations, Error Bases and Quantum Codes," *LANL Preprint*, quant-ph/9608049, 1996.

[13] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900-911, 1997.

[14] E. Knill, R. Laflamme and L. Viola, "Theory of quantum error correction for general noise", *Phys. Rev. Lett.*, vol. 84, pp. 2525-2528, 2000.

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

[16] E. Rains, Nonbinary quantum codes, LANL e-print quant-ph/9703048.

[17] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S.Goldwasser, Editor, IEEE Computer Society Press, Los Alamitos, CA, p.124, 1994.

[18] P.W. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A, **52**, p. 2493, 1995.

[19] P.W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

[20] J.P. Serre, *Linear Representaion of Finite Groups*, Springer-Verlag, 1977.

[21] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*,vol. 77, pp. 793-797, 1996.

[22] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. London A*, vol. 452, pp. 2551-2577, 1996.