Chapter 1

Nonbinary Stabilizer Codes

Pradeep Kiran Sarvepalli

Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA, pradeep@cs.tamu.edu

Salah A. Aly

Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA, salah@cs.tamu.edu

Andreas Klappenecker

Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA, klappi@cs.tamu.edu

Abstract Recently, the field of quantum error-correcting codes has rapidly emerged as an important discipline. As quantum information is extremely sensitive to noise, it seems unlikely that any large scale quantum computation is feasible without quantum error-correction. In

this paper we give a brief exposition of the theory of quantum stabilizer codes. We review the stabilizer formalism of quantum codes, establish the connection between classical codes and stabilizer codes and the main methods for constructing quantum codes from classical codes. In addition to the expository part, we include new results that cannot be found elsewhere. Specifically, after reviewing some important bounds for quantum codes, we prove the nonexistence of pure perfect quantum stabilizer codes with minimum distance greater than 3. Finally, we illustrate the general methods of constructing quantum codes from classical codes by explicitly constructing two new families of quantum codes and conclude by showing how to construct new quantum codes by shortening.

1.1 Introduction

Quantum error-correcting codes were introduced by Shor [54] in the wake of serious doubts cast over the practical implementation of quantum algorithms. Since then the field has made rapid progress and the pioneering works of Gottesman and Calderbank et al., [10, 22] revealed a rich structure underlying the theory of quantum stabilizer codes. Their work spurred many researchers to study binary quantum codes, see [5–7, 9, 11, 14–17, 21, 23, 24, 26–30, 32, 37, 38, 40, 47, 50, 54, 56–59]. The theory was later extended to the nonbinary case [1–3, 8, 12, 13, 18, 19, 25, 31, 33, 36, 39, 45, 48, 49, 51–53]. This paper surveys the theory of nonbinary stabilizer codes – arguably, the most important class of quantum codes. There exists sufficient machinery to describe them compactly and make useful connections with classical coding theory. Moreover, they are very amenable to fault-tolerant implementation which makes them very attractive from a practical point of view.

We aim to provide an accessible introduction to the theory of nonbinary quantum codes. Section 1.2 gives a brief overview of the main ideas of stabilizer codes while Section 1.3 reviews the relation between quantum stabilizer codes and classical codes. This connection makes it possible to reduce the study of quantum stabilizer codes to the study of self-orthogonal classical codes, though the definition of self-orthogonality is a little broader than the classical one. Further, it allows us to use all the tools of classical codes to derive bounds on the parameters of good quantum codes. Section 1.4 gives an overview of the important bounds

for quantum codes. Finally, Section 1.5 illustrates the general ideas behind quantum code construction by constructing the quantum Hamming codes, some cyclic quantum codes and codes from projective geometry.

While this paper is primarily an exposition of the theory of nonbinary stabilizer codes, we also included new results. For instance, we prove the nonexistence of pure perfect quantum codes with distance greater than 3. Furthermore, we derive two new families of quantum codes, the quantum projective Reed-Muller codes and the quantum m-adic residue codes. Finally, we illustrate the key ideas of shortening quantum codes by taking the newly introduced quantum projective Reed-Muller codes as an example.

We tried to keep the prerequisites to a minimum, though we assume that the reader has a minimal background in quantum computing. Some familiarity with classical coding theory will help; we recommend [34] and [46] as references. In general, we omitted long proofs of basic material – readers interested in more details should consult [36]. However, we made an effort to keep the overlap with [36] to a minimum, although some material is repeated here to make this chapter reasonably self-contained.

Notations. The finite field with q elements is denoted by $\mathbf{F}_q$, where $q = p^m$ and p is assumed to be a prime. The trace function from $\mathbf{F}_{q^l}$ to $\mathbf{F}_q$ is defined as $\mathrm{tr}_{q^l/q}(x) = \sum_{k=0}^{l-1} x^{q^k}$, and we may omit the subscripts if $\mathbf{F}_q$ is the prime field. The center of a group G is denoted by $Z(G)$ and the centralizer of a subgroup S in G by $C_G(S)$. We denote by $H \leq G$ 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.

1.2 Stabilizer Codes

In this chapter, we use q-ary quantum digits, shortly called qudits, as the basic unit of quantum information. The state of a qudit is a nonzero vector in the complex vector space $\mathbf{C}^q$. This vector space is equipped with an orthonormal basis whose elements are denoted by $|x\rangle$, where x is an element of the finite field $\mathbf{F}_q$. The state of a system of n qudits is then a nonzero vector in $\mathbf{C}^{q^n}$. In general, quantum codes are just

nonzero subspaces[1] of $\mathbf{C}^{q^n}$. A quantum code that encodes k qudits of information into n qudits is denoted by $[[n,k]]_q$, where the subscript q indicates that the code is q-ary. More generally, an $((n,K))_q$ quantum code is a K-dimensional subspace encoding $\log_q K$ qudits into n qudits.

As the codes are subspaces, it seems natural to describe them by giving a basis for the subspace. However, in case of quantum codes this turns out to be an inconvenient description.[2] An alternative description of the quantum error-correcting code that are discussed in this chapter relies on error operators that act on $\mathbf{C}^{q^n}$. If we make the assumption that the errors are independent on each qudit, then each error operator E can be decomposed as $E = E_1 \otimes \cdots \otimes E_n$. Furthermore, linearity of quantum mechanics allows us to consider only a discrete set of errors. The quantum error-correcting codes that we consider here can be described as the joint eigenspace of subgroup of error operators. The subgroup of error operators is called the stabilizer of the code (because it leaves each state in the code unaffected) and the code is called a stabilizer code.

1.2.1 Error Bases

In general, we can regard any error as being composed of an amplitude error and a phase error. Let a and b be elements in $\mathbf{F}_q$. We can define unitary operators $X(a)$ and $Z(b)$ on $\mathbf{C}^q$ that generalize the Pauli X and Z operators to the q-ary case; they are defined as

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

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

Let $\mathcal{E} = \{X(a)Z(b) \,|\, a,b \in \mathbf{F}_q\}$ be the set of error operators. The error operators in $\mathcal{E}$ form a basis of the set of complex $q \times q$ matrices as the trace $\mathrm{Tr}(A^\dagger B) = 0$ for distinct elements A, B of $\mathcal{E}$. Further, we observe that

$$X(a)Z(b)\,X(a')Z(b') = \omega^{\mathrm{tr}(ba')}X(a+a')Z(b+b'). \tag{1.1}$$

[1] The more recent concept of an operator quantum error-correcting code generalizes this notion, but can be reduced to traditional error-correcting codes.

[2] For instance, for the $[[7,1]]_2$ code the basis is

$$\begin{aligned}|0_L\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &\quad +|0001111\rangle + |0111100\rangle + |1011010\rangle + |1101001\rangle, \\ |1_L\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &\quad +|0001111\rangle + |0111100\rangle + |1011010\rangle + |1101001\rangle,\end{aligned}$$

.

The error basis for n q-ary quantum systems can be obtained by tensoring the error basis for each system. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{F}_q^n$. Let us denote by $X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{a}) = Z(a_1) \otimes \cdots \otimes Z(a_n)$ for the tensor products of n error operators. Then we have the following result whose proof follows from the definitions of $X(\mathbf{a})$ and $Z(\mathbf{b})$.

LEMMA 1.1
The set $\mathcal{E}_n = \{X(\mathbf{a})Z(\mathbf{b}) \,|\, \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n\}$ *is an error basis on the complex vector space* $\mathbf{C}^{q^n}$.

1.2.2 Stabilizer Codes

Consider the error group G_n defined as

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

G_n is simply a finite group of order pq^{2n} generated by the matrices in the error basis $\mathcal{E}_n$.

Let S be an abelian subgroup of G_n, then a *stabilizer code* Q is a non-zero subspace of $\mathbf{C}^{q^n}$ defined as

$$Q = \bigcap_{E \in S} \{v \in \mathbf{C}^{q^n} \mid Ev = v\}. \tag{1.2}$$

Alternatively, Q is the joint $+1$ eigenspace of S. A stabilizer code contains *all* joint eigenvectors of S with eigenvalue 1, as equation (1.2) indicates. If the code is smaller and does not contain all the joint eigenvectors of S with eigenvalue 1, then it is not a stabilizer code for S.

1.2.3 Stabilizer and Error Correction

Now that we have a handle on the quantum code through its stabilizer, we next need to be able to describe the performance of the code, that is, we should be able to tell how many errors it can detect (or correct) and how the error-correction is done.

The central idea of error detection is that a detectable error acting on Q should either act as a scalar multiplication on the code space (in which case the error did not affect the encoded information) or it should map the encoded state to the orthogonal complement of Q (so that one can set up a measurement to detect the error). Specifically, we say that 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 [43].

We can show 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 1.2. In particular, an undetectable error in G_n has to commute with all elements of the stabilizer.

Let $S \leq G_n$ and $C_{G_n}(S)$ denote the centralizer of S in G_n,

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

Let $SZ(G_n)$ denote the group generated by S and the center $Z(G_n)$. We need the following characterization of detectable errors.

LEMMA 1.2

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 See [36]. See also [3]; the interested reader can find a more general approach in [41, 42]. ∎

Since detectability of errors is closely associated to commutativity of error operators, we will derive the following condition on commuting elements in G_n:

LEMMA 1.3

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 We can easily verify that $EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}')} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$ and $E'E = \omega^{\mathrm{tr}(\mathbf{b}'\cdot\mathbf{a})} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$ using equation (1.1). Therefore, $\omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})} E'E$ yields EE', as claimed. ∎

1.2.4 Minimum Distance

The *symplectic weight* swt of a vector $(\mathbf{a}|\mathbf{b})$ in $\mathbf{F}_q^{2n}$ is defined as

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

The weight $\mathrm{w}(E)$ of an element $E = \omega^c E_1 \otimes \cdots \otimes E_n = \omega^c X(\mathbf{a}) Z(\mathbf{b})$ in the error group G_n is defined to be the number of nonidentity tensor components i.e., $\mathrm{w}(E) = |\{E_i \neq I\}| = \mathrm{swt}((\mathbf{a}|\mathbf{b}))$.

A quantum code Q is said to have *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. 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.

Due to the linearity of quantum mechanics, a quantum error-correcting code that can detect a set $\mathcal{D}$ of errors, can also detect all errors in the linear span of $\mathcal{D}$. A code of minimum distance d can correct all errors of weight $t = \lfloor (d-1)/2 \rfloor$ or less.

1.2.5 Pure and Impure 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 error operators of weight less than t. A quantum code is called pure if and only if it is pure to its minimum distance. We will follow the same convention as in [10], that an $[[n, 0, d]]_q$ code is pure. Impure codes are also referred to as degenerate codes. Degenerate codes are of interest because they have the potential for passive error-correction.

1.2.6 Encoding Quantum Codes

Stabilizer also provides a means for encoding quantum codes. The essential idea is to encode the information into the code space through a projector. For an $((n, K, d))_q$ quantum code with stabilizer S, the projector is P is defined as

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

P is an orthogonal projector onto a vector space Q. Further, we have

$$K = \dim Q = \mathrm{Tr}\, P = q^n / |S|.$$

The stabilizer allows us to derive encoded operators, so that we can operate directly on the encoded data instead of decoding and then operating on them. These operators are in $C_{G_n}(S)$. See [24] and [33] for more details.

1.3 Quantum Codes and Classical Codes

In this section we show how stabilizer codes are related to classical codes (additive codes over $\mathbf{F}_q$ or over $\mathbf{F}_{q^2}$). The central idea behind this relation is the fact insofar as the detectability of an error is concerned the phase information is irrelevant. This means we can factor out the phase defining a map from G_n onto $\mathbf{F}_q^{2n}$ and study the images of S and $C_{G_n}(S)$. We will denote a classical code $C \leq \mathbf{F}_q^n$ with K codewords and distance d by $(n, K, d)_q$. If it is linear then we will also denote it by $[n, k, d]_q$ where $k = \log_q K$. The dual code $C^\perp$ is the set of vectors in $\mathbf{F}_q^n$ orthogonal to C i.e., $C^\perp = \{x \in \mathbf{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\}$. For more details on classical codes see [34] or [46].

1.3.1 Codes over $\mathbf{F}_q$.

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

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

Let $C^{\perp_s}$ be the trace-symplectic dual of C defined as

$$C^{\perp_s} = \{x \in \mathbf{F}_q^{2n} \mid \langle x| \, c\rangle_s = 0 \text{ for all } c \in C\}.$$

The centralizer $C_{G_n}(S)$ contains all elements of G_n that commute with each element of S; thus, by Lemma 1.3, $C_{G_n}(S)$ 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 next theorem crystallizes this connection between classical codes and stabilizer code and generalizes the well-known connection to symplectic codes [10, 22] of the binary case.

THEOREM 1.1

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 $\mathrm{swt}(C^{\perp_s} \backslash C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$).

PROOF See [3] or [36] for the proof. ∎

In 1996, Calderbank and Shor [11] and Steane [58] introduced the following method to construct quantum codes. It is perhaps the simplest method to build quantum codes via classical codes over $\mathbf{F}_q$.

LEMMA 1.4

[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 a $[[n, k_1 + k_2 - n, d]]_q$ 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 $C = C_1^{\perp} \times C_2^{\perp} \leq \mathbf{F}_q^{2n}$. Clearly $C \leq C_2 \times C_1$. If $(c_1 \mid c_2) \in C$ and $(c_1' \mid c_2') \in C_2 \times C_1$, then we observe that

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

Therefore, $C \leq C_2 \times C_1 \leq C^{\perp_s}$. Since $|C| = q^{2n-k_1-k_2}$, $|C^{\perp_s}| = q^{2n}/|C| = q^{k_1+k_2} = |C_2 \times C_1|$. Therefore, $C^{\perp_s} = C_2 \times C_1$. By Theorem 1.1 there exists an $((n, K, d))_q$ quantum code with $K = q^n/|C| = q^{k_1+k_2-n}$. The claim about the minimum distance and purity of the code is obvious from the construction. ∎

COROLLARY 1.1

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.

1.3.2 Codes over $\mathbf{F}_{q^2}$.

Sometimes it is more convenient to extend the connection of the quantum codes to codes over $\mathbf{F}_{q^2}$, especially as it allows us the use of codes over quadratic extension fields. The binary case was done in [10] and partial generalizations were done in [39, 48] and [49]. We provide a slightly alternative generalization using a trace-alternating 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

$$\langle v|w\rangle_a = \mathrm{tr}_{q/p}\left(\frac{v\cdot w^q - v^q\cdot w}{\beta^{2q}-\beta^2}\right). \tag{1.3}$$

The argument of the trace is an element of $\mathbf{F}_q$ as it is invariant under the Galois automorphism $x \mapsto x^q$.

Let $\phi : \mathbf{F}_q^{2n} \to \mathbf{F}_{q^2}^n$ take $(\mathbf{a}|\mathbf{b}) \mapsto \beta\mathbf{a} + \beta^q\mathbf{b}$. The map ϕ is isometric in the sense that the symplectic weight of $(\mathbf{a}|\mathbf{b})$ is equal to the Hamming weight of $\phi((\mathbf{a}|\mathbf{b}))$. This map allows us to transform the trace-symplectic duality into trace-alternating duality. In particular it can be easily verified that if $c, d \in \mathbf{F}_q^{2n}$, then $\langle c \,|\, d\rangle_s = \langle \phi(c) \,|\, \phi(d)\rangle_a$. If $D \leq \mathbf{F}_{q^2}^n$, then we denote its trace-alternating dual by $D^{\perp_a} = \{v \in \mathbf{F}_{q^2}^n \mid \langle v|w\rangle_a = 0 \text{ for all } w \in D\}$. Now Theorem 1.1 can now be reformulated as:

LEMMA 1.5
Suppose that c and d are two vector 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

$$\phi(c)\cdot\phi(d)^q = \beta^{q+1}\,\mathbf{a}\cdot\mathbf{a}' + \beta^2\,\mathbf{a}\cdot\mathbf{b}' + \beta^{2q}\,\mathbf{b}\cdot\mathbf{a}' + \beta^{q+1}\,\mathbf{b}\cdot\mathbf{b}'$$
$$\phi(c)^q\cdot\phi(d) = \beta^{q+1}\,\mathbf{a}\cdot\mathbf{a}' + \beta^{2q}\,\mathbf{a}\cdot\mathbf{b}' + \beta^2\,\mathbf{b}\cdot\mathbf{a}' + \beta^{q+1}\,\mathbf{b}\cdot\mathbf{b}'$$

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

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

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

THEOREM 1.2
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 $D \leq D^{\perp_a}$ and $\mathrm{wt}(D^{\perp_a} \setminus D) = d$ if $K > 1$ (and $\mathrm{wt}(D^{\perp_a}) = d$ if $K = 1$).

PROOF From Theorem 1.1 we know that an $((n, K, d))_q$ stabilizer code exists if and only if there exists a code $C \leq \mathbf{F}_q^{2n}$ such that $|C| = q^n/K$, $C \leq C^{\perp_s}$, and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$). The theorem follows simply by applying the isometry ϕ. ∎

If we restrict our attention to linear codes over $\mathbf{F}_{q^2}$, then the hermitian form is more useful. The hermitian inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbf{F}_{q^2}^n$ is given by $\mathbf{x}^q \cdot \mathbf{y}$. From the definition of the trace-alternating form it is clear that if two vectors are orthogonal with respect to the hermitian form they are also orthogonal with respect to the trace-alternating form. Consequently, if $D \leq \mathbf{F}_{q^2}^n$, then $D^{\perp_h} \leq D^{\perp_a}$, where $D^{\perp_h} = \{v \in \mathbf{F}_{q^2}^n \mid v^q \cdot w = 0 \text{ for all } w \in D\}$.

LEMMA 1.6
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 $D \leq \mathbf{F}_{q^2}^n$, then $D^{\perp_h} \leq D^{\perp_a}$.

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.

COROLLARY 1.2
If there exists an $\mathbf{F}_{q^2}$-linear $[n, k, d]_{q^2}$ code D such that $D^{\perp_h} \leq D$, then

there exists an $[[n, 2k-n, \geq d]]_q$ *quantum code that is pure to* d.

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 a $(n-k)$-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 $D^{\perp_a} = D^{\perp_h}$. The claim follows from Theorem 1.2. ∎

So it is sufficient to consider the hermitian form in case of $\mathbf{F}_{q^2}$-linear codes. For additive codes (that are not linear) over $\mathbf{F}_{q^2}$ we have to use the rather inconvenient trace-alternating form.

1.4 Bounds on Quantum Codes

We need some bounds on the achievable minimum distance of a quantum stabilizer code. Perhaps the simplest one is the Knill-LaFlamme bound, also called the quantum Singleton bound. The binary version of the quantum Singleton bound was first proved by Knill and Laflamme in [43], see also [4, 6], and later generalized by Rains using weight enumerators in [49].

THEOREM 1.3 Quantum Singleton Bound
An $((n, K, d))_q$ *stabilizer code with* $K > 1$ *satisfies*

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

Codes which meet the quantum Singleton bound are called quantum MDS codes. In [36] we showed that these codes cannot be indefinitely long and showed that the maximal length of a q-ary quantum MDS codes is upper bounded by $2q^2 - 2$. This could probably be tightened to $q^2 + 2$. It would be interesting to find quantum MDS codes of length greater than $q^2 + 2$ since it would disprove the MDS Conjecture. A related open question is regarding the construction of codes with lengths between q and $q^2 - 1$. At the moment there are no analytical methods for constructing a quantum MDS code of arbitrary length in this range (see [31] for some numerical results).

Another important bound for quantum codes is the quantum Hamming bound. The quantum Hamming bound states (see [20, 22]) that:

THEOREM 1.4 Quantum Hamming Bound
Any pure $((n, K, d))_q$ *stabilizer code satisfies*

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

While the quantum Singleton bound holds for all quantum codes, it is not known if the quantum Hamming bound is of equal applicability. So far no degenerate quantum code has been found that that beats this bound. Gottesman showed that impure single and double error-correcting binary quantum codes cannot beat the quantum Hamming bound [24].

Perfect Quantum Codes. A quantum code that meets the quantum Hamming bound with equality is known as a perfect quantum code. In fact the famous $[[5, 1, 3]]_2$ code [44] is one such. We will show that there do not exist any pure perfect quantum codes other than the ones mentioned in the following theorem. It is actually a very easy result and follows from known results on classical perfect codes, but we had not seen this result earlier in the literature.

THEOREM 1.5
There do not exist any pure perfect quantum codes with distance greater than 3.

PROOF Assume that Q is a pure perfect quantum code with the parameters $((n, K, d))_q$. Since it meets the quantum Hamming bound we have

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

By Theorem 1.2 the associated classical code C is such that $C^{\perp_a} \leq C \leq \mathbf{F}_{q^2}^n$ and has parameters $(n, q^n K, d)_{q^2}$. Its distance is d because the quantum code is pure. Now C obeys the classical Hamming bound

(see [34, Theorem 1.12.1] or any textbook on classical codes). Hence

$$|C| = q^n K \leq \frac{q^{2n}}{\sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (q^2-1)^j}.$$

Substituting the value of K we see that this implies that C is a perfect classical code. But the only perfect classical codes with distance greater than 3 are the Golay codes and the repetition codes [34]. The perfect Golay codes are over $\mathbf{F}_2$ and $\mathbf{F}_3$ not over a quadratic extension field as C is required to be. The repetition codes are of dimension 1 and cannot contain their duals as C is required to contain. Hence C cannot be anyone of them. Therefore, there are no pure quantum codes of distance greater than 3 that meet the quantum Hamming bound. ∎

Since it is not known if the quantum Hamming bound holds for degenerate quantum codes, it would be interesting to find degenerate quantum codes that either meet or beat the quantum Hamming bound.

1.5 Families of Quantum Codes

We shall now restrict our attention to linear quantum codes and derive several families of quantum codes from classical linear codes. We make use of the CSS construction given in Lemma 1.4. Hence, we need to look for classical codes that are self-orthogonal with respect to the euclidean product or for families of nested codes.

1.5.1 Quantum m-adic Residue Codes

In this section we will construct a family of quantum codes based on the m-adic residue codes. These codes are a generalization of the well-known quadratic residue codes and share many of their structural properties. Quantum quadratic residue codes were first constructed by Rains [49] for prime alphabet.

Let $Q_0 = \{\alpha^m | \alpha \in \mathbf{Z}_p^\times\}$ be the m-adic residues of $\mathbf{Z}_p^\times$, where p is a prime. And let $Q_i = b^i Q_0$, where b is a generator of $\mathbf{Z}_p^\times$ and $i \in \{0, 1, \ldots, m-1\}$. Let α be a primitive root of pth root of unity. Then we can define the following four families of m-adic residue codes.

Let C_i be the cyclic code with the generator polynomial $g_i(x) = (x^p - 1)/\prod_{z\in Q_i}(x - \alpha^z)$. These codes C_i form the even-like codes of class I. Every code C_i has the parameters $[p, (p-1)/m]_q$. The complement of C_i is denoted by $\hat{C}_i$ and its generator polynomial is given by $\hat{g}_i(x) = \prod_{z\in Q_i}(x - \alpha^z)$. These codes constitute the family of odd-like codes of class I. These codes have the parameters $[p, p - (p-1)/m]_q$.

The code with generator polynomial $h_i(x) = (x-1)\hat{g}_i(x)$ is denoted by D_i. It has parameters $[p, p - (p-1)/m - 1]_q$. These codes form the even-like codes of class II. The complement of D_i is denoted by $\hat{D}_i$ and its generator polynomial $\hat{h}_i(x) = g_i(x)/(x-1)$. The codes $\hat{D}_i$ make up the odd-like codes of class II. Their parameters are $[p, (p-1)/m + 1]_q$.

These definitions imply that $C_i \subset \hat{D}_i$ and $D_i \subset \hat{C}_i$. Further it can be shown that $C_i^\perp = \hat{C}_i$ and $D_i^\perp = \hat{D}_i$ [35, Theorem 2,3] if -1 is a m-adic residue. If -1 is not a residue, then $C_i \subseteq C_i^\perp = C_j$ and $D_i^\perp = D_j$, where $i \neq j$. We thus have families of nested codes and the CSS construction is applicable.

THEOREM 1.6
Let q be an m-adic residue modulo of a prime p such that $\gcd(p, q) = 1$. *Then there exists a quantum code with the parameters $[[p, 1, d]]_q$, where $d^m \geq p$. If -1 is a m-adic reside modulo p, then $(d^2 - d + 1)^{m/2} \geq p$.*

PROOF By the CSS construction there exists a quantum code with the parameters $[[p, (p-1)/m + 1 - (p-1)/m, d]]_q$, where $d = \mathrm{wt}\{(\hat{D}_i \setminus C_i) \cup (C_i^\perp \setminus \hat{D}_i^\perp)\}$.

If -1 is a m-adic residue modulo p, then we know from [35, Theorem 2,3] that $C_i^\perp = \hat{C}_i$ and $D_i^\perp = \hat{D}_i$. Since $C_i^\perp = \hat{C}_i$ and $\hat{D}_i^\perp = D_i$, this means $d = \mathrm{wt}\{(\hat{D}_i \setminus C_i) \cup (\hat{C}_i \setminus D_i)\}$. But this is the set of odd-like vectors in $\hat{C}_i$ and $\hat{D}_i$ which is lower bounded as $d^m \geq p$ [35, Theorem 5].

If -1 is a m-adic residue modulo p, then again from [35, Theorem 2,3] we know that $C_i \subseteq C_i^\perp = \hat{C}_j$ and $\hat{D}_i^\perp = D_j$ with $i \neq j$. Then $(d^2 - d + 1)^{m/2} \geq p$ by [35, Theorem 5]. ∎

1.5.2 Quantum Projective Reed-Muller Codes

We study projective Reed-Muller (PRM) codes and construct the corresponding quantum PRM codes. Let us denote by $\mathbf{F}_q[X_0, X_1, ..., X_m]$ the polynomial ring in $X_0, X_1, ..., X_m$ with coefficients in $\mathbf{F}_q$. Furthermore, let $\mathbf{F}_q[X_0, X_1, ..., X_m]_h^\nu \cup \{0\}$ be the vector space of homogeneous

polynomials in $X_0, X_1, ..., X_m$ with coefficients in $\mathbf{F}_q$ with degree ν (cf. [55]). Let $P^m(\mathbf{F}_q)$ be the m-dimensional projective space over $\mathbf{F}_q$.

Projective Reed-Muller Codes. The PRM code over $\mathbf{F}_q$ of integer order ν and length $n = (q^{m+1} - 1)/(q - 1)$ is denoted by $\mathcal{P}_q(\nu, m)$ and defined as

$$\mathcal{P}_q(\nu, m) = \{(f(P_1), ..., f(P_n) \,|\, f(X_0, ..., X_m) \in \mathbf{F}_q[X_0, ..., X_m]_h^\nu \cup \{0\}\}, \\ \text{and } P_i \in P^m(\mathbf{F}_q) \text{ for } 1 \leq i \leq n. \tag{1.4}$$

LEMMA 1.7

The projective Reed-Muller code $\mathcal{P}_q(\nu, m)$, $1 \leq \nu \leq m(q-1)$, is an $[n, k, d]_q$ code with length $n = (q^{m+1} - 1)/(q - 1)$, dimension

$$k(\nu) = \sum_{\substack{t=\nu \bmod (q-1) \\ t \leq \nu}} \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t - jq + m}{t - jq} \tag{1.5}$$

and minimum distance $d(\nu) = (q-s)q^{m-r-1}$ where $\nu = r(q-1)+s+1$, $0 \leq s < q-1$

PROOF See [55, Theorem 1]. ∎

The duals of PRM codes are also known and under some conditions they are also PRM codes. The following result gives more precise details.

LEMMA 1.8

Let $\nu^\perp = m(q-1) - \nu$, then the dual of $\mathcal{P}_q(\nu, m)$ is given by

$$\mathcal{P}_q(\nu, m)^\perp = \begin{cases} \mathcal{P}_q(\nu^\perp, m) & \nu \not\equiv 0 \bmod (q-1) \\ \text{Span}_{\mathbf{F}_q}\{1, \mathcal{P}_q(\nu^\perp, m)\} & \nu \equiv 0 \bmod (q-1) \end{cases} \tag{1.6}$$

PROOF See [55, Theorem 2]. ∎

As mentioned earlier our main methods of constructing quantum codes are the CSS construction and the Hermitian construction. This requires us to identify nested families of codes and/or self-orthogonal codes. First we identify when the PRM codes are nested i.e., we find out when a PRM code contains other PRM codes as subcodes.

LEMMA 1.9
If $\nu_2 = \nu_1 + k(q-1)$, where $k > 0$, then $\mathcal{P}_q(\nu_1, m) \subseteq \mathcal{P}_q(\nu_2, m)$ and $\mathrm{wt}(\mathcal{P}_q(\nu_2, m) \setminus \mathcal{P}_q(\nu_1, m)) = \mathrm{wt}(\mathcal{P}_q(\nu_2, m))$.

PROOF In $\mathbf{F}_q$, we can replace any variable x_i by x_i^q, hence every function in $\mathbf{F}_q[x_0, x_1, \ldots, x_m]_\nu^h$ is present in $\mathbf{F}_q[x_0, x_1, \ldots, x_m]_{\nu+k(q-1)}^h$. Hence $\mathcal{P}_q(\nu_1, m) \subseteq \mathcal{P}_q(\nu_2, m)$. Let $\nu_1 = r(q-1) + s + 1$, then $\nu_2 = (k+r)(q-1) + s + 1$. By Lemma 1.7, $d(\nu_1) = (q-s)q^{m-r-1} > (q-s)q^{m-r-k-1} = d(\nu_2)$. This implies that there exists a vector of weight $d(\nu_2)$ in $\mathcal{P}_q(\nu_2, m)$ and $\mathrm{wt}(\mathcal{P}_q(\nu_2, m) \setminus \mathcal{P}_q(\nu_1, m)) = \mathrm{wt}(\mathcal{P}_q(\nu_2, m))$. ∎

Quantum Projective Reed-Muller Codes. We now construct stabilizer codes using the CSS construction.

THEOREM 1.7
Let $n = (q^{m+1} - 1)/(q-1)$ and $1 \leq \nu_1 < \nu_2 \leq m(q-1)$ such that $\nu_2 = \nu_1 + l(q-1)$ with $\nu_1 \not\equiv 0 \bmod (q-1)$. Then there exists an $[[n, k(\nu_2) - k(\nu_1), \min\{d(\nu_2), d(\nu_1^\perp)\}]]_q$ stabilizer code, where the parameters $k(\nu)$ and $d(\nu)$ are given in Theorem 1.7.

PROOF A direct application of the CSS construction in conjunction with Lemma 1.9. ∎

We do not need to use two pairs of codes as we had seen in the previous two cases, we could use a single self-orthogonal code for constructing a quantum code. We will illustrate this idea by finding self-orthogonal PRM codes.

COROLLARY 1.3
Let $0 \leq \nu \leq \lfloor m(q-1)/2 \rfloor$ and $2\nu \equiv 0 \bmod q-1$, then $\mathcal{P}_q(\nu, m) \subseteq \mathcal{P}_q(\nu, m)^\perp$. If $\nu \not\equiv 0 \bmod q-1$ there exists an $[[n, n - 2k(\nu), d(\nu^\perp)]]_q$ quantum code where $n = (q^{m+1} - 1)/(q-1)$.

PROOF We know that $\nu^\perp = m(q-1) - \nu$ and if $\mathcal{P}_q(\nu, m) \subseteq \mathcal{P}_q(\nu, m)^\perp$, then $\nu \leq \nu^\perp$ and by Lemma 1.9 $\nu^\perp = \nu + k(q-1)$ for some $k \geq 0$. It follows that $2\nu \leq \lfloor m(q-1)/2 \rfloor$ and $2\nu = (m-k)(q-1)$, i.e., $2\nu \equiv 0 \bmod q-1$. The quantum code then follows from Theorem 1.7. ∎

1.5.3 Puncturing Quantum Codes

Finally we will briefly touch upon another important aspect of quantum code construction, which is the topic of shortening quantum codes. In the literature on quantum codes, there is not much distinction made between puncturing and shortening of quantum codes and often the two terms are used interchangeably. Obtaining a new quantum code from an existing one is more difficult task than in the classical case, the main reason being that the code must be so modified such the resulting code is still self-orthogonal. Fortunately, however there exists a method due to Rains [49] that can solve this problem.

From Lemma 1.4 we know that with every quantum code constructed using the CSS construction, we can associate two classical codes, C_1 and C_2. Define C to be the direct product of $C_1^{\perp}$ and $C_2^{\perp}$ viz. $C = C_1^{\perp} \times C_2^{\perp}$. Then we can associate a puncture code $P(C)$ [33, Theorem 12] which is defined as

$$P(C) = \{(a_i b_i)_{i=1}^{n} \mid a \in C_1^{\perp}, b \in C_2^{\perp}\}^{\perp}. \tag{1.7}$$

Surprisingly, $P(C)$ provides information about the lengths to which we can puncture the quantum codes. If there exists a vector of nonzero weight r in $P(C)$, then the corresponding quantum code can be punctured to a length r and minimum distance greater than or equal to distance of the parent code.

THEOREM 1.8
Let $0 \leq \nu_1 < \nu_2 \leq m(q-1) - 1$ *where* $\nu_2 \equiv \nu_1 \bmod q-1$. *Also let* $0 \leq \mu \leq \nu_2 - \nu_1$ *and* $\mu \equiv 0 \bmod q-1$. *If* $\mathcal{P}_q(\mu, m)$ *has codeword of weight* r, *then there exists an* $[[r, \geq (k(\nu_2) - k(\nu_1) - n + r), \geq d]]_q$ *quantum code, where* $n = (q^m - 1)/(q-1)$ $d = \min\{d(\nu_2), d(\nu_1^{\perp})\}$. *In particular, there exists a* $[[d(\mu), \geq (k(\nu_2) - k(\nu_1) - n + d(\mu)), \geq d]]_q$ *quantum code.*

PROOF Let $C_i = \mathcal{P}_q(\nu_i, m)$ with ν_i as stated. Then by Theorem 1.7, an $[[n, k(\nu_2) - k(\nu_1), d]]_q$ quantum code Q exists where $d = \min\{d(\nu_2), d(\nu_1^{\perp})\}$. From equation (1.7) we find that $P(C)^{\perp} = \mathcal{P}_q(\nu_1 + \nu_2^{\perp}, m)$, so

$$\begin{aligned} P(C) &= \mathcal{P}_q(m(q-1) - \nu_1 - \nu_2^{\perp}, m), \\ &= \mathcal{P}_q(\nu_2 - \nu_1, m). \end{aligned} \tag{1.8}$$

By [33, Theorem 11], if there exists a vector of weight r in $P(C)$, then there exists an $[[r, k', d']]_q$ quantum code, where $k' \geq (k(\nu_2) - k(\nu_1) -$

$n + r$) and distance $d' \geq d$. obtained by puncturing Q. Since $P(C) = \mathcal{P}_q(\nu_2 - \nu_1, m) \supseteq \mathcal{P}_q(\mu, m)$ for all $0 \leq \mu \leq \nu_2 - \nu_1$ and $\mu \equiv \nu_2 - \nu_1 \equiv 0 \bmod q - 1$, the weight distributions of $\mathcal{P}_q(\mu, m)$ give all the lengths to which Q can be punctured. Moreover $P(C)$ will certainly contain vectors whose weight $r = d(\mu)$, that is the minimum weight of $PC(\mu, m)$. Thus there exist punctured quantum codes with the parameters $[[d(\mu), \geq (k(\nu_2) - k(\nu_1) - n + d(\mu)), \geq d]]_q$. ∎

1.6 Conclusion

We have given a brief introduction to the theory of nonbinary stabilizer codes. Our goal was to emphasize the key ideas so we have omitted long and cumbersome proofs. Most of these details can be found in our companion papers on stabilizer codes. After introducing the stabilizer formalism for quantum codes, we showed how these were related to classical codes. Essentially we mapped the stabilizer and its centralizer to a classical code and its dual. And from then on all properties of the quantum codes could be studied by studying the classical codes. The construction of stabilizer codes can be reduced to identifying classical codes that are self-orthogonal. Then, we discussed the question of optimal codes and some well known bounds. We showed the nonexistence of a class of perfect codes of distance greater than 3. Finally we illustrated these ideas by constructing two new families of quantum codes.

Acknowledgments. This work was supported by NSF grant CCF-0218582 and a NSF CAREER award CCF-0347310.

References

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proc. of the 29th Annual ACM Symposium on Theory of Computation (STOC)*, pages 176–188, New York, 1997. ACM.

[2] 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)*, Trends Math., pages 133–153. Birkhäuser, 2003.

[3] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.

[4] A. Ashikhmin and S. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inform. Theory*, 45(4):1206–1215, 1999.

[5] A.E. Ashikhmin, A.M. Barg, E. Knill, and S.N. Litsyn. Quantum error detection I: Statement of the problem. *IEEE Trans. on Information Theory*, 46(3):778–788, 2000.

[6] A.E. Ashikhmin, A.M. Barg, E. Knill, and S.N. Litsyn. Quantum error detection II: Bounds. *IEEE Trans. on Information Theory*, 46(3):789–800, 2000.

[7] T. Beth and M. Grassl. The quantum Hamming and hexacodes. *Fortschr. Phys.*, 46(4-5):459–491, 1998.

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

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

[10] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.

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

[12] H.F. Chau. Correcting quantum errors in higher spin systems. *Phys. Rev. A*, 55:R839–R841, 1997.

[13] H.F. Chau. Five quantum register error correction code for higher spin systems. *Phys. Rev. A*, 56:R1–R4, 1997.

[14] R. Cleve. Quantum stabilizer codes and classical linear codes. *Phys. Rev. A*, 55(6):4054–4059, 1997.

[15] R. Cleve and D. Gottesman. Efficient computations of encodings for quantum error correction. *Phys. Rev. A*, 56(1):76–82, 1997.

[16] G. Cohen, S. Encheva, and S. Litsyn. On binary constructions of quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2495–2498, 1999.

[17] A. Ekert and C. Macchiavello. Error correction in quantum communication. *Phys. Rev. Lett.*, 76:2585–2588, 1996.

[18] K. Feng. Quantum codes $[[6, 2, 3]]_p$, $[[7, 3, 3]]_p$ ($p \geq 3$) exist. *IEEE Trans. Inform. Theory*, 48(8):2384–2391, 2002.

[19] K. Feng. Quantum error-correcting codes. In *Coding Theory and Cryptology*, pages 91–142. World Scientific, 2002.

[20] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory*, 50(12):3323–3325, 2004.

[21] M.H. Freedman and D.A. Meyer. Projective plane and planar quantum codes. *Found. Comput. Math.*, 1(3):325–332, 2001.

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

[23] D. Gottesman. Pasting quantum codes. eprint: quant-ph/9607027, 1996.

[24] D. Gottesman. Stabilizer codes and quantum error correction. Caltech Ph. D. Thesis, eprint: quant-ph/9705052, 1997.

[25] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos, Solitons, Fractals*, 10(10):1749–1758, 1999.

[26] D. Gottesman. An introduction to quantum error correction. In S. J. Lomonaco, Jr., editor, *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, pages 221–235, Rhode Island, 2002. American Mathematical Society. eprint: quant-ph/0004072.

[27] D. Gottesman. Quantum error correction and fault-tolerance. eprint: quant-ph/0507174, 2005.

[28] M. Grassl. Algorithmic aspects of error-correcting codes. In R. Brylinski and G. Chen, editors, *The Mathematics of Quantum Computing*, pages 223–252. CRC Press, 2001.

[29] M. Grassl and T. Beth. Quantum BCH codes. In *Proc. X. Int'l. Symp. Theoretical Electrical Engineering, Magdeburg*, pages 207–212, 1999.

[30] M. Grassl and T. Beth. Cyclic quantum error-correcting codes and quantum shift registers. *Proc. Royal Soc. London Series A*, 456(2003):2689–2706, 2000.

[31] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Internat. J. Quantum Information*, 2(1):757–775, 2004.

[32] M. Grassl, W. Geiselmann, and T. Beth. Quantum Reed-Solomon codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 231–244. Springer, Berlin, 1999.

[33] M. Grassl, M. Rötteler, and T. Beth. Efficient quantum circuits for non-qubit quantum error-correcting codes. *Internat. J. Found. Comput. Sci.*, 14(5):757–775, 2003.

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

[35] V. R. Job. m-adic residue codes. *IEEE Trans. Inform. Theory*, 38(2):496–501, 1992.

[36] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. Submitted, 2005.

[37] J.-L. Kim. New quantum-error-correcting codes from Hermitian self-orthogonal codes over GF(4). In *Proc. of the Sixth Intl. Conference on Finite Fields and Applications, Oaxaca, Mexico, May 21-25*, pages 209–213. Springer-Verlag, 2002.

[38] J.-L. Kim and V. Pless. Designs in additive codes over GF(4). *Designs, Codes and Cryptography*, 30:187–199, 2003.

[39] J.-L. Kim and J. Walker. Nonbinary quantum error-correcting codes from algebraic curves. submitted to a special issue of Com^{2}MaC Conference on Association Schemes, Codes and Designs in Discrete Math, 2004.

[40] A.Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52(6):1191–1249, 1997.

[41] A. Klappenecker and M. Rötteler. Beyond stabilizer codes II: Clifford codes. *IEEE Transaction on Information Theory*, 48(8):2396–2399, 2002.

[42] E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.

[43] E. Knill and R. Laflamme. A theory of quantum error–correcting codes. *Physical Review A*, 55(2):900–911, 1997.

[44] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correction code, 1996.

[45] R. Li and X. Li. Binary construction of quantum codes of minimum distance three and four. *IEEE Trans. Inform. Theory*, 50(6):1331–1336, 2004.

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

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

[48] R. Matsumoto and T. Uyematsu. Constructing quantum error correcting codes for p^m-state systems from classical error correcting codes. *IEICE Trans. Fundamentals*, E83-A(10):1878–1883, 2000.

[49] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45:1827–1832, 1999.

[50] E.M. Rains. Quantum codes of minimum distance two. *IEEE Trans. Inform. Theory*, 45(1):266–271, 1999.

[51] M. Rötteler, M. Grassl, and T. Beth. On quantum MDS codes. In *Proc. 2004 IEEE Intl. Symposium on Information Theory, Chicago, USA*, page 355, 2004.

[52] D. Schlingemann. Stabilizer codes can be realized as graph codes. *Quantum Inf. Comput.*, 2(4):307–323, 2002.

[53] D. Schlingemann and R.F. Werner. Quantum error-correcting codes associated with graphs. eprint: quant-ph/0012111, 2000.

[54] P. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.

[55] A. B. Sorensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

[56] A. Steane. Quantum Reed-Muller codes. *IEEE Trans. Inform. Theory*, 45(5):1701–1703, 1999.

[57] A.M. Steane. Multiple-particle interference and quantum error correction. *Proc. Roy. Soc. London A*, 452:2551–2577, 1996.

[58] A.M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.

[59] A.M. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory*, 45(7):2492–2495, 1999.