Chapter 1

Quantum error-correcting codes from algebraic curves

Jon-Lark Kim and Gretchen L. Matthews

Department of Mathematics, University of Louisville, Louisville, KY 40292 USA, jl.kim@louisville.edu
Department of Mathematical Sciences, Clemson University, Clemson, SC 29634 USA, gmatthe@clemson.edu

This chapter discusses quantum error-correcting codes constructed from algebraic curves. We give an introduction to quantum coding theory including bounds on quantum codes. We describe stabilizer codes which are the quantum analog of classical linear codes and discuss the binary and q-ary CSS construction. Then we focus on quantum codes from algebraic curves including the projective line, Hermitian curves, and hyperelliptic curves. In addition, we describe the asymptotic behaviors of quantum codes from the Garcia-Stichtenoth tower attaining the Drinfeld-Vlăduţ bound.

1.1. Introduction

One of the applications of algebraic geometry (AG) codes is their use in the construction of quantum error-correcting codes. Quantum error-correction was developed by Shor [31] and has become one of key ingredients in quantum computation and quantum information theory. Calderbank and Shor [6] and Steane [34] independently showed that quantum error-correcting codes can be constructed via classical linear codes over finite fields, known as the CSS construction. At the same time, Gottesman developed the stabilizer formalism [13]. Shortly thereafter, nonbinary quantum codes were studied by Rains [28] and Ashikhmin and Knill [2].

In this chapter, we start with a brief introduction to quantum information and quantum correction (Section 1.2). Interested readers can refer to the book [27]. Then in Section 1.3, we describe how to construct quantum error-correcting codes (in particular, stabilizer codes) from clas-

sical codes via the CSS construction. Finally Section 1.3 explains quantum codes from algebraic geometry codes. We consider quantum Reed-Solomon codes, quantum Hermitian codes, quantum codes from hyperelliptic curves, and quantum codes from multipoint AG codes. We also discuss asymptotic behaviors of quantum codes from AG codes.

1.2. Quantum information and error correction

1.2.1. *Background and terminology*

The classical unit of information is the bit, which is either 0 or 1. The quantum analog of the classical $0-1$ bit is the qubit, which is short for quantum bit. A qubit is of the form

$$\alpha|0\rangle + \beta|1\rangle \text{ where } \alpha, \beta \in \mathbb{C}.$$

Often, the normalization condition that $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$ is assumed to reflect that upon observation the qubit collapses to 0 with probability $\mid \alpha \mid^2$ and to 1 with probability $\mid \beta \mid^2$. Notice that the qubit may be viewed as a vector in $\mathbb{C}^2$. As in classical coding theory, one may consider larger alphabets such as $\mathbb{F}_q$ where $q = p^m$ and p is prime. Here, the units of information are quantum digits, called qudits. To describe a qudit, fix a basis $\{|a\rangle : a \in \mathbb{F}_q\}$ for the complex vector space $\mathbb{C}^q$. Then a qudit (also called a q-ary quantum state) is of the form

$$\sum_{a \in \mathbb{F}_q} \alpha_a |a\rangle \text{ where } \alpha_a \in \mathbb{C}.$$

Now the state of an n-qubit system may be viewed as a vector in the n-fold tensor product

$$(\mathbb{C}^q)^{\otimes n} = \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n} \cong \mathbb{C}^{q^n}.$$

In this setting, we now define a quantum code.

Definition 1.1. Given a prime power q, a q-ary quantum code of length n is a complex subspace of $(\mathbb{C}^q)^{\otimes n}$.

Throughout this chapter, q denotes a power of a prime p.

We next discuss how quantum codes guard against errors. Unlike the classical case, it is not immediately obvious that this is even possible. More pointedly, classical codes protect information by adding redundancy with

the most elementary example of this being a repetition code. However, quantum information cannot be duplicated in the same sense due to the following observation, called the No Cloning Theorem.

Theorem 1.1. *(No Cloning Theorem) There is no quantum operation that takes the state $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$ for all states $|\psi\rangle$.*

Proof. Suppose there is such an operation. Then given $|\psi\rangle \neq |\phi\rangle$,

$$|\psi\rangle + |\phi\rangle \mapsto |\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle$$

since $|\psi\rangle \mapsto |\psi\rangle$ and $|\phi\rangle \mapsto |\phi\rangle$. However,

$$|\psi\rangle + |\phi\rangle \mapsto (|\psi\rangle + |\phi\rangle)\,(|\psi\rangle + |\phi\rangle)$$

which is a contradiction since

$$|\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle \neq (|\psi\rangle + |\phi\rangle)\,(|\psi\rangle + |\phi\rangle)\,.$$

□

Despite the inability to copy quantum information, quantum codes do exist. Peter Shor produced the first example in 1995 [31] which was followed by a larger family found by Shor and Calderbank in 1996 [6]. To better understand the errors in a quantum system, it is helpful to consider the following (albeit oversimplified) analogy as in [15]: Given a linear code C of length n and dimension k over $\mathbb{F}_q$, C partitions $\mathbb{F}_q^n$ into cosets

$$\mathbb{F}_q^n = C \cup (C + e_1) \cup (C + e_2) \cup \cdots \cup \left(C + e_{q^{n-k}-1}\right)$$

and errors act on C by translation whereas a q-ary quantum code Q of length n and dimension k gives rise to an orthogonal decomposition

$$\mathbb{C}^{q^n} = Q \oplus E_1 Q \oplus E_2 Q \oplus \cdots \oplus E_{q^{n-k}-1} Q$$

and errors act on Q as unitary transformations. To be more precise, we next describe the types of errors encountered by an n-qudit q-ary system.

When dealing with qubits, there are three types of errors that may occur: a bit flip, phase flip, and a combination of bit and phase flips. These errors on a single qubit may be represented by 2×2 matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = iXZ.$$

Indeed,

$$X|a\rangle = |a \oplus 1\rangle, Z|a\rangle = (-1)^a|a\rangle, \text{ and } Y|a\rangle = i(-1)^a|a \oplus 1\rangle.$$

The matrices X, Y, and Z are called Pauli matrices.

More generally, let $q = p^m$ where p is prime. Given $a, b \in \mathbb{F}_q$ we have dit flip and phase flip errors acting on a single qudit as

$$T_a|u\rangle = |u + a\rangle$$

and

$$R_b|u\rangle = \xi^{Tr(bu)}|u\rangle$$

where $\xi = e^{\frac{2\pi i}{p}}$ is a p^{th} root of unity and $Tr : \mathbb{F}_q \to \mathbb{F}_p$ is the trace function. These operators may be expressed by matrices as follows. Suppose that $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ is a basis for $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space. Given $a, b \in \mathbb{F}_q$, $a = \sum_{i=1}^m a_i\gamma_i$ and $b = \sum_{i=1}^m b_i\gamma_i$ for some $a_i, b_i \in \mathbb{F}_p$. Let $T, R \in \mathbb{C}^{p\times p}$ be the matrices

$$T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \text{ and } R = \begin{bmatrix} \xi & & & & \\ & \xi^2 & & & \\ & & \xi^3 & & \\ & & & \ddots & \\ & & & & \xi^{p-1} \end{bmatrix};$$

that is,

$$[T]_{i,j} = \delta_{i,j-1 \bmod p} \text{ and } [R]_{i,j} = \xi^i\delta_{i,j}$$

where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

and the rows and columns are indexed $0, \ldots, p-1$. Now, matrices corresponding to the dit flip and phase flip errors described above are

$$T_a := T^{a_1} \otimes T^{a_2} \otimes \cdots \otimes T^{a_m} \text{ and } R_b := R^{b_1} \otimes R^{b_2} \otimes \cdots \otimes R^{b_m}.$$

Clearly,

$$\begin{aligned} T_aR_b &= \left(T^{a_1} \otimes T^{a_2} \otimes \cdots \otimes T^{a_m}\right)\left(R^{b_1} \otimes R^{b_2} \otimes \cdots \otimes R^{b_m}\right) \\ &= T^{a_1}R^{b_1} \otimes T^{a_2}R^{b_2} \otimes \cdots \otimes T^{a_m}R^{b_m}. \end{aligned}$$

Note that $\{T_aR_b : a, b \in \mathbb{F}_q\}$ is an orthogonal basis for $\mathbb{C}^q$ under the trace inner product $\langle A, B\rangle := Tr\left(A^\dagger B\right)$ where $A^\dagger$ denotes the Hermitian transpose of A. Thus, the span of $\{T_aR_b : a, b \in \mathbb{F}_q\}$ is the set of errors on a single qudit.

Next, we consider errors on an n-state system, that is, a system of n qudits. Given $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, define

$$T_a := T_{a_1} \otimes T_{a_2} \otimes \cdots \otimes T_{a_n} \text{ and } R_b := R_{b_1} \otimes R_{b_2} \otimes \cdots \otimes R_{b_n}.$$

Then

$$\begin{aligned} T_a R_b &= (T_{a_1} \otimes T_{a_2} \otimes \cdots \otimes T_{a_n})\,(R_{b_1} \otimes R_{b_2} \otimes \cdots \otimes R_{b_n}) \\ &= T_{a_1} R_{b_1} \otimes T_{a_2} R_{b_2} \otimes \cdots \otimes T_{a_n} R_{b_n}. \end{aligned}$$

Given $a, b \in \mathbb{F}_q^n$, set $E_{a,b} := T_a R_b$. Then the set

$$\mathcal{E}_n := \left\{ E_{a,b} : a, b \in \mathbb{F}_q^n \right\}$$

is an error basis for $\mathbb{C}^{q^n}$. Hence, the error group for an n-state q-ary system is

$$G_n = \left\{ \xi^i E_{a,b} : a, b \in \mathbb{F}_q^n, 0 \le i \le q-1 \right\},$$

a group of order pq^{2n} with center $Z(G_n) = \langle \xi I \rangle$.

We now discuss when errors are correctable by a quantum code C. Let $\{|\psi_j\rangle : 1 \le j \le k\}$ be a basis for C. In order for errors E and F to be correctable, $E|\psi_i\rangle$ and $F|\psi_j\rangle$ must be distinguishable (meaning orthogonal) for all $i \neq j$; that is,

$$\langle \psi_i | E^\dagger F | \psi_j \rangle = 0.$$

Because measurement disturbs the state, error correction cannot be done by measurement; that is, an operation that causes measurement is not allowed. This includes anything that gives information about the state. For example, if $\langle \psi_i | E^\dagger F | \psi_i \rangle \neq \langle \psi_j | E^\dagger F | \psi_j \rangle$ for some $1 \le i, j \le k$, then this measurement gives information about the state. Hence, an additional requirement for E and F to be correctable errors is that

$$\langle \psi_i | E^\dagger F | \psi_i \rangle = \langle \psi_j | E^\dagger F | \psi_j \rangle$$

for all $1 \le i, j \le k$. This discussion is summarized in the following result due to Knill and Laflamme [24] and Bennett, DiVincenzo, Smolin, and Wooters [4].

Theorem 1.2. *A set $\mathcal{A}$ of errors is correctable by a code C with basis $\{|\psi_j\rangle : 1 \le j \le k\}$ if and only if*

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = C_{ab} \delta_{ij}$$

where E_a and E_b run over all possible errors in $\mathcal{A}$ and C_{ab} depends only on a and b (not on i and j).

The weight of an error $\xi^i E_{\mathbf{a},\mathbf{b}} \in G_n$ is the number of its nonidentity components, meaning

$$wt\left(\xi^i E_{\mathbf{a},\mathbf{b}}\right) = n - |\{i : a_i = b_i = 0\}|.$$

Given this notion of weight, we can now define the minimum distance of a q-ary quantum code C of length n to be

$$d = \max\left\{ d : \begin{array}{r} \langle u|v\rangle = 0 \text{ and } wt(E) \leq d-1 \Rightarrow \langle u|E|v\rangle = 0 \\ \forall |u\rangle, |v\rangle \in C \text{ and } \forall E \in G_n \end{array} \right\}.$$

Definition 1.2. An $[[n,k,d]]_q$ code is a q-ary quantum code of length n, dimension k, and minimum distance d.

We will write $[[n,k,\geq d]]_q$ code to mean an q-ary quantum code of length n, dimension k, and minimum distance at least d. As is standard, a classical linear code of length n, dimension k, and minimum distance d (resp. at least d) is called an $[n,k,d]$ (resp. $[n,k,\geq d]$) code.

An $[[n,k,d]]_q$ code C is pure if and only if

$$wt(E) \leq d-1 \Rightarrow \langle u|E|v\rangle = 0$$

for all $|u\rangle, |v\rangle \in C$ and all $E \in G_n$. Notice that the words u and v are not required to be orthogonal here. A weaker condition is that of nondegeneracy. An $[[n,k,d]]_q$ code C is nondegenerate if and only if

$$wt(E) \leq d-1 \Rightarrow |u\rangle \text{ and } E|v\rangle \text{ are linearly independent}$$

for all $|u\rangle, |v\rangle \in C$ and all $E \in G_n$; otherwise C is said to be degenerate. While the term degenerate has seemingly negative connotations, we will see in the next subsection that this is not necessarily the case.

1.2.2. *Bounds on quantum codes*

Many of the classical coding theory bounds have analogs that apply to quantum codes.

Theorem 1.3. *(Quantum Hamming Bound) Given any $[[n,k,d]]_q$ nondegenerate quantum code,*

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

Proof. Suppose that C is a $[[n,k,d]]_q$ nondegenerate quantum code. Since C is nondegenerate, any two linearly independent correctable errors produce orthogonal q^k-dimensional subspaces of $\mathbb{C}^{q^n}$. Given $0 \leq j \leq \frac{d-1}{2}$, any j errors are correctable and there are

$$\binom{n}{j} (q^2-1)^j$$

such errors. From this, the bound follows. □

Notice that this bound only applies to nondegenerate codes. This suggests that it might be possible for a degenerate code to have parameters exceeding this bound. In 1997, Gottesman [13] proved that degenerate single- and double-error-correcting binary codes satisfy the bound given in Theorem 1.3. Nearly a decade later, it was shown for degenerate q-ary stabilizer codes of minimum distance 3 [22] and minimum distance 5 [1]. A major open problem in quantum coding theory is to determine if there is a Hamming bound that applies to degenerate codes.

Quantum codes also satisfy MacWilliams identities [32]. Using these, one can prove a quantum analog of the classical singleton bound.

Theorem 1.4. *(Quantum Singleton Bound) If C is a $[[n, k, d]]_q$ code with $k > 1$, then*

$$k + 2d \leq n + 2.$$

A quantum maximum distance separable (MDS) code is a quantum code which attains the Singleton bound. Rains [28, Theorem 2] showed that all quantum MDS codes are pure. There is an interesting relationship betweeen quantum MDS codes and classical MDS codes. If Q is a quantum MDS stabilizer code with $n-2d+2 > 0$, then it gives rise to classical MDS codes [22, Lemma 61]. Recall that the MDS conjecture for classical codes says: "If there is a nontrivial $[n, k, d]_q$ MDS code, then $n \leq q + 1$ unless q is even and $k = 3$ or $k = q - 1$ in which case $n \leq q + 2$." The classical MDS conjecture implies that there are no nontrivial MDS stabilizer codes of lengths greater than $q^2 + 1$, except when q is even and $d = 4$ or $d = q^2$ in which case $n \leq q^2 + 2$ [22, Corollary 65]. Therefore, the discovery of certain quantum MDS codes could provide a route to disproving the classical MDS conjecture. This is an active area of research in quantum error-correcting codes.

Theorem 1.5. *(Quantum Gilbert-Varshamov Bound) Suppose that $2 \leq k < n$, $d \geq 2$ and $n \equiv k \bmod 2$. If*

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

then there exists a $[[n, k, d]]_q$ code.

Recently, Feng and Ma proved a Gilbert-Varshamov type bound which guarantees the existence of pure codes.

Theorem 1.6. *(Gilbert-Varshamov Bound for pure stabilizer codes) [9, Theorem 1.4] Suppose that* $2 \leq k < n$, $d \geq 2$ *and* $n \equiv k \bmod 2$. *If*

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

then there exists a $[[n,k,d]]_q$ *pure code.*

Asymptotically, these two bounds coincide. We will consider the asymptotic version in Section 1.4. The statements in Theorems 1.5 and 1.6 may be made a bit stronger. Under the given hypotheses, there exists a stabilizer code with the given parameters. Stabilizer codes are discussed in the next section.

1.3. Relating quantum codes and classical codes

While classical linear codes may be compactly described in terms of a basis, this may not be the most concise expression for a quantum code (see Gottesman's thesis [13] for some examples illustrating this). In fact, for a large class of quantum codes called stabilizer codes, another algebraic structure is more useful. Stabilizer codes over $\mathbb{F}_2$ were introduced by Gottesman in his thesis [13], and many of the same ideas were discovered independently by Calderbank, Rains, Shor, and Sloane [5] and used in the famous CSS constuction.

1.3.1. *Stabilizer codes*

Some believe stabilizer codes to be the quantum analog of linear codes. The stabilizer can be thought of as the quantum analog of a classical parity check matrix. While not every code is a stabilizer code, the following is true: Given a quantum code C, there is a stabilizer code C' such that $C \subseteq C'$ [22]; hence, knowledge of (lower bounds on) the error-correcting capability of stabilizer codes provides information about the capabilities of arbitrary quantum codes.

Definition 1.3. A q-ary quantum stabilizer code C of length n is a joint eigenspace of operators of an abelian subgroup S of G_n; that is,

$$C = \left\{ u \in \mathbb{C}^{q^n} : Mu = u \ \forall M \in S \right\}.$$

The fact that S is abelian guarantees that the code is nontrivial. To see this, suppose $M, N \in S$. Then

$$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \text{ and } NM|\psi\rangle = N|\psi\rangle = |\psi\rangle$$

which imply

$$(MN - NM)\,|\psi\rangle = MN|\psi\rangle - NM|\psi\rangle = 0.$$

It follows that $MN = NM$ or $|\psi\rangle = 0$. As a result, S must be abelian or $C = \{|0\rangle\}$. (If S is nonabelian, it is standard to extend S by $Z(G_n)$.)

We do not have space to prove or even mention all of the facts on stabilizer codes. Instead, we point the reader to the excellent references [2], [13], and [22]. There one can find the following result.

Proposition 1.1. *A stabilizer code C with stabilizer $S \subseteq G_n$ has $\frac{q^n}{|S|}$ codewords and minimum distance* $\min wt\{M \in N(S) \setminus S\}$ *where $N(S)$ denotes the normalizer of S.*

In the next subsection, we consider some stabilizer codes constructed from classical linear codes.

1.3.2. *CSS construction*

In this section, we describe a large class of quantum stabilizer codes based on classical linear codes.

Recall that an additive code of length n over $\mathbb{F}_4$ is an additive subgroup of $\mathbb{F}_4^n$. Write $\mathbb{F}_4 = \{0, \omega, \omega^2, 1\}$ where $\omega^2 = \omega + 1$ so that $\overline{\omega} = \omega^2$. Then $\{\omega, \overline{\omega}\}$ is a basis for $\mathbb{F}_4$ as an $\mathbb{F}_2$-vector space. Hence, given $v \in \mathbb{F}_4^n$,

$$v = \omega a + \overline{\omega} b$$

for some $a, b \in \mathbb{F}_2^n$. This defines a bijection

$$\begin{array}{rccc} f: & \mathbb{F}_4^n & \to & \mathbb{F}_2^{2n} \\ & \omega a + \overline{\omega} b & \mapsto & (a|b)\,. \end{array}$$

This bijection may be composed with

$$\begin{array}{rccc} g: & \mathbb{F}_2^{2n} & \to & G_n \\ & (a|b) & \mapsto & E_{ab} \end{array}$$

to produce

$$\begin{array}{rccc} \phi: & \mathbb{F}_4^n & \to & G_n \\ & \omega a + \overline{\omega} b & \mapsto & E_{ab}. \end{array}$$

In [5], additive codes over $\mathbb{F}_4$ are used to construct quantum codes via the following major result. Here, the inner product employed is the trace inner product defined by

$$u * v := Tr(u \cdot v)$$

for all $u, v \in \mathbb{F}_4^n$, where the trace map is

$$\begin{aligned} Tr : \mathbb{F}_4 &\to \mathbb{F}_2 \\ x &\mapsto \overline{x} \end{aligned}$$

and $u \cdot v := \sum_{i=1}^{n} u_i v_i$ is the usual inner product. Recall that a code C is self-orthogonal (or weakly self-dual) provided $C \subseteq C^{\perp}$.

Theorem 1.7. *[5, Theorem 2] Suppose that $D \subseteq \mathbb{F}_4^n$ is an additive self-orthogonal code such that $|D| = 2^{n-k}$ and $D^{\perp} \setminus D$ has no vectors of weight less than d. Then any eigenspace of $\phi(D)$ is a $[[n, k, d]]_2$ code.*

Classical binary linear codes may be employed in Theorem 1.7 as follows. Suppose that C_1 is a $[n, k_1, d_1]_2$ code and C_2 is $[n, k_2, d_2]_2$ code where $C_1 \subseteq C_2$. Then

$$D = \omega C_1 + \overline{\omega} C_2^{\perp} \subseteq \mathbb{F}_4^n$$

is an additive code over $\mathbb{F}_4$. Moreover, D is self-orthogonal with respect to the trace inner product. To see this, note that

$$\begin{aligned} Tr\left((\omega a + \overline{\omega} b) \cdot \overline{(\omega a' + \overline{\omega} b')}\right) &= \sum_{i=1}^{n} a_i b_i' Tr(\overline{\omega}) + a_i' b_i Tr(\omega) \\ &= (a|b) \cdot (a'|b') \\ &= 0 \end{aligned}$$

for all $(\omega a + \overline{\omega} b), (\omega a' + \overline{\omega} b') \in D$ as $a, a' \in C_1 \subseteq C_2$ and $b, b' \in C_2^{\perp}$. Applying Theorem 1.7 to D as above produces what is commonly called the CSS construction for binary quantum codes, one of the most important constructions of quantum codes. This turns out to be a special case of a q-ary construction which is given in Corollary 1.1.

Theorem 1.8. *(Binary CSS construction) Suppose that C_1 and C_2 are binary linear codes of length n and dimensions k_1 and k_2 respectively with $C_1 \subseteq C_2$. Then there exists a $\left[[n, k_2 - k_1, min\{d(C_2 \setminus C_1), d\left(C_1^{\perp} \setminus C_2\right)\}\right]_2$ code.*

Following Rains' work on nonbinary quantum codes [28], Ashikhmin and Knill developed a q-ary analog to Theorem 1.7. Notice that a code C of length n over $\mathbb{F}_4$ is additive if and only if C is an $\mathbb{F}_2$-subspace of $\mathbb{F}_4^n$.

Hence, in the q-ary case where $q = p^m$, the notion of an additive code is replaced with that of an $\mathbb{F}_p$-subspace. Such a code is said to be $\mathbb{F}_p$-linear. More precisely, we have the following definition.

Definition 1.4. Suppose $q = p^m$ where p is prime. An $\mathbb{F}_p$-linear code of length n over $\mathbb{F}_q$ is an $\mathbb{F}_p$-subspace of $\mathbb{F}_q^n$.

Consider

$$\begin{array}{rccc} g: & \mathbb{F}_q^{2n} & \to & G_n \\ & (a|b) & \mapsto & E_{ab}. \end{array}$$

To generalize Theorem 1.7 to the q-ary case, one may use a generalization of the trace inner product defined about. Given $(a|b), (a'|b') \in \mathbb{F}_q^{2n}$, set

$$(a|b) * (a'|b') = Tr\left(a \cdot b' - a' \cdot b\right)$$

where $Tr : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace map.

Theorem 1.9. *[2, p. 3069] Suppose that $D \subseteq \mathbb{F}_q^{2n}$ is an $\mathbb{F}_p$-linear code which is self-orthogonal with respect to $*$ such that $|D| = p^r$. Then any eigenspace of $g(D)$ is a $\left[\left[n, n - \frac{r}{m}, d\left(D^{\perp_*} \setminus D\right)\right]\right]_q$ code.*

Classical q-ary codes may be employed in Theorem 1.9. To do so, consider a degree two extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. Suppose that ω is a primitive element of $\mathbb{F}_{q^2}$ so that $\{\omega, \overline{\omega}\}$ is a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Define

$$\begin{array}{rccc} f: & \mathbb{F}_{q^2}^n & \to & F_q^{2n} \\ & \omega a + \overline{\omega} b & \mapsto & (a|b). \end{array}$$

This results in a q-ary version of the CSS construction.

Corollary 1.1. *(q-ary CSS construction) [16, 22, 23] Suppose that C_1 and C_2 are linear codes over $\mathbb{F}_q$ of length n and dimensions k_1 and k_2 respectively with $C_1 \subseteq C_2$. Then there exists a $\left[\left[n, k_2 - k_1, min\{d(C_2 \setminus C_1), d\left(C_1^{\perp} \setminus C_2\right)\}\right]\right]_q$ code.*

Proof. Set $C = \omega C_1 + \overline{\omega} C_2^{\perp} \subseteq \mathbb{F}_{q^2}^n$ and $D = f(C) \subseteq \mathbb{F}_q^{2n}$. Then D is self-orthogonal with respect to $*$ (see [23, Lemma 2.5, Proposition 2.6]). Now Theorem 1.9 gives the desired result. □

Next, we see how another inner product on $\mathbb{F}_{q^2}^n$ may be utilized to construct quantum codes over $\mathbb{F}_q$. Recall that the Hermitian inner product on $\mathbb{F}_{q^2}^n$ is given by

$$u *_h v := \sum_{i=1}^{n} u_i v_i^q.$$

In [2, Theorem 4], it is shown that a code which is self-orthogonal with respect to the Hermitian inner product is also self-orthogonal with respect to $*$. This idea can be used to construct q-ary quantum codes.

Corollary 1.2. *[2, Corollary 1] Suppose that D is a $[n,k,d]_{q^2}$ code which is self-orthogonal with respect to the Hermitian inner product. Let $D^{\perp_h}$ denote the Hermitian dual of D. Then there exists a $\left[\left[n, n-2k, min\{wt\left(D^{\perp_h} \setminus D\right)\}\right]\right]_q$ code.*

An $[n,k,d]_q$ code is pure if its dual contains no nonzero vectors of weight less than d. For example, a self-dual code is pure. Suppose a quantum code Q is constructed from a classical code C in the CSS construction (taking $C_1 = C_2 = C$ in Corollary 1.1). Then Q is pure if and only if C is pure.

1.4. Quantum codes constructed from algebraic geometry codes

In this section we employ algebraic geometry codes in the construction of quantum codes. We consider several families of such codes as well as asymptotic results. To begin, we review the notation used in this section.

Let X be a smooth, projective, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_q$. Let $\mathbb{F}_q(X)$ denote the field of rational functions on X defined over $\mathbb{F}_q$, and let $\Omega(X)$ denote the set of differentials on X defined over $\mathbb{F}_q$. The divisor of a rational function f (resp. differential η) will be denoted by (f) (resp. (η)). Given a divisor A on X defined over $\mathbb{F}_q$, let

$$\mathcal{L}(A) = \{f \in \mathbb{F}_q(X) : (f) \geq -A\} \cup \{0\}$$

and

$$\Omega(A) = \{\eta \in \Omega(X) : (\eta) \geq A\} \cup \{0\}.$$

Let $\ell(A)$ denote the dimension of $\mathcal{L}(A)$ as an $\mathbb{F}_q$-vector space. The support of a divisor D is denoted by $suppD$.

Algebraic geometry codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ can be constructed using divisors $D = \sum_{i=1}^{n} P_i$ and $G = \sum_{i=1}^{m} \alpha_i Q_i$ on X where $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ are pairwise distinct $\mathbb{F}_q$-rational points and $\alpha_i \in \mathbb{N}$ for all i, $1 \leq i \leq m$. In particular,

$$C_{\mathcal{L}}(D,G) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

and

$$C_{\Omega}(D,G) := \{(res_{P_1}(\eta), \ldots, res_{P_n}(\eta)) : \eta \in \Omega(G-D)\}.$$

These codes are sometimes called m-point codes since the divisor G has m distinct $\mathbb{F}_q$-rational points in its support. Typically, an m-point code is constructed by taking the divisor D to be the sum of all $\mathbb{F}_q$-rational points not in the support of G, and we will keep this convention. We will use the term multipoint code to mean an m-point code with $m \geq 2$.

The two algebraic geometry codes above are related in that

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\Omega}(D,G).$$

If $\deg G < n$, then $C_{\mathcal{L}}(D,G)$ has length n, dimension $\ell(G)$, and designed distance $n - \deg G$. If $\deg G > 2g-2$, then $C_{\Omega}(D,G)$ has dimension $\ell(K+D-G)$, where K is a canonical divisor, and designed distance $\deg G-(2g-2)$. The minimum distance of each of the codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ is at least its designed distance.

For more background on AG codes, the reader may consult [12], [35], or [39].

1.4.1. *Families of quantum codes from one-point AG codes*

1.4.1.1. *Quantum Reed-Solomon codes*

Perhaps the most popular family of AG codes is the class of Reed-Solomon codes which are one-point AG codes on the projective line. Prior to the work on nonbinary quantum codes [2], Grassl, Geiselmann and Beth [17] generalized some of the ideas in [5] from $\mathbb{F}_4$ to higher degree extensions of $\mathbb{F}_2$. Specifically, they considered Reed-Solomon codes over $\mathbb{F}_{2^t}$ and their binary expansions. Let $\{b_1, \ldots b_t\}$ be a basis for $\mathbb{F}_{2^t}$ as an $\mathbb{F}_2$-vector space. Define

$$\begin{array}{rccc} \mathcal{B}: & \mathbb{F}_{2^t} & \rightarrow & \mathbb{F}_2^t \\ & \sum_{i=1}^{t} a_i b_i & \mapsto & (a_1, \ldots, a_t)\,. \end{array}$$

Given a $[n,k,d]_{2^t}$ code C, $\mathcal{B}(C)$ is a $[tn, tk, \geq d]_2$ code. By [17, Theorem 1],

$$\mathcal{B}(C)^{\perp} = \mathcal{B}^{\perp}\left(C^{\perp}\right).$$

Hence, if the basis is chosen to be self-dual (which it can be according to [30, Theorem 4]) and the code C is self-orthogonal, then

$$\mathcal{B}(C) \subseteq \mathcal{B}\left(C^{\perp}\right) = \mathcal{B}\left(C\right)^{\perp}.$$

Recall that an $[n,k,d]_{2^t}$ Reed-Solomon code is self-dual provided $2k < n$. Using this fact together with their precursor to Corollary 1.1, Grassl et. al. obtain the following.

Proposition 1.2. *[17] Given* $\delta > \frac{2^t-1}{2} + 1$*, there is a quantum Reed-Solomon code with parameters* $[[t\left(2^t-1\right), t\left(2\delta - 2^t - 1\right), \geq 2^t - \delta + 1]]_2$.

Proof. Let C be an $[2^t - 1, 2^t - \delta, \delta]_{2^t}$ Reed-Solomon code where $\delta > \frac{2^t-1}{2} + 1$. Then C is self-orthogonal. Now apply Corollary 1.1 with $C_1 = C_2 = \mathcal{B}(C)$ where $\mathcal{B}$ is a self-dual basis for $\mathbb{F}_{2^t}$ over $\mathbb{F}_2$. The result follows immediately. □

See [14] for applications of other cyclic codes to the construction of quantum codes.

Quantum Reed-Solomon codes over fields of odd characteristic may be constructed too. We do not provide the details here as this construction is a special case of a result in Subsection 1.4.2. Extended Reed-Solomon codes have also been used to construct quantum MDS codes as in [16].

1.4.1.2. *Quantum Hermitian codes*

Next to Reed-Solomon codes, Hermitian codes are certainly the most studied algebraic geometry codes. Recall that the exact parameters of one-point Hermitian codes are known due to [41]. For reference, Table 1. gives the dimension $k\left(\alpha\right)$ and minimum distance $d\left(\alpha\right)$ of the code $C_{\mathcal{L}}(P_1 + \cdots + P_{q^3}, \alpha P_\infty)$ where $P_1, \ldots, P_{q^3}, P_\infty$ are all of the $\mathbb{F}_{q^2}$-rational points of the Hermitian curve defined by $y^q + y = x^{q+1}$. Here $\underline{\alpha} = max\{a \in H\left(P_\infty\right) : a \leq \alpha\}$ is the largest element of the Weierstrass semigroup at the point P_∞ that is no bigger than α.

α	$k\left(\alpha\right)$	$d\left(\alpha\right)$
$0 \leq \alpha \leq q^2 - q - s$ $\underline{\alpha} = sq + t$ $0 \leq b \leq a \leq q - 1$	$\frac{a(a+1)}{2} + b + 1$	$q^3 - \underline{\alpha}$
$q^2 - q - 2 < \alpha < q^3 - q^2 + q$	$\alpha + 1 - \frac{q(q-1)}{2}$	$n - \alpha$
$q^3 - q^2 + q \leq \alpha < q^3$ $\alpha = q^3 - q^2 + aq + b$ $0 \leq a, b \leq q - 1$	$\alpha + 1 - \frac{q(q-1)}{2}$	$q^3 - \alpha$ if $a < b$ $q^3 - \alpha + b$ if $a \geq b$
$q^3 \leq \alpha \leq q^3 + q^2 - q - 2$ $q^3 + q^2 - q - 2 - \underline{\alpha} = aq + b$ $0 \leq b \leq a \leq q - 1$	$q^3 - \frac{a(a+1)}{2} - b - 1$	$a + 2$ if $b = a$ $a + 1$ if $b < a$

Table 1.
Parameters of the Hermitian code $C_{\mathcal{L}}(P_1 + \cdots + P_{q^3}, \alpha P_\infty)$

If $\alpha_1 < \alpha_2$, then

$$C_{\mathcal{L}}(D, \alpha_1 P_\infty) \subseteq C_{\mathcal{L}}(D, \alpha_2 P_\infty).$$

Applying Corollary 1.1 with $C_1 = C_{\mathcal{L}}(D, \alpha_1 P_\infty)$ and $C_2 = C_{\mathcal{L}}(D, \alpha_2 P_\infty)$ yields the following fact.

Theorem 1.10. *[29, Theorem 3] For $0 \leq \alpha_1 < \alpha_2 \leq q^3 + q^2 - q - 2$, there exists a $\left[\left[q^3, k(\alpha_2) - k(\alpha_1), \geq min\{d(\alpha_2), d\left(q^3 + q^2 - q - 2 - \alpha_1\right)\}\right]\right]_{q^2}$ code where $k(\alpha)$ and $d(\alpha)$ are given in Table 1.*

Quantum Hermitian codes can also be constructed using Hermitian codes which are self-orthogonal with respect to the Hermitian inner product. Recall that the dual of the one-point Hermitian code $C_{\mathcal{L}}(D, \alpha P_\infty)$ over $\mathbb{F}_{q^2}$ is given by

$$C_{\mathcal{L}}\left(D, \alpha P_\infty^{\perp}\right) = C_{\mathcal{L}}\left(D, \left(q^3 + q^2 - q - 2 - \alpha\right) P_\infty\right)$$

as shown in [36, 38]. It follows that $C_{\mathcal{L}}(D, \alpha P_\infty)$ is self-orthogonal if $2\alpha \leq q^3 + q^2 - q - 2 - \alpha$. Using this, one can prove that $C_{\mathcal{L}}(D, \alpha P_\infty)$ is self-orthogonal with respect to the Hermitian inner product for $0 \leq \alpha \leq q^2 - 2$ (see [29, Lemma 7] for details). Now Corollary 1.2 gives another family of quantum Hermitian codes.

Theorem 1.11. *[29, Theorem 8] If $0 < \alpha \leq q^2 - 2$, then there exists a $\left[\left[q^3, q^3 - 2k(\alpha), \geq d\left(q^3 + q^2 - q - 2 - \alpha\right)\right]\right]_q$ where $k(\alpha)$ and $d(\alpha)$ are given in Table 1.*

1.4.2. *More general AG constructions*

The quantum Reed-Solomon and quantum Hermitian codes defined earlier in this section are special cases of a more general construction for quantum codes from AG codes detailed in this section.

Let X be a smooth, projective, absolutely irreducible curve of genus g over a finite field $\mathbb{F}_q$. Suppose that A and B are divisors on X such that $A \leq B$, and let $D = P_1 + \cdots + P_n$ be another divisor on X whose support consists of n distinct $\mathbb{F}_q$-rational points none of which are in the support of A or B. Then

$$\mathcal{L}(A) \subseteq \mathcal{L}(B)$$

and so

$$C_{\mathcal{L}}(D, A) \subseteq C_{\mathcal{L}}(D, B).$$

Applying Corollary 1.1, we find a large family of quantum codes from AG codes.

Theorem 1.12. *Let A, B, and $D = P_1 + \cdots + P_n$ be divisors on a smooth, projective, absolutely irreducible curve X of genus g over $\mathbb{F}_q$. Assume that $A \leq B$ and $(suppA \cup suppB) \cap suppD = \emptyset$ and $\deg B < n$. Then there exists a $[[n, \ell(B) - \ell(A), d]]_q$ code where*

$$\begin{aligned} d &\geq \min\{d\left(C_{\mathcal{L}}\left(D,B\right) \setminus C_{\mathcal{L}}\left(D,A\right)\right), d\left(C_{\Omega}\left(D,A\right) \setminus C_{\Omega}\left(D,B\right)\right)\} \\ &\geq \min\{n - \deg B, \deg A - (2g-2)\}. \end{aligned}$$

Proof. This follows immediately from Corollary 1.1 (taking $C_1 = C_{\mathcal{L}}(D,A)$ and $C_2 = C_{\mathcal{L}}(D,B)$) and the fact that $\deg A \leq \deg B < n$ implies $dim C_{\mathcal{L}}(D,B) = \ell(B)$ and $dim C_{\mathcal{L}}(D,A) = \ell(A)$. □

In the next example, we see how one may apply Theorem 1.12 to a multipoint code.

Example 1.1. Let X be a smooth, projective, absolutely irreducible curve of genus g over $\mathbb{F}_q$. Consider the m-point code $C_{\mathcal{L}}(D, \sum_{i=1}^{m} a_i Q_i)$ on X over $\mathbb{F}_q$. Since $\mathbb{F}_q$ is finite, the class number of the function field of X over $\mathbb{F}_q$ is finite [35, Proposition V.1.3]. Hence, there exists a rational function f with divisor

$$(f) = \sum_{i=2}^{m} b_i Q_i - b_1 Q_1$$

where $b_i \geq a_i$ for all i, $2 \leq i \leq m$, and $b_1 := \sum_{i=2}^{m} b_i$. Multiplication by f gives rise to a vector space isomorphism

$$\begin{array}{ccc} \phi : \mathcal{L}\left(\sum_{i=1}^{m} a_i Q_i\right) & \to & \mathcal{L}\left(\left(a_1+b_1\right)Q_1 - \sum_{i=2}^{m}\left(b_i - a_i\right)Q_i\right) \\ h & \mapsto & fh \end{array}$$

which in turn induces an isometry ϕ^* of codes

$$C_{\mathcal{L}}\left(D, \sum_{i=1}^{m} a_i Q_i\right) \cong C_{\mathcal{L}}\left(D, \left(a_1+b_1\right)Q_1 - \sum_{i=2}^{m}\left(b_i - a_i\right)Q_i\right).$$

Since $\left(a_1+b_1\right)Q_1 - \sum_{i=2}^{m}\left(b_i - a_i\right)Q_i \leq \left(a_1+b_1\right)$,

$$C_{\mathcal{L}}\left(D, \left(a_1+b_1\right)Q_1 - \sum_{i=2}^{m}\left(b_i - a_i\right)Q_i\right) \subseteq C_{\mathcal{L}}\left(D, \left(a_1+b_1\right)Q_1\right).$$

Therefore, if $a_1 + b_1 < |suppD|$ then Theorem 1.12 yields a quantum code over $\mathbb{F}_q$ of length $|suppD|$ and dimension

$$\ell\left(\left(a_1+b_1\right)Q_1\right) - \ell\left(\left(a_1+b_1\right)Q_1 - \sum_{i=2}^{m}\left(b_i-a_i\right)Q_i\right).$$

A bound on the minimum distance is given by the theorem also. However, the weights of words in multipoint codes are not typically known. As a result, determining the minimum distance of the quantum code may be challenging. A notable exception to this is family of two-point Hermitian codes whose exact minimum distance has been determined in the extensive recent work of Homma and Kim [18], [19], [20], [21].

Of course, one may also apply Theorem 1.12 to nested multipoint codes. While this construction provides a great deal of flexibility, it produces codes whose minimum distances may be hard to determine. For this reason, we will not elaborate on this idea here.

Next, we consider how Corollary 1.2 may be applied to AG codes. The idea is a generalization of Theorem 1.11.

Lemma 1.1. *The algebraic geometry code $C_{\mathcal{L}}(D,G)$ is self-orthogonal with respect to the Hermitian inner product if there exists a differential η such that $v_{P_i}(\eta) = -1$, $\eta_{P_i}(1) = 1$ for $1 \leq i \leq n$, and*

$$D + (\eta) \geq (q+1)\,G. \tag{1.1}$$

Proof. Let $D = P_1 + \cdots + P_n$ and G be divisors on a smooth, projective, absolutely irreducible curve X over $\mathbb{F}_q$ where $P_1, \ldots, P_n$ are distinct $\mathbb{F}_q$-rational points not in the support of G. Recall that the dual of $C_{\mathcal{L}}(D,G)$ may be expressed as

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, D - G + (\eta))$$

where η is a differential on X such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $1 \leq i \leq n$. Notice that for $h \in \mathcal{L}(G)$,

$$\begin{array}{rll} ev(f) *_h ev(h) = 0 & \text{iff} & \sum_{i=1}^{n} f(P_i)h^q(P_i) = 0 \forall f \in \mathcal{L}(G) \\ & \text{iff} & h^q \in \mathcal{L}(D - G + (\eta)) \\ & \text{iff} & q(h) \geq G - D + (\eta) \\ & \text{if} & -qG \geq G - D + (\eta) \end{array}$$

It follows that given $h \in \mathcal{L}(G)$, $ev(f) *_h ev(h) = 0$ for all $f \in \mathcal{L}(G)$ if

$$D + (\eta) \geq (q+1)\,G.$$

□

The next result is a consequence of the lemma above. Here, P_{00} denotes the common zero of the functions x and y on the Hermitian curve over $\mathbb{F}_{q^2}$.

Proposition 1.3. *Suppose that* $0 \leq a+b < q^2-2$. *Then the two-point code* $C_{\mathcal{L}}(D, aP_\infty + bP_{00})$ *on the Hermitian curve defined by* $y^q + y = x^{q+1}$ *over* $\mathbb{F}_{q^2}$ *is self-orthogonal with respect to the Hermitian inner product.*

Proof. Take $\eta = \frac{y^{b+1}}{z}dz$. Then

$$(\eta) = \left(q^3+q^2-q-(b+1)(q+1)\right)P_\infty - ((b+1)(q+1)+1)P_{00} - D$$

and the conditions of Lemma 1.1 are satisfied. □

Proposition 1.4. *Let* $0 \leq a+b < q^2-2$. *Then there exists a* $\left[\left[q^3-1, q^3-2\ell(aP_\infty+bP_{00})-l, d\right]\right]_q$ *code where*

$$d = min\{wt\left(C_{\mathcal{L}}(D, aP_\infty+bP_{00})^{\perp_h} \setminus C_{\mathcal{L}}(D, aP_\infty+bP_{00})\right)\}.$$

1.4.3. *Quantum codes from hyperelliptic curves*

In this subsection, we review Niehage's construction of quantum codes using hyperelliptic curves over finite fields [26]. This approaches uses ideas of Matsumoto [25].

Given $a_1, \ldots, a_n \in \mathbb{F}_q \setminus \{0\}$, define a weighted symplectic inner product on $\mathbb{F}_q^{2n}$ by

$$u *_a v := \sum_{i=1}^{n} a_i (u_i v_{i+n} - u_{i+n} v_i).$$

The weighted symplectic inner product gives more flexibility in the construction of quantum codes. However, a code C which is self-orthogonal with respect to $*_a$ may not be self-orthogonal with respect to the standard symplectic inner product $*$. To correct for this, the codewords of C are multiplied by $(a_1, \ldots, a_n, 1, \ldots, 1)$. This is detailed in the following lemma.

Lemma 1.2. *[26, Lemma 1] Let* C *be a linear code of length* $2n$ *over* $\mathbb{F}_q$ *that is self-orthogonal with respect to* $*_a$. *Let* M *denote the generator matrix for the quantum code defined by* C. *Then the code* C' *with generator matrix*

$$M' := M \cdot diag(a_1, \ldots, a_n, 1, \ldots, 1)$$

is a stabilizer code (with respect to the standard symplectic inner product) with the same parameters as C.

Proof. Suppose that $C \subseteq \mathbb{F}_q^{2n}$ is self-orthogonal with respect to $*_a$. Then

$$0 = u *_a v = \sum_{i=1}^{n} a_i \left(u_i v_{i+n} - u_{i+n} v_i\right) = \sum_{i=1}^{n} \left(\left(a_i u_i\right) v_{i+n} - u_{i+n} \left(a_i v_i\right)\right)$$

for all $u, v \in C$. This proves that

$$C' := \{(a_1 c_1, \ldots, a_n c_n, c_{n+1}, \ldots, c_{2n}) : c \in C\}$$

is self-orthogonal with respect to $*$. □

Next, we describe how to use $*_a$ and a hyperelliptic curve X over $\mathbb{F}_q$ to produce quantum codes. Let X be a smooth, projective, absolutely irreducible curve over $\mathbb{F}_q$ with an automorphism σ of order two that fixes the elements of $\mathbb{F}_q$. Set

$$D = P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n$$

where $P_1, \ldots, P_n, \sigma P_1, \ldots, \sigma P_n$ are distinct $\mathbb{F}_q$-rational points on X, and take G to be a divisor on X defined over $\mathbb{F}_q$ that is fixed by σ and $suppG \cap suppD = \emptyset$. Suppose η is a differential on X satisfying

$$v_{P_i}(\eta) = v_{\sigma P_i}(\eta) = -1$$

and

$$res_{P_i}(\eta) = -res_{\sigma P_i}(\eta)$$

for all $1 \leq i \leq n$. Then it can be shown (as in [26, Proposition 3] and [25, Proposition 1]) that

$$C_{\mathcal{L}}(D, G)^{\perp_a} = C_{\mathcal{L}}(D, D - G + (\eta)).$$

By an argument similar to that of Lemma 1.1, if $G \leq D - G + (\eta)$ then $C_{\mathcal{L}}(D, G)$ is self-orthogonal with respect to $*_a$. Now Lemma 1.2 implies that $C_{\mathcal{L}}(D, G)'$ is self-orthogonal with respect to $*$. This construction gives rise to quantum AG codes from hyperelliptic curves as discussed in [26].

1.4.4. *Asymptotic results*

Since their introduction by Goppa [11], algebraic geometry codes have been a tool for obtaining asymptotic results [40]. In this section, we describe families of asymptotically good quantum codes from AG codes.

Given a family of quantum $[[n_i, k_i, d_i]]$ codes, let $R = \lim_{n\to\infty} \frac{k_i}{n_i}$ and $\delta = \lim_{n\to\infty} \frac{d_i}{n_i}$. If $R > 0$ and $\delta > 0$, then the family is called *good*.

In [3], Ashikhmin, Litsyn, and Tsfasman proved that there exist asymptotically good families of binary quantum codes as follows.

Theorem 1.13. *[3] For any $\delta \in (0, \frac{1}{18}]$ and R lying on the broken line given by the piecewise linear function*

$$R(\delta) = 1 - \frac{1}{2^{m-1}-1} - \frac{10}{3}m\delta \text{ for } \delta \in [\delta_m, \delta_{m-1}],$$

where $m = 3, 4, 5, \ldots, \delta_2 = \frac{1}{18}, \delta_3 = \frac{3}{56}$, and

$$\delta_m = \frac{3}{5}\frac{2^{m-2}}{(2^{m-1}-1)(2^m-1)} \text{ for } m = 4, 5, 6, \ldots,$$

there exist polynomially constructible families of binary quantum codes with $n \to \infty$ and asymptotic parameters greater than or equal to (δ, R).

Later, Chen, Ling, and Xing improved the above theorem on certain intervals.

Theorem 1.14. *[8] Let*

$$\delta_t = \frac{2}{3}\frac{2^t - 3}{(2t+1)(2^t-1)}.$$

For $t \geq 3$ and $\delta \in (0, \delta_t)$, there exist polynomially constructible families of binary quantum codes with $n \to \infty$ and asymptotic parameters $(\delta, R_1(\delta))$, where $R_1(\delta) = 3t(\delta_t - \delta)$.

Remark 1.1. When $t = 3$, the above theorem gives the line given by $R_1 + 9\delta = \frac{30}{49}$ in $(0, \frac{10}{147})$. This line exceeds the Ashikhmin-Litsyn-Tsfasman bound in the interval $(\frac{8}{147}, \frac{1}{18})$.

Kim and Walker [23] generalized the ideas of Chen-Ling-Xing's construction to non-binary quantum codes and obtained the following.

Theorem 1.15. *[23] Let p be any prime number. If p is odd, choose integers $t \geq 1$ and $r \geq 0$ such that $2t + r \leq p + 1$. If $p = 2$, then choose integers $t \geq 3$ and $r = 1$. Let*

$$\delta(p, r, t) = \frac{(r+1)(p^t - 3)}{(r+2)(2t+r)(p^t-1)}.$$

Then for any δ with $0 < \delta < \delta(p, r, t) < \frac{1}{4}$, there exist polynomially constructible families of p-ary quantum codes with $n \to \infty$ and asymptotic parameters at least $(\delta, R_p(\delta))$, where

$$R_p(\delta) = \frac{2t(r+2)}{r+1}(\delta(p,r,t) - \delta).$$

Note that when $p = 2$, this theorem implies Theorem 1.14.

Proof. (Sketch of proof) We follow [23]. Let X be a smooth, projective, absolutely irreducible curve over $\mathbb{F}_q$ of genus g. Let G be a divisor, which is a multiple of a fixed $\mathbb{F}_q$-rational point P_0, and let D be the sum of all the other N $\mathbb{F}_q$-rational points on X. We pick any integers m_1 and m_2 such that $2g - 2 < m_1 < m_2 < N$. Then we consider the codes $T_j := C_{\mathcal{L}}(D, m_j P_0)$ for $j = 1, 2$. Then $T_1 \subset T_2$ and T_j $(j = 1, 2)$ is an $[N, m_j - g + 1, \geq N - m_j]$ code over $\mathbb{F}_q$ and its dual $T_j^{\perp}$ is an $[N, N - m_j + g - 1, \geq m_j - 2g + 2]$ code over $\mathbb{F}_q$.

From now on, we assume that the ground field is $\mathbb{F}_{q^2}$, where $q = p^t$ with p a prime. We want to obtain linear codes C_j over $\mathbb{F}_p$ from T_j over $\mathbb{F}_{q^2}$ for $j = 1, 2$ via concatenation defined as follows. Consider an $\mathbb{F}_p$-linear map $\sigma : \mathbb{F}_{q^2} \to \mathbb{F}_p^{2t+r}$ such that the image of σ is a $[2t + r, 2t, r + 1]$ Reed-Solomon code over $\mathbb{F}_p$ for some nonnegative integer r. If p is 2, we can choose $t \geq 1$ and $r = 1$. If p is odd, we choose t and r such that $2t + r \leq p + 1$ or $0 \leq r \leq p - 2t + 1$ due to the fact that Reed-Solomon codes over $\mathbb{F}_p$ exist only for lengths at most $p + 1$. We map T_j via σ componentwisely to get $C_j := \sigma(T_j)$. Then C_j $(j = 1, 2)$ is an $\mathbb{F}_p$-linear $[(2t + r)N,\ 2t(m_j - g + 1),\ \geq (r + 1)(N - m_j)]$ code. Further it can be shown [8] that for any vector $\mathbf{x} \in C_1^{\perp} \backslash C_2^{\perp}$, we have the weight of $\mathbf{x}$ is $\geq m_1 - 2g + 2$.

Hence using the CSS construction (Corollary 1.1), we obtain a quantum $[[n, k, d]]_p$ code $B = B(X)$ with parameters $n = (2t + r)N,\ k = 2t(m_2 - m_1),\ d \geq \min\{(r + 1)(N - m_2),\ m_1 - 2g + 2\}$. Furthermore, by letting $l = m_2 - m_1$, one can show that for any integers l and r with $0 < l \leq N - 2g$ and $0 \leq r \leq p + 1 - 2t$, there is a quantum $[[n, k, d]]_p$ code $B = B(X)$ with parameters $n = (2t + r)N,\ k = 2tl,\ d \geq \frac{r+1}{r+2}(N - 2g - l + 1)$.

Let $\mathbf{X} = \{X\}$ be a Garcia-Stichtenoth tower of polynomially constructible curves over $\mathbb{F}_{q^2}$ where $q = p^t$ with increasing genus $g = g(X)$ [10]. We know that $\mathbf{X}$ attains the Drinfeld-Vlăduţ bound, i.e., $\limsup_{X \in \mathbf{X}} \frac{\#X(\mathbb{F}_{q^2})}{g} = q - 1$. Then for any sequence of integers $\{l = l(X) \mid X \in \mathbf{X}\}$ with $0 < l \leq N - 2g$ for each X, we have $0 < \limsup_{x \in \mathbf{X}} \frac{l}{N} \leq 1 - \frac{2}{q-1}$. As in [8], for a fixed $\lambda \in (0, 1 - \frac{2}{q-1})$, we let $\lambda := \limsup_{x \in \mathbf{X}} \frac{l}{N}$.

Then

$$R := \limsup_{x \in \mathbf{X}} \frac{2tl}{(2t+r)N} = \frac{2t}{2t+r}\lambda,$$

and

$$\delta := \limsup_{x \in \mathbf{X}} \frac{\frac{r+1}{r+2}(N-2g-l+1)}{(2t+r)N)} = \frac{r+1}{(r+2)(2t+r)}\left(1 - \frac{2}{q-1} - \lambda\right).$$

Solving for λ in terms of δ, we get the following.

$$R_p(\delta) := R = \frac{2t}{2t+r}\left(1 - \frac{2}{q-1}\right) - \frac{2t(r+2)}{r+1}\delta.$$

Using $\delta(p,r,t)$ defined in Theorem 1.15, we finally get

$$R_p(\delta) = \frac{2t(r+2)}{r+1}(\delta(p,r,t) - \delta).$$

□

Another approach to finding asymptotically good quantum codes uses the construction of Subsection 1.4.3 and the tower of function fields in [37, Theorem 1.7]. We refer the reader to [26] for these results.

1.5. Bibliographical notes

The literature on quantum error-correcting codes is massive. The first paper on quantum error-correcting codes is by Shor (Scheme for reducing decoherence in quantum memory Phys. Rev. A 52 (1995)). Calderbank, Rains, Shor, and Sloane (Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory, vol. 44, (1998)) described the correspondence between binary additive quantum codes and additive self-orthogonal codes over $\mathbb{F}_4$. Nielsen and Chuang (Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000) is a widely used textbook in both quantum computation and quantum information theory.

Motivated by the fact that there exist good families of algebraic geometry codes meeting the Tsfasman-Vladut-Zink bound, which is better than the Gilbert-Varshamov bound, Ashikhmin, Litsyn, and Tsfasman (Asymptotically good quantum codes, Phys. Rev. A 63 (2001)) showed that asymptotically good binary quantum codes can be obtained from algebraic geometry codes in a polynomial construction. Some improvements in this direction have been made by Chen (Some good quantum error-correcting codes from algebraic-geometric codes, IEEE Trans. Inform. Theory, vol.

47, 2001), Chen, Ling, and Xing (Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, IEEE Trans. Inform. Theory, vol. 47, 2001), Kim and Walker (Nonbinary quantum error-correcting codes from algebraic curves, Discrete Math. (2007)), Sarvepalli, Klappenecker (Nonbinary quantum codes from Hermitian curves, Applied algebra, algebraic algorithms and error-correcting codes, 136–143, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006), Niehage (Nonbinary quantum Goppa codes exceeding the quantum Gilbert-Varshamov bound, Quantum Inf. Process. 6 (2007)), and others.

References

[1] S. A. Aly, A note on the quantum Hamming bound, arXiv:0711.4603v1 [quant-ph].
[2] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory 47 (2001), no. 7, 3065–3072.
[3] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, Asymptotically good quantum codes, Phys. Rev. A 63 (2001), 032311.
[4] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Mixed state entanglement and quantum error correction, Phys. Rev. A 54 (1996), 3824.
[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory, vol. 44, pp. 1369–1387, 1998.
[6] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54 (1996), 1098–1105.
[7] H. Chen, Some good quantum error-correcting codes from algebraic-geometric codes, IEEE Trans. Inform. Theory, vol. 47, pp. 2059–2061, 2001.
[8] H. Chen, S. Ling, and C. Xing, Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, IEEE Trans. Inform. Theory, vol. 47, pp. 2055–2058, 2001.
[9] K. Feng and Z. Ma, A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, IEEE Trans. Inform. Theory, vol. 50 (2004), no. 12, 3323–3325.
[10] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound, Invent. Math. 121 (1995), no. 1, 211–222.
[11] V. D. Goppa, *Algebraico-geometric codes*, Math. USSR-Izv. **21** (1983), 75–91.
[12] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.
[13] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. dissertation, California Inst. of Technol., Pasadena, CA, 1997.
[14] M. Grassl and T. Beth, Cyclic quantum error-correcting codes and quantum shift registers, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. 456 (2000), no. 2003, 2689–2706.

[15] M. Grassl and T. Beth, Relations between classical and quantum error-correcting codes, in Proceedings Workshop "Physik und Informatik", DPG-Frhjahrstagung, Heidelberg, Mrz 1999, 45–57.
[16] M. Grassl, T. Beth, and M. Rötteler, On optimal quantum codes, Intl. J. Quantum Information 2 (2004) 55-64.
[17] M. Grassl, W. Geiselmann, and Th. Beth, Quantum Reed-Solomon codes, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), 231–244, Lecture Notes in Comput. Sci., 1719, Springer, Berlin, 1999.
[18] M. Homma and S. J. Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, Des. Codes Cryptogr. 40 (2006), no. 1, 5–24.
[19] M. Homma and S. J. Kim, Toward the determination of the minimum distance of two-point codes on a Hermitian curve, Des. Codes Cryptogr. 37 (2005), no. 1, 111–132.
[20] M. Homma and S. J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance, Des. Codes Cryptogr. 38 (2006), no. 1, 55–81.
[21] M. Homma and S. J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic, Des. Codes Cryptogr. 39 (2006), no. 3, 375–386.
[22] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary Stabilizer Codes over Finite Fields IEEE Transactions on Information Theory, Volume 52, Issue 11, pages 4892 - 4914, 2006.
[23] J.-L. Kim and J. L. Walker, Nonbinary quantum error-correcting codes from algebraic curves, Discrete Math. (2007), doi:10.1016/j.disc.2007.08.038.
[24] E. Knill and R. Laflamme, A theory of quantum error-correcting codes, Phys. Rev. A, vol. 55, no. 2, pp. 900–911, 1997.
[25] R. Matsumoto, Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, IEEE Trans. Inform. Theory 48 (2002), no. 7, 2122–2124.
[26] A. Niehage, Nonbinary quantum Goppa codes exceeding the quantum Gilbert-Varshamov bound, Quantum Inf. Process. 6 (2007), no. 3, 143–158.
[27] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[28] E. M. Rains, Nonbinary quantum codes, IEEE Trans. Inform. Theory 45 (1999), 1827–1832.
[29] P. K. Sarvepalli and A. Klappenecker, Nonbinary quantum codes from Hermitian curves, Applied algebra, algebraic algorithms and error-correcting codes, 136–143, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.
[30] G. Seroussi and A. Lempel, Factorization of symmetric matrices and trace-orthogonal bases in finite fields, SIAM J. Comput. 9 (1980), no. 4, 758–767.
[31] P. W. Shor, Scheme for reducing decoherence in quantum memory Phys. Rev. A 52 (1995), 2493.
[32] P. Shor and R. Laflamme, Quantum analog of the MacWilliams identities for classical coding theory, Phys. Rev. Lett 78 (1997), 1600-1602.
[33] A. M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes.

IEEE Trans. Inform. Theory 45 (1999), no. 7, 2492–2495.
[34] A. M. Steane, Multiple-particle interference and quantum error correction. Proc. Roy. Soc. London Ser. A 452 (1996), no. 1954, 2551–2577.
[35] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.
[36] H. Stichtenoth, Self-dual Goppa codes, J. Pure Appl. Algebra 55 (1988), no. 1-2, 199–211.
[37] H. Stichtenoth, Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound. IEEE Trans. Inform. Theory 52 (2006), no. 5, 2218–2224.
[38] H. J. Tiersma, Remarks on codes from Hermitian curves, IEEE Trans. Inform. Theory 33 (1987), no. 4, 605–609.
[39] M. A. Tsfasman and S. G. Vlădut, Geometric approach to higher weights, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1564–1588.
[40] M. A. Tsfasman, S. G. Vlădut, and T. Zink, Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachrichtentech., **109** (1982), 21–28.
[41] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes, Coding Theory and Algebraic Geometry, Proceedings, Luminy, 1991, Lecture Notes in Mathematics **1518**, Springer-Verlag, 1992, 99–107.