Error-Correcting Nonbinary Quantum Codes Based on Algebraic Curves

Venkata chalapathi Uday[1], Gautam Kumar Rajput[2]

1. Research Scholar ,Department of Mathematics,Sunrise university, Alwar, Rajasthan

2. Associate professor,Department of Mathematics, Sunrise University, Alwar,Rajasthan

Received: 13.07.2024 Revised: 11.08.2024 Accepted: 06.09.2024

ABSTRACT
For nonbinary quantum error-correcting codes, we present a new explanation and demonstrate a generalized CSS construction. Nonbinary quantum stabilizer codes of various lengths, dimensions, and minimum distances from algebraic curves can be constructed using this method. From a Garcia-Stichtenoth tower of function fields, we also provide polynomial-time constructible asymptotic good nonbinary quantum codes.

Keywords: Algebraic geometric codes; Nonbinary quantum codes

INTRODUCTION

There are a number of ways that binary quantum error-correcting codes have been made. Algebraic geometry codes are used in one interesting construction. The idea is to apply the binary CSS construction to the asymptotically good algebraic geometry codes that come from the Garcia-Stichtenoth tower of function fields over$\mathbb{F}_{q^2}$ (where q is a power of 2) attaining the Drinfeld-Vladut bound.

It makes sense to think about nonbinary quantum codes. Rains demonstrates that there are applications for which nonbinary quantum codes would be more appropriate than binary quantum codes, in addition to the straightforward fact that nonbinary error-correcting codes are intriguing in the classical context. Despite the fact that nonbinary quantum codes have been considered, the binary case has received the majority of attention thus far. The issue of asymptotically good nonbinary quantum codes, in particular, has not previously been investigated.

Based on two binary linear codes provided by Calderbank et al., we present a new exposition and proof of a nonbinary version of the generalized binary CSS construction. for an alternative strategy. For nonbinary quantum codes, we can derive a variety of parameters by employing this construction and algebraic curves. In order to obtain nonbinary quantum codes that are constructible in polynomial time and that are asymptotically good, we further apply this construction to the tower of function fields that are defined in by concatenating Reed-Solomon codes.

Preliminaries

We provide some definitions and fundamental information regarding quantum codes in this section. First, we recall the construction of quantum stabilizer codes using a generalized binary CSS. The nonbinary case is then generalized by us.

Definition 2.1 (Calderbank et al.). A binary $[[n,k,d]]_2$ quantum error-correcting code is a 2^k-dimensional subspace of $\mathbb{C}^{2^n} \simeq (\mathbb{C}^2)^{\otimes n}$ which can correct $\frac{d-1}{2}[$ errors.

In Calderbank et al., showed how to construct binary quantum error-correcting codes from additive $\mathbb{F}_4$-codes. Briefly, the construction is as follows: Let ω be a primitive element of $\mathbb{F}_4$. Any vector in $\mathbb{F}_4^n$ can be written uniquely as $\omega\mathbf{a} + \bar{\omega}\mathbf{b}$ with $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^{2n}$. This gives a bijection map $\psi: \mathbb{F}_4^n \to \mathbb{F}_2^{2n}, \psi(\omega\mathbf{a} + \bar{\omega}\mathbf{b}) = (\mathbf{a} \mid \mathbf{b})$. One interprets $\mathbb{F}_2^{2n}$ as $\bar{E} = E/\{\pm I, \pm iI\}$, where E is the quantum error group on $\mathbb{C}^{2^n}$. Now let C be an additive $\mathbb{F}_4$-code which is selforthogonal with respect to the trace inner product. Then $\bar{S} := \psi(C)$ is a subgroup of $\bar{E}$ whose inverse image $S \leqslant E$ is an abelian group acting on $\mathbb{C}^{2^n}$. Letting Q be any joint eigenspace of the elements of S, we have that Q is a binary quantum error-correcting code and the parameters of Q can be computed from the parameters of C. Moreover, one may start with a pair of binary linear codes $C_1 \subseteq C_2$ and form the additive $\mathbb{F}_4$ code $C := \omega C_1 + \bar{\omega} C_2^{\perp}$ Then the above construction yields:

Theorem 2.2 Suppose $C_1 \subseteq C_2 \subseteq \mathbb{F}_2^n$ are binary linear codes with dimensions k_1 and k_2, respectively. Then there exists a binary $[[n, k_2 - k_1, d]]_2$ quantum code, where $d = \min\{d(C_2 \setminus C_1), d(C_1^{\perp} \setminus C_2^{\perp})\}$.

In Theorem 2.2, and in the remainder of this paper, the notation $d(A \setminus B)$ means the minimum weight of any vector in A but not in B.

Our next goal is to explore CSS-type constructions for nonbinary quantum codes. We first give analogs of additive codes and the quantum error group for the nonbinary case. For the remainder of the paper, we write $q = p^m$, where p is an odd prime.

We call $C \subseteq \mathbb{F}_q^n$ an $\mathbb{F}_p$-linear code if C is linear over $\mathbb{F}_p$. This generalizes the notion of additive $\mathbb{F}_4$-codes, since being an additive subgroup of $\mathbb{F}_4^n$ is equivalent to being an $\mathbb{F}_2$-vector space contained in $\mathbb{F}_4^n$. Additive $\mathbb{F}_4$-codes which are self-orthogonal under the trace inner product were used to construct stabilizer quantum codes. This idea was generalized in to the relationship between self-orthogonal codes over $\mathbb{F}_{q^2}$ and q-ary quantum codes for any odd prime power q.

An explicit error basis for p^m -ary quantum codes is described as follows. Let T and R be the linear operators acting on the p-dimensional complex space $\mathbb{C}^p$ defined by

$$T_{i,j} = \delta_{i,j-1}(\text{mod} p) \quad \text{and} \quad R_{i,j} = \xi^i \delta_{i,j}$$

where $\xi = e^{2\pi\sqrt{-1}/p}$, the indices range from 0 to $p - 1$, and $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. The set of operators $T^i R^j$ forms an orthogonal basis under the inner product defined by $\langle A, B\rangle = \text{Tr}(A^* B)$, where A^* is the Hermitian transpose of A.

Fix a basis $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ for $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. For $a, b \in \mathbb{F}_{p^m}$ we can write uniquely

$$a = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_m\gamma_m, \quad b = b_1\gamma_1 + b_2\gamma_2 + \cdots + b_m\gamma_m$$

with $a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{F}_p$. Define

$$T_a R_b = (T^{a1} \otimes T^{a2} \otimes \cdots \otimes T^{am})(R^{b1} \otimes R^{b2} \otimes \cdots \otimes R^{bm})$$

The set of operators of the form $T_a R_b$, where a and b ranges over all of $\mathbb{F}_{p^m}$, forms an orthogonal basis of unitary operators acting on the p^m-dimensional complex vector space $\mathbb{C}^{p^m}$.

Let $\mathbf{a} = (a^{(1)}, \ldots, a^{(n)}), \mathbf{b} = (b^{(1)}, \ldots, b^{(n)}) \in \mathbb{F}_q^n$. As seen above, it is enough to consider the error operators given by

$$E_{\mathbf{a},\mathbf{b}} = T_{a^{(1)}} R_{b^{(1)}} \otimes T_{a^{(2)}} R_{b^{(2)}} \otimes \cdots \otimes T_{a^{(n)}} R_{b^{(n)}}$$

The set of operators

$$\mathcal{E} = \{\xi^i E_{\mathbf{a},\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \text{ and } 0 \leqslant i \leqslant p - 1\}$$

form an error group of order p^{2mn+1}. Quantum stabilizer codes are defined as joint eigenspaces of the operators of a commutative subgroup S of $\mathcal{E}$; see also the appendix of.

We are now ready to develop the q-ary CSS construction. We begin with a construction given inthat is analogous to the first construction presented in, and then follow the lead of to derive other constructions. We note that our q-ary CSS construction generalizes the p-ary CSS construction [Theorem 5] as the latter construction uses only self-orthogonal codes over $\mathbb{F}_{p^2}$ where p is a prime. The main result is Theorem 2.7, which will be used in Section 3 to construct asymptotically good sequences of nonbinary quantum codes.

As above, we write $q = p^m$, where p is an odd prime. For $\mathbf{a} = (a^{(1)}, \ldots, a^{(n)}), \mathbf{b} = (b^{(1)}, \ldots, b^{(n)}) \in \mathbb{F}_q^n$, let $\mathbf{a} \cdot \mathbf{b} = \sum a^{(i)} b^{(i)}$ be the usual inner product on $\mathbb{F}_q^n$. For $(\mathbf{a} \mid \mathbf{b}), (\mathbf{a}' \mid \mathbf{b}') \in \mathbb{F}_q^{2n}$, set $(\mathbf{a} \mid \mathbf{b}) * (\mathbf{a}' \mid \mathbf{b}') = \text{Tr}(\mathbf{a} \cdot \mathbf{b}' - \mathbf{a}' \cdot \mathbf{b})$, where $\text{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. We see that if $q = p$ then $(\mathbf{a} \mid \mathbf{b}) * (\mathbf{a}' \mid \mathbf{b}') = \mathbf{a} \cdot \mathbf{b}' - \mathbf{a}' \cdot \mathbf{b}$; this inner product on $\mathbb{F}_p^{2n}$ was studied in [16,17].

Definition 2.3

A q-ary $[[n, k, d]]_q$ quantum error-correcting code is a q^k-dimensional subspace of $\mathbb{C}^{q^n} \simeq (\mathbb{C}^q)^{\otimes n}$ which can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.

Proposition 2.4

Suppose $C \subseteq \mathbb{F}_q^{2n}$ is an $\mathbb{F}_p$-linear code of length $2n$ having p^r codewords. Let $C^{\perp *}$ be the dual of C with respect to the inner product " $*$ ". If $C \subseteq C^{\perp *}$, then there is a q-ary $[[n, n - \frac{r}{m}, d]]_q$ quantum code with $d = d(C^{\perp *} \setminus C)$.

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^2}^n$, define $\mathbf{x} \circ \mathbf{y} = \sum(x_i y_i^q - x_i^q y_i)$. This map is $\mathbb{F}_q$-bilinear and generalizes the inner product of [16, p. 1879]. Note that for any $\gamma_0 \in \mathbb{F}_q$, there exists $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfying $\gamma^q = \gamma_0 - \gamma$; indeed since the trace map $\text{Tr}\colon \mathbb{F}_{q^2} \to \mathbb{F}_q$ is onto and $\mathbb{F}_q$-linear, we may pick $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\text{Tr}(\gamma) = \gamma_0$. Further, for any such $\gamma, \{1, \gamma\}$ is a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ since $\gamma \notin \mathbb{F}_q$.

Lemma 2.5.
Suppose $D \subseteq \mathbb{F}^n_{q^2}$ is an $\mathbb{F}_q$-linear code satisfying $D \subseteq D^{\perp\circ}$, where $D^{\perp\circ}$ is the dual of D with respect to " $\circ$ ". Fix $\gamma_0 \in \mathbb{F}_q$ and choose $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfying $\gamma^q = \gamma_0 - \gamma$. Define an $\mathbb{F}_q$-linear map $f: \mathbb{F}^n_{q^2} \to \mathbb{F}^{2n}_q$ by $f(x_1, \dots, x_n) = (x^{(1)}_1, \dots, x^{(1)}_n \mid x^{(2)}_1, \dots, x^{(2)}_n)$, where $x_i = x^{(1)}_i + \gamma x^{(2)}_i$ for $i = 1, \dots, n$. Then $(D)^q \subseteq f(D^{\perp\circ}) = (f(D))^{\perp *}$, where $(f(D))^{\perp *}$ is the dual of $f(D)$ with respect to " $*$ ".

Proof.
Clearly, $f(D) \subseteq f(D^{\perp\circ})$ since $D \subseteq D^{\perp 0}$. It remains to show that $f(D^{\perp 0}) = (f(D))^{\perp *}$. To do this, let $\mathbf{x} \in D$, $\mathbf{y} \in D^{\perp 0}$. Then

$$\begin{aligned}
0 &= \mathbf{x} \circ \mathbf{y} \\
&= \sum (x_i y_i^q - x_i^q y_i) \\
&= \sum ((x^{(1)}_i + \gamma x^{(2)}_i)(y^{(1)}_i + \gamma y^{(2)}_i)^q - (x^{(1)}_i + \gamma x^{(2)}_i)^q (y^{(1)}_i + \gamma y^{(2)}_i)) \\
&= \sum ((x^{(1)}_i + \gamma x^{(2)}_i)(y^{(1)}_i + \gamma^q y^{(2)}_i) - (x^{(1)}_i + \gamma^q x^{(2)}_i)(y^{(1)}_i + \gamma y^{(2)}_i)) \\
&= \sum (x^{(1)}_i y^{(1)}_i + \gamma^q x^{(1)}_i y^{(2)}_i + \gamma x^{(2)}_i y^{(1)}_i + \gamma^{q+1} x^{(2)}_i y^{(2)}_i) \\
&\quad - (x^{(1)}_i y^{(1)}_i + \gamma x^{(1)}_i y^{(2)}_i + \gamma^q x^{(2)}_i y^{(1)}_i + \gamma^{q+1} x^{(2)}_i y^{(2)}_i) \\
&= (\gamma^q - \gamma) \sum (x^{(1)}_i y^{(2)}_i - x^{(2)}_i y^{(1)}_i) \\
&= (\gamma_0 - 2\gamma) \sum (x^{(1)}_i y^{(2)}_i - x^{(2)}_i y^{(1)}_i).
\end{aligned}$$

But $\gamma_0 - 2\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and so

$$\sum (x^{(1)}_i y^{(2)}_i - x^{(2)}_i y^{(1)}_i) = 0$$

Therefore

$$f(\mathbf{x}) * f(\mathbf{y}) = \mathrm{Tr}(\sum (x^{(1)}_i y^{(2)}_i - x^{(2)}_i y^{(1)}_i)) = 0$$

This shows $f(D^{\perp\circ}) \subseteq (f(D))^{\perp *}$. Since these two codes have the same number of codewords, they must be equal.

Proposition 2.6. Let $C_1 \subseteq C_2 \subseteq \mathbb{F}^n_q$ be $\mathbb{F}_q$-linear codes, so that $C^\perp_2 \subseteq C^\perp_1$, where $C^\perp_i$ is the dual of C_i under the usual inner product. Let ω be a primitive element of $\mathbb{F}_{q^2}$ and write $\bar{\omega} = \omega^q$. Set $D = \omega C_1 + \bar{\omega} C^\perp_2 \subseteq \mathbb{F}^n_{q^2}$. Then the dual $D^{\perp\circ}$ of D is given by $D^{\perp\circ} = \bar{\omega} C^\perp_1 + \omega C_2$. Hence $D \subseteq D^{\perp\circ}$ and

$$d(D^\perp \setminus D) = \min\{d(C_2 \setminus C_1), d(C^\perp_1 \setminus C^\perp_2)\}$$

Proof. Note first that $|D| = q^{k_1 + n - k_2}$, and so

$$|D^{\perp\circ}| = q^{2n-(n+k_1-k_2)} = q^{n-k_1+k_2} = |\bar{\omega} C^\perp_1 + \omega C_2|.$$

Now pick $\mathbf{x} \in C_1$, $\mathbf{y} \in C^\perp_2$, $\mathbf{a} \in C^\perp_1$, and $\mathbf{b} \in C_2$. Then

$(\omega\mathbf{x} + \bar{\omega}\mathbf{y}) \circ (\bar{\omega}\mathbf{a} + \omega\mathbf{b})$

$= \sum ((\omega x_i + \bar{\omega} y_i)(\omega a_i + \bar{\omega} b_i) - (\bar{\omega} x_i + \omega y_i)(\bar{\omega} a_i + \omega b_i)) = (\omega^2 - \bar{\omega}^2)(\sum x_i a_i - \sum y_i b_i) = 0$ since $\mathbf{x} \cdot \mathbf{a} = \mathbf{y} \cdot \mathbf{b} = 0$. The last sentence of the proposition follows since $C_1 \subseteq C_2, C^\perp_2 \subseteq C^\perp_1$, and $\omega C_1 \cap \bar{\omega} C^\perp_2 = \bar{\omega} C^\perp_1 \cap \omega C_2 = \{0\}$.

Next, we give a construction which produces a q-ary quantum code from any two $\mathbb{F}_q$-linear codes $C_1 \subseteq C_2 \subseteq \mathbb{F}^n_q$; for a different approach. This is a q-ary version of the binary CSS construction as it is also based on two linear codes over $\mathbb{F}_q$, and so it is a generalization of which is based on self-orthogonal codes.

Theorem 2.7. Let $q = p^m$, where p is an odd prime and $m \geqslant 1$ is an integer. Suppose $C_1 \subseteq C_2 \subseteq \mathbb{F}^n_q$ are $\mathbb{F}_q$-linear codes with dimensions k_1 and k_2, respectively. Then there exists a q-ary $[[n, k_2 - k_1, d]]_q$ quantum code, where $d = \min\{d(C_2 \setminus C_1), d(C^\perp_1 \setminus C^\perp_2)\}$.

Proof. Set $D = \omega C_1 + \bar{\omega} C^\perp_2$ as in Proposition 2.6. Then $f(D) \subseteq (f(D))^{\perp *}$ by Proposition 2.6 and Lemma 2.5. Note that $f(D)$ is an $\mathbb{F}_q$-linear code in $\mathbb{F}^{2n}_q$, hence an $\mathbb{F}_p$-linear code with p^r elements, where $r = m(k_1 + n - k_2)$. Our claim now follows by applying Proposition 2.4 by letting $C = f(D)$.

Example 2.8. Let C_2 be the ternary Golay [11,6,5] code and let C_1 be the subcode of C_2 consisting of codewords whose weight is divisible by 3. Then C_1 is a ternary [11,5,6] code and in fact is equal to $C^\perp_2$. By Theorem 2.7, we obtain a ternary double-error correcting quantum $[[11,1,5]]_3$ code.

Good sequences of q-ary quantum AG codes

We assume the results from Section II of and use the ideas of Section III of that paper. Note, however, that the authors of used only the trivial binary MDS code in the concatenation while we use Reed-Solomon codes over $\mathbb{F}_p$, which allows us to obtain various lengths, dimensions, and minimum distances of nonbinary quantum codes.

We first recall the basics of algebraic geometry codes. For more details.

Definition 3.1. Let X be a smooth, projective, absolutely irreducible curve over $\mathbb{F}_q$ of genus g. Let $P = \{P_1 , \dots , P_n \}$ be a set of distinct $\mathbb{F}_q$ -rational points on X, and let G be a divisor on X with support disjoint from P. Let $f(G) = \{f \in \mathbb{F}_q\ (X) \mid (f) + G \geqslant 0\} \cup \{0\}$ be the vector space of rational functions associated to G. The algebraic geometric code $C(X, P, G)$ associated to X, P and G is

$$C_X(P, G) := \{(f(P_1), \dots , f(P_n)) \mid f \in f(G)\}.$$

Theorem 3.2. Let X, P and G be as in Definition 3.1 with g the genus of X and n the number of points in P. Assume $2g - 2 < degG < n$. Then $C_X(P, G)$ is a linear code over $\mathbb{F}_q$ with length n, dimension $k = \deg G + 1 - g$ and minimum distance $d \geqslant n - \deg G$. Further, the minimum distance of the dual code $C_X(P, G)$ is at least $\deg G - 2g + 2$.

Algebraic geometry codes were first introduced by Goppa in 1977. Only a few years later, Tsfasman, et al. used modular curves to show that, for $q \geqslant 49$ a square, there exist sequences of algebraic geometry codes over $\mathbb{F}_q$ which are asymptotically better than the Gilbert-Varshamov bound on a certain interval of relative minimum distance. A few such sequences are explicitly known (or at least the curves on which they are based are explicitly known); we will use a sequence of curves given by Garcia and Stichtenoth to construct asymptotically good nonbinary quantum error-correcting codes.

For our construction, we need only one-point codes, that is, algebraic geometry codes where the divisor G is a multiple of some chosen $\mathbb{F}_q$-rational point P_0 and the set P consists of all the other $\mathbb{F}_q$-rational points on X. Set $= N(X): = |P| = \#X(\mathbb{F}_q\ ) - 1$. Pick integers m_1 and m_2 with $2g - 2 < m_1 < m_2 < N$. We consider the codes $T_j : = C_X(P, m_j P_0)$ for $j = 1,2$. Then $T_1 \subset T_2$ and, from Theorem 3.2, we see that T_j is an $[N, m_j - g + 1, \geqslant N - m_j]$ code over $\mathbb{F}_q$ and the dual $T_j^\perp$ of T_j is an $[N, N - m_j + g - 1, \geqslant m_j - 2g + 2]$ code over $\mathbb{F}_q$.

As in, we use concatenation to obtain $\mathbb{F}_p$-linear codes C_1 and C_2 from T_1 and T_2. As we will be working with fields of square order, we will now switch notation so that our ground field is $\mathbb{F}_{q^2}$, where $q = p^t$. We wish to have an $\mathbb{F}_p$-linear map $\pi_\star : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_p^{2t+r}$, for some nonnegative integer r, such that the image $C_\star$ of $\pi_\star$ is a $[\ 2t + r, 2t, r + 1]$ Reed-Solomon code over $\mathbb{F}_p$. Since Reed-Solomon codes of over $\mathbb{F}_p$ exist only for lengths at most $p + 1$, we must have

$$2t + r \leqslant p + 1, \quad \text{i.e.,} \quad 0 \leqslant r \leqslant p - 2t + 1$$

Define $\pi : \mathbb{F}_{q^2}^N \rightarrow \mathbb{F}_p^{N(2t+r)}$ by $\pi((x_1 , \dots , x_N)) = (\pi_* (x_1), \dots , \pi_\star (x_N))$. Then we have

$$C_1 : = \pi(T_1) \subset \pi(T_2) =: C_2$$

Thus $C_j , (j = 1,2)$ is an $\mathbb{F}_p$-linear $[(2t + r)N, 2t(m_j - g + 1), \geqslant (r + 1)(N - m_j)]$ code (see [10] or [8]). The dual of $C_j\ (j = 1,2)$ is $C_j^\perp = S \oplus (\pi' (T_j^\perp))$, where S is the direct sum of N copies of $C_\star^\perp$ and π' is the $\mathbb{F}_q$ -linear injective "dual basis" map, as. For any vector $\mathbf{x} \in C_1^\perp \setminus C_2^\perp$, we have $\mathrm{wt}(\mathbf{x}) \geqslant m_1 - 2g + 2$, just as in the binary case (see proof of Theorem 1.2).

Proposition 3.3. With notation as above, we get a p-ary quantum $[[n, k, d]]_p$ code $B = B(X)$ with
n $= (2t + r)N$
$k = 2t(m_2 - m_1)$
$d \geqslant \min\{(r + 1)(N - m_2), m_1 - 2g + 2\}$

Example 3.4. Let X be the Hermitian curve defined by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$with $q = p^t$; this is the base level of the Garcia-Stichtenoth tower. There are $q^3 + 1\mathbb{F}_{q^2}$-rational points on X, and the genus of X is $q(q - 1)/2$. We choose integers m_1 and m_2 with $q^2 - q - 2 = 2g - 2 < m_1 < m_2 < N = q^3$ and obtain $\mathbb{F}_{q^2}$-linear codes $T_j , j = 1,2$, with parameters $[q^3, m_j - \frac{q(q-1)}{2} + 1, \geqslant q^3 - m_j]$. For any integer r with $0 \leqslant r \leqslant p + 1 - 2t$ as above, we get a p-ary quantum $[[n, k, d]]_p$ code B with
$n = (2t + r)q^3$
$k = 2t(m_2 - m_1)$
$d \geqslant \min\{(r + 1)(q^3 - m_2), m_1 - q(q - 1) + 2\}$

As a final step before we consider the asymptotic behavior of our quantum codes, we make a few remarks. Let X be a curve of genus g with $N+1$ rational points. If we choose integers m_1 and m_2 with $2g-2 < m_1 < m_2 < N$, then $P := m_2 - m_1$ satisfies $0 < l \leqslant N - 2g$. Conversely, given an integer P satisfying $0 < l \leqslant N - 2g$, set

$$m_2 = \frac{(r+1)N + 2g + P - 2}{r+2}]$$

and $m_1 = m_2 - P$. Then since

$$\begin{aligned} m_1 - (2g-2) &= \frac{(r+1)N + 2g + P - 2}{r+2}] - P - (2g-2) \\ &\geqslant \frac{(r+1)N + 2g + P - 2}{r+2} - \frac{r+1}{r+2} - P - (2g-2) \\ &= \frac{r+1}{r+2}(N + 1 - 2g - P) \\ &> 0 \end{aligned}$$

$$\begin{aligned} m_2 - m_1 &= P \\ &> 0 \end{aligned}$$

and

$$\begin{aligned} N - m_2 &\geqslant N - \frac{(r+1)N + 2g + P - 2}{r+2} \\ &= \frac{N - 2g - P + 2}{r+2} \\ &\geqslant \frac{2}{r+2} \\ &> 0 \end{aligned}$$

we have $2g - 2 < m_1 < m_2 < N$. Also, since

$$\begin{aligned} (r+1)(N - m_2) &= (r+1)N - (r+2)m_2 + m_2 \\ &\geqslant (r+1)N - ((r+1)N + 2g + P - 2) + m_2 \\ &= -2g - k + P + m_2 \\ &= m_1 - m_2 - 2g + 2 + m_2 \\ &= m_1 - (2g-2) \\ &\geqslant \frac{r+1}{r+2}(N - 2g - P + 1) \end{aligned}$$

we have

Proposition 3.5. Let X be a curve of genus g with N rational points. For any integers P and r with $0 < l \leqslant N - 2g$ and $0 \leqslant r \leqslant p + 1 - 2t$, there is a p-ary quantum $[[n, k, d]]_p$ code $B = B(X)$ with parameters

$$\begin{aligned} n &= (2t + r)N \\ k &= 2tP \\ d &\geqslant \frac{r+1}{r+2}(N - 2g - P + 1) \end{aligned}$$

Now let $\mathbf{X} = \{X\}$ be a Garcia-Stichtenoth tower of polynomially constructible curves over $\mathbb{F}_{q^2}$ where $q = p^t$ having increasing genus $g = g(X)$ and attaining the Drinfeld-Vladut bound, i.e., satisfying

$$\limsup_{X \in \mathbf{X}} \frac{\#X(\mathbb{F}_{q^2})}{g} = q - 1$$

Then for any sequence of integers $\{P = P(X) \mid X \in \mathbf{X}\}$ with $0 < l \leqslant N - 2g$ for each X, we have $0 < lim\text{sup}_{X \in \mathbf{X}} \frac{P}{N} \leqslant 1 - \frac{2}{q-1}$. Indeed, by choosing the values of P appropriately, we can have $\limsup_{X \in \mathbf{X}} \frac{P}{N} = \lambda$ for any λ with $0 < \lambda \leqslant 1 - \frac{2}{q-1}$.

We put

$$R:=\limsup_{X\in\mathbf{X}}\frac{2tP}{(2t+r)N}$$
$$=\frac{2t}{2t+r}\lambda$$
$$\delta:=\limsup_{X\in\mathbf{X}}\frac{\frac{r+1}{r+2}(N-2g-P+1)}{(2t+r)N}$$
$$=\frac{r+1}{(r+2)(2t+r)}(1-\frac{2}{q-1}-\lambda)$$

Note that for a sequence of p-ary $[[n(B),k(B),d(B)]]_p$ quantum codes $\mathbf{B}=\{B=B(X)\}$ coming as in Proposition 3.5 from the Garcia-Stichtenoth tower, we have

$$\limsup_{B\in\mathbf{B}}\frac{k(B)}{n(B)}=R \quad \text{and} \quad \limsup_{B\in\mathbf{B}}\frac{d(B)}{n(B)}\geqslant\delta$$

To get an expression for R in terms of δ, we solve for λ in terms of δ and substitute, yielding

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

In order to have $R>0$, we need $\delta<\delta(p,r,t)$, where

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

We have proved the following.

Theorem 3.6. Let p be any odd prime number. Suppose that $t\geqslant 1$ and $r\geqslant 0$ are integers satisfying $2t+r\leqslant p+1$. Let $\delta(p,r,t)$ be as above. 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

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

In Figs. 1-3, we plot some of our bounds $(\delta,\ R_p\ (\delta))$ and compare them with Ashikhmin and Knill's nonbinary quantum Gilbert-Varshamov (qGV) bound, which is nonconstructive. We note that in the case of the binary quantum codes, there is a large information rate gap between the nonconstructive binary quantum Gilbert-Varshamov bound and the constructive bounds (for example, gap ≈ 0.5 at $\delta=0.06$), and the nonzero information rate from the constructive bound is possible up to $\delta\approx 0.07$. However our 53-ary quantum codes as seen in Fig. 3 have a small information rate gap ≈ 0.1 at $\delta=0.06$ when $r=0$ and $t=1$, and can have nonzero information rate up to $\delta\approx 0.24$. As p increases, the information rate gap is getting smaller although our bounds $(\delta,\ R_p\ (\delta))$ in Theorem 3.6 are under the nonbinary qGV bound as the δ-intercept $\delta(p,r,t)$ of the graph is $<\frac{1}{4}$.

Remark 3.7. The case when $p=2$ was discussed in [7]. In this case we require that $t\geqslant 3$ is an integer and $r=0$ or 1. Then plugging in $p=2$ and $r=1$ into $\delta(p,r,t)$ in Theorem 3.6 gives

$$\delta(2,1,t)=\delta_t=\frac{2(2^t-3)}{3(2t+1)(2^t-1)}$$
$$R_2(\delta)=3t(\delta_t-\delta)$$

which is Theorem 1.2.

Using the same ideas, we can construct p^t-ary quantum codes.

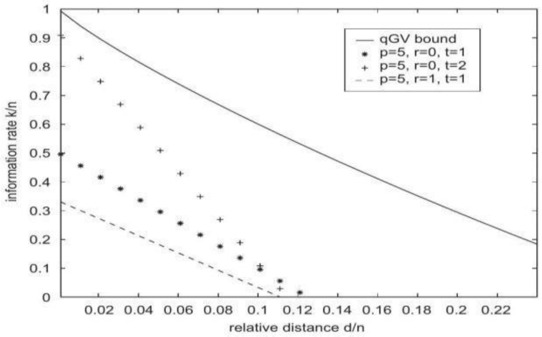

Fig 1. Asymptotically good sequences of p-ary quantum codes where $p=5$ with $r=0$ and $t=1,2$, or with $r=1$ and $t=1$.

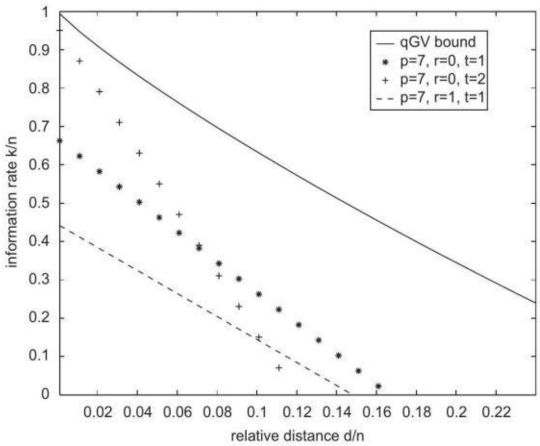

Fig 2. Asymptotically good sequences of p-ary quantum codes where $p = 7$ with $r = 0$ and $t = 1,2$, or with $r = 1$ and $t = 1$.

Theorem 3.8. Let p be an odd prime, and let $t \geqslant 1$ and $r \geqslant 1$ be integers with $r \leqslant p^t - 1$. Set

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

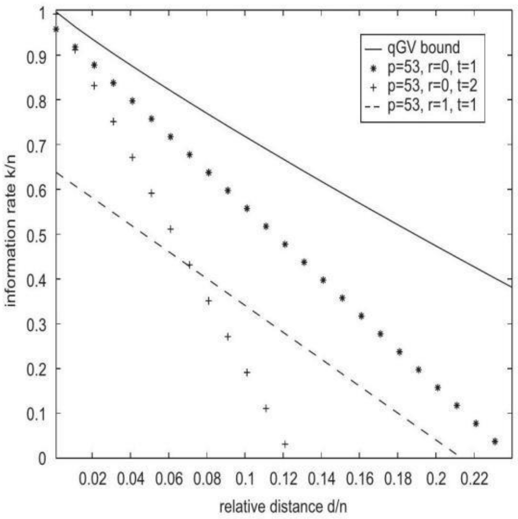

Fig 3. Asymptotically good sequences of p-ary quantum codes where $p = 53$ with $r = 0$ and $t = 1,2$, or with $r = 1$ and $t = 1$.

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

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

Proof. We proceed as in the proof of Theorem 3.6. For any integer r with $1 \leqslant r \leqslant p^t - 1$, we have a $[2+r, 2, r+1]$ Reed-Solomon code $C_\star$ over $\mathbb{F}_{p^t}$. Let $\pi_\star\colon \mathbb{F}_{p^{2t}} \to \mathbb{F}_{p^t}^{2+r}$ be an $\mathbb{F}_{p^t}$-linear injective map with $\pi_\star(\mathbb{F}_{p^{2t}}) = C_\star$. The code C_j will be an $\mathbb{F}_{p^t}$-linear $[(2+r)N, 2(m_j - g + 1), \geqslant (r+1)(N - m_j)]$ code with $C_j^\perp = S + \pi'(T_j^\perp)$, where S is the direct sum of N copies of $C_\star^\perp$ and π' is the dual basis map corresponding to π. Applying the CSS construction, we get a p^t-ary quantum code $B = B(X)$ with parameters

$$[[(2+r)N, 2l, \geqslant d \geqslant \frac{r+1}{r+2}(N - 2g - l + 1)]]_{p^t}$$

where l is any integer satisfying $0 < l \leqslant N - 2g$ as before.

Now set

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

$$\delta = \limsup_{X \in \mathbf{X}} \frac{d}{(2+r)N} = \frac{r+1}{(r+2)^2}(1 - \frac{2}{p^t - 1} - \lambda)$$

and write R_{p^t} in terms of δ to obtain the result.

CONCLUSION

An independent proof of [Theorem 3] for a generalized CSS construction for nonbinary quantum error-correcting codes is presented in this article. We are able to acquire a variety of parameters for nonbinary quantum codes by utilizing this construction and algebraic curves. We have, in particular, constructed families of asymptotically good nonbinary quantum codes by making use of a Garcia-Stichtenoth tower of function fields. It should be noted that the algorithm for decoding the algebraic geometry codes that correspond to our quantum codes is connected to the process of decoding them.

REFERENCES

[1] Cossidente, A., Korchmáros, G., Torres, F.: On curves covered by the Hermitian curve. J. Algebra 216(1), 56-76 (1999)

[2] Demirbas Y., Automorphism groups of hyperelliptic curves of genus 3 in characteristic 2, Computationalaspects of algebraic curves, T. Shaska (Edt), Lect. Notes in Comp., World Scientific, 2005.

[3] Jon-Lark Kima, Judy Walker(2008), Nonbinary quantum error-correcting codes from algebraic curves, Discrete Mathematics 308 (2008) 3115 – 3124.

[4] KazemifardA., TafazolianS., A note on some Picard curves over finite fields, FiniteFields and Their Applications, 34, (2015), 107-122

[5] MatthewsG.L., Weierstrass semigroups and codes from a quotient of the Hermitiancurve, Designs, Codes and Cryptography, 37(3), (2005), 473-492.

[6] Shaska T. (2008), Quantum codes from algebraic curves withautomorphisms. Condensed Matter Physics 2008, Vol. 11, No 2(54), pp. 383–396.

[7] Shor P.W. ‘Algorithms for quantum computation: discrete logarithms andfactoring”, 35thAnnualSymposium on Foundations of Computer Science(Santa Fe, NM, 1994), IEEE Comput. Soc. Press,Los Alamitos, CA (1994),124–134.

[8] Wang, L., Feng, K., Ling, S., & Xing, C. (2010). Asymmetric Quantum Codes: Characterization and Constructions. IEEE Transactions on Information Theory, 56(6), 2938-2945.