7-2008

# Nonbinary Quantum Error-Correcting Codes from Algebraic Curves

Jon-Lark Kim
*University of Nebraska-Lincoln*, jl.kim@louisville.edu

Judy L. Walker
*University of Nebraska - Lincoln*, judy.walker@unl.edu

Published in Discrete Mathematics 308 (2008) 3115 – 3124


# Nonbinary Quantum Error-Correcting Codes from Algebraic Curves

Jon-Lark Kim and Judy Walker
Department of Mathematics
University of Nebraska-Lincoln,
Lincoln, NE 68588-0130 USA
e-mail: {jlkim, jwalker}@math.unl.edu

November 15, 2004

**Abstract**

We give a generalized CSS construction for nonbinary quantum error-correcting codes. Using this we construct nonbinary quantum stabilizer codes from algebraic curves. We also give asymptotically good nonbinary quantum codes from a Garcia-Stichtenoth tower of function fields which are constructible in polynomial time.

**keywords** Algebraic geometric codes, nonbinary quantum codes.

## 1 Introduction

Binary quantum error-correcting codes have been constructed in several ways. One interesting construction uses algebraic-geometry codes [2], [6], [7], [12], with the main idea being to apply the binary CSS construction [4], [5], [16] to the asymptotically good algebraic-geometry codes arising from the Garcia-Stichtenoth [11] tower of function fields over $\mathbb{F}_{q^2}$ (where $q$ is a power of 2) attaining the Drinfeld-Vladut bound [17].

It is natural to consider nonbinary quantum codes. Beyond the simple fact that nonbinary error-correcting codes are interesting in the classical case, Rains [14] points out that there are indeed applications in which nonbinary quantum codes would be more appropriate than binary quantum codes. Though nonbinary quantum codes have been considered in [1], [3], [9], [14], the majority of attention has been given thus far to the binary case. In particular, the question of asymptotically good nonbinary quantum codes has not been studied until now.

In this paper we give a nonbinary version of the generalized binary CSS construction based on two binary linear codes given by Calderbank et al. [4]. We then apply this construction to the tower of function fields defined in [11] with concatenation to Reed-Solomon codes to obtain asymptotically good nonbinary quantum codes which are constructible in polynomial time.

# 2 Preliminaries

In this section we give some definitions and basic facts about quantum codes. First, we recall the generalized binary CSS construction of quantum stabilizer codes. In Section 3 we will generalize this construction to the nonbinary case.

**Theorem 2.1.** *[4, Theorem 9] 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 $[[n, k_2 - k_1, d]]$ quantum code, where $d = \min\{d(C_2 \setminus C_1), d(C_1^\perp \setminus C_2^\perp)\}$.*

Here, 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 $B$.

Let $q = p^m$, where $p$ is an odd prime throughout the paper. 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 in [4]. This idea was generalized in [1] 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 [1]. Let $T$ and $R$ be the linear operators acting on the $p$-dimensional complex space $\mathbb{C}^p$ defined by

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

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 $\langle A, B\rangle = \mathrm{Tr}(A^* B)$, where $A^*$ is the Hermitian transpose of $A$ [1], [15].

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

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

Define

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

The set of operators $T_a R_b$ forms an orthogonal basis of unitary operators acting on the $p^m$-dimensional complex vector space $\mathbb{C}^{p^m}$ [1].

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

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

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 $\mathcal{E}$ [1]. See also the appendix of [3].

# 3 A $q$-ary CSS Construction

In this section, we explore CSS constructions for nonbinary quantum codes. We begin with a construction given in [1] that is analogous to the first construction presented in [4], and then follow the lead of [4] to derive other constructions. We note that our $q$-ary CSS construction generalizes the $p$-ary CSS construction [13, 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 3.4, which will be used in Section 4 to construct asymptotically good sequences of nonbinary quantum codes.

As in the previous section, 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 $(\mathbf{a}|\mathbf{b})$, $(\mathbf{a}'|\mathbf{b}') \in \mathbb{F}_q^{2n}$, set $(\mathbf{a}|\mathbf{b}) * (\mathbf{a}'|\mathbf{b}') = \mathrm{Tr}(\mathbf{a} \cdot \mathbf{b}' - \mathbf{a}' \cdot \mathbf{b})$, where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. We see that if $q = p$ then $(\mathbf{a}|\mathbf{b}) * (\mathbf{a}'|\mathbf{b}') = (\mathbf{a} \cdot \mathbf{b}' - \mathbf{a}' \cdot \mathbf{b})$ which was studied in [13], [14].

**Proposition 3.1.** *[1, pp. 3069] 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 $(*)$. If $C \subseteq C^{\perp_*}$, then there is a $q$-ary $[[n, n - \frac{r}{m}, d]]$ 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 [13, pp. 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 $\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ is onto and $\mathbb{F}_q$-linear, we may pick $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\mathrm{Tr}(\gamma) = \gamma_0$. 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 3.2.** *Suppose $D \subseteq \mathbb{F}_{q^2}^n$ 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 $f : \mathbb{F}_{q^2}^n \to \mathbb{F}_q^{2n}$ by $f(x_1, \ldots, x_n) = (x_1^{(1)}, \ldots, x_n^{(1)} | x_1^{(2)}, \ldots, x_n^{(2)})$, where $x_i = x_i^{(1)} + \gamma x_i^{(2)}$ for $i = 1, \ldots, n$. Then $f(D) \subseteq f(D^{\perp_\circ}) = (f(D))^{\perp_*}$, where $(f(D))^{\perp_*}$ is the dual of $f(D)$ with respect to $(*)$.*

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

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

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

$$\sum \Big( x_i^{(1)} y_i^{(2)} - x_i^{(2)} y_i^{(1)} \Big) = 0.$$

Therefore

$$f(\mathbf{x}) * f(\mathbf{y}) = \mathrm{Tr}\left( \sum \Big( x_i^{(1)} y_i^{(2)} - x_i^{(2)} y_i^{(1)} \Big) \right) = 0.$$

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

$$d(D^{\perp\circ} \setminus D) = \min\{ d(C_2 \setminus C_1), d(C_1^\perp \setminus C_2^\perp) \}.$$

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

$$|D^{\perp\circ}| = q^{2n - (n + k_1 - k_2)} = q^{n - k_1 + k_2} = |\bar{\omega} C_1^\perp + \omega C_2|.$$

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

$$\begin{aligned}
&(\omega\mathbf{x} + \bar{\omega}\mathbf{y}) \circ (\bar{\omega}\mathbf{a} + \omega\mathbf{b}) \\
&\quad = \sum ((\omega x_i + \bar{\omega} y_i)(\omega a_i + \bar{\omega} b_i) - (\bar{\omega} x_i + \omega y_i)(\bar{\omega} a_i + \omega b_i)) \\
&\quad = (\omega^2 - \bar{\omega}^2)(\sum x_i a_i - \sum y_i b_i) \\
&\quad = 0,
\end{aligned}$$

since $\mathbf{x} \cdot \mathbf{a} = \mathbf{y} \cdot \mathbf{b} = 0$. The last sentence of the proposition follows since $C_1 \subseteq C_2$, $C_2^\perp \subseteq C_1^\perp$, and $\omega C_1 \cap \bar{\omega} C_2^\perp = \bar{\omega} C_1^\perp \cap \omega C_2 = \{0\}$. □

Next, we give a construction which produces a $q$-ary quantum code from any two $\mathbb{F}_q$-linear codes $C_1 \subseteq C_2 \subseteq \mathbb{F}_q^n$. This is a $q$-ary version of the binary CSS construction [4, Theorem 9] as it is also based on two linear codes over $\mathbb{F}_q$, and so it is a generalization of [13, Theorem 5] which is based on self-orthogonal codes.

**Theorem 3.4.** *Let $q = p^m$, where $p$ is an odd prime and $m \geq 1$ is an integer. Suppose $C_1 \subseteq C_2 \subseteq \mathbb{F}_q^n$ are $\mathbb{F}_q$-linear codes with dimensions $k_1$ and $k_2$, respectively. Then there exists a $q$-ary $[[n, k_2 - k_1, d]]$ quantum code, where $d = \min\{d(C_2 \setminus C_1), d(C_1^\perp \setminus C_2^\perp)\}$.*

*Proof.* Set $D = \omega C_1 + \bar{\omega} C_2^\perp$, as in Proposition 3.3. Then $f(D) \subseteq (f(D))^{\perp *}$ by Proposition 3.3 and Lemma 3.2. Note that $f(D)$ is an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{2n}$, 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 3.1 by letting $C = f(D)$. □

**Example 3.5.** 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 $C_2^\perp$. By Theorem 3.4, we obtain a ternary double-error correcting quantum $[[11, 1, 5]]_3$ code.

# 4 Good Sequences of $q$-ary Quantum AG Codes

We assume the results from Section II of [7] and use the ideas of Section III of that paper. Fix $t \geq 1$ and set $q = p^{2t} = (p^t)^2$. The authors [7] only used a trivial binary MDS code in the concatenation while we use Reed-Solomon codes over $\mathbb{F}_p$.

Let $X$ be a curve over $\mathbb{F}_q$ of genus $g$. Fix an $\mathbb{F}_q$-rational point $P = P(X) \in X(\mathbb{F}_q)$, let $D = D(X)$ be the sum of the $\mathbb{F}_q$-rational points on $X$ other than $P$, and set $N = N(X) = \deg D = \#X(\mathbb{F}_q) - 1$. Pick integers $m_1 = m_1(X)$ and $m_2 = m_2(X)$ with $2g - 2 < m_1 < m_2 < N$, and set $T_j = T_j(X) = C(m_j P, D)$, the (functional) algebraic geometric code defined on

$X$ from the divisors $m_jP$ and $D$. Then the code $T_j$ is an $[N, m_j - g + 1, \geq N - m_j]$ code over $\mathbb{F}_q$, $T_1 \subset T_2$, and the dual $T_j^\perp$ of $T_j$ is an $[N, N - m_j + g - 1, \geq m_j - 2g + 2]$ code over $\mathbb{F}_q$.

As in [7], we use concatenation [10] to obtain $\mathbb{F}_p$-linear codes $C_1$ and $C_2$ from $T_1$ and $T_2$. More precisely, for any integer $0 \leq r \leq p + 1 - 2t$, let $\pi_\star : \mathbb{F}_q = \mathbb{F}_{p^{2t}} \to \mathbb{F}_p^{2t+r}$ be an $\mathbb{F}_p$-linear injective map such that the image $C_\star$ of $\pi_\star$ is a $[2t + r, 2t, r + 1]$ Reed-Solomon code over $\mathbb{F}_p$. Define $\pi : \mathbb{F}_q^N \to \mathbb{F}_p^{N(2t+r)}$ by $\pi((x_1, \ldots, x_N)) = (\pi_\star(x_1), \ldots, \pi_\star(x_N))$. 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 $[(2t + r)N,\ 2t(m_j - g + 1),\ \geq (r + 1)(N - m_j)]$ 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 $\pi'$ is the $\mathbb{F}_q$-linear injective "dual basis" map, as described in [7]. For any vector $\mathbf{x} \in C_1^\perp \backslash C_2^\perp$, we have $\mathrm{wt}(\mathbf{x}) \geq m_1 - 2g + 2$, just as in the binary case (see [7], proof of Theorem 1.2). The following proposition follows from Theorem 3.4.

**Proposition 4.1.** *With notation as above, we get a $p$-ary quantum code $B = B(X)$ with parameters*

$$\begin{aligned}[[&(2t + r)N,\ 2t(m_2 - m_1),\\ &\geq \min\{(r + 1)(N - m_2), m_1 - 2g + 2\}]]_p.\end{aligned}$$

**Example 4.2.** Consider the Hermitian curve defined by $y^{p^t} + y = x^{p^t+1}$ over $\mathbb{F}_{p^{2t}}$; this is the base level of the Garcia-Stichtenoth tower [11]. In this case, the codes $T_j$, $j = 1, 2$, are $[p^{3t}, m_j - \frac{p^t(p^t-1)}{2} + 1, \geq p^{3t} - m_j]$ linear codes over $\mathbb{F}_{p^{2t}}$. For any integers $r$, $m_1$, and $m_2$ with $0 \leq r \leq p + 1 - 2t$ and $p^t(p^t - 1) - 2 < m_1 < m_2 < p^{3t}$, we get a $p$-ary quantum code $B$ with parameters

$$\begin{aligned}[[&(2t + r)p^{3t},\ 2t(m_2 - m_1),\\ &\geq \min\{(r + 1)(p^{3t} - m_2), m_1 - p^t(p^t - 1) + 2\}]]_p.\end{aligned}$$

Next, we consider the asymptotic behavior of our quantum codes. Let $\mathbf{X} = \{X\}$ be a Garcia-Stichtenoth tower [11] of polynomially constructible curves over $\mathbb{F}_q$ having increasing genus $g = g(X)$ and attaining the Drinfeld-Vladut bound, i.e., satisfying

$$\limsup_{X \in \mathbf{X}} \frac{\#X(\mathbb{F}_q)}{g} = p^t - 1.$$

Note that if $k = k(X) = m_2 - m_1$, then $0 < k \leq N - 2g$. Conversely, given any integer $k$ with $0 < k \leq N - 2g$, set

$$m_2 = \left\lfloor \frac{(r + 1)N + 2g + k - 2}{r + 2} \right\rfloor.$$

Then we have the following.

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

and

$$\begin{aligned}m_1-2g+2 &= m_2-k-2g+2\\ &= \left\lfloor \frac{(r+1)N+2g+k-2}{r+2}\right\rfloor\\ &\qquad -k-2g+2\\ &\geq \frac{(r+1)N+2g+k-2)}{r+2}\\ &\qquad -\frac{r+1}{r+2}-k-2g+2\\ &= \frac{r+1}{r+2}(N-2g-k+1).\end{aligned}$$

Therefore, $B$ has parameters

$$[[(2t+r)N,\ 2tk,\ \geq d := \frac{r+1}{r+2}(N-2g-k+1)]]_p.$$

For any sequence of integers $\{k=k(X)\,|\,X\in\mathbf{X}\}$ with $0<k<N-2g$ for each $X$, we have $0<\limsup_{X\in\mathbf{X}}\frac{k}{N}\leq 1-\frac{2}{\sqrt{q}-1}$ by the Drinfeld-Vladut bound. Indeed, by choosing the values of $k$ appropriately, we can have $\limsup_{X\in\mathbf{X}}\frac{k}{N}=\lambda$ for any $\lambda$ with $0<\lambda\leq 1-\frac{2}{\sqrt{q}-1}$.

We put

$$\begin{aligned}R &:= \limsup_{X\in\mathbf{X}}\frac{2tk}{(2t+r)N}\\ &= \frac{2t}{2t+r}\lambda,\\ \delta &:= \limsup_{X\in\mathbf{X}}\frac{d}{(2t+r)N}\\ &= \frac{r+1}{(r+2)(2t+r)}(1-\frac{2}{p^t-1}-\lambda).\end{aligned}$$

To get an expression for $R$ in terms of $\delta$, we solve for $\lambda$ in terms of $\delta$ and substitute, yielding

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

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 4.3.** *Let $p$ be any odd prime number. Suppose that $t \geq 1$ and $r \geq 0$ are integers satisfying $2t+r \leq p+1$. Let $\delta(p, r, t)$ be as above. Then for any $\delta$ with $0 < \delta < \delta(p, r, t)$, there exist polynomially constructible families of $p$-ary quantum codes with $n \to \infty$ and asymptotic parameters $(\delta, R_p(\delta))$, where*

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

**Remark 4.4.** The case when $p = 2$ was discussed in [7]. In this case we require that $t \geq 3$ is an integer and $r = 0$ or 1. Then plugging in $p = 2$ and $r = 1$ into $\delta(p, r, t)$ in Theorem 4.3 gives

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

which is Theorem 1.2 of [7].

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

**Theorem 4.5.** *Let $p$ be an odd prime, and let $t \geq 1$ and $r \geq 1$ be integers with $r \leq p^t - 1$. Set*

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

*Then for any $\delta$ 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 $(\delta, R_{p^t}(\delta))$, 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 4.3. For any integer $r$ with $1 \leq r \leq p^t - 1$, we have a $[2+r, 2, r+1]$ Reed-Solomon code $C_\star$ over $\mathbb{F}_{p^t}$. Let $\pi_\star : \mathbb{F}_{p^{2t}} \to \mathbb{F}_{p^t}^{2+r}$ 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 $[(2+r)N, 2(m_j - g + 1), \geq (r+1)(N - m_j)]$ code with $C_j^\perp = S + \pi'(T_j^\perp)$, where $S$ is the direct sum of $N$ copies of $C_\star^\perp$ and $\pi'$ is the dual basis map corresponding to $\pi$. Applying the CSS construction, we get a $p^t$-ary quantum code $B = B(X)$ with parameters

$$[[(2+r)N, 2k, \geq d := \frac{r+1}{r+2}(N - 2g - k + 1)]].$$

Now set

$$R_{p^t} := R = \limsup_{X \in \mathbf{X}} \frac{2k}{(2+r)N} = \frac{2}{2+r}\lambda,$$
$$\delta = \limsup_{X \in \mathbf{X}} \frac{d}{(2+r)N} = \frac{r+1}{(r+2)^2}\left(1 - \frac{2}{p^t - 1} - \lambda\right)$$

and write $R_{p^t}$ in terms of $\delta$ to obtain the result. □

# References


[1] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, IEEE Transactions on Information Theory 47 (2001), 3065-3072.

[2] A. Ashikhmin, S. Litsyn, and M.A. Tsfasman, Asymptotically good quantum codes, quant-ph/0006061.

[3] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, Authentication of quantum messages, quant-ph/0205128.

[4] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Transactions on Information Theory 44 (1998), 1369-1387.

[5] A.R. Calderbank and P.W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54 (1996) 1098-1105.

[6] H. Chen, Some good quantum error-correcting codes from algebraic geometry codes, IEEE Transactions on Information Theory 47 (2001) 2059-2061.

[7] H. Chen, S. Ling, and C. Xing, Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, IEEE Transactions on Information Theory 47 (2001), 2055-2058.

[8] I. Dumer, Concatenated codes and their multilevel generalizations, Handbook of coding theory, Vol. II, 1911–1988, North-Holland, Amsterdam, 1998.

[9] K. Feng, Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ ($p \geq 3$) exist, IEEE Transactions on Information Theory 48 (2002), 2384-2391.

[10] Forney, Jr., G.D., Concatenated codes, M.I.T. Research Monograph, No. 37, The M.I.T. Press, Cambridge, Mass., 1966.

[11] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math. 121 (1995), 211–222.

[12] R. Matsumoto, Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, IEEE Transactions on Information Theory 48 (2002), 2122-2124.

[13] 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 (2000), 1878–1883.

[14] E.M. Rains, Nonbinary quantum codes, IEEE Transactions on Information Theory 45 (1999), 1827–1832.

[15] J. Schwinger, Unitary operator bases, Proc. Nat. Acad. Sci. 46 (1960), 570-579.

[16] A.M. Steane, Multiple particle interference and quantum error correction, Proc. Roy. Soc. London A 452 (1996), 2551-2577.

[17] M.A. Tsfasman and S.G. Vladut, Algebraic-Geometric Codes, Kluwer,Dordrecht 1991.