Good and asymptotically good quantum codes derived from algebraic geometry codes

Giuliano G. La Guardia, Francisco Revson F. Pereira *

December 22, 2016

Abstract

In this paper we construct several new families of quantum codes with good and asymptotically good parameters. These new quantum codes are derived from (classical) algebraic geometry (AG) codes by applying the Calderbank-Shor-Steane (CSS) construction. Many of these codes have large minimum distances when compared with its code length and they have relatively small Singleton defect. For example, we construct a family $[[46, 2(t_2 - t_1), d]]_{25}$ of quantum codes, where $t_1, t_2$ are positive integers such that $1 < t_1 < t_2 < 23$ and $d \geq \min\{46 - 2t_2, 2t_1 - 2\}$, of length $n = 46$, with minimum distance in the range $2 \leq d \leq 20$, having Singleton defect four. Additionally, by utilizing $t$-point AG codes, with $t \geq 2$, we show how to obtain sequences of asymptotically good quantum codes.

1 Introduction

Methods and techniques to construct quantum codes with good parameters are extensively investigated in the literature [1, 3–5, 10, 11, 13, 14, 16]. In particular, constructions of quantum codes whose parameters are asymptotically good have also been presented [2, 4, 5, 12, 17]. All these codes are based on algebraic geometry (AG) classical codes. In fact, the class of AG codes is a good source of asymptotically good codes (see [7, 19]). In Refs. [2, 4, 5, 17], the authors constructed asymptotically good binary quantum codes and in Ref [12], the authors presented families of nonbinary asymptotically good quantum codes by means of one-point AG codes.

In this paper, by means of $t$-point algebraic geometry classical codes, as well as by means of algebraic geometry codes whose divisor $G$ is not a rational place, we construct nonbinary quantum codes with good parameters. In order to do

* Giuliano Gadioli La Guardia (corresponding author) is with Department of Mathematics and Statistics, State University of Ponta Grossa (UEPG), 84030-900, Ponta Grossa, PR, Brazil, e-mail: (gguardia@uepg.br). Francisco Revson F. Pereira is with Department of Electrical Engineering, Federal University of Campina Grande (UFCG), 58429-900, Campina Grande, PB, Brazil, e-mail: (francisco.pereira@ee.ufcg.edu.br).
this, we apply to these codes the Calderbank-Shor-Steane (CSS) quantum code construction. Additionally, by utilizing \( t \)-point AG codes, \( t \geq 2 \), we construct sequences of asymptotically good quantum codes.

The paper is arranged as follows. In Section 2, we recall the concepts utilized in this work. Section 3 deals with the contributions of this paper, i.e. constructions of quantum codes with good and asymptotically good parameters derived from classical AG codes. In Section 4, we compare the new code parameters with the ones shown in the literature and, in Section 5, we give a summary of this work.

## 2 Preliminaries

Let \( \mathbb{F}_q \) be the finite field with \( q \) elements, where \( q \) is a prime power and let \( F/\mathbb{F}_q \) be a algebraic function field of genus \( g \). We denote by \( \mathcal{P}_F \) the set of places of \( F/\mathbb{F}_q \) and by \( \mathcal{D}_F \) the (free) group of divisors of \( F/\mathbb{F}_q \). For each \( x \in F/\mathbb{F}_q \), the principal divisor \((x)\) of \( x \) is defined by \((x) := \sum_P v_P(x)P\), where \( v_P \) is the discrete valuation corresponding to the place \( P \). Let \( A \) be a divisor of \( F/\mathbb{F}_q \). Then we define \( l(A) := \dim \mathcal{L}(A) \), where \( \mathcal{L}(A) \) is the Riemann-Roch space associated to \( A \), given by \( \mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\} \). Let \( \Omega_F \) be the differential space of \( F/\mathbb{F}_q \), i.e. \( \Omega_F := \{w \mid w \text{ is a Weil differential of } F/\mathbb{F}_q\} \). For every nonzero differential \( w \), we denote its canonical divisor by \( (w) := \sum_P v_P(w)P \), where \( v_P(w) := v_P((w)) \). A divisor \( W \) is called canonical if \( W = (w) \) for some \( w \in \Omega_F \).

**Theorem 2.1** (Riemann-Roch)[20, Theorem 1.5.15, pg 30] Let \( W \) be a canonical divisor of \( F/\mathbb{F}_q \). Then for each divisor \( A \in \mathcal{D}_F \), the dimension of \( \mathcal{L}(A) \) is given by \( l(A) = \deg A + 1 - g + \dim(W - A) \).

In what follows, we assume that \( P_1, \ldots, P_n \) are pairwise distinct places of \( F/\mathbb{F}_q \) of degree 1 and \( D = P_1 + \ldots + P_n \) is a divisor. Let \( G \) be a divisor of \( F/\mathbb{F}_q \) such that \( \text{supp } G \cap \text{supp } D = \emptyset \). The geometric Goppa code \( C_L(D, G) \) associated with \( D \) and \( G \) is defined by \( C_L(D, G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n \).

**Theorem 2.2** [20, Theorem 2.2.2, and Corollary 2.2.3, pg 49] Under the hypotheses above, \( C_L(D, G) \) is an \([n, k, d]_q \) code with \( k = l(G) - l(G - D) \) and \( d \geq n - \deg G \). If, in addition, \( 2g - 2 < \deg G < n \), then one has \( k = \deg G + 1 - g \).

Let \( D \) and \( G \) as above. We define the code \( C_Q(D, G) \subseteq \mathbb{F}_q^n \) by \( C_Q(D, G) := \{(\text{resp}_{P_1}(w), \ldots, \text{resp}_{P_n}(w)) \mid w \in \Omega_F(G - D)\} \), where \( \text{resp}_{P_i}(w) \) denotes the residue of \( w \) at \( P_i \).

**Theorem 2.3** [20, Theorem 2.2.7., pg 51] Let \( 2g - 2 < \deg G < n \). Then \( C_Q(D, G) \) is an \([n, k^*, d^*]_q \) code with \( k^* = n + g - 1 - \deg G \) and \( d^* \geq \deg G - (2g - 2) \).
Theorem 2.4 [20, Theorem 2.2.8, pg 52] The codes $C_L(D,G)$ and $C_Q(D,G)$ are (Euclidean) dual of each other, i.e. $C_Q(D,G) = C_L(D,G)^\perp$.

Recall that a $q$-ary quantum code $Q$ of length $n$ is a $K$-dimensional subspace of the $q^n$-dimensional Hilbert space $(C^q)^\otimes n$, where $\otimes n$ denotes the tensor product of vector spaces. If $K = q^k$ we write $[[n,k,d]]_q$ to denote a $q$-ary quantum code of length $n$ and minimum distance $d$. Let $[[n,k,d]]_q$ be a quantum code. The Quantum Singleton Bound (QSB) asserts that $k + 2d \leq n + 2$. If the equality holds then the code is called a maximum distance separable (MDS) code. For more details on quantum codes, the reader can consult [11, 18].

Lemma 2.5 [3, 11, 18] (CSS construction) Let $C_1$ and $C_2$ denote two classical linear codes with parameters $[[n,k_1,d_1]]_q$ and $[[n,k_2,d_2]]_q$, respectively, such that $C_1 \subset C_2$. Then there exists an $[[n,K = k_2 - k_1,D]]_q$ quantum code, where $D = \min \{\text{wt}(c) : c \in (C_2 \backslash C_1) \cup (C_1^+ \backslash C_2^+)\}$.

3 The New Codes

This section is divided in three parts. The first subsection deals with constructions of quantum $t$-point algebraic geometry codes; in the second one, we construct AG codes where the divisor $G$ is a sum of non-rational places, and in the third subsection, we construct sequences of asymptotically good quantum AG codes.

3.1 Construction I

In this section we present the contributions of this work. The first result utilizes two $t$-point AG codes in order to derive quantum codes with good parameters.

Theorem 3.1 (General $t$-point construction) Let $q$ be a prime power and $F/\mathbb{F}_q$ be an algebraic function field of genus $g$ with $n + t$ pairwise distinct rational places. Assume that $a_i, b_i$, $i = 1, \ldots, t$, are positive integers such that $a_i \leq b_i$ for all $i$ and $2g - 2 < \sum_{i=1}^{t} a_i < \sum_{i=1}^{t} b_i < n$. Then there exists a quantum code with parameters $[[n,k,d]]_q$, with $k = \sum_{i=1}^{t} b_i - \sum_{i=1}^{t} a_i$ and $d \geq \min \left\{n - \sum_{i=1}^{t} b_i, \sum_{i=1}^{t} a_i - (2g - 2)\right\}$.

Proof: Let $\{P_1, P_2, \ldots, P_n, P_{n+1}, \ldots, P_{n+t}\}$ be the set of places of $F/\mathbb{F}_q$ of degree one. Let $D = P_1 + \ldots + P_n$ be a divisor of $F/\mathbb{F}_q$. Assume also that $G_1$ and $G_2$ are two divisors of $F/\mathbb{F}_q$ given respectively by $G_1 = a_1 P_{n+1} + \ldots + a_t P_{n+t}$ and $G_2 = b_1 P_{n+1} + \ldots + b_t P_{n+t}$, where $a_i \leq b_i$ for all $i = 1, \ldots, t$ and $2g - 2 < \sum_{i=1}^{t} a_i < \sum_{i=1}^{t} b_i$. Then $G_1 \subset G_2$ and there exists a quantum code with parameters $[[n,k,d]]_q$, with $k = \sum_{i=1}^{t} b_i - \sum_{i=1}^{t} a_i$ and $d \geq \min \left\{n - \sum_{i=1}^{t} b_i, \sum_{i=1}^{t} a_i - (2g - 2)\right\}$.
\[ \sum_{i=1}^{t} b_i < n. \] From construction, \( \text{supp} G_1 \cap \text{supp} D = \emptyset \) and \( \text{supp} G_2 \cap \text{supp} D = \emptyset. \) Since \( G_1 \leq G_2 \) one has \( \mathcal{L}(G_1) \subset \mathcal{L}(G_2), \) so \( C_{\mathcal{L}}(D, G_1) \subset C_{\mathcal{L}}(D, G_2). \) From Theorem 2.2, the code \( C_1 := C_{\mathcal{L}}(D, G_1) \) has parameters \([n, k_1, d_1]_q, \) where \( d_1 \geq n - \sum_{i=1}^{t} a_i \) and \( k_1 = \sum_{i=1}^{t} a_i - g + 1 \) and the code \( C_2 := C_{\mathcal{L}}(D, G_2) \) has parameters \([n, k_2, d_2]_q, \) where \( d_2 \geq n - \sum_{i=1}^{t} b_i \) and \( k_2 = \sum_{i=1}^{t} b_i - g + 1. \) On the other hand, from Theorems 2.3 and 2.4, the dual code \( C_1^\perp = C_{\Omega}(D, G_1) \) of \( C_1 \) has parameters \([n, k_1^\perp, d_1^\perp]_q, \) where \( d_1^\perp \geq \sum_{i=1}^{t} a_i - (2g - 2) \) and \( k_1^\perp = n + g - 1 - \sum_{i=1}^{t} a_i, \) and the dual code \( C_2^\perp = C_{\Omega}(D, G_2) \) of \( C_2 \) has parameters \([n, k_2^\perp, d_2^\perp]_q \) with \( d_2^\perp \geq \sum_{i=1}^{t} b_i - (2g - 2) \) and \( k_2^\perp = n + g - 1 - \sum_{i=1}^{t} b_i. \)

Applying the CSS construction to the codes \( C_1 \) and \( C_2, \) we obtain an \([n, k, d]_q \) quantum code with the mentioned parameters, as required. \( \square \)

**Remark 3.2** Note that in the papers [5, 12], the authors utilize one-point AG codes to construct good/(asymptotically good) quantum codes. In [4], the author applied two-point AG codes to derive good/(asymptotically good) quantum codes. In Theorem 3.1 we generalize, in a natural way, the one-point and two-point code constructions to the \( t \)-point code construction, where \( t \geq 1. \)

**Corollary 3.3 (One-Point codes)** There exists a quantum code with parameters \([[[q(1+(q-1)m), b-a, d]_q^2, where (q - 1)(m - 1) - 2 < a < b < q(1 + (q - 1)m), m](q + 1) \text{ and } d \geq \min\{q(1 + (q - 1)m) - b, a - (q - 1)(m - 1) + 2\}. \]

**Proof:** Let \( F = \mathbb{F}_{q^2}(x, y) \) with \( y^q + y = x^m \) and \( m|(q + 1). \) It is known that the genus of \( F \) is \( g = (q - 1)(m - 1)/2 \) and the number of places of degree one is \( N = 1 + q(1 + (q - 1)m) \) (see [20, Example 6.4.2., pg 234]). Let \( \{P_1, P_2, \ldots, P_n, P_{n+1}, \ldots, P_N\} \) be these pairwise distinct places. Without loss of generality, choose the \( \mathbb{F}_{q^2}\)-rational point \( P_N. \) Let \( D = P_1 + \ldots + P_{N-1} \) be a divisor and \( G_1 = aP_N \) and \( G_2 = bP_N \) other two divisors such that \( \text{supp} G_1 \cap \text{supp} D = \emptyset \) and \( \text{supp} G_2 \cap \text{supp} D = \emptyset, \) where \( (q - 1)(m - 1) - 2 < a < b < q(1 + (q - 1)m). \) From Theorem 3.1, there exists a quantum code with parameters \([[[q(1 + (q - 1)m), b-a, d]_q^2, where d \geq \min\{q(1 + (q - 1)m) - b, a - (q - 1)(m - 1) + 2\}. \) The proof is complete. \( \square \)

**Remark 3.4** Note that the Hermitian curve defined by \( y^q + y = x^{q+1} \) over \( \mathbb{F}_{q^2} \) is a particular case of the curve \( y^q + y = x^m \) considered in the proof of Corollary 3.3.
Corollary 3.5 (Two-Point codes) There exists a quantum code with parameters \(|q(1 + (q-1)m) - 1, b_1 + b_2 - a_1 - a_2, d|_{q^2}\), where \(a_i \leq b_i\) for \(i = 1, 2\), \((q-1)(m-1) - 2 < a_1 + a_2 < b_1 + b_2 < q(1 + (q-1)m) - 1\), \(m|(q+1)\) and \(d \geq \min\{q(1 + (q-1)m) - b_1 - b_2 - 1, a_1 + a_2 - (q-1)(m-1) + 2\}\).

Proof: Let \(D = P_1 + \ldots + P_{N-2}\) be a divisor and \(G_1 = a_1 P_{N-2} + a_2 P_{N-1}\) and \(G_2 = b_1 P_{N-2} + b_2 P_{N-1}\) other two divisors with \(\text{supp} G_1 \cap \text{supp} D = \emptyset\) and \(\text{supp} G_2 \cap \text{supp} D = \emptyset\), where \((q-1)(m-1) - 2 < a_1 + a_2 < b_1 + b_2 < q(1 + (q-1)m) - 1\). From Theorem 3.1, there exists a quantum code with parameters \(|q(1 + (q-1)m) - 1, b_1 + b_2 - a_1 - a_2, d|_{q^2}\), where \(d \geq \min\{q(1 + (q-1)m) - b_1 - b_2 - 1, a_1 + a_2 - (q-1)(m-1) + 2\}\).

\(\square\)

Corollary 3.6 (t-Point codes) There exists a quantum code with parameters \(|q(1 + (q-1)m) - t + 1, b_1 + \ldots + b_t - (a_1 + \ldots + a_t), d|_{q^2}\), where \(a_i \leq b_i\) for \(i = 1, \ldots, t\), \((q-1)(m-1) - 2 < a_1 + \ldots + a_t < b_1 + \ldots + b_t < q(1 + (q-1)m) - t + 1\), \(m|(q+1)\) and \(d \geq \min\{q(1 + (q-1)m) - (b_1 + \ldots + b_t) - t + 1, a_1 + \ldots + a_t - (q-1)(m-1) + 2\}\).

Proof: Similar to that of Corollary 3.5. \(\square\)

3.2 Construction II

In this section we deal with quantum codes derived from AG codes whose divisors are multiples of a non rational divisor \(G\). The first result is given in the sequence.

Theorem 3.7 (General construction) Let \(q\) be a prime power and \(F/F_q\) be an algebraic function field of genus \(g\) with \(n\) pairwise distinct rational places \(P_i\), \(i = 1, \ldots, n\). Assume that there exist pairwise distinct places \(Q_1, \ldots, Q_t\) of \(F/F_q\) of degree \(\alpha_i \geq 2\), respectively, \(i = 1, \ldots, t\). Let \(G_1 = \sum_{i=1}^{t} a_i Q_i\) and \(G_2 = \sum_{i=1}^{t} b_i Q_i\), where \(a_i \leq b_i\), for all \(i = 1, \ldots, t\), and \(2g - 2 < a_1 \alpha_1 + \ldots + a_t \alpha_t < b_1 \alpha_1 + \ldots + b_t \alpha_t < n\). Let \(D = P_1 + \ldots + P_n\) be a divisor of \(F/F_q\) and consider that \(\text{supp} G_1 \cap \text{supp} D = \emptyset\) and \(\text{supp} G_2 \cap \text{supp} D = \emptyset\). Then there exists a quantum code with parameters \(|[n, k, d]|_{q}\), where \(k = (b_1 - a_1) \alpha_1 + \ldots + (b_t - a_t) \alpha_t\) and \(d \geq \min\{n - (a_1 \alpha_1 + \ldots + a_t \alpha_t) - (2g - 2)\}\).

Proof: The proof is similar to that of Theorem 3.1. \(\square\)

Corollary 3.8 Let \(q\) be a prime power and \(F/F_q\) be a hyperelliptic function field of genus \(g\) with \(n\) rational places. Then there exists a quantum code with parameters \(|[n, 2(t_2 - t_1), d]|_{q}\), where \(t_1, t_2\) are positive integers such that \(2g - 2 < t_1 < t_2 < n\) and \(d \geq \min\{n - 2t_2, 2t_1 - 2g + 2\}\).
Proof: Since $F$ is a hyperelliptic function field then there exists a place $G$ of degree two (see [20, Lemma 6.2.2.(a), pg 224]). Let $D = P_1 + \ldots + P_n$ be a divisor, where $P_i$ are all rational points of $F$. Let $G_2 = t_2 G$ and $G_1 = t_1 G$, where $2g - 2 < 2t_1 < 2t_2 < n$. Applying the ideas of the proof of Theorem 3.1, we get the result. \hfill $\square$

Corollary 3.9 There exists a quantum code with parameters $[[46, 2(t_2 - t_1), d]]_{25}$, where $t_1, t_2$ are positive integers such that $1 < t_1 < t_2 < 23$ and $d \geq \min\{46 - 2t_2, 2t_1 - 2\}$.

Proof: It suffices to consider the function field $F = \mathbb{F}_q^* (x, y)$ with $y^3 + y = x^m$ and $m | (q + 1)$ and take $m = 2$ and $q = 5$. As the genus of $F$ is $g = 2$, then $F$ is a hyperelliptic function field (see [20, Lemma 6.2.2.(b), pg 224]) and the result follows from Corollary 3.8. \hfill $\square$

3.3 Construction III

In this subsection, we propose constructions of sequence of asymptotically good quantum codes derived from AG codes.

Recall that a tower of function fields (see [7, Definition 1.3]) over $\mathbb{F}_q$ is a sequence $T = (F_1, F_2, \ldots)$ of function fields $F_i/\mathbb{F}_q$ with the properties:

1. $F_1 \subseteq F_2 \subseteq F_3 \cdots$.

2. For each $n \geq 1$, the extension $F_{n+1}/F_n$ is separable of degree $[F_{n+1} : F_n] > 1$.

3. $g(F_j) > 1$, for some $j > 1$.

By the Hurwitz genus formula, the condition (3) implies that $g(F_n) \to \infty$ for $n \to \infty$. The tower is said to be asymptotically good if $\lambda(T) = \limsup_{i \to \infty} N(F_i)/g(F_i) > 0$, where $N(F_i)$ and $g(F_i)$ denote the number of $\mathbb{F}_q$-rational points and the genus of $F_i$, respectively. In the case of tower of function field one can replace $\limsup_{i \to \infty} N(F_i)/g(F_i)$ by $\lim_{i \to \infty} N(F_i)/g(F_i)$ because the sequence $(N(F_i)/g(F_i))_{i \geq 1}$ is convergent. We say that the tower $T$ (over $\mathbb{F}_q$) attains the Drinfeld-Vladut bound if $\lambda(T) = \limsup_{i \to \infty} N(F_i)/g(F_i) = \sqrt{q} - 1$.

To simplify the notation we put $N(F_i) = N_i$ and $g(F_i) = g_i$.

Let $(Q_i)_{i \geq 1}$ be a sequence of quantum codes over $\mathbb{F}_q$ with parameters $[[n_i, k_i, d_i]]_q$, respectively. We say that $(Q_i)_{i \geq 1}$ is asymptotically good if $\limsup_{i \to \infty} k_i/n_i > 0$ and $\limsup_{i \to \infty} d_i/n_i > 0$. Now we can show the next result.

Theorem 3.10 (Two-point asymptotically good codes) Assume that the tower $T = (F_1, F_2, \ldots)$ of function field over $\mathbb{F}_q$ attains the Drinfeld-Vladut bound. Then there exists a sequence $(Q_i)_{i \geq 1}$ of asymptotically good quantum codes over $\mathbb{F}_q$ derived from classical two-point AG codes.
Proof: For each $F_i$, let us consider the set of rational places $P_1(i), \ldots, P_{N_i-2}(i)$, $P_{N_i-1}(i), P_{N_i}(i)$ of $F_i$. We set the divisors $D(i) = P_1(i) + \ldots + P_{N_i-2}(i)$, $G_1(i) = a_1(i)P_{N_i-1}(i) + a_2(i)P_{N_i}(i)$ and $G_2(i) = b_1(i)P_{N_i-1}(i) + b_2(i)P_{N_i}(i)$, where $a_1(i) \leq b_1(i)$ and $a_2(i) \leq b_2(i)$ with $2g_i - 2 < a_1(i) + a_2(i) < b_1(i) + b_2(i) < N_i - 2$. Let us consider $C_1(i) := C_L(i)[D(i), G_1(i)]$ and $C_2(i) := C_L(i)[D(i), G_2(i)]$ be the two-point AG codes over $F_q$ corresponding to $G_1(i)$ and $G_2(i)$, respectively; thus $C_1(i) \subset C_2(i)$. The code $C_1(i)$ has parameters $[N_i - 2, a_1(i) + a_2(i) - g_i + 1, d_1(i)]_q$, where $d_1(i) \geq N_i - 2 - (a_1(i) + a_2(i))$ and the code $C_2(i)$ has parameters $[N_i - 2, b_1(i) + b_2(i) - g_i + 1, d_2(i)]_q$, where $d_2(i) \geq N_i - 2 - (b_1(i) + b_2(i))$. The corresponding CSS code has parameters $[[N_i - 2, K_i = b_1(i) + b_2(i) - (a_1(i) + a_2(i)), D_i]]_q$, where $D_i \geq \min\{N_i - 2 - (b_1(i) + b_2(i)), a_1(i) + a_2(i) - (2g_i - 2)\}$. We know that $K_i$ assume all the values from 1 to $N_i - 2g_i - 2$, i.e. $0 < K_i \leq N_i - 2g_i - 2$. For any such $K_i$ set $b_1(i) + b_2(i) = \lfloor (N_i + 2g_i + K_i - 4)/2 \rfloor$; thus it follows that $N_i - 2 - (b_1(i) + b_2(i)) \geq a_1(i) + a_2(i) - (2g_i - 2)$, where $a_1(i) + a_2(i) - (2g_i - 2) \geq (N_i - K_i - 2g_i - 1)/2$. The sequence of positive integers $(K_i)_{i \geq 1}$ satisfies $0 < \limsup_{i \to \infty} K_i/N_i \leq \limsup_{i \to \infty} N_i/(N_i - 2) - \limsup_{i \to \infty} 2g_i/(N_i - 2) + \limsup_{i \to \infty} -2/(N_i - 2) = 1 - 2/\sqrt{q} - 1$, where in the last equality we use the fact that $\limsup_{i \to \infty} N_i/g_i = \sqrt{q} - 1$. For each $0 < \epsilon < 1 - 2/\sqrt{q} - 1$, we can choose convenient values for $K_i$ such that $\lim_{i \to \infty} K_i/N_i = \epsilon$. Thus, $\limsup_{i \to \infty} K_i/(N_i - 2) = c > 0$. Moreover, one has $\limsup_{i \to \infty} (N_i - K_i - 2g_i - 1)/2(N_i - 2) = 1/2 \cdot [1 - 2/\sqrt{q} - 1 - c] > 0$. Therefore, there exists a sequence $(Q_i)_{i \geq 1}$ of asymptotically good quantum codes over $F_q$. The proof is complete.





Theorem 3.11 (t-point asymptotically good codes) Assume that the tower $T = (F_1, F_2, \ldots)$ of function field over $F_q$ attains the Drinfeld-Vladut bound. Then there exists a sequence $(Q_i)_{i \geq 1}$ of asymptotically good quantum codes over $F_q$ derived from classical $t$-point AG codes.

Proof: We adopt the same notation of the proof of Theorem 3.10. For each $F_i$, let us consider the set of rational places $P_1(i), \ldots, P_n(i), P_{n+1}(i), \ldots, P_{n+t}(i)$ of $F_i$, where $N_i = n_i + t$. Set $D(i) = P_1(i) + \ldots + P_n(i)$, $G_1(i) = a_1(i)P_{n+1}(i) + \ldots + a_t(i)P_{n+t}(i)$ and $G_2(i) = b_1(i)P_{n+1}(i) + \ldots + b_t(i)P_{n+t}(i)$, where $a_j(i) \leq b_j(i)$ for all $j = 1, \ldots, t$ with $2g_i - 2 < \sum_{j=1}^{t} a_j(i) < \sum_{j=1}^{t} b_j(i) < N_i - t$. Let us consider the $t$-point AG codes $C_1(i) := C_L(i)[D(i), G_1(i)]$ and $C_2(i) := C_L(i)[D(i), G_2(i)]$. It follows that $C_1(i) \subset C_2(i)$, and $C_1(i)$ has parameters

\[
\begin{bmatrix}
N_i - t, \sum_{j=1}^{t} a_j(i) - g_i + 1, d_1(i)
\end{bmatrix}_q,
\]

where $d_1(i) \geq N_i - t - \sum_{j=1}^{t} a_j(i)$, and $C_2(i)$ has parameters

\[
\begin{bmatrix}
N_i - t, \sum_{j=1}^{t} b_j(i) - g_i + 1, d_2(i)
\end{bmatrix}_q,
\]

where $d_2(i) \geq N_i - t - \sum_{j=1}^{t} b_j(i)$.}


Setting \( \sum_{j=1}^{t} b_j(i) = \lfloor (N_i + 2g_i + K_i - t - 2)/2 \rfloor \) and proceeding similar as in the proof of Theorem 3.10, the result follows.

Let \( q \) be a prime power. Let \( C = [n, k, d]_{\mathbb{F}_q} \) be a linear code over \( \mathbb{F}_q \) and let \( \beta \) be a basis of \( \mathbb{F}_q \) over \( \mathbb{F}_p \). Assume also that \( \beta^\perp \) is a dual basis of \( \beta \). Let \( C^\perp \) be the Euclidean dual of \( C \). Then one has \( [\beta(C)]^\perp = \beta^\perp(C^\perp) \) (see [8, 15]).

**Theorem 3.12** For any prime \( p \), there exists a sequence \( (Q_i)_{i \geq 1} \) of asymptotically good quantum codes over \( \mathbb{F}_p \).

**Proof:** Let \( q^2 = p^{2r} \), \( p \) prime. Consider the tower of function field \( T = (F_1, F_2, \ldots) \) over \( \mathbb{F}_q^2 \), shown in [7], defined by \( F_t = \mathbb{F}_q(x_1, \ldots, x_t) \), where \( x_{i+1}^p + x_i = x_t^p/(x_1^{q-1} + 1) \), for \( i = 1, \ldots, t-1 \). This tower attains the Drinfeld-Vladut bound. We next expand the codes \( C_1(i) \) and \( C_2(i) \) shown in the proof of Theorem 3.10 with respect to some basis \( \beta \) of \( \mathbb{F}_q^2 \) over \( \mathbb{F}_p \) obtaining, in this way, codes \( \beta(C_1(i)) \) and \( \beta(C_2(i)) \) both over \( \mathbb{F}_p \) with parameters \( [2r(N_i - 2), 2r(a_1(i) + a_2(i) - g_i + 1), \geq d_1^2(i)]_p \), where \( d_1^2(i) = d_1(i) = N_i - 2 - (a_1(i)+a_2(i)) \) and \( [2r(N_i - 2), 2r(b_1(i) + b_2(i) - g_i + 1), d_2^2(i)]_p \), where \( d_2^2(i) = d_2(i) = N_i - 2 - (b_1(i)+b_2(i)) \), respectively. Because \( \beta(C_1(i)) \subset \beta(C_2(i)) \), we can apply the CSS construction to these codes, obtaining therefore an \( [2r(N_i - 2), 2rK_i, D_i]_p \) quantum code, where \( D_i \geq \min[N_i - 2 - (b_1(i) + b_2(i)), a_1(i) + a_2(i) - (2g_i - 2)] \) (note that since \( [\beta(C_1(i))]^\perp = \beta^\perp(C_1(i))^\perp \) then the minimum distance of \( [\beta(C_1(i))]^\perp \) is at least \( a_1(i) + a_2(i) - (2g_i - 2) \)). Proceeding similarly as in the proof of Theorem 3.10 we get \( N_i - 2 - (b_1(i) + b_2(i)) \geq a_1(i) + a_2(i) - (2g_i - 2) \geq (N_i - K_i - 2g_i + 1)/2 \). Consequently, one has \( \limsup_{t \to \infty} 2rK_i/2r(N_i - 2) > 0 \) and \( \limsup_{t \to \infty} (N_i - K_i - 2g_i + 1)/4r(N_i - 2) = 1/4r[1 - 2/(p^r - 1) - c] > 0 \), as desired.

**Remark 3.13** Although the proofs of Theorems 3.10 and 3.12 are similar to that of given in Refs. [5, 12] in our case we utilize \( t \)-point (\( t \geq 2 \)) AG codes whereas in such references, the authors utilized one-point AG codes to this end. Other difference is that in Refs. [5, 12] the authors utilized code concatenation to obtain codes over prime fields. Here we use code expansion.

### 4 Examples and Code Comparison

In Table 1, we present some good quantum codes obtained from Corollaries 3.3 and 3.5. All the codes shown in Table 1 seem to be new. Note that the new \([26, 16, d \geq 3]_9\) code is better than the \([26, 14, 3]_9\) code shown in Ref. [6] and the new \([26, 14, d \geq 4]_9\) code is much better than the \([26, 4, 4]_9\) code shown in Ref. [6].
Table 1: New quantum codes

| New codes from Corollary 3.5 |  |
|-------------------------------|  |
| $q = 3, m = 4, a_1 = 3, a_2 = 4, b_1 = 7, b_2 = 16$ | [26, 16, $d \geq 3]_9$ |
| $q = 3, m = 4, a_1 = 3, a_2 = 5, b_1 = 7, b_2 = 15$ | [26, 14, $d \geq 4]_9$ |
| $q = 3, m = 4, a_1 = 3, a_2 = 6, b_1 = 7, b_2 = 14$ | [26, 12, $d \geq 5]_9$ |
| $q = 3, m = 4, a_1 = 3, a_2 = 10, b_1 = 7, b_2 = 10$ | [26, 4, $d \geq 9]_9$ |
| $q = 3, m = 4, a_1 = 4, a_2 = 10, b_1 = 6, b_2 = 10$ | [26, 2, $d \geq 10]_9$ |

| New codes from Corollary 3.3 |  |
|-------------------------------|  |
| $q = 3, m = 4, a = 7, b = 24$ | [27, 17, $d \geq 3]_{16}$ |
| $q = 3, m = 4, a = 8, b = 23$ | [27, 15, $d \geq 4]_{16}$ |
| $q = 3, m = 4, a = 9, b = 22$ | [27, 13, $d \geq 5]_{16}$ |
| $q = 3, m = 4, a = 10, b = 21$ | [27, 11, $d \geq 6]_{16}$ |
| $q = 3, m = 4, a = 11, b = 20$ | [27, 9, $d \geq 7]_{16}$ |
| $q = 3, m = 4, a = 12, b = 19$ | [27, 7, $d \geq 8]_{16}$ |
| $q = 3, m = 4, a = 13, b = 18$ | [27, 5, $d \geq 9]_{16}$ |
| $q = 3, m = 4, a = 14, b = 17$ | [27, 3, $d \geq 10]_{16}$ |
| $q = 3, m = 4, a = 15, b = 16$ | [27, 1, $d \geq 11]_{16}$ |
| $q = 4, m = 5, a = 13, b = 61$ | [64, 48, $d \geq 3]_{16}$ |
| $q = 4, m = 5, a = 14, b = 60$ | [64, 46, $d \geq 4]_{16}$ |
| $q = 4, m = 5, a = 15, b = 59$ | [64, 44, $d \geq 5]_{16}$ |
| $q = 4, m = 5, a = 25, b = 49$ | [64, 24, $d \geq 15]_{16}$ |
| $q = 4, m = 5, a = 35, b = 39$ | [64, 4, $d \geq 25]_{16}$ |
| $q = 4, m = 5, a = 36, b = 38$ | [64, 2, $d \geq 26]_{16}$ |
| $q = 5, m = 3, a = 9, b = 62$ | [65, 53, $d \geq 3]_{25}$ |
| $q = 5, m = 3, a = 10, b = 61$ | [65, 51, $d \geq 4]_{25}$ |
| $q = 5, m = 3, a = 11, b = 60$ | [65, 49, $d \geq 5]_{25}$ |
| $q = 5, m = 3, a = 31, b = 40$ | [65, 9, $d \geq 25]_{25}$ |
| $q = 7, m = 4, a = 19, b = 172$ | [175, 153, $d \geq 3]_{49}$ |
| $q = 7, m = 4, a = 20, b = 171$ | [175, 151, $d \geq 4]_{49}$ |
| $q = 7, m = 4, a = 21, b = 170$ | [175, 149, $d \geq 5]_{49}$ |
| $q = 7, m = 4, a = 41, b = 150$ | [175, 109, $d \geq 25]_{49}$ |
| $q = 7, m = 4, a = 80, b = 111$ | [175, 31, $d \geq 64]_{49}$ |
| $q = 7, m = 4, a = 95, b = 96$ | [175, 1, $d \geq 79]_{49}$ |

New codes from Corollary 3.9

| New codes from Corollary 3.9 |  |
|-------------------------------|  |
| $q = 5, m = 2, t_1 = 3, t_2 = 21$ | [46, 36, $d \geq 4]_{25}$ |
| $q = 5, m = 2, t_1 = 4, t_2 = 20$ | [46, 32, $d \geq 6]_{25}$ |
| $q = 5, m = 2, t_1 = 5, t_2 = 19$ | [46, 28, $d \geq 8]_{25}$ |
| $q = 5, m = 2, t_1 = 11, t_2 = 13$ | [46, 4, $d \geq 20]_{25}$ |
When the alphabet is large, it is difficult to find codes over such alphabets available in the literature. Because of this, we will compare the parameters of the new codes based on the quantum Singleton bound (QSB). Recall that an $[[n, k, d]]_q$ quantum code satisfies $k + 2d \leq n + 2$ (QSB). Note that our new quantum codes of length 46 has Singleton defect 4. Moreover, all new quantum codes of length $n = 26$ and $n = 27$ exhibited in Table 1 have Singleton defect 6. It is also interesting to observe the our new codes of length $n = 175$ shown in Table 1 have Singleton defect 18. For example, the $[[175, 31, d \geq 64]]_{49}$ new code achieve minimum distance greater that 64 and its Singleton defect is 18, whereas the codes $[[165, 99, 18]]_9$ and $[[194, 144, 8]]_9$ available in Ref. [6], with similar code length only attains minimum distances 18 and 8, respectively, and they have Singleton defect 32 and 36, respectively. Additionally, the codes shown in Ref. [6] have their Singleton defects increased when the minimum distance increases. In other words, the $[[161, 143, 7]]_9$ code has Singleton defect 6, the $[[161, 131, 11]]_9$ code has Singleton defect 10 and the $[[161, 113, 17]]_9$ has Singleton defect 16. As more one example, the $[[165, 151, 5]]_9$ has Singleton defect 6 but the $[[165, 99, 18]]_9$ code has Singleton defect 32. Therefore, based on these fact, the new quantum codes have good parameters. Additionally, note that our new $[[27, 3, d \geq 10]]_9$, $[[27, 5, d \geq 9]]_9$, $[[65, 9, d \geq 25]]_{25}$, $[[175, 31, d \geq 64]]_{49}$ and $[[175, 1, d \geq 79]]_{49}$ codes has extremely large minimum distance when compared to its code length.

5 Final Remarks

We have constructed several new families of quantum codes with good and asymptotically good parameters. These new quantum codes are derived from algebraic geometry codes. Many of these quantum codes have large minimum distances when compared with its code length. Additionally, they have relatively small Singleton defect. Moreover, we have shown how to obtain sequences of asymptotically good quantum codes derived from $t$-point AG codes, where $t \geq 2$. Therefore, the class of algebraic geometry is a good source to construct quantum codes with good or asymptotically good parameters.

Acknowledgements

This research has been partially supported by the Brazilian Agencies CAPES and CNPq.

References

[1] S.A. Aly and A. Klappenecker. On quantum and classical BCH codes. IEEE Trans. Inform. Theory, 53(3):1183–1188, 2007.
[2] A. Ashikhmin, S. Litsyn, M.A. Tsfasman. Asymptotically good quantum codes Phys. Rev. A, 63(3):032311(1–5), 2001.
[3] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory, 44(4):1369–1387, 1998.

[4] H. Chen. Some good quantum error-correcting codes from algebraic-geometric codes. IEEE Trans. Inform. Theory, 47(5):2059–2061, 2001.

[5] H. Chen, S. Ling, and C. Xing Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound. IEEE Trans. Inform. Theory, 47(5):2055–2058, 2001.

[6] Yves Edel. Table of quantum twisted codes. electronic address: www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html

[7] A. Garcia and H. Stichtenoth. On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields. J. Number Theory, 61:248–273, 1996.

[8] M. Grassl, W. Geiselmann, T. Beth. Quantum Reed-Solomon codes. AAECC-13, 1709:231-244, 1999.

[9] W.C. Huffman and V. Pless. Fundamentals of Error-Correcting Codes. Cambridge Univ. Press, New York, 2003.

[10] L. Jin and C. Xing. Euclidean and hermitian self-orthogonal algebraic geometry codes and their application to quantum codes. IEEE Trans. Inform. Theory, 58(8):5484–5489, 2012.

[11] A. Ketkar, A. Klappenecker, S. Kumar and P.K. Sarvepalli. Nonbinary stabilizer codes over finite fields. IEEE Trans. Inform. Theory, 52(11):4892–4914, 2006.

[12] J-L. Kim and J. Walker Nonbinary quantum error-correcting codes from algebraic curves. Discrete Math., 308:3115–3124, 2008.

[13] G.G. La Guardia. Constructions of new families of nonbinary quantum codes. Phys. Rev. A, 80(4):042331(1–11), 2009.

[14] G.G. La Guardia. New quantum MDS codes. IEEE Trans. Inform. Theory, 57(8):5551–5554, 2011.

[15] G.G. La Guardia. Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes. Quantum Inf. Process., 11:591-604, 2012.

[16] G.G. La Guardia. On the construction of nonbinary quantum BCH codes. IEEE Trans. Inform. Theory, 60(3):1528–1535, 2014.

[17] R. Matsumoto. Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes. IEEE Trans. Inform. Theory, 48(7):2122–2124, 2002.

[18] M.A. Nielsen and I.L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[19] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound. IEEE Trans. Inform. Theory, 52(5):2218–2224, 2006.

[20] H. Stichtenoth. Algebraic Function Fields and Codes. Springer, 2009.