Iranian Journal of Mathematical Sciences and Informatics
Vol. 16, No. 1 (2021), pp 65-76
DOI: 10.29252/ijmsi.16.1.65

One-point Goppa Codes on Some Genus 3 Curves with Applications in Quantum Error-Correcting Codes

Rasoul Mohammadi

Department of Mathematics, Tarbiat Modares University, Tehran, Iran.

E-mail: rasool.mohammadi@modares.ac.ir

Abstract. We investigate one-point algebraic geometric codes $C_L(D, G)$ associated to maximal curves recently characterized by Tafazolian and Torres given by the affine equation $y^l = f(x)$, where $f(x)$ is a separable polynomial of degree r relatively prime to l. We mainly focus on the curve $y^4 = x^3 + x$ and Picard curves given by the equations $y^3 = x^4 - x$ and $y^3 = x^4 - 1$. As a result, we obtain exact value of minimum distance in several cases and get many records that don't exist in MinT tables (tables of optimal parameters for linear codes), such as codes over $\mathbb{F}_{7^2}$ of dimension less than 36. Moreover, using maximal Hermitian curves and their sub-covers, we obtain a necessary and sufficient condition for self-orthogonality and Hermitian self-orthogonally of $C_L(D, G)$.

Keywords: Algebraic geometric codes, Maximal curves, Minimum distance, *Goppa* bound, Quantum error-correcting codes.

2010 Mathematics subject classification: 11T71, 94B27, 14G05, 14G50.

1. Introduction

Algebraic geometric codes (AG codes) are a type of linear error-correcting codes introduced by *Goppa* in 1981 [9, 10] using concepts from algebraic geometry.

*Corresponding Author

Received 20 February 2018; Accepted 25 April 2018

Throughout this paper, by a curve we mean a geometrically irreducible, projective non-singular curve defined over a finite field $\mathbb{F}_q$ of characteristic p. One is often interested in curves $\mathcal{C}$ with many rational points. The celebrated theorem of Weil states that the number $N(\mathcal{C})$ of rational points of a curve $\mathcal{C}$ of genus g over $\mathbb{F}_q$ satisfies the inequality:

$$|N(\mathcal{C}) - (q+1)| \leq 2gq^{1/2}. \tag{1.1}$$

This bound is important for many applications such as in coding theory [26] and elliptic curve cryptography [11]. The curve $\mathcal{C}$ is said to be maximal over $\mathbb{F}_{q^2}$, if the upper bound in 1.1 is attained, namely:

$$N(\mathcal{C}) = q^2 + 1 + 2gq.$$

From now on, $f(x)$ is a separable polynomial of degree r. The class $\mathcal{C}^{l,r}$ denotes curve given by the affine equation $y^l = f(x)$, where $\gcd(l, r) = 1$. AG codes over the curves $\mathcal{C}^{l,r}$ have been the subject of many papers, e.g. [19, 25]. In [4], Castellanos, Masuda and Quoos computed the Weierstrass semigroup at certain totally ramified places and constructed AG codes with good parameters, specifically on the curves $y^3 = x^5 - x$ over $\mathbb{F}_{25}$ and $y^9 = x^4 + x^2 + x$ over $\mathbb{F}_{64}$. In [13], Hu and Yang described bases for the Riemann-Roch spaces associated to totally ramified places in the Kummer extensions given by $y^l = f(x)^\lambda$ where $\gcd(l, \deg(f(x)).\lambda) = 1$, and extended the results of [4] to multi-point codes. In particular, they studied codes on the curves $y^5 = x^9 + x$ over $\mathbb{F}_{81}$ and $y^9 = x^4 + x^2 + x$ over $\mathbb{F}_{64}$, and attained many improvements over MinT tables. In [2], Bartoli, Quoos and Zini computed the number of Weierstrass gaps at two totally ramified places and applied their results to construct AG codes with good parameters.

In [27], Tafazolian and Torres classified certain maximal curves of type $\mathcal{C}^{l,r}$ given by $y^l = x^r + x$ over $\mathbb{F}_{q^2}$. As a result, $y^l = x^r + x$ is maximal over $\mathbb{F}_{q^2}$ if $l.(r-1)$ divides $q+1$. Another special form of $\mathcal{C}^{l,r}$ are Picard curves which correspond to $l = 3$ and $\deg(f) = 4$. These curves have been studied by many authors, e.g. [12, 28]. Also, the authors in [16] classified Newton Polygons of the curves $y^3 = x^4 - x$ and $y^3 = x^4 - 1$ and found all fields where these curves are maximal.

This paper is concerned with AG codes over maximal curves defined by the affine equation $\mathcal{C}^{l,r} : y^l = f(x)$, where $\gcd(l, r) = 1$.

We mainly focus on the curve $\mathcal{C}_0^{4,3} : y^4 = x^3 + x$ and Picard curves given by the equations $\mathcal{C}_1^{3,4} : y^3 = x^4 - x$ and $\mathcal{C}_2^{3,4} : y^3 = x^4 - 1$ (by ([26], Prop. 6.3.1), the genus of $\mathcal{C}^{l,r}$ is equal to $g = \dfrac{(l-1)(r-1)}{2}$). To find the minimum distance of codes in the above genus 3 curves, we use the Weil lower bound on the number of rational points on a curve to prove that certain equations have enough solutions in the ground field. As a result, we obtain new records

over MinT tables [20] as well as improvements on the *Goppa* bound using the order bound. In addition, we use some sub-covers of maximal Hermitian curves and prove a necessary and sufficient condition to obtain self-orthogonal and Hermitian self-orthogonal codes. As an example, using these Hermitian self-orthogonal codes, we generate new non-binary quantum error-correcting codes over [6].

The rest of this paper is organized as follows. In Section 2 we recall preliminary results needed for our main results. In Section 3 we obtain parameters of some codes on $\mathcal{C}^{l,r}$ over $\mathbb{F}_{q^2}$, mainly focusing on genus 3 curves. Specifically, in Subsection 3.1 and Subsection 3.2 we respectively obtain minimum distance of codes over the curve $\mathcal{C}_0^{4,3}$ and the Picard curves $\mathcal{C}_1^{3,4}$ and $\mathcal{C}_2^{3,4}$. Finally, in Section 4, using some Hermitian self-orthogonal AG codes over maximal Hermitian curves and their sub-covers, some quantum error-correcting codes are generated.

2. Preliminaries

Let $\mathcal{C}$ be an algebraic curve of genus g over $\mathbb{F}_q$. Denote by $\mathcal{C}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$ rational points on the curve, by $\mathbb{F}_q(\mathcal{C})$ the function field of $\mathcal{C}$, and for a function $f \in \mathbb{F}_q(\mathcal{C})$ let $\mathrm{div}(f)$ be the divisor of f. Let $P_1, ..., P_n$ be pairwise distinct rational points on $\mathcal{C}$ and $D = P_1 + ... + P_n$. Furthermore, let G be a divisor such that $P_i \notin \mathrm{supp}(G)$ for all i, where $\mathrm{supp}(G)$ stands for the support of G. Let $\mathcal{L}(A)$ denote the Riemann-Roch space associated to a divisor A, namely:

$$\mathcal{L}(A) = \{f \in \mathbb{F}_q(\mathcal{C}) \mid \mathrm{div}(f) \geq -A\} \cup \{0\}.$$

$\mathcal{L}(A)$ is a vector space over $\mathbb{F}_q$ and its dimension $l(A)$ is

$$l(A) = \deg(A) + 1 - g + i(A),$$

where $\deg(A)$ and $i(A)$ respectively denote the degree of A and the index of specialty of A, see ([26], Def. 1.5.1).

A (q-array) linear code C of length n is a linear subspace of the n-dimensional vector space $\mathbb{F}_q^n$; the elements of C are called codewords. The Hamming weight of a codeword $c \in \mathbb{F}_q^n$ denoted by $w(c)$ is defined as the number of its non-zero components. The minimum distance d of a code C is the minimum of $w(c)$ where c varies over all non-zero codewords of C. A code with length n, dimension k (as an $\mathbb{F}_q$-vector space) and minimum distance d is called an $[n, k, d]$ code.

Definition 2.1. The algebraic geometric code (AG code) $C_L(D, G)$ associated to the divisors D and G is defined as

$$C_L(D, G) = \{(z(P_1), ..., z(P_n)) \mid z \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

The following proposition gives the dimension k of a $C_L(D, G)$ code and a lower bound on its minimum distance d.

Proposition 2.2. *([26], Thm. 2.2.2) $C_L(D,G)$ is an $[n,k,d]$ code with parameters*

$$k = l(G) - l(G-D) \quad \textit{and} \quad d \geq n - \deg(G)$$

.

The bound in Proposition 2.2 on d is called *Goppa* bound. As a result, if $\deg(G) < n$, then $k = l(G)$. Therefore, by 2.2 and singleton bound ([26], Prop. 2.1.8), $n+1-g \leq k+d \leq n+1$. In addition, if $2g-2 < \deg(G) < n$, then $k = \deg(G)+1-g$ (such codes also called strong algebraic geometric codes).

$C_L(D,G)$ is called an a-point code, if $\mathrm{supp}(G)$ contains exactly a-distinct points. In this paper, we consider one-point codes.

Note that we have a trivial case: if $\deg(G-D) > 2g-2$, then $i(G-D) = 0$. Thus, $k = \deg(D) = n$ and by singleton bound, $d = 1$. Therefore, in this case we have trivial *MDS* codes. Hence, we assume that $\deg(G-D) \leq 2g-2$.

The following theorem ensures that all roots of the polynomial $f(x)$ belong to $\mathbb{F}_{q^2}$. In Theorem 3.1, we will use this result to determine the exact number of rational points that correspond to rational places ramified in $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$.

Theorem 2.3. [27] *Let q be a prime power, $l \geq 2$ an integer, and $f(x)$ be a separable polynomial in $\mathbb{F}_{q^2}[x]$ of degree $r \geq 2$ with $\gcd(l, rq) = 1$. Let $\mathcal{C}$ be the non-singular model over $\mathbb{F}_{q^2}$ of the plane curve defined by $y^l = f(x)$. Suppose that $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$. Then l divides $q+1$ if and only if $f(x)$ has a root in $\mathbb{F}_{q^2}$. In this case, all the roots of $f(x)$ belong to $\mathbb{F}_{q^2}$.*

Definition 2.4. The Weierstrass semigroup at a point P denoted by $H(P)$ is defined as the semigroup of non-negative integers t, called *non-gaps*, such that $l(tP) > l((t-1)P)$.

The Weierstrass semigroup plays a considerable role in the construction of AG codes, in particular for computing the dimension of the Riemann-Roch space associated to a one-point divisor. We have:

Proposition 2.5. *([26], proof of Thm. 1.6.8) Let $m \geq 0$ be an integer. Then*

$$l(mP) = |i \in H(P),\ i \leq m|.$$

In other words, $l(mP)$ is equal to the number of non-gaps which are less than or equal to m.

The curve $y^l = f(x)$ in Theorem 2.3 has a unique point at infinity, denoted by P_∞. By [4], the Weierstrass semigroup at P_∞ is generated by l and r.

3. Codes on $\mathcal{C}^{l,r} : y^l = f(x)$ over $\mathbb{F}_{q^2}$

In this section, we consider maximal curves of type $\mathcal{C}^{l,r} : y^l = f(x)$ of genus g defined over $\mathbb{F}_{q^2}$ of characteristic p for $f(x)$ a separable polynomial of degree

r, where $\gcd(r,l)=1$ and l divides $q+1$. In our setting, $C_L(D,G)$ is a one-point code constructed by divisors G and D where G is a multiple of P_∞ - the unique point at infinity - and D is the sum of the $n=q^2+2gq$ remaining rational points.

By Theorem 2.3, all roots of $f(x)$ belong to $\mathbb{F}_{q^2}$. Therefore, corresponding to any root of $f(x)$ there is a rational place ramified in $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$. There are $a_1,...,a_s \in \mathbb{F}_{q^2}$ such that the rational place associated to $x-a_i, i=1,...,s$, splits in $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$, where $s=(q^2+2gq-r)/l$.
In the following theorem, we describe some results about the minimum distance of certain codes over $\mathcal{C}^{l,r}$. In addition, we show that $G-D$ is equivalent to some one-point divisor.

Theorem 3.1. *Let $\mathcal{C}^{l,r}$ be maximal over $\mathbb{F}_{q^2}$ and D be the sum of all its affine $n=q^2+2gq$ rational points over $\mathbb{F}_{q^2}$.*
(a) *Suppose that $m\in\mathbb{N}$, $m\le (q^2+2gq-r)/l$. Then for $G=mlP_\infty$, the minimum distance of $C_L(D,G)$ is equal to $d=n-\deg(G)$,*
(b) *For m as in* (a)*, If $G=(ml+r)P_\infty$, then $d=n-\deg(G)$,*
(c) *For $G=\deg(G)P_\infty$, $G-D$ is equivalent to a one-point divisor.*

Proof. (a) Put $z=\prod_{i=1}^{m}(x-a_i)\in\mathbb{F}_q(\mathcal{C})$. Then $z\in\mathcal{L}(G)$ and z has exactly $ml=\deg(G)$ zeros in $\mathcal{C}(\mathbb{F}_{q^2})$. Therefore, $d\le n-\deg(G)$ and by Proposition 2.2, $d=n-\deg(G)$.
(b) Similarly to (a), $z=y.\prod_{i=1}^{m}(x-a_i)\in\mathcal{L}(G)$ gives the result.
(c) Let $z=y.\prod_{i=1}^{s}(x-a_i)$. Then, we have $\mathrm{div}(z)=D-(q^2+2gq)P_\infty$. Consequently, $G-D=(\deg(G)-(q^2+2gq))P_\infty-div(z)$. It follows that $G-D$ is equivalent to the one-point divisor $(\deg(G)-(q^2+2gq))P_\infty$ as required. □

Using the following theorem, one can compute the exact dimension of all codes $C_L(D,G)$ over $\mathcal{C}^{l,r}$.

Theorem 3.2. *Let $G=\deg(G)P_\infty$. The dimension of $C_L(D,G)$ is equal to*

$$k=|i\in H(P_\infty),\ i\le\deg(G)|-|i\in H(P_\infty),\ i\le(\deg(G)-(q^2+2gq))|.$$

Proof. By part (c) of Theorem 3.1, $G-D$ is equivalent to the one-point divisor $(\deg(G)-(q^2+2gq))P_\infty$. Accordingly, Proposition 2.5 gives the exact dimension $k=l(G)-l(G-D)$.

□

Remark 3.3. Let $g=3$ and $\mathcal{L}(G-D)$ be non-trivial. We give another approach for computing the exact dimension of $\mathcal{L}(G-D)$ in some cases:

Case 1. $\deg(G-D)=0$. By our assumption, there is a non-trivial function $f\in\mathcal{L}(G-D)$. Therefore, $\mathrm{div}(f)+G-D\ge 0$. Since $\deg(\mathrm{div}(f))=\deg(G-D)=0$, we conclude that $\mathrm{div}(f)+G-D=0$. Consequently, $G-D$ is equivalent to the null divisor 0 and $l(G-D)=l(0)=1$.

Case 2. $\deg(G-D)=1$. By Clifford's theorem ([26], Thm. 1.6.13), we have $l(G-D)\leq 1+\frac{1}{2}\deg(G-D)$. Therefore, $l(G-D)=1$.

Case 3. $\deg(G-D)=2$. By Clifford's theorem, $l(G-D)\leq 2$. From [21], $l(G-D)=2$ if and only if one of the following conditions holds:
(a) $\mathcal{C}^{l,r}$ is hyperelliptic and $G-D$ is a hyperelliptic divisor, or
(b) $G-D$ is a principal divisor, or
(c) $G-D$ is a canonical divisor.
By ([26], Def. 6.2.1), condition (a) is not true. Condition (b) is not true because $\deg(G-D)\neq 0$. Moreover, condition (c) is wrong since $\deg(G-D)\neq 2g-2$. Therefore in this case, $l(G-D)=1$.

The *Goppa* bound $d\geq n-\deg(G)$ doesn't give the true minimum distance in many cases. For example, if $\deg(G)\geq n$, it doesn't give any information. Besides the *Goppa* bound, we recall some results about the order bound of one-point AG codes based on Weierstrass semigroup.

Let $H(P_\infty)=\{\varrho_1=0<\varrho_2<...\}$ be the Weierstrass semigroup at P_∞ and $H^*=H(P_\infty)-(n+H(P_\infty))=\{\varrho_1^*=0<...<\varrho_n^*\}$. For $i=1,...,n$ define $\Lambda_i^*:=\{\varrho\in H^*\mid \varrho-\varrho_i^*\in H^*\}$. Then for $G_i=\varrho_i^*P_\infty$, the minimum distance d of $C_L(D,G_i)$ satisfies [8]

$$d\geq \min\{|\Lambda_1^*|,...,|\Lambda_i^*|\}.$$

Example 3.4. Consider the maximal curve $y^7=x^3+x$ over $\mathbb{F}_{13^2}$ of genus 6. This curve has 326 rational points. The Weierstrass semigroup at P_∞ is generated by 7 and 3. Thus, $H^*=\{0,3,6,7,9,10,12,13,...,324,326,327,329,330,333,336\}$. Use of the order bound gives the codes $[325,316,\geq 6]$ and $[325,320,3]$ that improve the *Goppa* bound.

Remark 3.5. The curve $y^7=x^3+x$ over $\mathbb{F}_{13^2}$, gives new records that don't exist in MinT tables.

3.1. **Codes on $\mathcal{C}_0^{4,3}:y^4=x^3+x$ over $\mathbb{F}_{q^2}$.** In this section we consider a curve of genus 3, namely the maximal curve $\mathcal{C}_0^{4,3}:y^4=x^3+x$ over $\mathbb{F}_{q^2}$. By [27], $\mathcal{C}_0^{4,3}$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q\equiv -1,3 \pmod 8$.

In our paper's initial version, the results obtained by Theorem 3.6 over $\mathbb{F}_{49}$ had significant improvements compared to MinT tables. However, just recently, MinT tables have been updated matching our results except for Table 1. These codes still don't exist in MinT tables.

Recall that for every $i=1,...,s$, the element $a_i\in\mathbb{F}_{q^2}$ corresponds to the place associated to $x-a_i$ in the rational function field. This place splits in $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$.

Theorem 3.6. *Set $s=(q^2+2gq-3)/4$. Then we have:*
(a) *If $G=(4m+1)P_\infty$, then $d=n-\deg(G)$, for $m\leq(s-1)$.*
(b) *If $G=(4m+2)P_\infty$, then $d=n-\deg(G)$, for $m\leq(s-2)$.*

n	deg(G)	k	d	n	deg(G)	k	d
91	2	1	≥ 89	91	20	18	71
91	3	2	88	91	21	19	70
91	4	3	87	91	22	20	69
91	5	3	≥ 86	91	23	21	68
91	6	4	85	91	24	22	67
91	7	5	84	91	25	23	66
91	8	6	83	91	26	24	65
91	9	7	82	91	27	25	64
91	10	8	81	91	28	26	63
91	11	9	80	91	29	27	62
91	12	10	79	91	30	28	61
91	13	11	78	91	31	29	60
91	14	12	77	91	32	30	59
91	15	13	76	91	33	31	58
91	16	14	75	91	34	32	57
91	17	15	74	91	35	33	56
91	18	16	73	91	36	34	55
91	19	17	72	91	37	35	54

TABLE 1. Minimum distance of codes on $\mathcal{C}_0^{4,3} : y^4 = x^3 + x$ over $\mathbb{F}_{49}$ of dimensions less than 36

Proof. (a). One can see that for every non-zero $\lambda \in \mathbb{F}_q$, the equation $y^2 = \lambda$ has two solutions in $\mathbb{F}_{q^2}$. Suppose that $q-4\sqrt{q} > 5$. We claim that for a non-zero $\lambda \in \mathbb{F}_q$, the equation $x^3+x = \lambda^2$ has three solutions in $\mathbb{F}_q$ (and therefore in $\mathbb{F}_{q^2}$). Suppose this claim is not true. In fact, suppose that for every non-zero $\lambda \in \mathbb{F}_q$, the equation $x^3 + x = \lambda^2$ has at most one solution in $\mathbb{F}_q$. Then the elliptic curve $x^3 + x = \lambda^2$ has at most $(q-1)/2 + 4$ solutions in $\mathbb{F}_q$. This contradicts Weil's bound 1.1. So, the assertion follows. Now suppose that $q - 4\sqrt{q} \leqslant 5$. Due to the maximality of $\mathcal{C}_0^{4,3}$, five cases arise:

Case 1. $q = 3$. Let $\lambda = 2$. The equation $y^2 = 2$ gives 6 rational points corresponding to the solutions of $x^3+x-4 = (x-2)(x+1+\sqrt{-1})(x+1-\sqrt{-1})$.

Case 2. $q = 7$. Let $\lambda = 2$. The equation $y^2 = 2$ gives 6 rational points corresponding to the solutions of $x^3+x-4 = (x+2)(x-1-\sqrt{3})(x-1+\sqrt{3})$.

Case 3. $q = 11$. Let $\lambda = 3$. Let $a = 2^{-1}$. The equation $y^2 = 3$ gives 6 rational points corresponding to the solutions of $x^3 + x - 9 = (x+1)(x-a-\sqrt{-7a^2})(x-a+\sqrt{-7a^2})$.

Case 4. $q = 19$. Let $\lambda = 3$. The equation $y^2 = 3$ gives 6 rational points corresponding to the solutions of $x^3+x-9 = (x+2)(x-1-\sqrt{-4})(x-1+\sqrt{-4})$.

Case 5. $q = 23$. Let $\lambda = 1$. The equation $y^2 = 1$ gives 6 rational points corresponding to the solutions of $x^3+x-1 = (x+4)(x-2-\sqrt{-13})(x-2+\sqrt{-13})$.

For such λ, put $z = (y^3 - \lambda y).\prod_{i=1}^{m-2}(x - a_i) \in \mathcal{L}(G)$. Then z has exactly $4m + 1$ zeros in $\mathcal{C}_0^{4,3}(\mathbb{F}_{q^2})$. This gives (a).
(b) Let $z = (y^2 - \lambda).\prod_{i=1}^{m-1}(x - a_i)$, and argue as in (a). □

Remark 3.7. The Weierstrass semigroup at P_∞ is generated by 3 and 4 and is equal to $H(P_\infty) = \{\varrho_1 = 0, \varrho_2 = 3, \varrho_3 = 4, ...\}$. A simple computation gives $H^* = \{\varrho_1^* = 0, \varrho_2^* = 3, \varrho_3^* = 4, \varrho_4^* = 6, \varrho_5^* = 7, ..., \varrho_{88}^* = 90, \varrho_{89}^* = 92, \varrho_{90}^* = 93, \varrho_{91}^* = 96\}$. By the order bound, we find codes with parameters $[91, 88, 3]$ and $[91, 84, \geq 6]$ which improve the *Goppa* bound.

3.2. **Codes on $\mathcal{C}_1^{3,4} : y^3 = x^4 - x$ and $\mathcal{C}_2^{3,4} : y^3 = x^4 - 1$ over $\mathbb{F}_{q^2}$.** The curves $\mathcal{C}_1^{3,4} : y^3 = x^4 - x$ and $\mathcal{C}_2^{3,4} : y^3 = x^4 - 1$ are special forms of Picard curves. A Picard curve over a finite field k of characteristic $p > 3$ can be defined as the affine model $y^3 = f(x)$ where $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is a polynomial over k without multiple roots in $\overline{k}$ (the algebraic closure of k). We have the following theorem about the maximality of these curves.

Theorem 3.8. [16] *Let $p > 3$ be a prime number and q a power of p. Then:*

- *The smooth complete Picard curve $y^3 = x^4 - x$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1$ (mod 9).*
- *The smooth complete Picard curve $y^3 = x^4 - 1$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1$ (mod 12).*

Now we obtain the minimum distance of some codes over the above curves $\mathcal{C}_1^{3,4}$ and $\mathcal{C}_2^{3,4}$.

Theorem 3.9. *Set $s = (q^2 + 2gq - 4)/3$. Then we have:*
(a) *If $G = (3m + 1)P_\infty$, then $d = n - \deg(G)$, for $m \leq (s + 1)$.*
(b) *If $G = (3m + 2)P_\infty$, then $d = n - \deg(G)$, for $m \leq (s - 2)$.*

Proof. (a) In this case, choose $z = y.\prod_{i=1}^{m-1}(x - a_i)$. Then $z \in \mathcal{L}(G)$ and has $3m + 1$ zeros in $\mathcal{C}_1^{3,4}(\mathbb{F}_{q^2})$ and $\mathcal{C}_2^{3,4}(\mathbb{F}_{q^2})$.
(b) We claim that for a non-zero $\lambda \in \mathbb{F}_{q^2}$, the equation $x^4 - x = \lambda^3$ has four solutions in $\mathbb{F}_{q^2}$. Let $q^2 - 18q > 10$ and suppose this claim is not true. In fact, suppose that for every non-zero $\lambda \in \mathbb{F}_{q^2}$, the equation $x^4 - x = \lambda^3$ has at most two solutions in $\mathbb{F}_{q^2}$. Then by the fact that there are $(q^2 - 1)/3$ possible values for λ^3, the curve $x^4 - x = \lambda^3$ has at most $2.(q^2 - 1)/3 + 5$ rational points in $\mathbb{F}_{q^2}$. This contradicts Weil's bound 1.1. Therefore, the assertion follows. The same holds for the equation $x^4 - 1 = \lambda^3$. Now suppose that $q^2 - 18q \leq 10$. By Theorem 3.8, two cases arise:

Case 1. $q = 17$ for the curve $y^3 = x^4 - x$. Choose $\lambda = 1$. The equation $x^4 - x - 1$ gives 4 rational points corresponding to the roots of $x^4 - x - 1 = (x + 2)(x + 5)(x + 5 - \sqrt{3})(x + 5 + \sqrt{3})$.

Case 2. $q = 11$ for the curve $y^3 = x^4 - 1$. Choose $\lambda = 1$. The equation $x^4 - 2$ gives 4 rational points corresponding to the roots of $x^4 - 2$=$(x + 2 - \sqrt{-4})(x + 2 + \sqrt{-4})(x - 2 - \sqrt{-4})(x - 2 + \sqrt{-4})$.

For such λ, put $z = (y^2 - \lambda y).\prod_{i=1}^{m-2}(x - a_i) \in \mathcal{L}(G)$. Then z has exactly $3m + 2$ zeros in $\mathcal{C}_1^{3,4}(\mathbb{F}_{q^2})$ and $\mathcal{C}_2^{3,4}(\mathbb{F}_{q^2})$. This gives the result. □

Remark 3.10. For $q^2 - 18q > 10$ and $q^2 \equiv 1(\text{mod } 3)$, Theorem 3.9 can be generalized straightforwardly to every Picard curve $y^3 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ over $\mathbb{F}_{q^2}$.

4. Application to quantum error-correcting codes

To protect information from errors in a quantum channel, quantum error-correction has a crucial role. We refer to [1, 23] for the use of classical codes and [3, 5, 7, 14, 15, 17, 22, 24] for algebraic geometric codes to generate quantum error-correcting codes. Consider the maximal Hermitian curve $\mathcal{C}_H^{q+1,q} : y^{q+1} = x^q + x$ over $\mathbb{F}_{q^2}$. Suppose that the ground curve is a sub-cover $y^l = x^q + x$ of $\mathcal{C}_H^{q+1,q}$, where l divides $q + 1$. Accordingly, $v_{P_\infty}(y) = -q$ and $v_{P_\infty}(x) = -l$, where v_{P_∞} denotes the valuation at P_∞. Recall that D is the sum of all affine $n = q^2 + 2gq$ rational points of $y^l = x^q + x$ over $\mathbb{F}_{q^2}$. By [22], the dual of $C_L(D, mP_\infty)$ is equal to $C_L(D, (n - m + 2g - 2)P_\infty)$.

Definition 4.1. The Hermitian inner product over $\mathbb{F}_{q^2}^n$ is defined as $\langle a, b\rangle_H = \langle a, b^q\rangle$, where $\langle ., .\rangle$ denotes the usual inner product. The dual of a linear code $C \subset \mathbb{F}_{q^2}^n$ corresponding to the Hermitian inner product is

$$C_H^\perp = \{x \in \mathbb{F}_{q^2}^n \mid \langle a, c\rangle_H = 0,\ c \in C\}.$$

Consider c^q by taking the componentwise q-th power of c and let $C^q = \{c^q \mid c \in C\}$. The code C is Hermitian self-orthogonal if $C \subset C_H^\perp$ or equivalently, $C^q \subset C^\perp$. We use the later condition to generate Hermitian self-orthogonal codes. The following theorem gives a necessary and sufficient condition to obtain self-orthogonal and Hermitian self-orthogonal codes. We use the notation $\overline{m} = n - m + 2g - 2$.

Theorem 4.2. *Using the notations as above, we have:*
(a) $C_L(D, mP_\infty)$ *is self-orthogonal if and only if* $m \le \overline{m}$.
(b) $C_L(D, mP_\infty)$ *is Hermitian self-orthogonal if and only if* $(q+1)m \le n+2g-2$.

Proof. (a) $C_L(D, mP_\infty)$ is self-orthogonal if $C_L(D, mP_\infty) \subseteq C_L(D, \overline{m}P_\infty)$, that is a consequence of $m \le \overline{m}$. Conversely, suppose that $m > \overline{m}$. we show that there is a rational function $z = x^iy^j$ such that $v_{P_\infty}(z) \ge -m$ and $v_{P_\infty}(z) < -\overline{m}$ which implies that $C_L(D, mP_\infty) \nsubseteq C_L(D, \overline{m}P_\infty)$. There are integers i_1 and j_1 such that $i_1l+j_1q = 1$. Consequently, $mi_1l+mj_1q = m$. Choose $i = mi_1$ and $j = mj_1$. Then $v_{P_\infty}(z) = -m$ which results in $v_{P_\infty}(z) \ge -m$ and $v_{P_\infty}(z) < -\overline{m}$.

(b) $C_L(D, mP_\infty)$ is Hermitian self-orthogonal if $C_L(D, qmP_\infty) \subseteq C_L(D, \overline{m}P_\infty)$, that is a consequence of $(q+1)m \leq n+2g-2$. Conversely, suppose that $(q+1)m > n+2g-2$. We show that there is a rational function $z = x^i y^j$ such that $v_{P_\infty}(z) \geq -m$ and $v_{P_\infty}(z^q) < -\overline{m}$ which implies that $C_L(D, mP_\infty)^q \nsubseteq C_L(D, \overline{m}P_\infty)$. The remaining of the proof is similar to part (a) and we omit the details. □

Remark 4.3. In Theorem 4.2 part (a), the converse can be obtained using maximality of $y^l = x^q + x$ over $\mathbb{F}_{q^2}$, where q is odd. For this, the condition $m > \overline{m}$ implies that $m \geq n/2 + g$. We show that there are integers i and j such that $\overline{m} < il + jq \leq m$ which results in $C_L(D, mP_\infty) \nsubseteq C_L(D, \overline{m}P_\infty)$. Note that the maximum value of $\overline{m}$ occurs when m is minimum, i.e. $n/2+g$, which results in $\max(\overline{m}) = n/2 + g - 2$. Accordingly, the integer $\lfloor n/2 + g \rfloor$ satisfies $\lfloor n/2 + g \rfloor \leq m$ and $\lfloor n/2 + g \rfloor > \overline{m}$, where $\lfloor . \rfloor$ denotes the floor function. So, it is sufficient to show that $\lfloor n/2 + g \rfloor \in H(P_\infty)$, the Weierstrass semigroup at P_∞ which is generated by l and q. By maximality of $y^l = x^q + x$ over $\mathbb{F}_{q^2}$, we have $n = q^2 + 2gq$. The following equalities arise:

$$\begin{aligned} \lfloor n/2 + g \rfloor &= \lfloor q^2/2 \rfloor + (q+1)g \\ &= \lfloor (q^2 - 1 + 1)/2 \rfloor + (q+1)g \\ &= (q-1)/2.(q+1) + (q+1)g \\ &= (q+1)((q-1)/2 + g). \end{aligned}$$

Since l divides $q+1$, we conclude that $q+1 \in H(P_\infty)$. It follows that $\lfloor n/2 + g \rfloor \in H(P_\infty)$ as required.

We use the following theorem to obtain a lower bound of the minimum distance of quantum codes.

Theorem 4.4. [1] *Let $C = [n, k, d(C)]$ be a classical Hermitian self-orthogonal code over $\mathbb{F}_{q^2}$. There exists a q-array $[[n, n-2k, \geq d(C^\perp)]]_q$ quantum code, where $d(C^\perp)$ denotes the minimum distance of the dual code $C^\perp$.*

Corollary 4.5. *Let $C_L(D, mP_\infty)$ be an $[n, k, d(C)]$ AG code over $\mathbb{F}_{q^2}$ such that $(q+1)m \leq n+2g-2$. Then we have an $[[n, n-2k, \geq m-2g+2]]_q$ quantum code.*

Proof. By the *Goppa* bound on the dual code $C^\perp = C_L(D, \overline{m}P_\infty)$, we conclude that $d(C^\perp) \geq m - 2g + 2$. □

Remark 4.6. Let $C_L(D, mP_\infty) = [n, k, d(C)]$ be a Hermitian self-orthogonal AG code and $[[n, n-2k, d]]_q$ the corresponding quantum code. Suppose that $C_L(D, mP_\infty)$ is a strong code. By singleton bound for quantum codes [23], we have $n - 2k + 2d \leq n + 2$ which results in $d \leq k + 1 = m - g + 2$. On the other hand, by Corollary 4.5, $d \geq m - 2g + 2$. Subsequently, the difference between

the upper bound and the lower bound of d equals g and the use of low genus curves, gives quantum codes with good parameters.

EXAMPLE 4.7. Consider the maximal Hermitian curve $\mathcal{C}_H^{4,3}$ of genus 3 over $\mathbb{F}_9$. $C_L(D, mP_\infty)$ is Hermitian self-orthogonal if and only if $m \leq 7$. Using Magma calculator [18], we obtain new records over [6] with parameters: $[[27, 17, 3]]_3$, $[[27, 21, 3]]_3$, $[[27, 23, 2]]_3$ and $[[27, 25, 2]]_3$.

EXAMPLE 4.8. Using $\mathcal{C}_H^{6,5}$ of genus 10 over $\mathbb{F}_{25}$ and $\mathcal{C}_H^{8,7}$ of genus 21 over $\mathbb{F}_{49}$, we obtain new quantum codes over [6] with parameters: $[[125, 97, \geq 5]]_5$, $[[125, 101, \geq 3]]_5$, $[[125, 103, \geq 2]]_5$, $[[343, 289, \geq 7]]_7$, $[[343, 291, \geq 6]]_7$ and $[[343, 295, \geq 4]]_7$.

ACKNOWLEDGMENTS

We thank Carlos Munuera for his helpful comments and suggestions.

REFERENCES

1. A. Ashikhim, E. Knill, Non-binary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47**(7), (2001), 3065-3072.
2. D. Bartoli, L. Quoos, G. Zini, Algebraic Geometric Codes on Many Points from Kummer Extensions, *arXiv*, 1606.04143, (2016).
3. A.R. Calderbank, P.W. Shor, Good quantum error-correcting codes exist, *Physical Review A*, **54**(2), (1996), 1098-1105.
4. A.S. Castellanos, A.M. Masuda, L. Quoos, One- and Two-Point Codes Over Kummer Extensions, *IEEE Trans. Inf. Theory*, **62**(9), (2016), 4867-4872.
5. H. Chen, Some good quantum error-correcting codes from algebraic geometry codes, *IEEE Trans. Inf. Theory*, **47**(5), (2001), 2059-2061.
6. Y. Edel, Some good quantum twisted codes, `http://www.mathi.uni-heidelberg.de/~yves/Matrizen/QTBCH/QTBCHindex.html`.
7. C. Galindo, F. Hernando, Quantum codes from affine variety codes and their subfield subcodes, *Designs, Codes and Cryptography*, **76**(1), (2015), 89-100.
8. O. Geil, C. Munuera, D. Ruano, F. Torres, On the order bound for one-point codes, *Advances in Mathematics of Communication*, **5**(3), (2011), 489-504.
9. V.D. Goppa, Codes on algebraic curves, *Dokl. Akad. NAUK, SSSR*, **259**(6), (1981), 1289-1290.
10. V.D. Goppa, Algebraic geometric codes, *Izv. Akad. NAUK, SSSR*, **46**(4), (1982), 762-781.
11. D.Hankerson, A.Menezes, S.Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Professional Computing, Springer-Verlag, New York, 2004.
12. T. Hasegawa, Some remarks on superspecial and ordinary curves of low genus, *Math. Nachr*, **286**(1), (2013), 17-33.
13. C. Hu, S.Yang, Multi-point codes over Kummer extensions, *Designs, Codes and Cryptography*, **86**(1), (2018), 211-230.
14. L. Jin, Quantum stabilizer codes from maximal curves, *IEEE Trans. Inf. Theory*, **60**(1), (2014), 313-316.
15. L. Jin, C.P. Xing, Euclidean and Hermitian self-orthogonal Algebraic Geometry codes and their application to Quantum codes, *IEEE Trans. Inf. Theory*, **58**(8), (2012), 5484-5489.

16. A. Kazemifard, S. Tafazolian, A note on some Picard curves over finite fields, *Finite Fields and Their Applications*, **34**, (2015), 107-122.
17. J. Kim, J. Walker, Non-binary quantum error-correcting codes from algebraic curves, *Discrete Mathematics*, **308**(14), (2008), 3115-3124.
18. Magma Computational Algebra System, `http://magma.maths.usyd.edu.au/magma/`.
19. G.L. Matthews, Weierstrass semigroups and codes from a quotient of the Hermitian curve, *Designs, Codes and Cryptography*, **37**(3), (2005), 473-492.
20. MinT, Tables of optimal parameters for linear codes, Univ. Salzburg, Salzburg. Austria, (2009), `http://mint.sbg.ac.at/`.
21. C. Munuera, R. Pellikaan, Equality of geometric Goppa codes and equivalence of divisors, *J. Pure Appl. Algebra*, **90**(3), (1993), 229-252.
22. C. Munuera, W. Tenrio, F. Torres, Quantum error-correcting codes from algebraic geometry codes of Castle type, *Quantum Information Processing*, **16**(10), (2016), 4071-4088.
23. E.M. Rains, Non-binary quantum codes, *IEEE Trans. Inform. Theory*, **45**(6), (1999), 1827–1832.
24. P.K. Sarpevalli, A. Klappenecker, Non-binary quantum codes from Hermitian curves, *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Lecture Notes in Computer Science*, **3857**, Springer, Berlin, (2006), 136-143.
25. H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inf. Theory*, **34**(5), (1988), 1345-1348.
26. H. Stichtenoth, *Algebraic Function Fields and Codes*, Second edition, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 2009.
27. S. Tafazolian, F. Torres, On the curve $y^n = x^m + x$ over finite fields, *J. Number Theory*, **145**, (2014), 51-66.
28. Y. Takizawa, Some remarks on the Picard curves over a finite field, *Math. Nachr*, **280**(7), (2007), 802-811.