AG Codes on certain Maximal Curves

Stefania Fanali and Massimo Giulietti *†

February 22, 2013

Abstract

Algebraic Geometric codes associated to a recently discovered class of maximal curves are investigated. As a result, some linear codes with better parameters with respect to the previously known ones are discovered, and 70 improvements on MinT's tables [1] are obtained.

1 Introduction

Algebraic Geometric codes (AG codes) are linear error-correcting codes constructed from algebraic curves [2, 3]. Roughly speaking, the parameters of an AG code are good when the underlying curve has many rational points with respect to its genus. AG codes from specific curves with many points, such as the Hermitian curve and its quotients, the Suzuki curve, and the Klein quartic, have been the object of several works, see e.g. [4, 5, 6, 7, 8, 9, 10, 11, 12] and the references therein.

In this paper we provide an explicit construction of one-point AG codes from the GK curves, together with some results on the permutation automorphism groups of such codes. The GK curves are defined over any finite field of order q^2 with $q = \bar{q}^3$, and they are maximal curves in the sense that the number of their $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2gq$$

where g is the genus of the curve. Significantly, for $q > 8$, GK curves are the first known examples of maximal curves which are proven not to be $\mathbb{F}_{q^2}$-covered by the Hermitian curve, see [13].

Interestingly, some of the codes constructed in this paper have better parameters compared with the known linear error-correcting codes, see Section 5.

*S. Fanali and M. Giulietti are with the Dipartimento di Matematica e Informatica, Università di Perugia, Via Vanvitelli 1, 06123, Perugia, Italy (e-mail: stefania.fanali@dipmat.unipg.it; giuliet@dipmat.unipg.it)

†This research was performed within the activity of GNSAGA of the Italian INDAM.

More precisely, we obtain an improvement on the best known mininum distance for linear codes over the finite field with 64 elements in the following cases

length	codimension
$200-224$	20
$210-224$	22
$210-224$	23
$210-224$	28

(see Theorem 5.3).

The paper is organized as follows. In Section 2, some basic facts on AG codes and maximal curves are recalled. In Section 3, we introduce the GK curves, by summarizing some of the results in [13]. The Weierstrass semigroup at rational points of GK curves is investigated in Section 4. Finally, certain AG codes associated to the GK curves are constructed and their parameters are discussed for $\bar{q}=2,3$, see Section 5.

2 Preliminaries

2.1 Curves

Throughout the paper, by a curve we mean a projective, geometrically irreducible, non-singular algebraic curve defined over a finite field. Let q be a prime power, and let $\mathcal{X}$ be a curve defined over the finite field $\mathbb{F}_{q^2}$ of order q^2. Let g be the genus of $\mathcal{X}$. Henceforth, the following notation is used:

- $\mathcal{X}(\mathbb{F}_{q^2})$ (resp. $\mathbb{F}_{q^2}(\mathcal{X})$) denotes the set of $\mathbb{F}_{q^2}$-rational points (resp. the field of $\mathbb{F}_{q^2}$-rational functions) of $\mathcal{X}$.
- For $f \in \mathbb{F}_{q^2}(\mathcal{X})$, $div(f)$ (resp. $div_\infty(f)$) denotes the divisor (resp. the pole divisor) of f.
- Let P be a point of $\mathcal{X}$. Then v_P (resp. $H(P)$) stands for the valuation (resp. for the Weierstrass non-gap semigroup) associated to P. The ith non-gap at P is denoted as $m_i(P)$.
- Let D be a divisor on $\mathcal{X}$ and $P \in \mathcal{X}$. Then $deg(D)$ denotes the degree of D, $supp(D)$ the support of D, and $v_P(D)$ the coefficient of P in D. For D an $\mathbb{F}_{q^2}$-divisor, let

$$L(D) := \left\{f \in \mathbb{F}_{q^2}(\mathcal{X}) | div(f)+D \geq 0\right\},$$

$$l(D) := dim_{\mathbb{F}_{q^2}}(L(D)).$$

- The symbol "$\sim$" denotes linear equivalence of divisors.
- The symbol g_d^r stands for a linear series of projective dimension r and degree d.

2.2 One-point AG Codes and Improved AG Codes

Let $\mathcal{X}$ be a curve, let $P_1, P_2, \ldots, P_n$ be $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$, and let D be the divisor $P_1 + P_2 + \ldots + P_n$. Furthermore, let G be some other divisor that has support disjoint from D. The AG code $C(D, G)$ of length n over $\mathbb{F}_{q^2}$ is the image of the linear map $\alpha : L(G) \to \mathbb{F}_{q^2}^n$ defined by $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n))$. If n is bigger than $deg(G)$, then α is an embedding, and the dimension k of $C(D, G)$ is equal to $\ell(G)$. The Riemann-Roch theorem makes it possible to estimate the parameters of $C(D, G)$. In particular, if $2g-2 < deg(G) < n$, then $C(D, G)$ has dimension $k = deg(G) - g + 1$ and minimum distance $d \geq n - deg(G)$, see e.g. [14, Theorem 2.65]. A generator matrix M of $C(D, G)$ is

$$M = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ldots & \vdots \\ f_k(P_1) & \ldots & f_k(P_n) \end{pmatrix},$$

where $f_1, f_2, \ldots, f_k$ is an $\mathbb{F}_{q^2}$-basis of $L(G)$. The dual code $C^{\perp}(D, G)$ of $C(D, G)$ is an AG code with dimension $n-k$ and minimum distance greater than or equal to $deg(G) - 2g + 2$. When $G = \gamma P$ for an $\mathbb{F}_{q^2}$-rational P point of $\mathcal{X}$, and a positive integer γ, AG codes $C(D, G)$ and $C^{\perp}(D, G)$ are referred to as one-point AG codes. We recall some results on the minimum distance of one-point AG codes. By [15, Theorem 3], we can assume that γ is a non-gap at P. Let

$$H(P) = \{\rho_1 = 0 < \rho_2 < \ldots\},$$

and set $\rho_0 = 0$. Let f_ℓ be a rational function such that $div_\infty(f_\ell) = \rho_\ell P$, for any $\ell \geq 1$. Let $D = P_1 + P_2 + \ldots + P_n$. Let also

$$h_\ell = (f_\ell(P_1), f_\ell(P_2), \ldots, f_\ell(P_n)) \in \mathbb{F}_{q^2}^n. \tag{2.1}$$

Set

$$\nu_\ell := \# \left\{(i, j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\right\}$$

for any $\ell \geq 0$. Denote with $C_\ell(P)$ the dual of the AG code $C(D, G)$, where $D = P_1 + P_2 + \ldots + P_n$, and $G = \rho_\ell P$.

Lemma 2.1 *[14, Proposition 4.11] If $y \in C_\ell(P) \setminus C_{\ell+1}(P)$, then the weight of y is greater than or equal to ν_ℓ.*

The integer

$$d_{ORD}(C_\ell(P)) := min \{\nu_m : m \geq \ell\}$$

is called the order bound or the Feng-Rao designed minimum distance of $C_\ell(P)$.

Theorem 2.2 *[14, Theorem 4.13] The minimum distance $d(C_\ell(P))$ of $C_\ell(P)$ satisfies*

$$d(C_\ell(P)) \geq d_{ORD}(C_\ell(P)).$$

Theorem 2.3 *[14, Theorem 5.24] Let*

$$c := max\{m \in \mathbb{Z} | m-1 \notin H(P)\}.$$

Then $d_{ORD}(C_\ell(P)) \geq \ell+1-g$. *If* $\ell \geq 2c-g-1$, *then* $\nu_\ell = \ell+1-g$ *and hence equality* $d_{ORD}(C_\ell(P)) \geq \ell+1-g$ *holds.*

Let d be an integer greater than 1. The improved AG code $\tilde{C}_d(P)$ is the code

$$\tilde{C}_d(P) := \left\{x \in \mathbb{F}_{q^2}^n : \langle x, h_{i+1}\rangle = 0 \text{ for all } i \text{ such that } \nu_i < d\right\},$$

see [14, Def. 4.22].

Theorem 2.4 *[14, Proposition 4.23] Let*

$$r_d := \#\{i \geq 0 : \nu_i < d\}.$$

Then $\tilde{C}_d(P)$ *is an* $[n, k, d']$*-code, where* $k \geq n - r_d$, *and* $d' \geq d$.

2.3 Weierstras point theory [16]

Let $\mathcal{D}$ be a g_d^r base-point-free $\mathbb{F}_{q^2}$-linear series on a curve $\mathcal{X}$. For a point $P \in \mathcal{X}$, let

$$j_0(P) = 0 < j_1(P) < \ldots < j_r(P) \leq d$$

be the $(\mathcal{D}, P)$-orders, that is, the integers j such that there exists a divisor $D \in \mathcal{D}$ with $v_P(D) = j$. This sequence is the same for all but finitely many points. The finitely many points P where exceptional $(\mathcal{D}, P)$-orders occur, are called the $\mathcal{D}$-Weierstrass points of $\mathcal{X}$. Let $\epsilon_0 < \epsilon_1 < \ldots < \epsilon_r$ denote the sequence of the $(\mathcal{D}, Q)$-orders for a generic point $Q \in \mathcal{X}$. Then $\epsilon_i \leq j_i(P)$, for each $i = 0, 1, \ldots r$ and for any point P. The ramification divisor of $\mathcal{D}$ is a divisor R whose support consists exactly of the $\mathcal{D}$-Weierstrass points, and such that $deg(R) = (\epsilon_0 + \epsilon_1 + \ldots + \epsilon_r)(2g-2) + (r+1)d$.

2.4 Maximal Curves

A curve $\mathcal{X}$ is called $\mathbb{F}_{q^2}$-maximal if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is,

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq,$$

where g is the genus of $\mathcal{X}$.

A key tool for the investigation of maximal curves is Weiestrass Points theory. The Frobenius linear series of a maximal curve $\mathcal{X}$ is the complete linear series $\mathcal{D} = |(q+1)P_0|$, where P_0 is any $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$. The next result provides a relationship between $\mathcal{D}$-orders and non-gaps at points of $\mathcal{X}$.

Proposition 2.5 *[17, Proposition 1.5] Let* $\mathcal{X}$ *be a maximal curve over* $\mathbb{F}_{q^2}$, *and let* $\mathcal{D}$ *be the Frobenius linear series of* $\mathcal{X}$. *Then* *(i) For each point P on $\mathcal{X}$, we have $\ell(qP) = r$, i.e.,*

$$0 < m_1(P) < \ldots < m_{r-1}(P) \leq q < m_r(P).$$

(ii) If P is not rational over $\mathbb{F}_{q^2}$, the $\mathcal{D}$-orders at the point P are

$$0 \leq q - m_{r-1}(P) < \ldots < q - m_1(P) < q.$$

(iii) If P is rational over $\mathbb{F}_{q^2}$, the $(\mathcal{D}, P)$-orders are

$$0 < q + 1 - m_{r-1}(P) < \ldots < q + 1 - m_1(P) < q + 1.$$

In particular, if j is a $\mathcal{D}$-order at a rational point P, then $q + 1 - j$ is a non-gap at P.

(iv) If $P \in \mathcal{X}(\mathbb{F}_{q^2})$, then q and $q + 1$ are non-gaps at P.

Maximal curves are characterized by the so-called Natural Embedding Theorem.

Theorem 2.6 *[18, Theorem 10.22] Every $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus $g \geq 0$ is isomorphic over $\mathbb{F}_{q^2}$ to a curve of $\mathbb{P}^m(\bar{\mathbb{F}}_{q^2})$ of degree $q + 1$ lying on a non-degenerate Hermitian variety $\mathcal{H}_m$ defined over $\mathbb{F}_{q^2}$.*

The dimension m in Theorem 2.6 is less than or equal to the dimension r of the Frobenius linear series of $\mathcal{X}$. Also, by [18, Theorem 10.22], the osculating hyperplane of $\mathcal{X}$ at any point $P \in \mathcal{X}$ coincides with the tangent hyperplane at P to the non-degenerate Hermitian variety $\mathcal{H}_m$ in which $\mathcal{X}$ lies.

3 GK-Curves

Let $q = \bar{q}^3$, where $\bar{q} \geq 2$ is a prime power. The GK-curve over $\mathbb{F}_{q^2}$ is the curve of $\mathbb{P}^3(\bar{\mathbb{F}}_{q^2})$ with affine equations

$$\begin{cases} Z^{\bar{q}^2 - \bar{q} + 1} = Y h(X) \\ X^{\bar{q}} + X = Y^{\bar{q}+1} \end{cases}, \tag{3.1}$$

where $h(X) = \sum_{i=0}^{\bar{q}} (-1)^{i+1} X^{i(\bar{q}-1)}$. We first recall some important proprieties of this curve, for which we refer to [13, Section 2]. The curve $\mathcal{X}$ is absolutely irreducible, non-singular, and it lies on the Hermitian surface $\mathcal{H}_3$ with affine equation

$$X^{\bar{q}^3} + X = Y^{\bar{q}^3+1} + Z^{\bar{q}^3+1}.$$

Hence, by [18, Theorem 10.31], $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal. Significantly, for $q > 8$, $\mathcal{X}$ is the only known curve that is maximal but not $\mathbb{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}_2$ defined over $\mathbb{F}_{q^2}$ (see [13, Theorem 5]). The genus of $\mathcal{X}$ is

$$g = \frac{1}{2}(\bar{q}^3 + 1)(\bar{q}^2 - 2) + 1.$$

In order to investigate one-point AG codes associated to $\mathcal{X}$, we need to describe the Weierstrass semigroup $H(P)$ associated to an $\mathbb{F}_{q^2}$-rational point $P \in \mathcal{X}$. In the rest of this section we establish some general properties of $H(P)$.

Let Λ be the cyclic group consisting of all collineations

$$g_u : (T : X : Y : Z) \longmapsto (uT : uX : uY : Z),$$

with $u^{\bar{q}^2-\bar{q}+1} = 1$. Clearly Λ is a projective group preserving $\mathcal{X}$. It is easily seen that a plane model for the quotient curve $\mathcal{X}/\Lambda$ has equation $X^{\bar{q}} + X = Y^{\bar{q}+1}$. Consider the projection $\psi : \mathcal{X} \to \mathcal{X}/\Lambda$. Let $P = (X_P, Y_P, Z_P)$ be any affine $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$. Then, either ψ is fully ramified at P, or ψ splits completely at $\bar{P} = \psi(P)$, according to whether $\psi(P)$ is an $\mathbb{F}_{\bar{q}^2}$-rational point of $\mathcal{X}/\Lambda$ or not, that is, whether $Z_P = 0$ or not.

In the former case, let $aX + bY + c = 0$ be an equation of any line through $\psi(P)$, distinct from the tangent of $\mathcal{X}/\Lambda$ at $\psi(P)$. Then

$$v_P(ax + by + c) = (\bar{q}^2 - \bar{q} + 1)v_{\psi(P)}(ax + by + c) = \bar{q}^2 - \bar{q} + 1$$

holds. Hence, by [18, Prop. 10.6 (IV)], $\bar{q}^3 + 1 - (\bar{q}^2 - \bar{q} + 1) = \bar{q}^3 - \bar{q}^2 + \bar{q} \in H(P)$.

By [13, Proposition 1], together with [13, Theorem 7], $\bar{q}^3 - \bar{q}^2 + \bar{q}, \bar{q}^3, \bar{q}^3 + 1$ are actually a set of generators for $H(P)$. The same holds when P is the only infinite point of $\mathcal{X}$.

Proposition 3.1 *If either P is the only infinite point of $\mathcal{X}$ or $P = (X_P, Y_P, 0) \in \mathcal{X}(\mathbb{F}_{q^2})$, then the Weierstrass semigroup at P is the subgroup generated by $\bar{q}^3 - \bar{q}^2 + \bar{q}$, $\bar{q}^3$, and $\bar{q}^3 + 1$.*

Assume now that $\psi(P)$ is a non-$\mathbb{F}_{\bar{q}^2}$-rational point of $\mathcal{X}/\Lambda$. Let $aX+bY+c = 0$ be an equation of the tangent line of $\mathcal{X}/\Lambda$ at $\psi(P)$. The order of contact of the tangent line to $\mathcal{X}/\Lambda$ at a non-$\mathbb{F}_{\bar{q}^2}$-rational point is equal to $\bar{q}$ (see e.g. [18, p. 302]). Then

$$v_P(ax + by + c) = v_{\psi(P)}(ax + by + c) = \bar{q}$$

holds. Again by [18, Prop. 10.6 (IV)], $\bar{q}^3 - \bar{q} + 1 \in H(P)$. Then the following result is obtained.

Proposition 3.2 *If $P = (X_P, Y_P, Z_P) \in \mathcal{X}(\mathbb{F}_{q^2})$ is such that $Z_P \neq 0$, then the Weierstrass semigroup at P contains the subgroup generated by $\bar{q}^3 - \bar{q} + 1$, $\bar{q}^3$, and $\bar{q}^3 + 1$.*

Providing a general description of $H(P)$ for affine points P of $\mathcal{X}$ with $Z_P \neq 0$ seems to be quite a difficult task. In the next section, this will be done for the cases $\bar{q} = 2, 3$.

We end this section by describing the automorphism group $Aut(\mathcal{X})$ of $\mathcal{X}$, together with its action on the set of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$.

Theorem 3.3 *[13, Theorem 6] The automorphism group of $\mathcal{X}$ has order $\bar{q}^3(\bar{q}^3+1)(\bar{q}^2-1)(\bar{q}^2-\bar{q}+1)$, and has a normal subgroup isomorphic to $SU(3,\bar{q})$. If $\gcd(3,\bar{q}+1)=1$ then $Aut(\mathcal{X})$ is isomorphic to the direct product of $SU(3,\bar{q})$ and a cyclic group of order $\bar{q}^2-\bar{q}+1$. If $\gcd(3,\bar{q}+1)=3$ then $Aut(\mathcal{X})$ has a normal subgroup of index 3 which is isomorphic to the direct product of $SU(3,\bar{q})$ and a cyclic group of order $(\bar{q}^2-\bar{q}+1)/3$.*

Theorem 3.4 *[13, Theorem 7] The set of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ splits into two orbits under the action of $Aut(\mathcal{X})$. One orbit, say $\mathcal{O}_1$, has size $\bar{q}^3+1$ and consists of the points $(X_P,Y_P,0)\in\mathcal{X}(\mathbb{F}_{q^2})$, together with the infinite point $X_\infty=(0:1:0:0)$. The other orbit, say $\mathcal{O}_2$, has size $\bar{q}^3(\bar{q}^3+1)(\bar{q}^2-1)$ and consists of the points $(X_P,Y_P,Z_P)\in\mathcal{X}(\mathbb{F}_{q^2})$ with $Z_P\neq 0$. Furthermore, $Aut(\mathcal{X})$ acts on $\mathcal{O}_1$ as $PGU(3,\bar{q})$ in its doubly transitive permutation representation.*

Corollary 3.5 *For a point $P\in\mathcal{O}_1$, the stabilizer of P under the action of $Aut(\mathcal{X})$ has size $\bar{q}^3(\bar{q}^2-1)(\bar{q}^2-\bar{q}+1)$, and it acts transitively on the points of $\mathcal{O}_1\setminus\{P\}$. For a point $P\in\mathcal{O}_2$, the stabilizer of P under the action of $Aut(\mathcal{X})$ has size $(\bar{q}^2-\bar{q}+1)$.*

4 The Weierstrass semigroup at an $\mathbb{F}_{q^2}$-rational point of the GK curves

In this section we describe the Weierstrass semigroup $H(P)$ at any $\mathbb{F}_{q^2}$-rational point P of the GK curves for the cases $\bar{q}=2,3$. Also, for each non-gap m we provide a rational function f such that $div_\infty(f)=mP$.

First, consider the point at infinity $X_\infty=(0:1:0:0)$ of $\mathcal{X}$. By Proposition 3.1, $H(X_\infty)=\langle \bar{q}^3-\bar{q}^2+\bar{q},\bar{q}^3,\bar{q}^3+1\rangle$. Taking into account that the osculating plane of $\mathcal{X}$ at X_∞ is the plane with equation $T=0$, and that $X_\infty\in\mathcal{X}(\mathbb{F}_{q^2})$,

$$div_\infty(x)=(\bar{q}^3+1)X_\infty \tag{4.1}$$

holds. Moreover, by the equations of $\mathcal{X}$ it follows that

$$div_\infty(y)=(\bar{q}^3-\bar{q}^2+\bar{q})X_\infty,\quad div_\infty(z)=\bar{q}^3X_\infty. \tag{4.2}$$

It should be noted that taking into account [13, Theorem 7] one can easily construct rational functions corresponding to the non-gaps $\bar{q}^3-\bar{q}^2+\bar{q},\bar{q}^3,\bar{q}^3+1$ at any point $P=(a,b,0)\in\mathcal{X}(\mathbb{F}_{q^2})$.

Now fix $P=(a,b,c)\in\mathcal{X}(\mathbb{F}_{q^2})$, with $c\neq 0$, and consider the planes $\pi_1: T=0$, $\pi_2: Y-bT=0$, $\pi_3: -a^{\bar{q}}T-X+b^{\bar{q}}Y=0$, and $\pi_4: -a^{\bar{q}^3}T-X+b^{\bar{q}^3}Y+c^{\bar{q}^3}Z=0$. It is straightforward to check that these planes meet $\mathcal{X}$ at P with multiplicity 0, 1, $\bar{q}$, and $\bar{q}^3+1$ respectively. By Proposition 2.5, $\pi_1,\ldots,\pi_4$ correspond to the rational functions associated to the following non-gaps at P: $\bar{q}^3+1$, $\bar{q}^3$, $\bar{q}^3-\bar{q}+1$, and 0. Let ϕ be the linear transformation

$$\phi(T:X:Y:Z)=$$

$$(-a^{\bar{q}^3}T - X + b^{\bar{q}^3}Y + c^{\bar{q}^3}Z : T : -bT + Y : -a^{\bar{q}}T - X + b^{\bar{q}}Y).$$

Note that the planes $\phi(\pi_1), \dots, \phi(\pi_4)$ are the planes $X = 0$, $Y = 0$, $Z = 0$, and $T = 0$. Also, $\phi(P) = X_\infty$. The equations of $\phi(\mathcal{X})$ are

$$\left(\frac{T}{c^{\bar{q}^3}} + cX + \left(\frac{b^{\bar{q}} - b^{\bar{q}^3}}{c^{\bar{q}^3}}\right)Y - \frac{Z}{c^{\bar{q}^3}}\right)^{\bar{q}^2-\bar{q}+1} =$$

$$(bX + Y)\, h(aX + b^{\bar{q}}Y - Z)$$

and

$$X\left(aX + b^{\bar{q}}Y - Z\right)^{\bar{q}} + X^{\bar{q}}\left(aX + b^{\bar{q}}Y - Z\right) = (bX + Y)^{\bar{q}+1}.$$

The rational functions x, y, z correspond to the first non-gaps at X_∞, namely

$$v_{X_\infty}(x) = -(\bar{q}^3 + 1), v_{X_\infty}(y) = -\bar{q}^3, v_{X_\infty}(z) = -(\bar{q}^3 - \bar{q} + 1). \tag{4.3}$$

We now look for non-gaps at X_∞ which are not in the subgroup generated by $\bar{q}^3 - \bar{q} + 1$, $\bar{q}^3$, and $\bar{q}^3 + 1$.

Let $f_0(X, Y, Z), f_1(X, Y, Z), \dots, f_v(X, Y, Z)$ be distinct monomials of the same degree m, and such that X is not a common factor of $f_0, f_1, \dots, f_v$. Consider the set of rational functions

$$\mathcal{L} = \left\{\sum_{i=0}^{v} l_i f_i(x, y, z) : (l_0 : l_1 : \dots : l_v) \in \mathbb{P}^v(\mathbb{F}_{q^2})\right\}. \tag{4.4}$$

Note that the second equation of $\phi(\mathcal{X})$ and $\sum_{i=0}^{v} l_i f_i(X, Y, Z) = 0$ are the equations of two cones with the same vertex $O = (1 : 0 : 0 : 0)$. Hence, the zeros of any $\alpha \in \mathcal{L}$ lie in the common lines of the two cones. Let π be the plane with equation $X = T$. Denote by $\mathcal{C}_1$ and $\mathcal{C}_2$ the plane curves obtained as the intersection of π with the two cones. Clearly, the common lines of the two cones are the lines joining O to the intersection points of $\mathcal{C}_1$ and $\mathcal{C}_2$. Assume that $\alpha = \sum_{i=0}^{v} l_i f_i(x, y, z)$. Then, in the YZ-plane the equations of $\mathcal{C}_1$ and $\mathcal{C}_2$ are

$$\mathcal{C}_1 : \left(a + b^{\bar{q}}Y - Z\right)^{\bar{q}} + (a + b^{\bar{q}}Y - Z) = (b + Y)^{\bar{q}+1} \tag{4.5}$$

and

$$\mathcal{C}_2 : \sum_{i=0}^{v} l_i f_i(1, Y, Z) = 0. \tag{4.6}$$

Since these curves have order $\bar{q} + 1$ and m, they have $m(\bar{q} + 1)$ common points (not necessary distinct). Hence, the common lines of the cones are $m(\bar{q} + 1)$. Note that the number of affine common points of $\mathcal{X}$ and one of these lines ℓ is either $\bar{q}^2 - \bar{q}$ or $\bar{q}^2 - \bar{q} + 1$ according to whether ℓ passes through $(1 : 1 : 0 : 0)$ or not. Let N be the number of affine zeros of the function α. Then,

$$N = (\bar{q}^2 - \bar{q} + 1)(m(\bar{q} + 1) - M) + (\bar{q}^2 - \bar{q})M,$$

where M is the intersection multiplicity of $\mathcal{C}_1$ and $\mathcal{C}_2$ at the origin of the YZ-plane.

Consider now the morphism

$$\eta : \mathcal{C}_1 \to \mathbb{P}^v(\bar{\mathbb{F}}_{q^2}), \quad \eta = (g_0 : g_1 : \ldots : g_v),$$

where $g_i = f_i(1, y, z)$. Note that if $g_0, g_1, \ldots, g_v$ are $\bar{\mathbb{F}}_{q^2}$-linearly indipendent in the function field of $\mathcal{C}_1$, then the morphism η is non-degenerate. Let

$$\mathcal{D}_\eta = \left\{ E + div(\sum_{i=0}^{v} l_i g_i) : (l_0 : l_1 : \ldots : l_v) \in \mathbb{P}^v(\mathbb{K}) \right\}$$

be the linear series associated to η, where E is the divisor of $\mathcal{C}_1$ such that

$$v_Q(E) = -min \left\{ v_Q(g_0), v_Q(g_1), \ldots, v_Q(g_v) \right\},$$

for any $Q \in \mathcal{C}_1$. Therefore, we have $v+1$ distinct values for M, namely the integers $v_P(E) + j_i(P)$, $i = 0, 1, \ldots, v$, where $(j_0(P), j_1(P), \ldots, j_v(P))$ is the order sequence at P of the morphism η.

Then the following result is obtained.

Theorem 4.1 *Let $P = (a, b, c)$ be an $\mathbb{F}_{q^2}$-rational point of the GK-curve $\mathcal{X}$, with $c \neq 0$. Let $\mathcal{C}_1$ be the plane curve with equation (4.5), and let $g_0, g_1, \ldots, g_v$ be monomial functions in y, z, which are $\bar{\mathbb{F}}_{q^2}$-linearly indipendent in the function field of $\mathcal{C}_1$. Let m be the maximum degree of $g_0, g_1, \ldots, g_v$, and let $v_O(E) = -min \{v_O(g_0), v_O(g_1), \ldots, v_O(g_v)\}$, where O is the origin of the YZ-plane. Then there exist $v+1$ non-gaps at P, say $N_0, N_1, \ldots, N_v$, such that $m(\bar{q}^3 - \bar{q}) \leq N_i \leq m(\bar{q}^3 + 1) + v_O(E)$. More precisely $N_i = m(\bar{q}^3 + 1) - M_i$, where $M_0, M_1, \ldots, M_v$ are the intersection multiplicities at O of $\mathcal{C}_1$ and the plane curves with equation $\sum_{i=0}^{v} l_i g_i(Y, Z) = 0$.*

Thanks to Theorem 4.1, we are in a position to obtain a description of the Weierstrass semigroup at an $\mathbb{F}_{q^2}$-rational point of the GK-curve $\mathcal{X}$ for $\bar{q} = 2$ and $\bar{q} = 3$.

4.1 $\bar{q} = 2$

In this case, $\mathcal{X}$ has affine equations

$$\begin{cases} Z^3 = Y\left(1 + X + X^2\right) \\ X^2 + X = Y^3 \end{cases},$$

and $g = 10$ is the genus of $\mathcal{X}$. Let $P = (a, b, c)$ be an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$ such that $c \neq 0$. Then, the Weierstrass semigroup at P coincides with the Weierstrass semigroup at X_∞ of the curve $\phi(\mathcal{X})$ with equations

$$\left(\frac{T}{c^8} + cX + \left(\frac{b^2 - b^8}{c^8} \right) Y - \frac{Z}{c^8} \right)^3 =$$

$$(bX+Y)\,h(aX+b^2Y-Z)$$

and

$$X\left(aX+b^2Y-Z\right)^2+X^2\left(aX+b^2Y-Z\right)=(bX+Y)^3\,.$$

By (4.3),

$$div_\infty(x)=9X_\infty,\quad div_\infty(y)=8X_\infty,\quad div_\infty(z)=7X_\infty,$$

that is, 7, 8, and 9 are non-gaps at P. Let Υ be the semigroup generated by 7, 8, and 9. Since $\#(\Upsilon\cap[0,2g-1])=9<10=g$, $H(P)$ is larger than Υ. Hence, there is precisely one non-gap not bigger than $2g-1=19$ that does not belong to Υ.

Let

$$f_0=XZ,\quad f_1=Z^2,\quad f_2=Y^2,\quad f_3=YZ,$$

and let $\eta:\mathcal{C}_1\to\mathbb{P}^3(\bar{\mathbb{F}}_{q^2})$, $\eta=(z:z^2:y^2:yz)$; here, $\mathcal{C}_1$ is the plane curve with equation $\mathcal{C}_1: Z+Z^2+c^3Y^2+Y^3=0$. Since z,z^2,y^2,yz are $\bar{\mathbb{F}}_{q^2}$-linearly indipendent in the function field of $\mathcal{C}_1$, the morphism η is non-degenerate. Consider now the linear series associated to η:

$$\mathcal{D}_\eta=\left\{E+div(\sum_{i=0}^{i=3}l_ig_i)|(l_0:l_1:l_2:l_3)\in\mathbb{P}^3(\bar{\mathbb{F}}_{q^2})\right\},$$

where $g_i(y,z)=f_i(1,y,z)$, and E is a divisor of $\mathcal{C}_1$ such that

$$v_Q(E)=-min\left\{v_Q(z),v_Q(z^2),v_Q(y^2),v_Q(yz)\right\},$$

for any $Q\in\mathcal{C}_1$. Note that the line with equation $Z=0$ is the tangent line to $\mathcal{C}_1$ at the origin O of the YZ-plane, and its intersection multiplicity with $\mathcal{C}_1$ is 2. Hence, $v_O(E)=-2$ holds. Therefore, from Theorem 4.1 there exist four non-gaps in $I=[12,16]$. Taking into account that $14,15,16$ are precisely the integers in $I\cap\langle 7,8,9\rangle$, then the non-gap N is either 12 or 13. According to Theorem 4.1, we implemented a standard intersection multiplicity algorithm in order to compute the intersection multiplicities at O of $\mathcal{C}_1$ and the plane curves with equation $\sum_{i=0}^3 l_ig_i(Y,Z)=0$. It turned out that $N=13$, and that a rational function β such that $div_\infty(\beta)=13X_\infty$ was

$$\beta=xz+\left(\frac{1}{c^9}+1\right)z^2+c^3y^2+\frac{1}{c^3}yz.$$

It is easly seen that any integer greater than 20 belongs to the numerical semigroup Δ generated by $7,8,9,13$. Hence, the genus of Δ equals g, and the following result is obtained.

Theorem 4.2 *Let $P=(a,b,c)$ be an $\mathbb{F}_{8^2}$-rational point of the GK-curve $\mathcal{X}$, such that $c\neq 0$. Then the Weierstrass semigroup of $\mathcal{X}$ at P is generated by* $7,8,9$*, and* 13. *Moreover,*

$$div_\infty(\bar{x})=9P,\qquad div_\infty(\bar{y})=8P,\qquad div_\infty(\bar{z})=7P,$$
$$div_\infty\left(\bar{z}\bar{x}+\left(\frac{1}{c^9}+1\right)\bar{z}^2+c^3\bar{y}^2+\frac{1}{c^3}\bar{y}\bar{z}\right)=13P$$

where $\bar{x} = \frac{1}{-a^8-x+b^8y+c^8z}$, $\bar{y} = \frac{-b+y}{-a^8-x+b^8y+c^8z}$, *and* $\bar{z} = \frac{-a^2-x+b^2y}{-a^8-x+b^8y+c^8z}$.

4.2 $\bar{q} = 3$

Let $\bar{q} = 3$. In this case, $\mathcal{X}$ has affine equations

$$\begin{cases} Z^7 = Y\left(2 + X^2 + 2X^4 + X^6\right) \\ X^3 + X = Y^4 \end{cases},$$

and $g = 99$. Let $P = (a, b, c)$ be an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$ such that $c \neq 0$. Then, the Weierstrass semigroup at P coincides with the Weierstrass semigroup at X_∞ of the curve $\phi(\mathcal{X})$ with equations

$$\left(\frac{T}{c^{27}} + cX + \left(\frac{b^3 - b^{27}}{c^{27}}\right)Y - \frac{Z}{c^{27}}\right)^7 =$$

$$(bX + Y)\, h(aX + b^3Y - Z)$$

and

$$X\left(aX + b^3Y - Z\right)^3 + X^3\left(aX + b^3Y - Z\right) = (bX + Y)^4 .$$

By (4.3),

$$div_\infty(x) = 28X_\infty, \quad div_\infty(y) = 27X_\infty, \quad div_\infty(z) = 25X_\infty,$$

that is 25, 27, and 28 are non-gaps at P. Let Υ be the semigroup generated by 25, 27, and 28. Since $\#(\Upsilon \cap [0, 2g-1]) = 85 < 99 = g$, $H(P)$ is larger than Υ.

As for the case $\bar{q} = 2$, we use Theorem 4.1 to find the non-gaps at P that do not belong to Υ. Let

$$f_0 = X^2Z, \quad f_1 = XZ^2, \quad f_2 = XYZ,$$

$$f_3 = Y^2Z, \quad f_4 = Z^3, \quad f_5 = YZ^2, \quad f_6 = Y^3;$$

here, $\mathcal{C}_1 : 2Z + 2Z^3 + c^7Y^3 + 2Y^4 = 0$. Since $z, z^2, yz, y^2z, z^3, yz^2, y^3$ are $\bar{\mathbb{F}}_{q^2}$-linearly indipendent in the function field of $\mathcal{C}_1$, the morphism $\eta = (z : z^2 : yz : y^2z : z^3 : yz^2 : y^3) : \mathcal{C}_1 \to \mathbb{P}^6(\bar{\mathbb{F}}_{q^2})$ is non-degenerate. Consider now the linear series associated to η:

$$\mathcal{D}_\eta = \left\{ E + div(\sum_{i=0}^{i=6} l_i g_i) | (l_0 : l_1 : \ldots : l_6) \in \mathbb{P}^6(\bar{\mathbb{F}}_{q^2}) \right\},$$

where $g_i(y, z) = f_i(1, y, z)$, and E is a divisor of $\mathcal{C}_1$ such that

$$v_Q(E) = -min \left\{v_Q(g_0), v_Q(g_1), \ldots, v_Q(g_6)\right\},$$

for any $Q \in \mathcal{C}_1$. Note that the line with equation $Z = 0$ is the tangent line to $\mathcal{C}_1$ at the origin O of the YZ-plane, and its intersection multiplicity with $\mathcal{C}_1$

is 3. Hence, $v_O(E) = -3$ holds. Therefore, by Theorem 4.1 there exist seven non-gaps in $I = [72, 81]$.

As for the case $\bar{q} = 2$, we implemented a standard intersection multiplicity algorithm in order to compute the intersection multiplicities at O of $\mathcal{C}_1$ and the plane curves with equation $\sum_{i=0}^{6} l_i g_i(Y, Z) = 0$. We obtained that 74 was a non-gap at X_∞ not belonging to Υ, and that a rational function β such that $div_\infty(\beta) = 74X_\infty$ was

$$\beta = x^2z + \frac{1}{c^{28}}xz^2 + \frac{1}{c^7}xzy + \frac{1}{c^{14}}zy^2 +$$
$$\left(1 + \frac{1}{c^{56}}\right)z^3 + \frac{2}{c^{35}}z^2y + 2c^7y^3.$$

By straightforward computation, the number of integers less than $2g = 198$ that belong to the subgroup generated by $25, 27, 28$, and 74 is $96 < g$. Therefore, some other non-gap is missing and we need to apply Theorem 4.1 to another set of monomial functions. Note that the following rational functions of $\mathcal{C}_1$ are $\bar{\mathbb{F}}_{q^2}$-linearly indipendent

$$y^3,\ z,\ yz,\ y^2z,\ z^2,\ y^3z,\ yz^2,$$
$$y^2z^2,\ z^3,\ y^3z^2,\ yz^3,\ y^2z^3,\ z^4,\ yz^4,\ z^5.$$

Consider the morphism associated to these rational functions. Arguing as before, we applied a standard intersection algorithm to find a non-gap not belonging to the semigroup generated by $25, 27, 28$, and 74. A non-gap with this property turned out to be 121. By straightforward computation it is easily seen that the genus of the numerical semigroup Δ generated by $25, 27, 28, 74$, and 121 is 99. Therefore, Δ coincides with the Weierstrass semigroup of $\varphi(\mathcal{X})$ at X_∞.

An explicit description of a rational function γ such that $div_\infty(\gamma) = 121X_\infty$ for a generic choice (a, b, c) seems to be difficult to achieve. The intersection multiplicity algorithm provided such a function for a specific choice of $(a, b, c) \in \mathcal{O}_2$ (note that this is not a restriction, since by Theorem 3.4 the automorphism group $Aut(\mathcal{X})$ acts transitively on $\mathcal{O}_2$). Let ω be an element of $\mathbb{F}_{27^2}$ such that $\omega^6 - \omega^4 + \omega^2 - \omega - 1 = 0$. Then $(\omega^{11}, \omega^{280}, \omega^{88})$ is a point in $\mathcal{O}_2$, and

$$\begin{aligned}\gamma = \omega^{588}x^2y^3 + \omega^{336}x^4z + \omega^{448}x^3yz + \omega^{560}x^2y^2z +\\ \omega^{700}x^3z^2 + \omega^{112}xy^3z + \omega^{112}x^2yz^2 + \omega^{84}xy^2z^2 +\\ \omega^{196}x^2z^3 + 2y^3z^2 + \omega^{392}xyz^3 + \omega^{28}y^2z^3 +\\ \omega^{504}xz^4 + \omega^{644}yz^4 + \omega^{280}z^5\end{aligned}$$

is such that $div_\infty(\gamma) = 121X_\infty$.

Therefore, the following result is obtained.

Theorem 4.3 *Let ω be an element of $\mathbb{F}_{27^2}$ such that*

$$\omega^6 - \omega^4 + \omega^2 - \omega - 1 = 0.$$

Let $P=(a,b,c)$ be an $\mathbb{F}_{27^2}$-rational point of the GK-curve $\mathcal{X}$, such that $c \neq 0$. Then, the Weierstrass semigroup of $\mathcal{X}$ at P is generated by $25, 27, 28, 74$, and 121. Moreover,

$$div_\infty(\bar{x}) = 28P, \quad div_\infty(\bar{y}) = 27P,$$

$$div_\infty(\bar{z}) = 25P, \quad div_\infty\left(\bar{\beta}\right) = 74P$$

where $\bar{x} = \frac{1}{-a^{27}-x+b^{27}y+c^{27}z}$, $\bar{y} = \frac{-b+y}{-a^{27}-x+b^{27}y+c^{27}z}$, $\bar{z} = \frac{-a^3-x+b^3y}{-a^{27}-x+b^{27}y+c^{27}z}$, *and*

$$\bar{\beta} = \bar{z}\bar{x}^2 + \frac{1}{c^{28}}\bar{x}\bar{z}^2 + \frac{1}{c^7}\bar{x}\bar{y}\bar{z} + \frac{1}{c^{14}}\bar{z}\bar{y}^2 +$$

$$\left(1+\frac{1}{c^{56}}\right)\bar{z}^3 + \frac{2}{c^{35}}\bar{z}^2\bar{y} + 2c^7\bar{y}^3.$$

When $a=\omega^{11}$, $b=\omega^{280}$, $c=\omega^{88}$ then

$$div_\infty(\bar{\gamma}) = 121P$$

where

$$\begin{aligned}\bar{\gamma} = \omega^{588}\bar{x}^2\bar{y}^3 + \omega^{336}\bar{x}^4\bar{z} + \omega^{448}\bar{x}^3\bar{y}\bar{z} + \omega^{560}\bar{x}^2\bar{y}^2\bar{z} +\\ \omega^{700}\bar{x}^3\bar{z}^2 + \omega^{112}\bar{x}\bar{y}^3\bar{z} + \omega^{112}\bar{x}^2\bar{y}\bar{z}^2 + \omega^{84}\bar{x}\bar{y}^2\bar{z}^2 +\\ \omega^{196}\bar{x}^2\bar{z}^3 + 2\bar{y}^3\bar{z}^2 + \omega^{392}\bar{x}\bar{y}\bar{z}^3 + \omega^{28}\bar{y}^2\bar{z}^3 +\\ \omega^{504}\bar{x}\bar{z}^4 + \omega^{644}\bar{y}\bar{z}^4 + \omega^{280}\bar{z}^5.\end{aligned}$$

5 AG Codes and Improved AG Codes associated to the GK-curve

Throughout this section we keep the notation of the previous Sections. For $q=\bar{q}^3$, let $\mathcal{X}$ be the GK curve defined by (3.1). Let P be an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$, and let D be the divisor consisting of the sum of all the remaining $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$. Let $C_\ell(P)$ be the dual of the AG code $C(D, \rho_\ell P)$, with $\rho_\ell \in H(P)$. Let $\tilde{C}_d(P)$ be the improved AG code, as defined in Section 2.

The aim of this section is to determine the parameters of both codes $C_\ell(P)$ and $\tilde{C}_d(P)$, and to compare such parameters with those of the known codes. We apply Theorems 2.2 and 2.4. Note that the bounds appearing in the statements of Theorems 2.2 and 2.4 depend only on Weierstrass semigroup $H(P)$. As $H(P)$ is invariant under the action of $Aut(\mathcal{X})$, we only consider one point per orbit under the action of $Aut(\mathcal{X})$. Henceforth, we assume that P_i is a point of $\mathcal{O}_i$, for $i=1,2$.

Note that by Proposition 3.1, Equations (4.1) and (4.2), and Theorems 4.2 and 4.3, for each P_i and for every $m \in H(P_i)$ we can construct a rational function f such that $div_\infty f = mP_i$. Therefore, it is possible to construct a parity check matrix for all codes $C_\ell(P_i)$ and $\tilde{C}_d(P_i)$

Remark 5.1 *It is well-known, see e.g. [19], that the permutation automorphism group of a code $C_\ell(P)$ contains a subgroup isomorphic to the stabilizer of P in $Aut(\mathcal{X})$, provided that the length of the code is larger than $2g+2$. Then by Corollary 3.5 the code $C_\ell(P_1)$ has an automorphism group of size $\bar{q}^3(\bar{q}^2-1)(\bar{q}^2-\bar{q}+1)$, whereas $C_\ell(P_2)$ has a cyclic automorphism group of size $\bar{q}^2-\bar{q}+1$.*

5.1 $\bar{q}=2$

Tables 2-5 describe the parameters of the codes $C_\ell(P_1)$, $C_\ell(P_2)$, $\tilde{C}_d(P_1)$, $\tilde{C}_d(P_2)$; the entries can be easily deduced from Proposition 3.1 and Theorem 4.2. In some cases the entries in MinT's tables [1] are improved.

Other improvements can be obtained by using the following propagation rules.

Proposition 5.2 (see Exercise 7 in [20])

- *If there is a q-ary linear code of lenght n, dimension k and minimum distance d, then for each non-negative integer $s<d$ there exists a q-ary linear code of length n, dimension k and minimum distance $d-s$.*
- *If there is a q-ary linear code of lenght n, dimension k and minimum distance d, then for each non-negative integer $s<k$ there exists a q-ary linear code of length n, dimension $k-s$ and minimum distance d.*
- *If there is a q-ary linear code of lenght n, dimension k and minimum distance d, then for each non-negative integer $s<k$ there exists a q-ary linear code of length $n-s$, dimension $k-s$ and minimum distance d.*
- *If there is a q-ary linear code of lenght n, dimension k and minimum distance d, then for each non-negative integer $s<\min\{n-k-1,d\}$ there exists a q-ary linear code of length $n-s$, dimension k and minimum distance $d-s$.*

Therefore, the following result is obtained.

Theorem 5.3 *Linear codes over $\mathbb{F}_{64}$ with parameters as in Table 1 exist.*

5.2 $\bar{q}=3$

Table 6 describes some of the codes $\tilde{C}_d(P_i)$, $d\le 2g$, $i=1,2$, over the field $\mathbb{F}_{3^6}$. The parameters of these codes can be easily obtained taking into account Proposition 3.1 and Theorem 4.3, together with Proposition 5.2.

References

[1] MinT. (2009, January). Tables of optimal parameters for linear codes, University of Salzburg. Available: http://mint.sbg.ac.at/.

Table 1: Improvements on [1] - $q = 64$

n	k	d	Ref.	n	k	d	Ref.	n	k	d	Ref.
224	204	13	$C_{19}(P_2)$, $\tilde{C}_{13}(P_2)$	223	203	13	Prop. 5.2	222	202	13	Prop. 5.2
221	201	13	Prop. 5.2	220	200	13	Prop. 5.2	219	199	13	Prop. 5.2
218	198	13	Prop. 5.2	217	197	13	Prop. 5.2	216	196	13	Prop. 5.2
215	195	13	Prop. 5.2	214	194	13	Prop. 5.2	213	193	13	Prop. 5.2
212	192	13	Prop. 5.2	211	191	13	Prop. 5.2	210	190	13	Prop. 5.2
209	189	13	Prop. 5.2	208	188	13	Prop. 5.2	207	187	13	Prop. 5.2
206	186	13	Prop. 5.2	205	185	13	Prop. 5.2	204	184	13	Prop. 5.2
203	183	13	Prop. 5.2	202	182	13	Prop. 5.2	201	181	13	Prop. 5.2
200	180	13	Prop. 5.2	224	202	14	$C_{21}(P_1)$, $\tilde{C}_{14}(P_i)$	223	201	14	Prop. 5.2
222	200	14	Prop. 5.2	221	199	14	Prop. 5.2	220	198	14	Prop. 5.2
219	197	14	Prop. 5.2	218	196	14	Prop. 5.2	217	195	14	Prop. 5.2
216	194	14	Prop. 5.2	215	193	14	Prop. 5.2	214	192	14	Prop. 5.2
213	191	14	Prop. 5.2	212	190	14	Prop. 5.2	211	189	14	Prop. 5.2
210	188	14	Prop. 5.2	224	201	15	$\tilde{C}_{15}(P_1)$	223	200	15	Prop. 5.2
222	199	15	Prop. 5.2	221	198	15	Prop. 5.2	220	197	15	Prop. 5.2
219	196	15	Prop. 5.2	218	195	15	Prop. 5.2	217	194	15	Prop. 5.2
216	193	15	Prop. 5.2	215	192	15	Prop. 5.2	214	191	15	Prop. 5.2
213	190	15	Prop. 5.2	212	189	15	Prop. 5.2	211	188	15	Prop. 5.2
210	187	15	Prop. 5.2	224	196	20	$C_{27}(P_i)$, $\tilde{C}_{20}(P_i)$	223	195	20	Prop. 5.2
222	194	20	Prop. 5.2	221	193	20	Prop. 5.2	220	192	20	Prop. 5.2
219	191	20	Prop. 5.2	218	190	20	Prop. 5.2	217	189	20	Prop. 5.2
216	188	20	Prop. 5.2	215	187	20	Prop. 5.2	214	186	20	Prop. 5.2
213	185	20	Prop. 5.2	212	184	20	Prop. 5.2	211	183	20	Prop. 5.2
210	182	20	Prop. 5.2								

Table 2: Codes $C_\ell(P_1)$ - $q = 64$

n	k	ρ_ℓ	ν_ℓ	d_{ORD}
224	223	0	2	2
224	222	6	2	2
224	222	8	2	2
224	220	9	3	3
224	219	12	4	3
224	218	14	4	3
224	217	15	3	3
224	216	16	4	4
224	215	17	5	5
224	214	18	6	6
224	213	20	6	6
224	212	21	6	6
224	211	22	8	6
224	210	23	9	6
224	209	24	6	6
224	208	25	10	8
224	207	26	8	8
224	206	27	9	9
224	205	28	12	12
224	204	29	13	12
224	203	30	12	12
224	202	31	15	14
224	201	32	14	14
224	200	33	15	15
224	199	34	16	16
224	198	35	17	17
224	197	36	18	18
224	196	37	20	20
224	195	38	20	20

Table 3: Codes $C_\ell(P_2)$ - $q = 64$

n	k	ρ_ℓ	ν_ℓ	d_{ORD}
224	223	0	2	2
224	222	7	2	2
224	221	8	2	2
224	220	9	2	2
224	219	13	3	3
224	218	14	4	3
224	217	15	5	3
224	216	16	4	3
224	215	17	3	3
224	214	18	4	4
224	213	20	6	6
224	212	21	8	7
224	211	22	8	7
224	210	23	8	7
224	209	24	8	7
224	208	25	7	7
224	207	26	8	8
224	206	27	9	9
224	205	28	12	12
224	204	29	13	13
224	203	30	14	13
224	202	31	13	13
224	201	32	14	14
224	200	33	15	15
224	199	34	16	16
224	198	35	17	17
224	197	36	18	18
224	196	37	20	20
224	195	38	20	20

Table 4: Codes $\tilde{C}_d(P_1)$ - $q = 64$

n	d	r_d	$k \geq$
224	3	4	220
224	4	6	218
224	5	9	215
224	6	10	214
224	7	14	210
224	8	14	210
224	9	16	208
224	10	18	206
224	11	19	205
224	12	19	205
224	13	21	203
224	14	22	202
224	15	23	201
224	16	25	199
224	17	26	198
224	18	27	197
224	19	28	196
224	20	28	196

Table 5: Codes $\tilde{C}_d(P_2)$ - $q = 64$

n	d	r_d	$k \geq$
224	3	5	219
224	4	7	217
224	5	10	214
224	6	11	213
224	7	12	212
224	8	13	211
224	9	18	206
224	10	19	205
224	11	19	205
224	12	19	205
224	13	20	204
224	14	22	202
224	15	24	200
224	16	25	199
224	17	26	198
224	18	27	197
224	19	28	196
224	20	28	196

Table 6: $q = 3^6$, $n = 6075$

k	d	Ref.	k	d	Ref.	k	d	Ref.	k	d	Ref.
6074	2	$\tilde{C}_2(P_1)$	6071	3	$\tilde{C}_3(P_1)$	6068	4	$\tilde{C}_4(P_1)$	6063	5	$\tilde{C}_5(P_1)$
6062	6	$\tilde{C}_6(P_1)$	6055	7	$\tilde{C}_7(P_1)$	6053	8	$\tilde{C}_8(P_1)$	6048	9	$\tilde{C}_9(P_1)$
6045	10	$\tilde{C}_{10}(P_1)$	6042	11	$\tilde{C}_{11}(P_1)$	6041	12	$\tilde{C}_{12}(P_1)$	6032	13	$\tilde{C}_{13}(P_1)$
6031	14	$\tilde{C}_{14}(P_1)$	6027	15	$\tilde{C}_{15}(P_1)$	6024	16	$\tilde{C}_{16}(P_1)$	6020	17	$\tilde{C}_{17}(P_1)$
6019	18	$\tilde{C}_{18}(P_1)$	6013	19	$\tilde{C}_{19}(P_1)$	6012	20	$\tilde{C}_{20}(P_1)$	6008	21	$\tilde{C}_{21}(P_1)$
6004	22	$\tilde{C}_{22}(P_1)$	6003	23	$\tilde{C}_{23}(P_1)$	6002	24	$\tilde{C}_{24}(P_1)$	5996	25	$\tilde{C}_{25}(P_2)$
5995	26	$\tilde{C}_{26}(P_1)$	5994	27	$\tilde{C}_{27}(P_1)$	5992	28	$\tilde{C}_{28}(P_1)$	5987	30	$\tilde{C}_{30}(P_1)$
5983	32	$\tilde{C}_{32}(P_1)$	5981	33	$\tilde{C}_{33}(P_1)$	5980	34	$\tilde{C}_{34}(P_1)$	5979	35	$\tilde{C}_{35}(P_1)$
5978	36	$\tilde{C}_{36}(P_1)$	5973	37	$\tilde{C}_{37}(P_1)$	5972	38	$\tilde{C}_{38}(P_1)$	5970	39	$\tilde{C}_{39}(P_1)$
5969	40	$\tilde{C}_{40}(P_1)$	5966	42	$\tilde{C}_{42}(P_1)$	5961	44	$\tilde{C}_{44}(P_1)$	5960	45	$\tilde{C}_{45}(P_1)$
5958	46	$\tilde{C}_{46}(P_1)$	5956	48	$\tilde{C}_{48}(P_1)$	5952	50	$\tilde{C}_{50}(P_2)$	5951	51	$\tilde{C}_{51}(P_2)$
5949	52	$\tilde{C}_{52}(P_2)$	5946	53	$\tilde{C}_{53}(P_1)$	5945	54	$\tilde{C}_{54}(P_1)$	5942	55	$\tilde{C}_{55}(P_1)$
5940	56	$\tilde{C}_{56}(P_1)$	5938	57	$\tilde{C}_{57}(P_1)$	5937	60	$\tilde{C}_{60}(P_1)$	5932	62	$\tilde{C}_{62}(P_1)$
5931	63	$\tilde{C}_{63}(P_1)$	5929	64	$\tilde{C}_{64}(P_1)$	5928	65	$\tilde{C}_{65}(P_1)$	5927	66	$\tilde{C}_{66}(P_1)$
5926	68	$\tilde{C}_{68}(P_1)$	5924	69	$\tilde{C}_{69}(P_1)$	5922	70	$\tilde{C}_{70}(P_1)$	5919	71	$\tilde{C}_{71}(P_1)$
5918	72	$\tilde{C}_{72}(P_1)$	5917	74	$\tilde{C}_{74}(P_2)$	5916	75	$\tilde{C}_{75}(P_2)$	5915	76	$\tilde{C}_{76}(P_2)$
5914	77	$\tilde{C}_{77}(P_2)$	5913	78	$\tilde{C}_{78}(P_2)$	5910	79	$\tilde{C}_{79}(P_2)$	5908	80	$\tilde{C}_{80}(P_1)$
5906	81	$\tilde{C}_{81}(P_1)$	5905	82	$\tilde{C}_{82}(P_1)$	5904	83	$\tilde{C}_{83}(P_1)$	5902	84	$\tilde{C}_{84}(P_1)$
5899	85	$\tilde{C}_{85}(P_1)$	5898	86	$\tilde{C}_{86}(P_1)$	5897	90	$\tilde{C}_{90}(P_1)$	5894	91	$\tilde{C}_{91}(P_1)$
5892	92	$\tilde{C}_{92}(P_1)$	5891	94	$\tilde{C}_{94}(P_1)$	5890	96	$\tilde{C}_{96}(P_2)$	5889	99	$\tilde{C}_{99}(P_2)$
5888	100	$\tilde{C}_{100}(P_2)$	5885	101	$\tilde{C}_{101}(P_2)$	5884	102	$\tilde{C}_{102}(P_2)$	5880	103	$\tilde{C}_{103}(P_1)$
5878	104	$\tilde{C}_{104}(P_1)$	5877	105	$\tilde{C}_{105}(P_1)$	5875	106	$\tilde{C}_{106}(P_1)$	5874	108	$\tilde{C}_{108}(P_1)$
5872	109	$\tilde{C}_{109}(P_1)$	5871	110	$\tilde{C}_{110}(P_1)$	5869	111	$\tilde{C}_{111}(P_1)$	5868	112	$\tilde{C}_{112}(P_1)$
5866	114	$\tilde{C}_{114}(P_1)$	5865	115	$\tilde{C}_{115}(P_1)$	5864	117	$\tilde{C}_{117}(P_1)$	5863	120	$\tilde{C}_{120}(P_2)$
5862	121	$\tilde{C}_{121}(P_2)$	5860	124	$\tilde{C}_{124}(P_2)$	5857	125	$\tilde{C}_{125}(P_2)$	5854	126	$\tilde{C}_{126}(P_1)$
5852	128	$\tilde{C}_{128}(P_1)$	5851	129	$\tilde{C}_{129}(P_1)$	5849	130	$\tilde{C}_{130}(P_1)$	5848	131	$\tilde{C}_{131}(P_1)$
5847	132	$\tilde{C}_{132}(P_1)$	5846	133	$\tilde{C}_{133}(P_1)$	5844	134	$\tilde{C}_{134}(P_1)$	5843	135	$\tilde{C}_{135}(P_1)$
5842	136	$\tilde{C}_{136}(P_1)$	5841	137	$\tilde{C}_{137}(P_1)$	5840	138	$\tilde{C}_{138}(P_1)$	5838	139	$\tilde{C}_{139}(P_1)$
5837	140	$\tilde{C}_{140}(P_1)$	5836	144	$\tilde{C}_{144}(P_1)$	5835	146	$\tilde{C}_{146}(P_2)$	5832	148	$\tilde{C}_{148}(P_2)$
5830	149	$\tilde{C}_{149}(P_2)$	5829	150	$\tilde{C}_{150}(P_1)$	5828	151	$\tilde{C}_{151}(P_1)$	5827	152	$\tilde{C}_{152}(P_1)$
5825	153	$\tilde{C}_{153}(P_1)$	5823	154	$\tilde{C}_{154}(P_1)$	5822	156	$\tilde{C}_{156}(P_1)$	5821	157	$\tilde{C}_{157}(P_1)$
5820	158	$\tilde{C}_{158}(P_1)$	5818	159	$\tilde{C}_{159}(P_1)$	5817	160	$\tilde{C}_{160}(P_1)$	5816	161	$\tilde{C}_{161}(P_1)$
5815	162	$\tilde{C}_{162}(P_1)$	5814	163	$\tilde{C}_{163}(P_1)$	5813	164	$\tilde{C}_{164}(P_1)$	5812	165	$\tilde{C}_{165}(P_1)$
5811	166	$\tilde{C}_{166}(P_1)$	5810	167	$\tilde{C}_{167}(P_1)$	5809	168	$\tilde{C}_{168}(P_1)$	5808	171	$\tilde{C}_{171}(P_1)$
5806	172	$\tilde{C}_{172}(P_1)$	5805	173	$\tilde{C}_{173}(P_2)$	5804	174	$\tilde{C}_{174}(P_2)$	5802	175	$\tilde{C}_{175}(P_1)$
5801	177	$\tilde{C}_{177}(P_1)$	5800	178	$\tilde{C}_{178}(P_1)$	5798	179	$\tilde{C}_{179}(P_1)$	5797	180	$\tilde{C}_{180}(P_1)$
5796	181	$\tilde{C}_{181}(P_1)$	5795	182	$\tilde{C}_{182}(P_1)$	5794	183	$\tilde{C}_{183}(P_1)$	5793	184	$\tilde{C}_{184}(P_1)$
5792	185	$\tilde{C}_{185}(P_1)$	5791	186	$\tilde{C}_{186}(P_1)$	5790	187	$\tilde{C}_{187}(P_1)$	5789	188	$\tilde{C}_{188}(P_1)$
5788	189	$\tilde{C}_{189}(P_1)$	5787	190	$\tilde{C}_{190}(P_1)$	5786	191	$\tilde{C}_{191}(P_1)$	5785	192	$\tilde{C}_{192}(P_1)$
5784	193	[illegible]	5783	194	[illegible]	5782	195	[illegible]	5781	196	[illegible]

[2] V.D. Goppa, "Codes on algebraic curves," *Dokl. Akad. NAUK, SSSR*, vol. 259, pp. 1289–1290, 1981.

[3] V.D. Goppa, "Algebraic-geometric Codes," *Izv. Akad. NAUK, SSSR*, vol. 46, pp. 75–91, 1982.

[4] J.P. Hansen, "Codes on the Klein Quartic, Ideals and decoding," *IEEE Trans. Inf. Theory*, vol. 33, pp. 923–925, 1987.

[5] J.P. Hansen and H. Stichtenoth, "Group Codes on Certain Algebraic Curves with Many Rational Points," *AAECC*, vol. 1, pp. 67–77, 1990.

[6] G.L. Matthews, "Codes from the Suzuki function field," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3298–3302, 2004.

[7] G.L. Matthews, "Weierstrass Semigroups and Codes from a Quotient of the Hermitian Curve," *Des. Codes Cryptogr.*, vol. 37, pp. 473–492, 2005.

[8] H. Stichtenoth, "A note on Hermitian Codes over $GF(q^2)$," *IEEE Trans. Inf. Theory*, vol. 34, pp. 1345–1348, 1988.

[9] H.J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inf. Theory*, vol. 33, pp. 605–609, 1987.

[10] C.P. Xing and H. Chen, "Improvements on parameters of one-point AG codes from Hermitian curves," *IEEE Trans. Inf. Theory*, vol. 48, pp. 535–537, 2002.

[11] C.P. Xing and S. Ling, "A class of Linear Codes with Good Parameters from Algebraic Curves," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1527–1532, 2000.

[12] K. Yang and P.V. Kumar, "On the true minimum distance of Hermitian codes," *Coding theory and algebraic geometry, Lecture Notes in Math.*, vol. 1518, pp. 99-107, 1992.

[13] M. Giulietti and G. Korchmáros, "A new family of maximal curves over a finite field," *Mathematische Annalen*, vol. 343, pp. 229–245, 2009.

[14] T. Høholdt, J.H. van Lint and R. Pellikaan, "Algebraic Geometry codes," in *Handbook of Coding Theory*, vol. 1, V.S. Pless, W.C.Huffman and R.A. Brualdi Eds. Amsterdam: Elsevier, 1998, pp. 871–961.

[15] A. Garcia, S.J. Kim and R.F. Lax, "Consecutive Weierstrass gaps and minimum distance of Goppa codes," *J. Pure Appl. Algebra*, vol. 84, pp. 199–207, 1993.

[16] K.O. Stöhr and J.F. Voloch, "Weierstrass points and curves over finite fields," *Proc. London Math. Soc.* (3), vol. 52, pp. 1–19, 1986.

[17] R. Fuhrmann, A. Garcia and F. Torres, "On maximal curves," *J. Number Theory*, vol. 67, pp. 29–51, 1997.

[18] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton/Oxford: Princeton University Press, 2008.

[19] H. Stichtenoth, "On automorphisms of geometric Goppa codes," *J. Algebra*, vol. 130, pp. 113-121, 1990.

[20] M.A. Tsfasman and S.G. Vladut, *Algebraic-goemetric codes*, Amsterdam: Kluwer, 1991.