ON GOPPA CODES AND WEIERSTRASS GAPS AT SEVERAL POINTS

CÍCERO CARVALHO AND FERNANDO TORRES

Abstract. We generalize results of Homma and Kim [2001, *J. Pure Appl. Algebra* **162**, 273–290] concerning an improvement on the Goppa bound on the minimum distance of certain Goppa codes.

1. Introduction

Ideas from Algebraic Geometry became useful in Coding Theory after Goppa constructed linear codes using the following data (see [9]):

- A projective, geometrically irreducible, non-singular algebraic curve $\mathcal{X}$ defined over a finite field $\mathbf{F}$;
- Two $\mathbf{F}$-divisors on $\mathcal{X}$, $D = P_1 + \ldots + P_n$ and F such that their support do not intersect, $P_i \neq P_j$ for $i \neq j$, and P_i a $\mathbf{F}$-rational point of $\mathcal{X}$ for all i.

Then the Goppa (or Algebraic Geometric) code $\mathcal{C} = \mathcal{C}_{\mathcal{X}}(D, F)$ is the image of the $\mathbf{F}$-linear map:

$$\mathrm{res} : \Omega(F - D) \to \mathbf{F}^n\,, \qquad \eta \mapsto (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta))\,,$$

where $\Omega(F-D)$ is the $\mathbf{F}$-space of differentials η on $\mathcal{X}$ such that $\eta = 0$ or $\mathrm{div}(\eta) \succeq F - D$. The dimension of $\mathcal{C}$ can be estimated using the Riemann-Roch theorem since it is equal to $\dim_{\mathbf{F}}\Omega(F-D) - \dim_{\mathbf{F}}\Omega(F)$, and one of the main features of this code is that its minimum distance d satisfies the so-called *Goppa bound*, namely

$$d \geq \deg(F) - (2g - 2)\,. \tag{1.1}$$

Goppa [10, pp. 139–141] gave an example where the above bound may be improved for $F = \alpha P$, a one-point divisor. Garcia, Kim and Lax (see [6], [5]) gave an explanation for this fact by showing that it depends on the arithmetical structure of the Weierstrass

MSC: 94B27; 14H55; 14G50.

*Keywords:*Error correcting codes; Goppa codes; Weierstrass gaps at several points; Gonality sequence of curves.

This paper was written while the second author was visiting The University of Valladolid (Dpto. Algebra, Geometría y Topología; Fac. de Ciencias) supported by the Grant SB2000-0225 from the "Secretaria de Estado de Educación y Universidades del Ministerio de Educación, Cultura y Deportes de España". The first author acknowledges partial support from FAPEMIG, proc. CEX 140/02.

Des. Codes Crypt. 35(2) (2005), 211–225.

semigroup at P. Matthews [16], Homma and Kim [12] proved similar results for $F = \alpha P + \beta Q$, a two-point divisor with $P, Q \in \mathcal{X}(\mathbf{F})$, by selecting α and β according to certain considerations about the arithmetical structure of the Weierstrass semigroup at P and Q (see below).

The notion of Weierstrass semigroups at several points was introduced by Arbarello, Cornalba, Griffiths, and Harris [1, p. 365]. The case of two points was extensively studied by Kim [14] and Homma [11] (see also [15]), and some arithmetical and geometrical properties concerning the general case can be found in [3], [2] and [13].

In this paper we extend Theorems 3.4 and 3.3 in [12] to the case of several points; see Theorems 3.3 and 3.4 here. The key point in [12] is the *Dual Series Trick Lemma* (see Lemma 3.2 here) which is a result that does not depend on F being a two-point divisor, and generalizes the fact that divisors of negative degree have no non-trivial sections. To be more precise, Theorem 3.4 in [12] states that

$$d \geq \deg(F) - (2g-2) + 2$$

when Lemma 3.2 is applied for $F = (n_1+p_1-1)P + (n_2+p_2-1)Q$ with $(n_1, n_2), (p_1, p_2) \in \mathbf{N}_0^2$ satisfying the following relations in (a, b) (notation as in Section 2):

$$\ell(aP + bQ) = \ell((a-1)P + bQ) = \ell(aP + (b-1)Q)\,.$$

Such pairs (a, b) are in particular Weierstrass gaps at P and Q; i.e., they are in the complement in $\mathbf{N}_0^2$ of the Weierstrass semigroup at P and Q, and were called *pure Weierstrass gaps* by Homma and Kim [12, p. 276]. It turns out that such pairs (a, b) are characterized by the relation [12, Lemma 2.3]

$$\ell(aP + bQ) = \ell((a-1)P + (b-1)Q)\,.$$

This characterization holds true for *pure Weierstrass gaps at several points* as we shall see in Lemma 2.5. Using the same approach, Theorem 3.3 in [12] gives

$$d \geq \deg(F) - (2g-2) + 2 + (p_2 - n_2) + (p_1 - n_1)$$

under additional hypotheses on the Weierstrass pure gaps (n_1, n_2) and (p_1, p_2) at P and Q. Therefore the proof of our Theorems 3.3 and 3.4 becomes essentially the same as the proof of Homma and Kim for the case of two points. We illustrate our results with Examples 4.1 and 4.3. Section 2 contains semigroup-theoretical properties on Weierstrass semigroups at several points. For instance, some results of Kim [14] are generalized; see Remark 2.15.

2. Basic facts on Weierstrass gaps at several points

The aim of this section is to recall the basic definitions and prove some facts on Weierstrass semigroups at several points.

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve defined over a perfect field $\mathbf{F}$ (or simply, a curve over $\mathbf{F}$) . Let m be a positive integer and let $Q_1, \ldots, Q_m$ be points of $\mathcal{X}$ defined over $\mathbf{F}$ (or simply, $\mathbf{F}$-rational points). The following sub-semigroup of $\mathbf{N}_0^m$ (with the usual addition)

$$\begin{aligned}\mathbf{H} =&\mathbf{H}(Q_1, \ldots, Q_m)\\ :=&\{(n_1, \ldots, n_m) \in \mathbf{N}_0^m : \exists f \in \mathbf{F}(\mathcal{X}) \text{ with } \operatorname{div}_\infty(f) = n_1Q_1 + \ldots + n_mQ_m\}\,,\end{aligned}$$

is called the *Weierstrass semigroup* of $\mathcal{X}$ at $Q_1, \ldots, Q_m$ (here $\operatorname{div}_\infty(f)$ denotes the divisor of poles of f, as defined next).

Notation

- As usual, for an $\mathbf{F}$-divisor D on the curve $\mathcal{X}$, $\ell(D)$ stands for the dimension over $\mathbf{F}$ of the $\mathbf{F}$-linear space $\mathcal{L}(D) = \{f \in \mathbf{F}(\mathcal{X})^* : D + \operatorname{div}(f) \succeq 0\} \cup \{0\}$;
- For $\mathbf{n} := (n_1, \ldots, n_m) \in \mathbf{Z}^m$, we set $\mathcal{L}(\mathbf{n}) := \mathcal{L}(n_1Q_1 + \ldots + n_mQ_m)$ and $\ell(\mathbf{n}) := \ell(\mathcal{L}(\mathbf{n}))$;
- For $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbf{N}_0^m$ and $i \in \{1, \ldots, m\}$, we set

  $$\nabla_i(\mathbf{n}) := \{(p_1, \ldots, p_m) \in \mathbf{H} : p_i = n_i \text{ and } p_j \leq n_j\ \forall j \neq i\}\,.$$

  We also set $\mathbf{n}_i := \mathbf{n} - n_i\mathbf{e}_i$, where $\mathbf{e}_i$ denotes the vector in $\mathbf{N}_0^m$ with 1 in the ith-position and 0 in the other ones;
- $\mathbf{1}$ stands for the vector with 1 in each position.
- For $i \in \{1, \ldots, m\}$, v_i stands for the valuation at the point Q_i.
- For any $f \in \mathbf{F}(\mathcal{X})^*$ we define $\operatorname{div}_\infty(f) := \sum_{Q\in\mathcal{X}(\mathbf{F}),\, v_Q(f)<0}(-v_Q(f))\,Q$ and $\operatorname{div}_0(f) := \sum_{Q\in\mathcal{X}(\mathbf{F}),\, v_Q(f)>0} v_Q(f)\,Q$, where v_Q is the valuation at the point Q.

The following two lemmas were proved by Delgado in the case where $\mathbf{F}$ is an algebraically closed field (cf. [3, p. 629]).

Lemma 2.1. *Let $\mathbf{n} \in \mathbf{N}_0^m$, $i \in \{1, \ldots, m\}$ and suppose that $\#\mathbf{F} \geq m$. Then $\ell(\mathbf{n}) = \ell(\mathbf{n} - \mathbf{e}_i) + 1$ if and only if $\nabla_i(\mathbf{n}) \neq \emptyset$.*

Proof. Let $f \in \mathcal{L}(\mathbf{n}) \setminus \mathcal{L}(\mathbf{n} - \mathbf{e}_i)$. Since $\#\mathbf{F} \geq m$ there is an $\alpha \in \mathbf{F}$ such that $(-v_1(f + \alpha), \ldots, -v_m(f + \alpha)) \in \nabla_i(\mathbf{n})$. The converse is clear. □

Lemma 2.2. *Let $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbf{N}_0^m$, and suppose that $\#\mathbf{F} \geq m$. Then the following statements are equivalent*:

1. $\mathbf{n} \in \mathbf{H}$;
2. $\ell(\mathbf{n}) = \ell(\mathbf{n} - \mathbf{e}_i) + 1$, *for all* $i = 1, \ldots, m$;
3. *The linear system* $|n_1Q_1 + \ldots + n_mQ_m|$ *is base-point-free.*

Proof. The equivalence between (1) and (3) as well as that (1) implies (2) are clear. To see that (2) implies (1), let $f_1, \ldots, f_m \in \mathbf{F}(\mathcal{X})$ such that $v_i(f_i) = -n_i$ and $v_j(f_i) \geq -n_j$ for $j \neq i$, where $i, j \in \{1, \ldots, m\}$. We are going to show that there exists a m-tuple

$(\alpha_1,\dots,\alpha_m)\in\mathbf{F}^m$ such that the pole divisor of $\sum_{i=1}^m \alpha_i f_i$ is precisely $\sum_{i=1}^m n_iQ_i$. For each $i=1,\dots,m$, let t_i be a local parameter at Q_i. Let

$$f_i = a_{i,j}t_j^{v_j(f_i)}+\dots\in\mathbf{F}((t_j))$$

be the local expansion of f_i at Q_j. Then $\mathrm{div}_\infty(\sum_{i=1}^m\alpha_if_i)\neq\sum_{i=1}^m n_iQ_i$ if and only if there exists $j\in\{1,\dots,m\}$ such that $\sum_{i=1}^m\alpha_ia_{i,j}=0$; i.e., in order to have $\mathrm{div}_\infty(\sum_{i=1}^m\alpha_if_i)=\sum_{i=1}^m n_iQ_i$ it is enough to choose the m-tuple $(\alpha_1,\dots,\alpha_m)\in\mathbf{F}^m$ outside the union of at most m linear sub-spaces of dimension $m-1$. That this can be done is guaranteed by the hypothesis $\#\mathbf{F}\geq m$ and the proof is complete. □

As an example that the condition on the cardinality of $\mathbf{F}$ in the above lemma is truly necessary, take a nonsingular plane curve $\mathcal{X}$ of degree 4 defined over the field with three elements $\mathbf{F}_3$, and let Q_1,Q_2,Q_3 and Q_4 be collinear points on the curve. Then $\ell(Q_1+Q_2+Q_3+Q_4)=3$ and $\ell(Q_i+Q_j+Q_k)=2$ for all $1\leq i<j<k\leq 4$; but there is no rational function $f\in\mathbf{F}_3(\mathcal{X})$ such that $\mathrm{div}_\infty(f)=Q_1+Q_2+Q_3+Q_4$.

The elements of the complement $\mathbf{G}=\mathbf{G}(Q_1,\dots,Q_m)$ of $\mathbf{H}$ in $\mathbf{N}_0^m$ will be called *Weierstrass gaps* at $Q_1,\dots,Q_m$. From the previous two lemmas we have the following.

Corollary 2.3. *Let $\mathbf{n}\in\mathbf{N}_0^m$ and suppose that $\#\mathbf{F}\geq m$. Then the following statements are equivalent:*

(1) $\mathbf{n}\in\mathbf{G}$;
(2) *There exists $i\in\{1,\dots,m\}$ such that $\ell(\mathbf{n})=\ell(\mathbf{n}-\mathbf{e}_i)$;*
(3) *There exists $i\in\{1,\dots,m\}$ such that $\nabla_i(\mathbf{n})=\emptyset$.*

Remark 2.4. For $\mathbf{n}=(n_1,\dots,n_m)\in\mathbf{N}_0^m$ and $i\in\{1,\dots,m\}$, the meaning of $\nabla_i(\mathbf{n})=\emptyset$ is that every m-tuple $(p_1,\dots,p_m)\in\mathbf{N}_0^m$ is a Weierstrass gap at $Q_1,\dots,Q_m$ provided that $p_i=n_i$ and $0\leq p_j\leq n_j$ for $j\neq i$.

Observe that $\mathbf{G}$ is a finite set; upper bounds for $\#\mathbf{G}$ have been found in terms of the genus g of the curve. For instance, when the base field is algebraically closed and of characteristic zero, Kim [14] showed that $\#\mathbf{G}(Q_1,Q_2)\leq(3g^2+g)/2$, with equality holding if and only if $\mathcal{X}$ is a hyperelliptic curve and Q_1 and Q_2 are Weierstrass points of $\mathcal{X}$; Ishii [13] showed that $\#\mathbf{G}(Q_1,Q_2,Q_3)\leq g(7g^2+6g+5)/6$, with equality holding if and only if $\mathcal{X}$ is a hyperelliptic curve and Q_1,Q_2,Q_3 are Weierstrass points of $\mathcal{X}$ (cf. also [2] for a conjecture on a upper bound for $\#\mathbf{G}(Q_1,\dots,Q_m)$).

Following Homma and Kim (cf. [12]), for applications to Goppa codes one is in fact interested in the so-called *pure Weierstrass gaps*, namely those Weierstrass gaps that satisfy Property (2) in the above corollary for all $i=1,\dots,m$. The set of such gaps will be denoted by $\mathbf{G}_0=\mathbf{G}_0(Q_1,\dots,Q_m)$. Homma and Kim [12] showed that $\#\mathbf{G}_0(Q_1,Q_2)\leq g(g-1)/2$, where g is the genus of $\mathcal{X}$. Observe that each coordinate of a pure Weierstrass gap is indeed a positive integer since $\ell(\mathbf{n}_i)=\ell(\mathbf{n}_i-\mathbf{e}_i)+1$.

Lemma 2.5. *Let $\mathbf{n}=(n_1,\dots,n_m)\in\mathbf{N}_0^m$ and suppose that $\#\mathbf{F}\geq m$. Then the following statements are equivalent*:

(1) $\mathbf{n}\in\mathbf{G}_0$;
(2) $\nabla_i(\mathbf{n})=\emptyset$, *for all* $i=1,\dots,m$;
(3) $\ell(\mathbf{n})=\ell(\mathbf{n}-\mathbf{1})$.

Proof. That (1) is equivalent to (2) follows from Lemma 2.1. Now as $\ell(\mathbf{n})\geq\ell(\mathbf{n}-\mathbf{e}_i)\geq\ell(\mathbf{n}-\mathbf{1})$ for all $i=1,\dots,m$, it is clear that (3) implies (1). To see the converse, let $f\in\mathcal{L}(\mathbf{n})\setminus\mathcal{L}(\mathbf{n}-\mathbf{1})$; then there exists $i\in\{1,\dots,m\}$ such that $v_i(f)=-n_i$ and $v_j(f)\geq -n_j$ for $j\neq i$; i.e., $f\in\mathcal{L}(\mathbf{n})\setminus\mathcal{L}(\mathbf{n}-\mathbf{e}_i)$ so that $\mathbf{n}\notin\mathbf{G}_0$. □

Corollary 2.6. *Assume that $\#\mathbf{F}\geq m$.*

(1) *If $(n_1,\dots,n_m)\in\mathbf{G}_0$, then n_i is a Weierstrass gap at Q_i for each $i=1,\dots,m$;*
(2) *If $\mathbf{1}\in\mathbf{H}$, then $\mathbf{G}_0=\emptyset$;*
(3) *Let $\mathbf{n}=(n_1,\dots,n_m)\in\mathbf{N}^m$ such that the gonality of $\mathcal{X}$ over $\mathbf{F}$ is at least $1+\sum_{i=1}^m n_i$. Then $\mathbf{n}\in\mathbf{G}_0$.*

Proof. Item (1) follows from Lemma 2.5(2) and Remark 2.4. To see (2), let us assume that $\mathbf{G}_0\neq\emptyset$ and let $\mathbf{n}=(n_1,\dots,n_m)\in\mathbf{G}_0$. Let n_i be the minimum among the coordinates of $\mathbf{n}$. Then, as $\nabla_i(\mathbf{n})=\emptyset$ by Lemma 2.5, we have $n_i\mathbf{1}\in\mathbf{G}$ so that $\mathbf{1}\notin\mathbf{H}$. Let us prove (3). We must have $\mathbf{n}\in\mathbf{G}$, otherwise the gonality of the curve is at most $\sum_{i=1}^m n_i$; moreover, $\ell(\mathbf{n})=1$. Now we also must have $\ell(\mathbf{n}-\mathbf{1})=1$ since $n_i\geq 1$ for all i; thus the result follows from Lemma 2.5. □

Example 2.7. The bound on the gonality of the curve in part (3) of the above corollary cannot be improved as the following example shows. Let $\mathcal{X}$ be the Fermat curve of degree $r\geq 2$,

$$X^r+Y^r+Z^r=0\,,$$

defined over $\mathbf{F}$, a finite field with q^2 elements. It is known that its gonality over $\mathbf{F}$ is $r-1$ provided that char$(\mathbf{F})$ does not divide r and that $\mathcal{X}(\mathbf{F})\neq\emptyset$; see Sect. 4.

Let us assume that r divides either $(q-1)$ or $(q+1)$. We are going to show that there are $(r-1)$ $\mathbf{F}$-rational points of $\mathcal{X}$ such that $\mathbf{1}\in\mathbf{N}_0^{r-1}$ belongs to the Weierstrass semigroup at such points.

Let $x:=X/Z$ and $y:=Y/Z$ denote the rational functions on $\mathcal{X}$ obtained from projective coordinates $(X:Y:Z)$ of $\mathbf{P}^2(\bar{\mathbf{F}})$. Let $b_1,\dots,b_r$ be the roots of $Y^r+1=0$ and set $Q_i:=(0:b_i:1)$. Then each Q_i is an $\mathbf{F}$-rational point of $\mathcal{X}$, and it follows that

$$\operatorname{div}(x)=\sum_{i=1}^r Q_i-D_\infty \qquad\text{and}\qquad \operatorname{div}(y-b_i)=rQ_i-D_\infty\,,$$

where D_∞ is the intersection divisor of $\mathcal{X}$ and the line $Z=0$. In particular,

$$\mathrm{div}(\frac{y-b_r}{x}) = (r-1)Q_r - \sum_{i=1}^{r-1} Q_i\,;$$

i.e., $\mathbf{1}$ belongs to $\mathbf{H}(Q_1,\ldots,Q_{r-1})$.

Next we prove more results about the semigroup $\mathbf{H}=\mathbf{H}(Q_1,\ldots,Q_m)$. Although these properties are not explicitly used in Sections 3 and 4, they are interesting in their own right and led us to natural generalizations of some results from [14]; see Remark 2.15. In what follows we will always assume that $\#\mathbf{F}\geq m$.

Lemma 2.8. *For $(n_1,\ldots,n_m),(p_1,\ldots,p_m)\in\mathbf{H}$, let $q_i:=\max(n_i,p_i)$ for $i=1,\ldots,m$. Then $(q_1,\ldots,q_m)\in\mathbf{H}$.*

Proof. Let $f,g\in\mathbf{F}(\mathcal{X})$ such that $\mathrm{div}_\infty(f)=\sum_{i=1}^m n_iQ_i$ and $\mathrm{div}_\infty(g)=\sum_{i=1}^m p_iQ_i$. For $i=1,\ldots,m$, let t_i be a local parameter at Q_i and

$$f=a_{i,-n_i}t_i^{-n_i}+\ldots\in\mathbf{F}((t_i))\,,\qquad g=b_{i,-p_i}t_i^{-p_i}+\ldots\in\mathbf{F}((t_i))$$

the local expansions of f and g at Q_i. Let $h=h_{\alpha,\beta}:=\alpha f+\beta g$ with $\alpha,\beta\in\mathbf{F}$. Then $v_i(h)=-q_i$ provided that either $n_i\neq p_i$, or $n_i=p_i$ and $\alpha a_{i,-n_i}+\beta b_{i,-p_i}\neq 0$. The last condition is satisfied for all i if (α,β) is chosen in the complement in $\mathbf{F}^2$ of the union of at most m linear sub-spaces of dimension one; since $\#F\geq m$, such a selection is possible and the proof follows. □

Corollary 2.9. *Let $\mathbf{n}=(n_1,\ldots,n_m)\in\mathbf{N}_0^m$ and $i\in\{1,\ldots,m\}$ such that $\nabla_i(\mathbf{n})\neq\emptyset$. Let p be a non-negative integer such that $p<n_i$. If $\mathbf{p}:=\mathbf{n}_i+p\mathbf{e}_i\in\mathbf{H}$, then $\mathbf{n}\in\mathbf{H}$.*

Proof. There exists $\mathbf{q}:=(q_1,\ldots,q_m)\in\mathbf{H}$ such that $q_i=n_i$ and $q_j\leq n_j$ for $j\neq i$. Then the result follows by applying Lemma 2.8 to $\mathbf{p}$ and $\mathbf{q}$. □

Lemma 2.10. *Let $j\in\{1,\ldots,m\}$ and $(n_1,\ldots,n_m),(p_1,\ldots,p_m)\in\mathbf{H}$ such that $n_j=p_j$. Then there exists $(q_1,\ldots,q_m)\in\mathbf{H}$ whose coordinates satisfy: $q_i=\max(n_i,p_i)$ for $i\neq j$ and $n_i\neq p_i$; $q_i\leq n_i$ for $i\neq j$ and $n_i=p_i$; and $q_j=n_j=0$, or $q_j<n_j$.*

Proof. With notation as in the proof of Lemma 2.8, let $h:=b_{j,-p_j}f-a_{j,-n_j}g$ and take the vector with coordinates $q_i:=\max(-v_i(h),0)$ for $i=1,\ldots,m$. □

Let us recall that by the Riemann-Roch theorem a vector $(n_1,\ldots,n_m)\in\mathbf{N}_0^m$ belongs to $\mathbf{H}$ whenever $\sum_{i=1}^m n_i\geq 2g$, where g is the genus of $\mathcal{X}$.

Corollary 2.11. *For $\mathbf{n}=(n_1,\ldots,n_m)\in\mathbf{N}_0^m$ and $i\in\{1,\ldots,m\}$, suppose that $\mathbf{n}_i\in\mathbf{G}$. Let*

$$n:=\min\{p\in\mathbf{N}:\mathbf{n}_i+p\mathbf{e}_i\in\mathbf{H}\}\,.$$

Then any vector $\mathbf{p}=(p_1,\ldots,p_m)\in\mathbf{N}_0^m$ belongs to $\mathbf{G}$ whenever $p_i=n$, and $p_j=n_j=0$ or $p_j<n_j$ for $j\neq i$. In particular, n is a Weierstrass gap at Q_i.

Proof. Suppose by means of absurd that such a vector $\mathbf{p}$ belongs to $\mathbf{H}$. Then from Lemma 2.10 applied to $\mathbf{p}$ and $\mathbf{n}_i + n\mathbf{e}_i$ we get that $\mathbf{n}_i + p\mathbf{e}_i \in \mathbf{H}$ for some non-negative integer $p < n$, a contradiction with the choice of n. □

Corollary 2.12. *Let $\mathbf{n} = (n_1, \ldots, n_m), i, \mathbf{n}_i$, and n be as in Corollary 2.11. Let $\mathbf{p} = (p_1, \ldots, p_m) \in \mathbf{N}_0^m$ such that $\mathbf{p}_i \in \mathbf{G}$. If either $p_j < n_j$ for all $j \neq i$, or $p_j > n_j$ for all $j \neq i$, then*

$$n \neq \min\{p \in \mathbf{N} : \mathbf{p}_i + p\mathbf{e}_i \in \mathbf{H}\}\,.$$

Proof. If the result is not true, then applying Lemma 2.10 to $\mathbf{n}_i + n\mathbf{e}_i$ and $\mathbf{p}_i + n\mathbf{e}_i$ we would have that either $\mathbf{n}_i + q\mathbf{e}_i \in \mathbf{H}$, or $\mathbf{p}_i + q\mathbf{e}_i \in \mathbf{H}$ for some non-negative integer $q < n$, a contradiction with the choice of n. □

Let us equip $\mathbf{N}_0^m$ with the partial order $\preceq$ defined by

$$(n_1, \ldots, n_m) \preceq (p_1, \ldots, p_m) \qquad \Leftrightarrow \qquad n_i \leq p_i \quad \text{for all } i = 1, \ldots, m\,.$$

Corollary 2.13. *Let $i \in \{1, \ldots, m\}$ and $\mathbf{n} = (n_1, \ldots, n_m)$ be a minimal element of the set*

$$\{(p_1, \ldots, p_m) \in \mathbf{H} : p_i = n_i\}$$

with respect to the partial order $\preceq$. Suppose that $n_i > 0$ and that there exists $j \in \{1, \ldots, m\}$, $j \neq i$, with $n_j > 0$. Then

(1) $\mathbf{n}_i \in \mathbf{G}$;
(2) $n_i = \min\{p \in \mathbf{N} : \mathbf{n}_i + p\mathbf{e}_i \in \mathbf{H}\}$; *in particular n_i is a Weierstrass gap at Q_i.*

Proof. (1) Suppose, on the contrary, that $\mathbf{n}_i \in \mathbf{H}$. Then from Lemma 2.10 applied to $\mathbf{n}_i$ and $\mathbf{n}$, and the hypothesis on n_j, there exists $(p_1, \ldots, p_m) \in \mathbf{H}$ such that $p_i = n_i$, $p_\ell \leq n_\ell$ for $\ell \neq i, j$, and $p_j < n_j$. This is a contradiction to the choice of $\mathbf{n}$.

(2) Let $p \in \mathbf{N}_0$. If $\mathbf{n}_i + p\mathbf{e}_i \in \mathbf{H}$, a similar argument as above implies $n_i \leq p$. Since $n_i > 0$ and $\mathbf{n} \in \mathbf{H}$ then the first part of (2) holds; the second part follows from Corollary 2.11. □

Next we give a bound on the dimension of the sections of the divisors arising from Corollary 2.11.

Lemma 2.14. *Let $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbf{N}_0^m, i, \mathbf{n}_i$, and n be as in Corollary 2.11. Then $\ell(\mathbf{n}_i + n\mathbf{e}_i) \leq g + 1$, where g is the genus of $\mathcal{X}$.*

Proof. Let $G := \sum_{j=1}^m n_j Q_j - n_i Q_i + nQ_i$. If G is a special divisor then $\ell(G) \leq g$; otherwise, by the Riemann-Roch theorem $\ell(G) = \deg(G) + 1 - g$. If $\ell(G) \geq g + 2$, then $\deg(G) \geq 2g + 1$ so that $\deg(G - Q_i - Q_j) \geq 2g - 1$. Then, again by the Riemann-Roch theorem, $\ell(G - Q_i) = \ell(G - Q_i - Q_j) + 1$ for all $j = 1, \ldots, m$. Thus by Lemma 2.2 we get that $\mathbf{n}_i + (n-1)\mathbf{e}_i \in \mathbf{H}$ which is a contradiction with the selection of n. □

Remark 2.15. Let $m \geq 2$ and $i \in \{1, \ldots, m\}$.

(1) Since $\ell(\mathbf{n}_i) = \ell(\mathbf{n}_i - \mathbf{e}_i) + 1$, the elements of the Weierstrass semigroup (resp. Weierstrass gaps) at $Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_m$ are in a one-to-one correspondence with those $\mathbf{n}_i \in \mathbf{N}_0^m$ such that $\mathbf{n}_i \in \mathbf{H}$ (resp. $\mathbf{n}_i \in \mathbf{G}$).

(2) Corollaries 2.11 and 2.13 determine the following surjective function:

$$\Gamma_i : \{\mathbf{n}_i \in \mathbf{N}_0^m : \mathbf{n}_i \in \mathbf{G}\} \to \mathbf{G}(Q_i)\,, \quad \mathbf{n}_i \mapsto \min\{n \in \mathbf{N} : \mathbf{n}_i + n\mathbf{e}_i \in \mathbf{H}\}\,.$$

For $m = 2$, this was already noticed by Kim in [14]. Indeed, here we have a bijection between $\mathbf{G}(Q_1)$ and $\mathbf{G}(Q_2)$:

$$n_1 \in \mathbf{G}(Q_1) \leftrightarrow (n_1, 0) \in \mathbf{G}(Q_1, Q_2) \mapsto \beta_{n_1} := \Gamma_2((n_1, 0)) \in \mathbf{G}(Q_2)\,.$$

Moreover, $n_1 = \min\{p \in \mathbf{N} : (p, \beta_{n_1}) \in \mathbf{H}(Q_1, Q_2)\}$.

For a pair of distinct Weierstrass points Q_1 and Q_2 of the Hermitian curve (i.e., the one in Example 2.7 with $r = q + 1$), Matthews [16, Sect. 4] computed the arithmetical function β_n and consequently $\mathbf{G}(Q_1, Q_2)$; based on these results Homma and Kim [12, Prop. 4.2] computed $\mathbf{G}_0(Q_1, Q_2)$.

3. Goppa codes arising from pure gaps

In this section we improve the Goppa bound on the minimum distance of certain Goppa codes.

Throughout this section $\mathcal{X}$ will be a curve defined over a finite field $\mathbf{F}$. Let us recall the following two results due to Homma and Kim.

Lemma 3.1. ([12, Lemma 3.1]) *Let $B, N,$ and P be $\mathbf{F}$-divisors on $\mathcal{X}$ with B and N effective. Suppose that $\ell(P) = \ell(P - B)$, and that* $\operatorname{Supp}(B) \cap \operatorname{Supp}(N) = \emptyset$. *Then $\ell(P - N) = \ell(P - N - B)$.*

Lemma 3.2. (Dual series trick, [12, Lemma 3.2]) *Let $B, E, L,$ and M be $\mathbf{F}$-divisors on $\mathcal{X}$ with B and E effective. Then* $\deg(B) \leq \deg(E)$ *provided that*:

(1) *$E + L + M$ is a canonical divisor;*
(2) *$\ell(L) = \ell(L + B)$;*
(3) *$\ell(M - B) = \ell(M)$.*

For a given positive integer m such that $\#\mathbf{F} \geq m$ and $\#\mathcal{X}(\mathbf{F}) > m$, we fix m pairwise different $\mathbf{F}$-rational points of $\mathcal{X}$, say $Q_1, \ldots, Q_m$. Let $\mathbf{n} = (n_1, \ldots, n_m)$ and $\mathbf{p} = (p_1, \ldots, p_m)$ be two pure gaps at $Q_1, \ldots, Q_m$. Let n be a positive integer. Set

- $D := P_1 + \ldots + P_n$, where $P_i \neq P_j$ for $i \neq j$, and each point P_i belongs to $\mathcal{X}(\mathbf{F}) \setminus \{Q_1, \ldots, Q_m\}$;
- $F := \sum_{i=1}^{m}(n_i + p_i - 1)Q_i$.

Suppose that $\Omega(F-D)\neq 0$ and let $\mathcal{C}=\mathcal{C}_{\mathcal{X}}(D,F)$ be the $[n,k,d]$ Goppa code defined in the introduction. Let us explain how to use Lemma 3.2 to improve the Goppa bound (1.1) on d.

Let $\eta\in\Omega(F-D)\setminus\{0\}$ and let w be the weight of the word $\mathrm{res}(\eta)$ in $\mathcal{C}$ corresponding to η. Without loss of generality we can assume that $\mathrm{res}_{P_i}(\eta)\neq 0$ for $i=1,\dots,w$ and that η is regular at P_i for $i\geq w+1$. Thus $\eta\in\Omega(F-\sum_{i=1}^{w}P_i)$ and the divisor

$$E:=\mathrm{div}(\eta)-F+\sum_{i=1}^{w}P_i \tag{3.1}$$

is effective with $\deg(E)=2g-2-\deg(F)+w$. Set

$$L:=\sum_{i=1}^{m}(n_i-1)Q_i\,,\quad\text{and}\quad M:=\sum_{i=1}^{m}p_iQ_i-\sum_{i=1}^{w}P_i\,. \tag{3.2}$$

Therefore

$$E+L+M=\mathrm{div}(\eta)$$

is a canonical divisor so that

$$w\geq\deg(F)-(2g-2)+\deg(B)$$

for any $\mathbf{F}$-divisor B which together with the divisors E,L and M defined above satisfy Lemma 3.2. Notice that the above considerations implies the Goppa bound (1.1) with $B=0$.

Theorem 3.3. $d\geq\deg(F)-(2g-2)+m$.

Proof. Let E,L,M be the divisors defined in (3.1) and (3.2). Let $B:=\sum_{i=1}^{m}Q_i$. Then the result will follow from Lemma 3.2 applied to B,E,L and M once we prove that conditions (1), (2), and (3) in that lemma are satisfied. We have already noticed that (1) holds true; from Lemma 2.5(3) we get $\ell(L)=\ell(L+B)$; finally $\ell(M-B)=\ell(B)$ follows from Lemma 3.1 applied to the divisors B above, $N:=\sum_{i=1}^{w}P_i$, and $P:=\sum_{i=1}^{m}p_iQ_i$ since the hypothesis of that lemma is satisfied again by Lemma 2.5(3). □

Under an additional and somewhat stronger hypothesis on pure gaps, the above lower bound can be improved as follows.

Theorem 3.4. *Suppose that $n_i\leq p_i$ for all $i=1,\dots,m$, and that each m-tuple $(q_1,\dots,q_m)$, with $n_i\leq q_i\leq p_i$ for each $i=1,\dots,m$, is also a pure gap at $Q_1,\dots,Q_m$. Then*

$$d\geq\deg(F)-(2g-2)+m+\sum_{i=1}^{m}(p_i-n_i)\,.$$

Proof. Let E, L, M be as in (3.1) and (3.2), and $B := \sum_{i=1}^{m}(p_i - n_i + 1)Q_i$. Then the proof is also a consequence of Lemma 3.2. Let us verify the hypothesis of that lemma. We know already that $E + L + M$ is canonical. Now $L + B = \sum_{i=1}^{m} p_i Q_i$ and so $\ell(L + B) = \ell(L)$ by Lemma 2.5(2)(3). Finally, $\ell(M - B) = \ell(B)$ follows from Lemma 3.1 applied to the divisors B, $N := \sum_{i=1}^{w} P_i$, and $P := \sum_{i=1}^{m} p_i Q_i$. □

4. Examples

In this section we present two examples illustrating Theorems 3.3 and 3.4. In Example 4.1 below we will need to know some elements of the gonality sequence of plane curves; hence we first recall some facts about such a sequence.

Let $\mathcal{X}$ be a curve over a perfect field $\mathbf{F}$. For $i \in \mathbf{N}_0$, let

$$\gamma_i = \gamma_i(\mathcal{X}, \mathbf{F}) := \min\{\deg(D) : D \in \mathrm{Div}_{\mathbf{F}}(\mathcal{X}) \text{ and } \ell(D) \geq i + 1\}.$$

Notice that $\gamma_0 = 0$ and that γ_1 is the $\mathbf{F}$-gonality of $\mathcal{X}$. The $\mathbf{F}$-*gonality sequence of the curve* $\mathcal{X}$ is the sequence $GS(\mathcal{X}) = GS(\mathcal{X}, \mathbf{F}) = (\gamma_i : i \in \mathbf{N}_0)$. This sequence was introduced and used by Yang, Kumar and Stichtenoth to get a lower bound for the weight hierarchy of Goppa codes [20, Thm. 12]. The following properties hold true (see [20, Prop. 11]):

- The sequence $GS(\mathcal{X})$ is strictly increasing;
- $\gamma_{g-1} = 2g - 2$ and $\gamma_i = i + g$ for $i \geq g$, where g is the genus of $\mathcal{X}$.

If $\mathcal{X}$ is plane curve of degree r such that $\mathcal{X}(\mathbf{F}) \neq \emptyset$, Pellikaan [17, Cor. 2.4] noticed that $GS(\mathcal{X})$ is the strictly increasing sequence obtained from the semigroup generated by $r - 1$ and r.

Example 4.1. Let $\mathcal{X}$ be the Hermitian curve over the finite field $\mathbf{F}$ of order q^2; i.e., the Fermat curve of degree $r := q + 1$. This curve has genus $g = q(q - 1)/2$, $(q^3 + 1)$ $\mathbf{F}$-rational points (i.e., it attains the Hasse-Weil upper bound over $\mathbf{F}$), see e.g. [7], and the Weierstrass semigroup at any $\mathbf{F}$-rational point is generated by q and $q + 1$ as follows from Example 2.7. In particular, the strictly increasing sequence obtained from such a semigroup is the $\mathbf{F}$-gonality sequence of $\mathcal{X}$. Let us assume $q > 5$. Thus $\gamma_{g-2r+4} = (r - 5)r$ and $\gamma_{g-2r+5} = (r - 4)(r - 1)$.

Let Q_1, Q_2 and Q_3 be three pairwise different $\mathbf{F}$-rational points of $\mathcal{X}$.

Claim. $\mathbf{n} := ((r-5)r+1, 1, 1)$ *and* $\mathbf{p} := (1, (r-5)r+1, 1)$ *belong to* $\mathbf{G}_0 = \mathbf{G}_0(Q_1, Q_2, Q_3)$.

Indeed, the facts that $\ell(\mathbf{n}) \geq g - 2r + 5$ and $\deg(((r - 5)r + 1)Q_1 + Q_2 + Q_3) < \gamma_{g-2r+5}$ imply $\ell(\mathbf{n}) = g - 2r + 5$. Now $\ell(\mathbf{n} - \mathbf{1}) = \ell((r - 5)rQ_1) = g - 2r + 5$ as $(r - 5)r$ is the $(g - 2r + 4)$-th non-gap at Q_1, and so $\mathbf{n} \in \mathbf{G}_0$ by Lemma 2.5(3). The proof for $\mathbf{p}$ is similar.

Applying Theorem 3.3 with $m = 3$ and $\mathbf{n}$ and $\mathbf{p}$ being as in the claim, we can construct an $[n, k, d]$ Goppa code $\mathcal{C} = \mathcal{C}_{\mathcal{X}}(D, F)$ on the Hermitian curve $\mathcal{X}$ such that

- $n = \deg(D) = q^3 - 2 > \deg(F) = 2r^2 - 10r + 3 = 2q^2 - 6q - 5 > 2g - 2$;
- $k = \dim_{\mathbf{F}}\Omega(F - D) - \dim_{\mathbf{F}}\Omega(F) = g - 1 + \deg(D) - \deg(F)$;
- $d \geq \deg(F) - (2g - 2) + 3 = r^2 - 7r + 6 = q^2 - 5q$.

Next we compare the parameters of $\mathcal{C}$ with those of a one-point Goppa code $\mathcal{C}_\alpha$, $\alpha \in \mathbf{N}$, defined on the Hermitian curve $\mathcal{X}$ as follows. Let us consider the following plane model of $\mathcal{X}$:

$$V^qW + VW^q = U^{q+1}\,.$$

Let $R := (0 : 1 : 0)$ be the unique point of $\mathcal{X}$ on the line $W = 0$, and let $D' := R_1 + \ldots + R_{q^3}$ with $R_i \neq R_j$ for $i \neq j$ and $R_i \in \mathcal{X}(\mathbf{F}) \setminus \{R\}$ for any i. Then $\mathcal{C}_\alpha$ is the Goppa code on $\mathcal{X}$ defined by D' and $F' := (q^3 + 2g - 2 - \alpha)R$. The dimension k_α and minimum distance d_α of $\mathcal{C}_\alpha$ depend on the parameter α and have been computed by Stichtenoth [18] and Yang and Kumar [19]. By observing that $\Omega(F' - D') \cong \mathcal{L}(\alpha R)$ and $\Omega(F') \cong \mathcal{L}((\alpha - q^3)R)$, we get $k_\alpha = \ell(\alpha R) - \ell((\alpha - q^3)R)$. Then

$$k_\alpha = k \quad \text{if and only if} \quad \alpha = \alpha_0 := 2g - 2 + \deg(D) - \deg(F) = q^3 - q^2 + 5q + 1\,.$$

Looking at the tables in [19] we then see that the minimum distance of $\mathcal{C}_{\alpha_0}$ is exactly $q^2 - 5q$. Thus our code $\mathcal{C}$ has better relative parameters k/n and d/n than the corresponding code $\mathcal{C}_{\alpha_0}$.

Remark 4.2. The previous example can also be constructed on a Fermat curve $\mathcal{X}$ of degree $r > 6$ over the finite field $\mathbf{F}$ of order q^2 such that r is a proper divisor of either $(q - 1)$ or $(q + 1)$, and such that $N := \#\mathcal{X}(\mathbf{F})$ is large enough (see below). Here the genus is $g = (r-1)(r-2)/2$, and Example 2.7 shows that there are at least $3r$ $\mathbf{F}$-rational points of $\mathcal{X}$ whose Weierstrass semigroup is generated by $r-1$ and r. Taking three pairwise different such points Q_1, Q_2 and Q_3 we have that $\mathbf{n} = ((r-5)r+1, 1, 1)$ and $\mathbf{p} = (1, (r-5)r+1, 1)$ are pure Weierstrass gaps at Q_1, Q_2 and Q_3. By Theorem 3.3 we obtain an $[n, k, d]$ Goppa code $\mathcal{C} = \mathcal{C}_{\mathcal{X}}(D, F)$ on the Fermat curve $\mathcal{X}$ such that

- $n = \deg(D) = N - 3$, $\deg(F) = 2r^2 - 10r + 3 > 2g - 2$;
- $k = \dim_{\mathbf{F}}\Omega(F - D) - \dim_{\mathbf{F}}\Omega(F) = g - 1 + \deg(D) - \deg(F) + \ell(F - D)$;
- $d \geq \deg(F) - (2g - 2) + 3 = r^2 - 7r + 6$;

provided that

$$\deg(D) = N - 3 > \deg(F) - (g - 1)\,.$$

For instance if r divides $q + 1$, then $\mathcal{X}$ attains the Hasse-Weil upper bound over $\mathbf{F}$; i.e., $N = 1 + q^2 + 2qg$ (see e.g. [8]) and the above bound is satisfied. Unfortunately, there is no available parameters in the literature of one-point Goppa codes on $\mathcal{X}$ that may allow us to assess the parameters of the code $\mathcal{C}$.

Example 4.3. Let $\mathcal{X}$ be the Hermitian curve as in Example 2.7 with $r = q + 1$ defined over the finite field $\mathbf{F}$ of order q^2. Let us assume that q is odd and greater than 5. For b a root of $Y^{q+1} + 1 = 0$, let $Q_1 := (0 : b : 1)$ and let $Q_2, \ldots, Q_{(q+1)/2}$ be $(q - 1)/2$

pairwise different points in the support of the intersection divisor D_∞ of $\mathcal{X}$ and the line $Z=0$. Notice that each point Q_i is $\mathbf{F}$-rational so that the Weierstrass semigroup at Q_i is generated by q and $q+1$.

Let $\mathbf{n} := (n_1,\ldots,n_{(q+1)/2}) \in \mathbf{N}^{(q+1)/2}$ with $1 \le n_1 \le (q-3)/2$, and $n_i = q+2$ for $i=2,\ldots,(q+1)/2$.

Claim. $\mathbf{n}$ *is an pure Weierstrass gap at* $Q_1,\ldots,Q_{(q+1)/2}$.

To see this, by Lemma 2.5 and the Riemann-Roch theorem we have to show that

$$\ell(K-G_2) = \ell(K-G_1) + (q+1)/2\,, \tag{4.1}$$

where K is a canonical divisor on $\mathcal{X}$,

$$G_1 := \sum_{i=1}^{(q+1)/2} n_iQ_i\,, \quad \text{and} \quad G_2 := \sum_{i=1}^{(q+1)/2} (n_i-1)Q_i\,.$$

Here we can assume that $K = (2g-2)Q_1 = (q-2)(q+1)Q_1$ because the Weierstrass semigroup at Q_1 is symmetric. Let us recall that $(q+1)P \sim (q+1)Q$ for any $P,Q \in \mathcal{X}(\mathbf{F})$ due to the fact that $\mathcal{X}$ attains the Hasse-Weil upper bound over $\mathbf{F}$ (see e.g. [4]). Therefore

$$K \sim \frac{q-3}{2}(q+1)Q_1 + \sum_{i=2}^{(q+1)/2}(q+1)Q_i\,,$$

so that

$$K-G_1 \sim ((q-3)(q+1)/2 - n_1)Q_1 - \sum_{i=2}^{(q+1)/2} Q_i\,, \qquad \text{and}$$
$$K-G_2 \sim ((q-3)(q+1)/2-(n_1-1))Q_1\,.$$

The hypothesis on n_1 implies $(q-3)q/2 \le (q-3)(q+1)/2 - n_1 < (q-3)(q+1)/2$ and hence $\ell(((q-3)(q+1)/2-n_1)Q_1) = \ell(\frac{q-3}{2}(q+1)\,Q_1) - n_1 = 1+\ldots+(q-1)/2 - n_1 = (q-1)(q+1)/8-n_1$. This hypothesis also implies $\ell(K-G_2) = (q-1)(q+1)/8-(n_1-1)$. Therefore, (4.1) holds true if and only if

$$\ell(K-G_1) = ((q-1)(q+1)/8-n_1)-(q-1)/2 = \ell(((q-3)(q+1)/2-n_1)Q_1)-(q-1)/2\,.$$

Now $\{f^ig^j : i,j \in \mathbf{N}_0, qi+(q+1)j \le (q-3)(q+1)/2-n_1\}$ is an $\mathbf{F}$-base of $\mathcal{L}((\frac{q-3}{2}(q+1)-n_1)Q_1$, where $f := x/(y-b)$ and $g := 1/(y-b)$, with x and y as in Example 2.7. Then the claim follows from the facts below:

(i) $\mathrm{Supp}(\mathrm{div}_0(f^ig^j)) \cap D_\infty = \emptyset$ if and only if $j=0$ and $i=0,1,\ldots,(q-3)/2$; otherwise $D_\infty \subseteq \mathrm{Supp}(\mathrm{div}_0(f^ig^j))$;

(ii) If $h := \sum_{i=0}^{(q-3)/2} a_if^i \in \mathcal{L}(K-G_1)$ with $a_i \in \mathbf{F}$ for all i, then $h=0$. Indeed, for $i=2,\ldots,(q+1)/2$ let $Q_i = (b_i : 1 : 0)$ where $b_2,\ldots,b_{(q+1)/2}$ are $(q-1)/2$ pairwise different roots of $X^{q+1}+1=0$. The fact that $h(Q_i)=0$ for $i=2,\ldots,(q+1)/2$ lead us to consider the linear equation system $M(a_0,\ldots,a_{(q-3)/2})^t = 0$, where $M=(m_{ij})$

with $m_{ij} = f^j(Q_i) = b_i^j/(1-b)^j$ for $i = 2, \dots, (q+1)/2$ and $j = 0, \dots, (q-3)/2$. We have that $\det(M) = \det(b_i^j)/(1-b)^{(q-3)(q-1)/8}$ is different from zero since $\det(b_i^j) = \prod_{2 \leq i < j \leq (q+1)/2}(b_j - b_i)$ and thus $h = 0$.

Applying Theorem 3.4 with $m = (q+1)/2$, $\mathbf{p} := (1, q+2, \dots, q+2)$, and $\mathbf{q} := ((q-3)/2, q+2, \dots, q+2)$ we can construct a $[n, k, d]$ Goppa code $\mathcal{C} = \mathcal{C}_{\mathcal{X}}(D, F)$ on the Hermitian curve $\mathcal{X}$ such that

- $n = \deg(D) = q^3 - (q-1)/2, n > \deg(F) = q^2 + q - 3 > 2g - 2$;
- $k = \dim_{\mathbf{F}}\Omega(F - D) - \dim_{\mathbf{F}}\Omega(F) = g - 1 + \deg(D) - \deg(F)$;
- $d \geq \deg(F) - (2g-2) + 3 + (q-5)/2 = (5q-1)/2$.

We compare the parameters of the code $\mathcal{C}$ with those of the codes $\mathcal{C}_\alpha$ introduced in Example 4.1. We have that

$$\dim_{\mathbf{F}}\mathcal{C}_\alpha = k \quad \text{if and only if} \quad \alpha = \alpha_0 := 2g - 2 + \deg(D) - \deg(F) = q^3 - (5q-3)/2\,.$$

Looking at the tables in [19] we see that the minimum distance d_{α_0} of $\mathcal{C}_{\alpha_0}$ is 16 for $q = 7$ and $3q$ for $q > 7$. Thus for $q = 7$ we have $d \geq 17$ and hence $\mathcal{C}$ has better parameters than the corresponding $\mathcal{C}_{\alpha_0}$; otherwise, $d_{\alpha_0} - d \leq (q+1)/2$.

References

[1] E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, *Geometry of algebraic curves*, Vol. I, Springer-Verlag (1985).

[2] E. Ballico and S.J. Kim, Weierstrass multiple loci of n-pointed algebraic curves, *J. Algebra*, Vol. 199 (1998) pp. 455–471.

[3] F. Delgado, The symmetry of the Weierstrass generalized semigroups and affine embeddings, *Proc. Amer. Math. Soc.*, Vol. 108 (1990) pp. 627–631.

[4] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.*, Vol. 89 (1996) pp. 103–106.

[5] A. Garcia, S.J. Kim and R. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, *J. Pure Appl. Algebra*, Vol. 84 (1993) pp. 199–207.

[6] A. Garcia and R. Lax, *Goppa codes and Weierstrass gaps*, Lectures Notes in Math., Springer-Verlag, Berlin-Heidelberg Vol. 1518 (1992) pp. 33–42.

[7] A. Garcia and P. Viana, Weierstrass points on certain non-classical curves, *Arch. Math.*, Vol. 46 (1986) pp. 315–322.

[8] A. Garcia and J.F. Voloch, Fermat curves over finite fields, *J. Number Theory*, Vol. 30 (1988) pp. 345–356.

[9] V.D. Goppa, Algebraic-Geometric codes, *Math. USRR-Izv.*, Vol 21 (1983) pp. 75–93.

[10] V.D. Goppa, *Geometry and codes*, Kluwer Academic Publishers (1983).

[11] M. Homma, The Weierstrass semigroup of a pair of points on a curve, *Arch. Math.*, Vol. 67 (1996) pp. 337–348.

[12] M. Homma and S.J. Kim, Goppa codes with Weierstrass pairs, *J. Pure Appl. Algebra*, Vol. 162 (2001) pp. 273–290.

[13] N. Ishii, A certain graph obtained from a set of several points on a Riemann surface, *Tsukuba J. Math.*, Vol. 23 (1999), 55–89.

[14] S.J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve, *Arch. Math.*, Vol. 62 (1994) pp. 73–82.

[15] S.J. Kim and J. Komeda, The Weierstrass semigroup of a pair of Galois Weierstrass points with prime degree on a curve, *preprint* (2001).

[16] G.L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, *Designs Codes Cryptogr.*, Vol. 22 (2001) pp. 107–221.

[17] R. Pellikaan, On special divisors and the two variable zeta function of algebraic curves over finite fields, In *Proceedings AGCT-4, Luminy*, (1997) pp. 175–184.

[18] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inform. Theory*, Vol. 34 (1988) pp. 1345–1348.

[19] K. Yang and P.V. Kumar, *On the true minimum distance of Hermitian codes*, Lectures Notes in Math., Springer-Verlag, Berlin-Heidelberg Vol. 1518 (1992) pp. 99–107.

[20] K. Yang, P.V. Kumar and H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, *IEEE Trans. Inform. Theory*, Vol. 40 (1994) pp. 913–920.

Universidade Federal de Uberlândia, Faculdade de Matemática, Av. J.N. de Ávila 2160, 38408-100 Uberlândia – MG, Brasil

E-mail address: cicero@ufu.br

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil

E-mail address: ftorres@ime.unicamp.br

Current Address: Departamento de Algebra, Geometría y Topología, Facultad de Ciencias - Universidad de Valladolid, c/ Prado de la Magdalena s/n 47005, Valladolid (Spain)

E-mail address: ftorres@agt.uva.es