Two-Point Codes for the Generalized GK Curve

Elise Barelli, Peter Beelen, Mrinmoy Datta, Vincent Neiger, Johan Rosenkilde

TWO-POINT CODES FOR THE GENERALISED GK CURVE

ÉLISE BARELLI, PETER BEELEN, MRINMOY DATTA, VINCENT NEIGER, JOHAN ROSENKILDE

Abstract. We improve previously known lower bounds for the minimum distance of certain two-point AG codes constructed using a Generalized Giulietti–Korchmaros curve (GGK). Castellanos and Tizziotti recently described such bounds for two-point codes coming from the Giulietti–Korchmaros curve (GK). Our results completely cover and in many cases improve on their results, using different techniques, while also supporting any GGK curve. Our method builds on the order bound for AG codes: to enable this, we study certain Weierstrass semigroups. This allows an efficient algorithm for computing our improved bounds. We find several new improvements upon the MinT minimum distance tables.

1. Introduction

Algebraic geometry (AG) codes are a class of linear codes constructed from algebraic curves defined over a finite field. This class continues to provide examples of good codes when considering their basic parameters: the length n, the dimension k, and the minimum distance d. If the algebraic curve used to construct the code has genus g, the minimum distance d satisfies the inequality $d \geq n - k + 1 - g$. This bound, a consequence of the Goppa bound, implies that the minimum distance of an AG code can be designed. It is well known that the Goppa bound is not necessarily tight, and there are various results and techniques which can be used to improve upon it in specific cases. Such a result has been given in [15, Thm. 2.1], where the Goppa bound is improved by one. Another approach to give lower bounds on the minimum distance of AG codes is described in [13] and the references therein. This type of lower bound is often called the *order bound*; various refinements and generalizations have been given, for example in [3, 6].

To obtain good AG codes, the choice of the algebraic curve in the construction plays a key role. A very good class of curves are the so-called maximal curves, i.e., algebraic curves defined over a finite field having as many rational points as allowed by the Hasse–Weil bound. More precisely, a maximal curve of genus g defined over a finite field $\mathbb{F}_q$ with q elements, has $q + 1 + 2\sqrt{q}g$ $\mathbb{F}_q$-rational points, i.e., points defined over $\mathbb{F}_q$; this only makes sense if the cardinality q is a square number. An important example of a maximal curve is the Hermitian curve, but recently other maximal curves have been described [11, 9], often called the *generalized Giulietti–Korchmáros (GK) curves*. In this article we continue the study of two-point AG codes coming from the generalized GK curves that was initiated in [5]. However, rather than using the improvement

Élise Barelli is partially supported by a DGA-MRIS scholarship and a French ANR-15-CE39-0013-01 "Manta". Peter Beelen gratefully acknowledges the support by The Danish Council for Independent Research (Grant No. DFF–4002-00367). Vincent Neiger has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement number 609405 (COFUNDPostdocDTU). Mrinmoy Datta is supported by The Danish Council for Independent Research (Grant No. DFF6108-00362).

Élise Barelli is with INRIA Saclay and LIX, École Polytechnique, 91120 Palaiseau Cedex, France (e-mail: elise.barelli@inria.fr). Peter Beelen, Mrinmoy Datta, Vincent Neiger, and Johan Rosenkilde are with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark (e-mails: pabe@dtu.dk, mrinmoy.dat@gmail.com, jsrn@dtu.dk). Vincent Neiger is also with XLIM, Université de Limoges, 87060 Limoges Cedex, France (e-mail: vincent.neiger@unilim.fr).

upon the Goppa bound from [15], we use the order bound as given in [3]. As a matter of fact, we also show that the order bound from [3] implies Theorem 2.1 in [15]. Thus, we will automatically recover all the results in [5], but on various occasions we obtain better bounds for the minimum distance than the ones reported in [5]. We will also paraphrase the order bound from [3] and explain how we have computed it. A key object in this computation is a two-point generalization of a Weierstrass semigroup given in [4], and therefore some time will be used to describe this semigroup explicitly in the case of certain pairs of points on the generalized GK curve.

After finishing this work, we were made aware of the contemporaneous work [14]. In [14] multi-point codes and their duals from the generalized GK function field are constructed and investigated. Proposition 4.3 is different from, but akin to [14, Thm. 2] and similar proof techniques were used. The techniques used in [14] to analyse the code parameters are very different from ours and more related to the ones used in [5]. Our main tools, the explicit computation of the map $\tau_{0,\infty}$ in Corollary 3.6 and the resulting algorithm to compute the order bound, were not employed in [14]. Our improvements on the MinT code tables are not present in [14].

2. Preliminaries

Though later we will only consider the generalized GK curves, we will in this section consider any algebraic curve χ defined over a finite field $\mathbb{F}_q$. The field of functions on χ, or briefly the function field of χ, will be denoted by $\mathbb{F}_q(\chi)$, while the genus of χ is denoted by $g(\chi)$. Rather than using the language of curves, we will formulate the theory using the language of function fields; see [17] for more details. In particular, we will speak about places of $\mathbb{F}_q(\chi)$ rather than points of χ. For any place Q of $\mathbb{F}_q(\chi)$, we denote by v_Q the valuation map at the place Q. The valuation $v_Q : \mathbb{F}_q(\chi) \setminus \{0\} \to \mathbb{Z}$ sends a nonzero function f to its order of vanishing at Q. If $v_Q(f) < 0$, one also says that f has a pole of order $-v_Q(f)$ at Q.

A divisor of $\mathbb{F}_q(\chi)$ is a finite formal sum $\sum_i n_i Q_i$ of places Q_i of $\mathbb{F}_q(\chi)$, where the n_i's are integers in $\mathbb{Z}$. The support of a divisor $\sum_i n_i Q_i$ is the (finite) set of places $\{Q_i \mid n_i \neq 0\}$. Finally, we call two divisors disjoint if they have disjoint supports. To any nonzero function $f \in \mathbb{F}_q(\chi)$ one can associate two divisors (f) and $(f)_\infty$ known as the divisor of f and the divisor of poles of f respectively, given by:

$$(f) := \sum_Q v_Q(f)\, Q \quad \text{and} \quad (f)_\infty := \sum_{Q; v_Q(f)<0} -v_Q(f)\, Q.$$

If all the coefficients n_i in a divisor $G = \sum_i n_i Q_i$ are nonnegative, we call G an effective divisor; notation $G \geq 0$.

We now recall some notations for AG codes; we again refer to [17] for a more comprehensive exposition. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct rational places of $\mathbb{F}_q(\chi)$, i.e., places of degree 1, and define the divisor $D = P_1 + \cdots + P_n$. Further let G be a divisor such that $\deg(G) < n$ and G does not contain any place of $\mathcal{P}$. We consider the following map:

$$\begin{array}{rccc} Ev_{\mathcal{P}} : & \mathbb{F}_q(\chi)_{\mathcal{P}} & \longrightarrow & \mathbb{F}^n \\ & f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

Here $\mathbb{F}_q(\chi)_{\mathcal{P}}$ denotes the subset of $\mathbb{F}_q(\chi)$ consisting of functions not having a pole at any $P \in \mathcal{P}$. Then we define the AG code $C_L(D,G)$ by $C_L(D,G) := \{Ev_{\mathcal{P}}(f) \mid f \in L(G)\}$. Here $L(G)$ denotes the Riemann–Roch space $L(G) := \{f \in \mathbb{F}_q(\chi) \setminus \{0\} \mid (f) + G \geq 0\} \cup \{0\}$. It is well known that the minimum distance d of $C_L(D,G)$ (resp. $C_L(D,G)^\perp$) satisfies the Goppa bound $d \geq n - \deg(G)$ (resp. $d \geq \deg(G) - 2g(\chi) + 2$).

Here, we will make use of another lower bound for the minimum distance of $C_L(D,G)^\perp$, obtained in [3]. We will use the notions of G-gaps and G-non-gaps at a place Q, which were for example also used in [10].

Definition 2.1. *Let Q be a rational place and G be a rational divisor of $\mathbb{F}_q(\chi)$. We define $L(G+\infty Q) := \bigcup_{i\in\mathbb{Z}} L(G+iQ)$ and*

$$H(Q;G) := \{-v_Q(f) \mid f \in L(G+\infty Q)\setminus\{0\}\}.$$

*We call $H(Q;G)$ the set of G-*non-gaps at Q*. The set*

$$\Gamma(Q;G) := \mathbb{Z}_{\geq v_Q(G)-\deg(G)} \setminus H(Q;G)$$

*is called the set of G-*gaps at Q*.*

Note that if $G=0$ we obtain $H(Q;0)=H(Q)$, the Weierstrass semigroup of Q, and $\Gamma(Q;0)=\Gamma(Q)$, the set of gaps at Q. Further, note that if $i\in H(Q;F_1)$ and $j\in H(Q;F_2)$, then $i+j\in H(Q;F_1+F_2)$. Finally, observe that the theorem of Riemann–Roch implies that the number of G-gaps at Q coincides with the genus of χ, that is, $|\Gamma(Q;G)|=g(\chi)$.

Remark 2.2. If $i<-\deg(G)$ then $\deg(G+iQ)<0$ and $L(G+iQ)=\{0\}$. So in the previous definition we can write $L(G+\infty Q)=\bigcup_{i\geq -\deg(G)} L(G+iQ)$. Further, note that for any $a\in\mathbb{Z}$ we have $L(G+aQ+\infty Q)=L(G+\infty Q)$ and hence $H(Q;G+aQ)=H(Q;G)$ as well as $\Gamma(Q;G+aQ)=\Gamma(Q;G)$. ◊

Definition 2.3. *Let Q be a rational place and let F_1, F_2 be two divisors of χ. As in* [3] *we define*

$$N(Q;F_1,F_2) := \{(i,j)\in H(Q;F_1)\times H(Q;F_2) \mid i+j=v_Q(G)+1\},$$
$$\nu(Q;F_1,F_2) := |N(Q;F_1,F_2)|.$$

Proposition 2.4. [3, Prop. 4] *Let $D=P_1+\cdots+P_n$ be a divisor that is a sum of n distinct rational places of $\mathbb{F}_q(\chi)$, Q be a rational place not occurring in D, and F_1, F_2 be two divisors disjoint from D. Suppose that $C_L(D,F_1+F_2)\neq C_L(D,F_1+F_2+Q)$. Then, for any codeword $c\in C_L(D,F_1+F_2)^\perp\setminus C_L(D,F_1+F_2+Q)^\perp$, we have*

$$w_H(c)\geq \nu(Q;F_1,F_2).$$

In particular, the minimum distance $d(F_1+F_2)$ of $C_L(D,F_1+F_2)^\perp$ satisfies

$$d(F_1+F_2)\geq \min\{\nu(Q;F_1,F_2), d(F_1+F_2+Q)\},$$

where $d(F_1+F_2+Q)$ denotes the minimum distance of $C_L(D,F_1+F_2+Q)^\perp$.

To arrive at a lower bound for the minimum distance of $C_L(D,G)^\perp$, one applies this proposition in a recursive manner. More precisely, one constructs a sequence $Q^{(1)},\ldots,Q^{(N)}$ of not necessarily distinct rational places, none occurring in D, such that $C_L(D,G+Q^{(1)}+\cdots+Q^{(N)})^\perp=0$. Such a sequence exists, since the theorem of Riemann–Roch implies that $C_L(D,G+Q^{(1)}+\cdots+Q^{(N)})=\mathbb{F}_q^n$ as soon as $N\geq 2g(\chi)-1+n-\deg(G)$. Then, the code $C_L(D,G)^\perp$ has for example minimum distance at least $\min \nu(Q^{(i)};G+Q^{(1)}+\cdots+Q^{(i-1)},0)$, where the minimum is taken over all i satisfying $1\leq i\leq N$ and $C_L(D,G+Q^{(1)}+\cdots+Q^{(i-1)})\neq C_L(D,G+Q^{(1)}+\cdots+Q^{(i)})$.

The well known Goppa bound is a direct consequence of Proposition 2.4 as shown in [3, Lem. 9]. We will need the following slightly more general version of [3, Lem. 9].

Lemma 2.5. *Let $D=P_1+\cdots+P_n$ be a sum of distinct rational places, let Q be a rational place not occurring in D, and let F_1,F_2 be two divisors disjoint from D. Then $\nu(Q;F_1,F_2)\geq \deg(F_1+F_2)-2g+2$.*

Proof. Define the formal Laurent series

$$p_{Q;F_1}(t) := \sum_{i\in H(Q;F_1)} t^i \qquad \text{and} \qquad p_{Q;F_2}(t) := \sum_{i\in H(Q;F_2)} t^i.$$

Then $\nu(Q; F_1, F_2)$ is the coefficient of $t^{v_Q(F_1+F_2)+1}$ in the Laurent series $p_{Q;F_1}(t) \cdot p_{Q;F_2}(t)$. The lemma follows by analyzing this product carefully. First we introduce

$$q_{Q;F_1}(t) := \sum_{i \in \Gamma(Q;F_1)} t^i \qquad \text{and} \qquad q_{Q;F_2}(t) := \sum_{i \in \Gamma(Q;F_2)} t^i.$$

Then

$$p_{Q;F_1}(t) + q_{Q;F_1}(t) = \frac{t^{v_Q(F_1)-\deg(F_1)}}{1-t} \qquad \text{and} \qquad p_{Q;F_2}(t) + q_{Q;F_2}(t) = \frac{t^{v_Q(F_2)-\deg(F_2)}}{1-t},$$

implying that

$$p_{Q;F_1}(t) \cdot p_{Q;F_2}(t) = t^{v_Q(F_1+F_2)-\deg(F_1+F_2)} \left(\frac{1}{(1-t)^2} - \frac{2g(\chi)}{1-t} \right.$$
$$\left. + \frac{g(\chi) - t^{-v_Q(F_2)+\deg(F_2)} q_{Q;F_2}(t)}{1-t} + \frac{g(\chi) - t^{-v_Q(F_1)+\deg(F_1)} q_{Q;F_1}(t)}{1-t} \right) + q_{Q;F_1}(t) \cdot q_{Q;F_2}(t).$$

Since both $t^{-v_Q(F_1)+\deg(F_1)} q_{Q;F_1}(t)$ and $t^{-v_Q(F_2)+\deg(F_2)} q_{Q;F_2}(t)$ are a sum of $g(\chi)$ distinct nonnegative powers of t, the last three Laurent series in the above expression are in fact finite Laurent series with nonnegative coefficients. Hence the coefficient of $t^{v_Q(F_1+F_2)+1}$ in $p_{Q;F_1}(t) \cdot p_{Q;F_2}(t)$ is bounded from below by the corresponding coefficient in

$$t^{v_Q(F_1+F_2)-\deg(F_1+F_2)} \left(1/(1-t)^2 - 2g(\chi)/(1-t)\right),$$

which is $\deg(F_1 + F_2) - 2g(\chi) + 2$. □

In this paper, we are interested in a lower bound on the minimum distance for two-point AG codes. We will typically apply Proposition 2.4 to the special setting where $F_1 = 0$ and $F_2 = G = a_1Q_1 + a_2Q_2$, with Q_1, Q_2 two rational places of $\mathbb{F}_q(\chi)$. Hence we want to compute $\nu(Q; G) := \nu(Q; 0, G)$ where $G = a_1Q_1 + a_2Q_2$. Furthermore, we will only consider the case where $Q \in \{Q_1, Q_2\}$. In order to compute the number $\nu(Q; G)$, we need to know the Weierstrass semigroup $H(Q)$ and the set $H(Q; G)$ of G-non-gaps at Q. A very practical object in this setting is a two-point generalization of the Weierstrass semigroup and a map between two Weierstrass semigroups considered in [4]:

Definition 2.6. *Let Q_1, Q_2 be two distinct rational places of $\mathbb{F}_q(\chi)$. We define $R(Q_1, Q_2) := \{f \in \mathbb{F}_q(\chi) \mid \mathrm{Supp}((f)_\infty) \subseteq \{Q_1, Q_2\}\}$, the ring of functions on χ that are regular outside the points Q_1 and Q_2. The two-point Weierstrass semigroup of Q_1 and Q_2 is then defined as:*

$$H(Q_1, Q_2) := \{(n_1, n_2) \in \mathbb{Z}^2 \mid \exists f \in R(Q_1, Q_2) \setminus \{0\},\ v_{Q_i}(f) = -n_i, i \in \{1, 2\}\}.$$

Further we define the following map:

$$\begin{array}{rccl} \tau_{Q_1,Q_2}: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & i & \longmapsto & \min\{j \mid (i, j) \in H(Q_1, Q_2)\}. \end{array}$$

Remark 2.7. Note that $H(Q_1, Q_2) \subseteq \{(i, j) \in \mathbb{Z}^2 \mid i + j \geq 0\}$, since $L(iQ_1 + jQ_2) = \{0\}$ if $i + j < 0$. In particular, we have for any $i \in \mathbb{Z}$ that $\tau_{Q_1,Q_2}(i) \geq -i$. Moreover, the theorem of Riemann–Roch implies that $\tau_{Q_1,Q_2}(a_1) \leq 2g(\chi) - a_1$. ◊

Proposition 2.8. [4, Prop. 14] *Let Q_1, Q_2 be two distinct rational places of $\mathbb{F}_q(\chi)$. The map τ_{Q_1,Q_2} is bijective and $\tau^{-1}_{Q_1,Q_2} = \tau_{Q_2,Q_1}$.*

By the definitions of τ_{Q_1,Q_2} and $H(Q_1, Q_2)$, for all $i \in \mathbb{Z}$ there exists a function $f^{(i)}_{Q_1,Q_2} \in R(Q_1, Q_2)$ such that $v_{Q_1}(f^{(i)}_{Q_1,Q_2}) = -i$ and $v_{Q_2}(f^{(i)}_{Q_1,Q_2}) = -\tau_{Q_1,Q_2}(i)$. Since τ_{Q_1,Q_2} is a bijection, the functions $f^{(i)}_{Q_1,Q_2}$ have distinct pole orders at Q_1 as well as Q_2.

Theorem 2.9. *Let Q_1, Q_2 be two distinct rational places of χ and $a_1, a_2 \in \mathbb{Z}_{\geq 0}$. The Riemann–Roch space $L(a_1Q_1 + a_2Q_2)$ has dimension $|\{i \leq a_1 \mid \tau_{Q_1,Q_2}(i) \leq a_2\}|$ and basis*

$$\{f^{(i)}_{Q_1,Q_2} \mid i \leq a_1 \text{ and } \tau_{Q_1,Q_2}(i) \leq a_2\}.$$

Proof. Consider the filtration of $\mathbb{F}$-vector spaces:

$$L(a_1Q_1+a_2Q_2) \supseteq L((a_1-1)Q_1+a_2Q_2) \supseteq \cdots \supseteq L(-a_2Q_1+a_2Q_2) \supseteq L(-(a_2+1)Q_1+a_2Q_2) = \{0\}.$$

For $-a_2 \leq i \leq a_1$, the strict inequality $\ell(iQ_1 + a_2Q_2) > \ell((i-1)Q_1 + a_2Q_2)$ holds if and only if there exists a function $f \in \mathbb{F}_q(\chi)$ such that $(f)_\infty = iQ_1 + jQ_2$ with $j \leq a_2$. Such a function exists if and only if $\tau_{Q_1,Q_2}(i) \leq a_2$. Hence, $\ell(a_1Q_1 + a_2Q_2) = |\{-a_2 \leq i \leq a_1 \mid \tau_{Q_1,Q_2}(i) \leq a_2\}|$. Since $\tau_{Q_1,Q_2}(i) \geq -i$, we see that $\ell(a_1Q_1 + a_2Q_2) = |\{i \leq a_1 \mid \tau_{Q_1,Q_2}(i) \leq a_2\}|$ as was claimed.

A basis for $L(a_1Q_1 + a_2Q_2)$ can be directly derived from the above, since the set

$$\{f^{(i)}_{Q_1,Q_2} \mid i \leq a_1 \text{ and } \tau_{Q_1,Q_2}(i) \leq a_2\}$$

is a subset of $L(a_1Q_1 + a_2Q_2)$ consisting of $\ell(a_1Q_1 + a_2Q_2)$ linearly independent functions. Note that the linear independence follows from the fact the functions have mutually distinct pole orders at Q_1. □

A direct corollary is an explicit description of the $(a_1Q_1 + a_2Q_2)$-gaps and non-gaps at Q_1.

Corollary 2.10. *Let $G = a_1Q_1 + a_2Q_2$. Then the set of G-non-gaps at Q_1 is given by*

$$\{a \in \mathbb{Z} \mid \tau_{Q_1,Q_2}(a) \leq a_2\}$$

and the set of G-non-gaps at Q_2 is given by

$$\{b \in \mathbb{Z} \mid \tau^{-1}_{Q_1,Q_2}(b) \leq a_1\}.$$

Proof. The first part follows directly from the previous theorem by considering basis of $L(aQ_1 + a_2Q_2)$ for a tending to infinity. Reversing the roles of Q_1 and Q_2, the second part follows. □

This corollary implies that for $G = a_1Q_1 + a_2Q_2$, it is not hard to compute the G-gaps at either Q_1 or Q_2 once the bijection τ_{Q_1,Q_2} can be computed efficiently. We show in an example that this does occur in a particular case. Moreover, in the next section we will give a very explicit description of τ_{Q_1,Q_2} for a family of function fields and pairs of rational points Q_1 and Q_2.

Example 2.11. The Hermitian curve $\mathcal{H}$ is the curve defined over $\mathbb{F}_{q^2}$ by the equation $x^q + x = y^{q+1}$. The corresponding function field $\mathbb{F}_{q^2}(\mathcal{H})$ is called the Hermitian function field. For any two distinct rational places Q_1 and Q_2 of $\mathbb{F}_{q^2}(\mathcal{H})$, the map τ_{Q_1,Q_2} satisfies $\tau_{Q_1,Q_2}(i) = -iq$ for $q \leq i \leq 0$. Since furthermore $\tau_{Q_1,Q_2}(i+q+1) = \tau_{Q_1,Q_2}(i) - (q+1)$ for any $i \in \mathbb{Z}$, this describes τ_{Q_1,Q_2} completely. See [4] for more details. This example also appears as a special case in the next section. ◊

3. The generalized Giulietti–Korchmáros function field

Let $e \geq 1$ be an odd integer. We consider the generalized Giulietti–Korchmáros (GK) curve χ_e, also known as the Garcia–Güneri–Stichtenoth curve [9]. It is defined over the finite field $\mathbb{F}_{q^{2e}}$ by the equations

$$x^q + x = y^{q+1} \text{ and } z^{\frac{q^e+1}{q+1}} = y^{q^2} - y.$$

This is a maximal curve when considered over the finite field $\mathbb{F}_{q^{2e}}$. Indeed, its genus and number of rational points are

$$g(\chi_e) := (q-1)(q^{e+1} + q^e - q^2)/2,$$
$$N_e := q^{2e+2} - q^{e+3} + q^{e+2} + 1.$$

As before, we will use the language of function fields and denote the corresponding function field $\mathbb{F}_{q^{2e}}(\chi_e)$ as the generalized GK function field. For $e = 1$ one simply obtains the Hermitian function field $\mathbb{F}_{q^2}(\mathcal{H})$, while for $e = 3$, one obtains what is known as the Giulietti–Korchmáros function field [11].

The function $x \in \mathbb{F}_{q^{2e}}(\chi_e)$ has exactly one zero and one pole, which we will denote by Q_0 and Q_∞ respectively. The functions y and z also have a pole at Q_∞ only. For a given rational place P of $\mathbb{F}_{q^{2e}}(\chi_e)$ different from Q_∞, we call $(x(P), y(P), z(P)) \in \mathbb{F}_{q^{2e}}^3$ the coordinates of P. For the function field $\mathbb{F}_{q^{2e}}(\chi_e)$, rational places are uniquely determined by their coordinates. A place with coordinates $(a, b, c) \in \mathbb{F}_{q^{2e}}^3$ will be denoted by $P_{(a,b,c)}$. In particular, we have $Q_0 = P_{(0,0,0)}$.

With these notations, we can express the divisors of x, y and z as follows:

$$\begin{aligned}(x) &= (q^e+1)(Q_0 - Q_\infty),\\ (y) &= \sum_{\substack{a\in\mathbb{F}_q\\ a^q+a=0}} \frac{q^e+1}{q+1} P_{(a,0,0)} \;-\; q\frac{q^e+1}{q+1} Q_\infty,\\ (z) &= \sum_{\substack{(a,b)\in\mathbb{F}_{q^2}\\ a^q+a=b^{q+1}}} P_{(a,b,0)} \;-\; q^3 Q_\infty.\end{aligned}$$

In each summation, the point $P_{(0,0,0)} = Q_0$ occurs. For future reference we also note that for $k \in \mathbb{Z}$ and $\ell \geq 0, m \geq 0$ we have

$$(1) \qquad (x^k y^\ell z^m) = \left(k(q^e+1) + \ell\frac{q^e+1}{q+1} + m\right) Q_0 - \left(k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3\right) Q_\infty + E,$$

with E an effective divisor with support disjoint from $\{Q_0, Q_\infty\}$. The above information is enough to determine that $H(Q_\infty)$, the Weierstrass semigroup of Q_∞, is generated by $q^3, q\frac{q^e+1}{q+1}$ and q^e+1.

Theorem 3.1 ([12], Cor.3.5)**.** *We have* $H(Q_\infty) = \left\langle q^3,\, q\frac{q^e+1}{q+1},\, q^e+1 \right\rangle$.

A direct consequence of this theorem is a description of $\Gamma(Q_\infty)$, the set of gaps of $H(Q_\infty)$.

Corollary 3.2. *The set* $\Gamma(Q_\infty)$ *of gaps of* $H(Q_\infty)$ *is given by*

$$\left\{ k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3 \;\middle|\; 0 \leq \ell \leq q, 0 \leq m < \frac{q^e+1}{q+1}, k < 0, k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3 \geq 0 \right\}.$$

Proof. Any integer can uniquely be written in the form $k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3$, with k, ℓ and m integers satisfying $0 \leq \ell \leq q, 0 \leq m < \frac{q^e+1}{q+1}$. To be an element of $H(Q_\infty)$ the additional requirement is simply that $k \geq 0$. Since $\Gamma(Q_\infty) = \mathbb{N} \setminus H(Q_\infty)$, the corollary follows. □

We now give a further consequence of Theorem 3.1: a complete description of the ring of functions that are regular outside Q_∞; that is to say, the functions having no poles except possibly at Q_∞. The next result follows directly from the similar statement in [12, Prop. 3.4].

Corollary 3.3. *The ring* $R(Q_\infty)$ *of functions in* $\mathbb{F}_{q^{2e}}(\chi_e)$ *regular outside* Q_∞ *is given by* $\mathbb{F}_{q^{2e}}[x, y, z]$.

For the AG codes that we wish to study, we in fact need to understand a larger ring of functions, allowing functions that may have a pole in Q_∞ as well as Q_0. An explicit description of this ring is given in the following corollary.

Corollary 3.4. *The ring $R(Q_0, Q_\infty)$ of functions in $\mathbb{F}_{q^{2e}}(\chi_e)$ regular outside $\{Q_0, Q_\infty\}$ is given by $\mathbb{F}_{q^{2e}}[x, x^{-1}, y, z]$.*

Proof. It is clear from Eq. (1) that any function in $\mathbb{F}_{q^{2e}}[x, x^{-1}, y, z]$ is regular outside $\{Q_0, Q_\infty\}$. Conversely, if a function f has no pole outside $\{Q_0, Q_\infty\}$, then for a suitably chosen exponent k, the function $x^k f$ has no pole outside Q_∞. Hence $x^k f \in R(Q_\infty)$. Corollary 3.3 implies that $f \in \mathbb{F}_{q^{2e}}[x, x^{-1}, y, z]$. □

Corollary 3.4 implies that the ring $R(Q_0, Q_\infty)$ has a natural module structure over $\mathbb{F}_{q^{2e}}[x, x^{-1}]$. When viewed as such a module, $R(Q_0, Q_\infty)$ is free of rank $q^e + 1$ with basis $y^\ell z^m$ where $0 \le \ell < q+1$ and $0 \le m < \frac{q^e+1}{q+1}$. For $e = 1$, the above theorem and the mentioned consequences are well known. For $e = 3$, these results are contained in [11, 7].

We now turn to the study of the two-point Weierstrass semigroup $H(Q_0, Q_\infty)$. We will determine this semigroup completely. Equation (1) will be used to describe the functions $f^{(i)}_{Q_0,Q_\infty}$, resp. the bijection τ_{Q_0,Q_∞}. For convenience, we will use the more compact notation $f^{(i)}_{0,\infty}$, resp. $\tau_{0,\infty}$. Similarly we write $\tau^{-1}_{0,\infty} = \tau_{\infty,0}$.

Theorem 3.5. *Let $i \in \mathbb{Z}$ and write $i = -k(q^e+1) - \ell\frac{q^e+1}{q+1} - m$ for a triple $(k, \ell, m) \in \mathbb{Z}^3$ satisfying $0 \le \ell < q+1$ and $0 \le m < \frac{q^e+1}{q+1}$. Then $f^{(i)}_{0,\infty} = x^k y^\ell z^m$.*

Proof. By definition of $f^{(i)}_{0,\infty}$ we have $-v_{Q_0}(f_i) = i$ and $v_{Q_\infty}(f_i) = \tau_{0,\infty}(i)$. Suppose $f^{(i)}_{0,\infty}$ cannot be chosen as a monomial in x^{-1}, x, y and z. Since by Corollary 3.4 we have $f^{(i)}_{0,\infty} \in \mathbb{F}_{q^{2e}}[x, x^{-1}, y, z]$ we can write

$$f^{(i)}_{0,\infty} = \sum_{\alpha=-N}^{M} \sum_{\beta=0}^{q} \sum_{\gamma=0}^{\frac{q^e-q}{q+1}} a_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma,$$

for integers N, M and constants $a_{k\ell m} \in \mathbb{F}_{q^{2e}}$. Note that the pole orders at Q_0 of each of the occurring monomials $x^\alpha y^\beta z^\gamma$ are distinct. Since $-v_{Q_0}(f^{(i)}_{0,\infty}) = i$, this implies that there exists a uniquely determined triple (k, ℓ, m) such that $a_{k\ell m} \neq 0$ and $i = -k(q^e+1) - \ell\frac{q^e+1}{q+1} - m$, while for all other monomials $x^\alpha y^\beta z^\gamma$ occurring in $f^{(i)}_{0,\infty}$ we have

$$-\alpha(q^e+1) - \beta\frac{q^e+1}{q+1} - \gamma < i.$$

Likewise, the pole orders at Q_∞ of all of the occurring monomials $x^\alpha y^\beta z^\gamma$ are distinct. Since $-v_{Q_\infty}(f^{(i)}_{0,\infty}) = \tau_{0,\infty}(i)$ there exists a uniquely determined triple (k', ℓ', m') such that $a_{k'\ell'm'} \neq 0$ and $\tau_{0,\infty}(i) = k'(q^e+1) + \ell' q\frac{q^e+1}{q+1} + m'q^3$, while for all other monomials $x^\alpha y^\beta z^\gamma$ occurring in $f^{(i)}_{0,\infty}$ we have

$$\alpha(q^e+1) + \beta q\frac{q^e+1}{q+1} + \gamma q^3 < \tau_{0,\infty}(i).$$

If $(k, \ell, m) \neq (k', \ell', m')$, the monomial $x^k y^\ell z^m$ would have pole order i in Q_0, but pole order strictly less than $\tau_{0,\infty}(i)$ in Q_∞, which gives a contradiction by the definition of $\tau_{0,\infty}$. Hence we may take $f^{(i)}_{0,\infty} = x^k y^\ell z^m$. □

Corollary 3.6. *Let $i \in \mathbb{Z}$, and let $(k, \ell, m) \in \mathbb{Z}^3$ be the unique triple such that $0 \le \ell < q+1$, $0 \le m < \frac{q^e+1}{q+1}$ and $i = -k(q^e+1) - \ell\frac{q^e+1}{q+1} - m$. Then*

$$\tau_{0,\infty}(i) = k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3.$$

Proof. For a given $i \in \mathbb{Z}$, the proof of Theorem 3.5 implies that $f_{0,\infty}^{(i)} = x^k y^\ell z^m$ for a uniquely determined triple $(k, \ell, m) \in \mathbb{Z}^3$ such that $-i = k(q^e+1)+\ell\frac{q^e+1}{q+1}+m$, $0 \le \ell \le q$ and $0 \le m < \frac{q^e+1}{q+1}$. Hence $\tau_{0,\infty}(i) = -v_{Q_\infty}(f_i) = k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3$ as claimed. □

It is interesting to see what can be said about the Weierstrass semigroups $H(Q_0)$ and $H(Q_\infty)$ using the above tools. First of all, it should be noted that for $e = 1$ and $e = 3$, it is well known that $H(Q_0) = H(Q_\infty)$. The reason is that there exists an automorphism interchanging Q_0 to Q_∞. For $e > 3$, the place Q_∞ is fixed by any automorphism of χ_e and in fact $H(Q_0)$ and $H(Q_\infty)$ were shown to be distinct in [12]. However, for any $e \ge 1$ the points of the form $P_{(a,b,0)}$ fall within the same orbit under the action of the subgroup of the automorphism group of χ_e consisting of automorphisms fixing Q_∞. This means that later on in the article, one can always exchange the point Q_0 with any point of the form $P_{(a,b,0)}$.

It is easy to describe the set $\Gamma(Q_0)$, but it should first be noted that the precise structure of $H(Q_0)$ (and hence of $\Gamma(Q_0)$) has already been determined in [2]. For the sake of completeness and since our description of $\Gamma(Q_0)$ is rather compact, we give the following corollary.

Corollary 3.7. *The set $\Gamma(Q_0)$ of gaps of the Weierstrass semigroup $H(Q_0)$ of the point Q_0 on χ_e is given by*

$$\Big\{-k(q^e+1) - \ell\frac{q^e+1}{q+1} - m \mid 0 \le \ell \le q, 0 \le m < \frac{q^e+1}{q+1}, k < 0, k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3 \ge 0\Big\}.$$

Proof. We denote by $\Gamma(Q_\infty)$ (resp. $\Gamma(Q_0)$) the set of gaps of Q_∞ (resp. Q_0). It is well known that $\tau_{\infty,0}$ gives rise to a bijection from $\Gamma(Q_\infty)$ to $\Gamma(Q_0)$. Since by Corollary 3.2 we have

$$\Gamma(Q_\infty) = \Big\{k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3 \mid 0 \le \ell \le q, 0 \le m < \frac{q^e+1}{q+1}, k < 0, k(q^e+1) + \ell q\frac{q^e+1}{q+1} + mq^3 \ge 0\Big\},$$

Corollary 3.6 implies that $\Gamma(Q_0)$ is as stated. □

4. Two-point AG codes on the generalized GK curve.

Since the curves χ_e are maximal, they are good candidates to be used for the construction of error-correcting codes. Let the divisor D be the sum of all the rational points of χ_e different from Q_0 and Q_∞. If the support of a divisor G consists of one rational point not in $\mathrm{supp}(D)$, the code $C_L(D, G)$ is called a one-point AG code. Similarly, if $G = a_1Q_0 + a_2Q_\infty$, the code $C_L(D, G)$ is called a two-point code. By slight abuse of notation, the dual of a one-point code (resp. two-point code) are sometimes also called one-point (resp. two-point) codes, but we will only use the terminology for the codes $C_L(D, G)$. The main reason we do this is that for any divisor G with $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$, there exists a divisor H with $\mathrm{supp}(H) \cap \mathrm{supp}(D) = \emptyset$ such that $C_L(D, G)^\perp = C_L(D, H)$, but even if the support of G is small, the support of H might be large. Therefore, in our sense of the word, $C_L(D, G)^\perp = C_L(D, H)$ may not be a one-point or two-point code, even if $C_L(D, G)$ is.

Duals of one-point codes with defining divisor of the form aQ_∞ or aQ_0 on the generalized GK curves were investigated in [8, 2]. As we will see below, their analysis of the parameters of these codes has direct implications for the study of the one-point codes $C_L(D + Q_0, aQ_\infty)$ and $C_L(D + Q_0, aQ_0)$ themselves. Duals of two-point AG codes on the GK curve (i.e. $e = 3$)

have been studied in [5]. As we will see, their analysis can be refined significantly, yielding more excellent AG codes. Furthermore, the case $e > 3$ will be considered.

The theorem used in [5] (which comes from [15, Thm. 2.1]) allows one to improve the Goppa bound by one for the minimum distance of a nontrivial code defined on an algebraic curve χ of the form $C_L(D, (a_1 + b_1 - 1)Q_1 + (a_2 + b_2 - 1)Q_2)$, where Q_1 and Q_2 are rational points not in $\mathrm{supp}(D)$. Here, the four nonnegative integers a_1, a_2, b_1, b_2 should satisfy

(1) $a_1 \geq 1$,
(2) $L((a_1 - 1)Q_1 + a_2Q_2) = L(a_1Q_1 + a_2Q_2)$,
(3) $(b_1, b_2 - 1 - t) \in \Gamma(Q_1; Q_2)$ for all t satisfying $0 \leq t \leq \min\{b_2 - 1, 2g - 1 - a_1 - a_2\}$.

In the next theorem we show that the order bound in the same situation improves upon the Goppa bound by at least one as well. Therefore, our results will automatically include all results in [5] as a special case. First note that $L((a_1 - 1)Q_1 + a_2Q_2) = L(a_1Q_1 + a_2Q_2)$ is equivalent to saying that $\tau_{Q_1,Q_2}(a_1) > a_2$ by Theorem 2.9. Further the condition that $(b_1, b_2 - 1 - t) \in \Gamma(Q_1; Q_2)$ for all t satisfying $0 \leq t \leq \min\{b_2 - 1, 2g - 1 - a_1 - a_2\}$ is equivalent to the statement that $\tau_{Q_1,Q_2}(b_1) \geq b_2$ or $\tau_{Q_1,Q_2}(b_1) < b_2 - 1 - \min\{b_2 - 1, 2g - 1 - a_1 - a_2\}$. With these reformulations in mind, we now show that Proposition 2.4 implies [15, Thm. 2.1].

Theorem 4.1. *Let a_1, a_2, b_1, b_2 be nonnegative integers and write $G := (a_1 + b_1 - 1)Q_1 + (a_2 + b_2 - 1)Q_2$. Further suppose that $\tau_{Q_1,Q_2}(a_1) > a_2$.*

(1) *If $\tau_{Q_1,Q_2}(b_1) \geq b_2$, then $\nu(Q_1; (b_2 - 1)Q_2, a_2Q_2) > \deg(G) - 2g(\chi) + 2$.*
(2) *If $\tau_{Q_1,Q_2}(b_1) < b_2 - 1 - \min\{b_2 - 1, 2g - a_1 - a_2\}$, then $\nu(Q_2; b_1Q_1, (a_1 - 1)Q_1) > \deg(G) - 2g(\chi) + 2$.*

In particular, in either case the minimum distance of the code $C_L(D, G)^\perp$ is at least $\deg(G) - 2g + 3$.

Proof. If $\tau_{Q_1,Q_2}(b_1) \geq b_2$, then $a_1 \in \Gamma(Q_1; a_2Q_2)$ and $b_1 \in \Gamma(Q_1; (b_2 - 1)Q_2)$. Combining Remark 2.2 with (the proof of) Lemma 2.5 we see that $\nu(Q_1; (a_1 - 1)Q_1 + a_2Q_2, b_1Q_1 + (b_2 - 1)Q_2) > \deg(G) - 2g(\chi) + 2$. Indeed, the term $q_{Q_1,(a_1-1)Q_1+a_2Q_2}(t)q_{Q_1,b_1Q_1+(b_2-1)Q_2}(t)$ will contribute to the coefficient of $t^{v_Q(G)+1}$ with at least 1. From Proposition 2.4 and the Goppa bound applied to $C_L(D, G + Q_1)^\perp$, we see that $C_L(D, G)$ has minimum distance at least $\deg(G) - 2g + 3$.

If $\tau_{Q_1,Q_2}(b_1) < b_2$ and $\min\{b_2 - 1, 2g - 1 - a_1 - a_2\} = b_2 - 1$, then we have $(b_1, b_2 - 1 - t) \in \Gamma(Q_1; Q_2)$ by assumption for all t satisfying $0 \leq t \leq b_2 - 1$. This implies that $\tau_{Q_1,Q_2}(b_1) < 0$. However, since $\tau_{Q_1,Q_2}(0) = 0$ and $b_1 \geq 0$, we see that $(b_1, 0) \in H(Q_1, Q_2)$, giving a contradiction. This situation can therefore not occur.

If $\tau_{Q_1,Q_2}(b_1) < b_2$ and $\min\{b_2 - 1, 2g - 1 - a_1 - a_2\} = 2g - 1 - a_1 - a_2$, then similarly as before we have $\tau(b_1) < b_2 - 2g + a_1 + a_2$. This implies that $b_2 - 1 - t \in \Gamma(Q_2; b_1Q_1)$ for all t satisfying $0 \leq t \leq 2g - 1 - a_1 - a_2$. On the other hand, we have $\tau_{Q_1,Q_2}(a_1) \in \Gamma(Q_2; (a_1 - 1)Q_1)$. Now using Remark 2.7, note that

$$b_2 - 2g - a_1 - a_2 \leq a_2 + b_2 - \tau_{Q_1,Q_2}(a_1) \leq b_2 - 1.$$

Hence $a_2 + b_2 - \tau_{Q_1,Q_2}(a_1) \in \Gamma(Q_2; b_1Q_1)$. The term $q_{Q_2,(a_1-1)Q_1+a_2Q_2}(t)q_{Q_2,b_1Q_1+(b_2-1)Q_2}(t)$ will then contribute to the coefficient of $t^{v_Q(G)+1}$ with at least 1. Hence $\nu(Q_2; (a_1 - 1)Q_1 + a_2Q_2, b_1Q_1 + (b_2 - 1)Q_2) > \deg(G) - 2g(\chi) + 2$. Proposition 2.4 and the Goppa bound applied to $C_L(D, G + Q_2)^\perp$, imply that $C_L(D, G)^\perp$ has minimum distance at least $\deg(G) - 2g + 3$. □

With the above theorem in place, we could in principle start to compute our lower bound on the minimum distance of the duals of two-point codes. Before doing that, we show in the remainder of this section that duals of two-point codes on the generalized GK curve are closely related to two-point codes. This means that our bounds not only can be applied to the duals of two-point codes, but to two-point codes themselves as well. In order to do this, we need to

understand the structure of the rational point of χ_e. The structure of these points is described explicitly in [1, 12]. Since e is odd, we write $e = 2t + 1$ for some nonnegative integer t. Apart from Q_∞, all rational points are of the form $P_{(a,b,c)}$. There are q^3 rational places of the form $P_{(a,b,0)}$ and $q^3(q^e + 1)(q^{e-1} - 1)$ of the form $P_{(a,b,c)}$ with $c \neq 0$. Both for $c = 0$ and $c \neq 0$, the place $P_{(a,b,c)}$ is unramified in the degree q^3 extension $\mathbb{F}_{q^{2e}}(\chi_e)/\mathbb{F}_{q^{2e}}(z)$ by [1, 12]. This means that there are exactly $(q^e + 1)(q^{e-1} - 1)$ possible nonzero values of $c \in \mathbb{F}_{q^{2e}}$ giving rise to q^3 rational places of $\mathbb{F}_{q^{2e}}(\chi_e)$ if the form $P_{(a,b,c)}$. By [1] these values of c are exactly the roots of the polynomial

$$f := 1 + \sum_{i=0}^{t-1} z^{\frac{q^e+1}{q+1}\left(q^{2i+2}-1+q^e-q\right)} + \sum_{i=0}^{t-1} z^{\frac{q^e+1}{q+1}\left(q(q^{2i+2}-1)\right)}.$$

Denoting, as before, by D the divisor which is the sum of all rational points distinct from Q_0 and Q_∞, this implies that

$$(zf) = Q_0 + D - q^3(q^{2e-1} - q^e + q^{e-1})Q_\infty. \tag{2}$$

This expression is very useful to determine whether or not two two-point codes are equal. This comes in very handy, when computing the order bound using Proposition 2.4, since one should only apply this proposition if the codes $C_L(D, G + Q)$ and $C_L(D, G)$ are distinct. We give a criterion in the following lemma.

Lemma 4.2. *Let χ_e be the generalized GK curve over $\mathbb{F}_{q^{2e}}$ and let the divisor D be the sum of all its rational places different from Q_0 and Q_∞. Further let $G = a_1Q_0 + a_2Q_\infty$ and $Q \in \{Q_0, Q_\infty\}$. Then*

$$\dim(C_L(D, G)) = \dim(L(G)) - \dim(L(G + Q_0 - q^3(q^{2e-1} - q^e + q^{e-1})Q_\infty)).$$

Furthermore $C_L(D, G + Q) = C_L(D, G)$ if and only if

$$\dim(L(G + Q)) - \dim(L(G + Q + Q_0 - q^3(q^{2e-1} - q^e + q^{e-1})Q_\infty)) = \dim(L(G)) - \dim(L(G + Q_0 - q^3(q^{2e-1} - q^e + q^{e-1})Q_\infty)).$$

Proof. First, note that $\dim(C_L(D, G)) = \dim(L(G)) - \dim(L(G - D))$. Since $\dim(L(G - D)) = \dim(L(G - D + (zf)))$, the first part of the lemma follows from Eq. (2). Now applying this formula to compute the dimension of $\dim(C_L(D, G + Q))$, the lemma follows. □

Since we know the map $\tau_{0,\infty}$ explicitly, it is very easy to check the above criterion using Theorem 2.9.

The function zf from equation (2) is also useful when identifying dual two-point codes and two-point codes. The standard way to identify the dual of an AG code $C_L(D, G)^\perp$ with a code of the form $C_L(D, H)$ is to identify a differential on the curve with simple poles in all evaluation points and residues in these points equal to 1. Equation (2) implies that the differential $\omega := \frac{1}{fz}dz$ has simple poles and nonzero residue in all rational points of the form $P_{(a,b,c)}$. More precisely, using the defining equations of the curve χ_e and equation (2), we obtain that

$$(\omega) = -Q_0 - D + (q^{2e+2} - q^{e+3} + 2q^{e+2} - q^e + q^2 - 1)Q_\infty. \tag{3}$$

Since the differential ω has simple poles in all the points in D, its residues at those points will all be nonzero. However, it turns out that in general these residues are not all 1. Nonetheless, we can identify an explicit relation between the class of codes $C_L(D, G)$ and $C_L(D, G)^\perp$. Two codes C_1 and C_2 are called equivalent up to column multipliers, which we denote by $C_1 \cong C_2$, if there exist nonzero elements $a_1, \ldots, a_n$ such that the map $\phi : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$ defined by $\phi(v_1, \ldots, v_n) = (a_1v_1, \ldots, a_nv_n)$ satisfies $\phi(C_1) = C_2$. Note that the basic parameters of such codes C_1 and C_2, such as the minimum distance, are the same.

Proposition 4.3. *Let χ_e be the generalized GK curve over $\mathbb{F}_{q^{2e}}$ and let the divisor D be the sum of all its rational places different from Q_0 and Q_∞. Further let $G = a_1Q_0 + a_2Q_\infty$. Then $C_L(D,G)^\perp \cong C_L(D,H)$, where*

$$H = -(a_1+1)Q_0 + (q^{2e+2} - q^{e+3} + 2q^{e+2} - q^e + q^2 - 1 - a_2)Q_\infty.$$

Proof. Let $h := (zf)'$ be the derivative of zf with respect to the variable z. Then the differential $\eta = h\omega = (zf)'/(zf)dz$ has simple poles in all the rational points $P_{(a,b,c)}$ of χ_e. Moreover, in each of those points, the residue of η is equal to 1. Therefore the standard theory of AG codes implies that $C_L(D,G)^\perp = C_L(D,H')$, with $H' = D - G + (\eta) = D - G + (h) + (\omega)$. Since zf has simple roots only, its derivative h is nonzero in Q_0 and the points in D. Hence the codes $C_L(D,H') \cong C_L(D,H)$, with $H = D - G + (\omega)$. Explicitly, the column multipliers are given by $(h(P))_{P\in\mathrm{supp}(D)}$. Using Eq. (3), the lemma follows. □

This proposition implies that the class of two-point codes $C_L(D, a_1Q_0 + a_2Q_\infty)$ on the generalized GK curve is essentially the same as the class of codes of the form $C_L(D, a_1Q_0 + a_2Q_\infty)^\perp$. In particular, the bounds on the minimum distance of codes of the form $C_L(D, a_1Q_0 + a_2Q_\infty)^\perp$ will imply bounds for the minimum distance of codes of the form $C_L(D, a_1Q_0 + a_2Q_\infty)$. Note that the above proof shows that $C_L(D,G)^\perp = C_L(D,H')$, where

$$H' = -(a_1+1)Q_0 + (q^{2e+2} - q^{e+3} + 2q^{e+2} - q^e + q^2 - 1 - a_2)Q_\infty + ((zf)').$$

However, for our purposes this is less useful, since the divisor of $(zf)'$ may contains other points of χ_e. Therefore $C_L(D,H')$ is in general not a two-point code, even if $C_L(D,G)$ is.

Using the same differential ω as above, we obtain the following corollary for one-point AG codes on the generalized GK curve.

Corollary 4.4. *Let χ_e be the generalized GK curve over $\mathbb{F}_{q^{2e}}$ and let the divisor D be the sum of all its rational places different from Q_0 and Q_∞. Further let $G = aQ_\infty$. Then $C_L(D+Q_0,G)^\perp \cong C_L(D+Q_0,H)$, where*

$$H = (q^{2e+2} - q^{e+3} + 2q^{e+2} - q^e + q^2 - 1 - a)Q_\infty.$$

5. Computation of the order bound and results

Now that all the theoretical tools are in place, all that is left is to give the lower bounds that we obtain using the above theory as well as state the improvements on the MinT tables [16]. We would also like to explain briefly how we computed these bounds. The given algorithm works for any of the generalized GK curves χ_e. We have already seen that the explicit description of the bijection $\tau_{0,\infty}$ in Corollary 3.6, implies that for $G = a_1Q_0 + a_2Q_\infty$ and $Q \in \{Q_0, Q_\infty\}$, it is computationally easy to determine:

(1) The dimension of $L(G)$, see Theorem 2.9.
(2) The dimension of $C_L(D,G)$ (and hence of $C_L(D,G)^\perp$), see Lemma 4.2.
(3) The sets $H(Q;G)$ (and hence the value of $\nu(Q;G)$), see Corollary 2.10.

What is left is to describe how to find the best recursive use of Proposition 2.4. We do this efficiently by using a dynamic programming approach, in the form of a backtracking algorithm which starts with large degree divisors, where the order bound coincides with the Goppa bound and is easy to compute, and then backtracks to smaller degree divisors. A pseudo-code description is given in Algorithm 1. For $q = 2$ and $e = 3$ our results supplement and improve those in [5], as indicated in Table 1.

Algorithm 1 : OrderBoundTable

Input: parameters q and e.

Output: array containing the order bound for $C_L(D, aQ_0 + bQ_\infty)^\perp$, for $a, b \in \mathbb{Z}_{\geq 0}$ whose sum $a + b$ is at most Δ, a bound beyond which the order bound and the Goppa bound coincide.

$g_e := (q-1)(q^{e+1} + q^e - q^2)/2$ `// genus of` χ_e
$N_e := q^{2e+2} - q^{e+3} + q^{e+2} + 1$ `// number of rational points`
$\Delta := N_e + 2g_e$ `// if larger degree, order bound coincides with Goppa bound`
orderBound := two-dimensional array of size $(\Delta + 1) \times (\Delta + 1)$
for a **from** Δ **to** 0 **do**
    orderBound$[a, \Delta - a] = \Delta - 2g_e + 2$ `// Goppa bound for degree` Δ
for δ **from** $\Delta - 1$ **to** 0 **do** `// backtrack: iterate on decreasing degree` $\delta = a + b$
    for a **from** 0 **to** δ **do**
        $b := \delta - a$
        `/* Walk on the horizontal edge */`
        $U := \{$Weierstrass semigroup at $Q_0\} \cap \{0, \ldots, \delta + 1\}$
        $V := \{bQ_\infty$-non-gaps at $Q_0\} \cap \{-b, \ldots, a + 1\}$
        $\overline{U} := \{a + 1 - u, u \in U\}$
        $w :=$ cardinality of $\overline{U} \cap V$
        if $w \neq 0$ and $\dim(C_L(D, aQ_0 + bQ_\infty)) \neq \dim(C_L(D, (a+1)Q_0 + bQ_\infty))$ **then**
            hbound := $\min(w,$ orderBound$[a + 1, b])$
        else hbound := orderBound$[a + 1, b]$
        `/* Walk on the vertical edge */`
        $U := \{$Weierstrass semigroup at $Q_\infty\} \cap \{0, \ldots, \delta + 1\}$
        $V := \{aQ_0$-non-gaps at $Q_\infty\} \cap \{-a, \ldots, b + 1\}$
        $\overline{U} := \{b + 1 - u, u \in U\}$
        $w :=$ cardinality of $\overline{U} \cap V$
        if $w \neq 0$ and $\dim(C_L(D, aQ_0 + bQ_\infty)) \neq \dim(C_L(D, aQ_0 + (b+1)Q_\infty))$ **then**
            vbound := $\min(w,$ orderBound$[a, b + 1])$
        else vbound := orderBound$[a, b + 1]$
        `/* Combine the obtained bounds */`
        orderBound$[a, b] := \max($hbound, vbound$)$

References

[1] M. Abdon, J. Bezerra and L. Quoos, Further examples of maximal curves, J. Pure Appl. Algebra, vol. 213 (2009), 1192–1196.

[2] D. Bartoli, M. Montanucci and G. Zini, AG codes and AG quantum codes from the GGS curve, preprint arXiv:1703.03178v1, 2017.

[3] P. Beelen, The order bound for general algebraic geometric codes, Finite Fields Appl., vol. 13 (2007), 665–680.

[4] P. Beelen and N. Tutaş, A generalization of the Weierstrass semigroup, J. Pure Appl. Algebra, vol. 207 (2006), no. 2, 243–260.

[5] A.S. Castellanos and G.C. Tizziotti, Two-point AG Codes on the GK Maximal Curves, IEEE Trans. Inform. Theory 62 (2016), no. 2, 681–686.

[6] I.M. Duursma, R. Kirov, S. Park, Distance bounds for algebraic geometric codes, J. Pure Appl. Algebra 215 (2011), no. 8, 1863-1878.

[7] I.M. Duursma, Two-point coordinate rings for GK–Curves, IEEE Trans. Inform. Theory 57 (2011), no. 2, 593–600.

[8] S. Fanali, M. Giulietti, One-Point AG codes on the GK Maximal Curves, IEEE Trans. Inform. Theory 56 (2010), no. 1, 202–210.

[9] A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. 10 (2010), 427–434.

n	k	(a_1, a_2)	d_{2P}	d_{1P}	n	k	(a_1, a_2)	d_{2P}	d_{1P}
223	222	$(0, 0)$	2	2	223	203	$(22, 7)$	**13**	12
223	221	$(6, 0)$	2	2	223	202	$(22, 8)$	13	12
223	220	$(8, 0)$	2	2	223	201	$(31, 0)$	14	14
223	219	$(11, 0)$	3	3	223	200	$(28, 4)$	**15**	14
223	218	$(13, 0)$	3	3	223	199	$(28, 5)$	16	15
223	217	$(14, 0)$	3	3	223	198	$(28, 6)$	17	16
223	216	$(8, 7)$	4	3	223	197	$(28, 7)$	**18**	17
223	215	$(16, 0)$	4	4	223	196	$(28, 8)$	**19**	18
223	214	$(17, 0)$	5	5	223	195	$(37, 0)$	20	20
223	213	$(19, 0)$	6	6	223	10	$(215, 7)$	205	204
223	212	$(20, 0)$	6	6	223	9	$(216, 7)$	206	206
223	211	$(21, 0)$	6	6	223	8	$(217, 7)$	207	206
223	210	$(22, 0)$	6	6	223	7	$(218, 7)$	208	207
223	209	$(19, 4)$	8	6	223	6	$(219, 7)$	209	208
223	208	$(19, 5)$	9	6	223	5	$(220, 7)$	211	209
223	207	$(19, 6)$	9	7	223	4	$(222, 7)$	214	212
223	206	$(19, 7)$	10	8	223	3	$(231, 0)$	215	215
223	205	$(19, 8)$	11	9	223	2	$(226, 6)$	217	214
223	204	$(28, 0)$	12	12	223	1	$(228, 6)$	223	220

TABLE 1. Table 1 gives for $q = 2$, $e = 3$, $n = 223$ and fixed k a value of (a_1, a_2) for which the estimate d_{2P} for the minimum distance of the code $C_L(D, a_1Q_0 + a_2Q_\infty)^\perp$ is largest. It is compared to the corresponding estimate d_{1P} for the minimum distance of a code of the same length and dimension of the form $C_L(D, a_1Q_0)^\perp$ or $C_L(D, a_2Q_\infty)^\perp$. The four entries in boldface indicate new improvements on the MinT tables. In [5] it was already shown that the entries for $k \in \{198, 199\}$ improve the MinT [16] table, which is why we have not put those two values in boldface.

[10] A. Garcia, S.J. Kim, R. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, J. Pure Appl. Algebra 84 (1993), no. 2, 199–207.

[11] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. 343 (2009), 229–245.

[12] C. Güneri, M. Özdemir, H. Stichtenoth, The automorphism group of the generalized Giulietti–Korchmáros function field, Adv. Geom 13 (2013), 369–380.

[13] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, Handbook of coding theory, Vol. I, II, 871–961, North-Holland, Amsterdam, 1998.

[14] C. Hu and S. Yang, Multi-point Codes from the GGS Curves, preprint arXiv: 1706.00313v3, 2017.

[15] G.L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, Designs, Codes and Cryptography 22 (2001), 107–121.

[16] MinT, The online database for optimal parameters of (t, m, s)-nets, (t, s)-sequences, orthogonal arrays, linear codes, and OOAs, http://mint.sbg.ac.at .

[17] H. Stichtenoth, Algebraic function fields and codes, Universitext, Springer Verlag, Berlin, 1993.