Available online at www.sciencedirect.com
ScienceDirect

Finite Fields and Their Applications 13 (2007) 665–680

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

The order bound for general algebraic geometric codes

Peter Beelen

Department of Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, DK-2800, Lyngby, Denmark

Received 4 July 2005; revised 16 September 2006

Available online 1 November 2006

Communicated by Gary L. Mullen

Abstract

The order bound gives an in general very good lower bound for the minimum distance of one-point algebraic geometric codes coming from curves. This paper is about a generalization of the order bound to several-point algebraic geometric codes coming from curves.

Keywords: Algebraic geometric codes; Minimum distance; Order bound; Algebraic curve

1. Introduction

Let $\mathcal{C}$ be an algebraic curve of genus g defined over a finite field $\mathbb{F}_q$. Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a collection of rational points of $\mathcal{C}$ and suppose that G is a rational divisor on $\mathcal{C}$ whose support is disjoint from the set $\mathcal{P}$. Note that we call a divisor rational if it is invariant under the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. In the language of function fields (see [15]) a rational divisor as described above, is equivalent to a divisor of the function field of the curve C with constant field $\mathbb{F}_q$. In the usual way we can associate an evaluation code to the divisor G by considering the linear map

$$\varphi_{\mathcal{P}} : L(G) \to \mathbb{F}_q^n$$

defined coordinate-wise by $\varphi(f)_{P_j} := f(P_j)$. The condition that the support of the divisor G be disjoint from the set $\mathcal{P}$ ensures that this map is well defined. We denote its image

E-mail address: p.beelen@mat.dtu.dk.

doi:10.1016/j.ffa.2006.09.006

by $E_{\mathcal{P}}(G)$. In this paper we will study the codes $C_{\mathcal{P}}(G) := E_{\mathcal{P}}(G)^{\perp}$. Sometimes these codes are also denoted by $C_{\Omega}(P_1 + \cdots + P_n, G)$. Note that the code $E_{\mathcal{P}}(G)$ is isomorphic to a code $C_{\mathcal{P}}(G')$ for a suitable rational divisor G' with support disjoint from $\mathcal{P}$ (see e.g. [15, Proposition II.2.10]). This implies that our results also give a bound for the minimum distance of the codes $E_{\mathcal{P}}(G)$.

Let Q be an additional rational point of the curve $\mathcal{C}$ not occurring in the set $\mathcal{P}$. The order bound gives a lower bound for the minimum distance of the codes $C_{\mathcal{P}}(mQ)$ (see [4]). Other lower bounds for these codes are known, for example the celebrated Feng–Rao bound (see [1]). The order bound improves the designed lower bound (or Goppa bound) $m - 2g + 2$ in many cases and is always at least as good. Note that the order bound not only can be applied to codes coming from curves, but also to codes coming from higher-dimensional objects. In this paper we will state and prove a bound that generalizes the order bound when restricted to codes coming from algebraic curves. Note that throughout this paper we only deal with codes coming from curves. This generalized bound will give lower bounds for the minimum distances of the codes $C_{\mathcal{P}}(G)$, where G is now a rational divisor with arbitrary support disjoint from $\mathcal{P}$. We then compare our results with some other known results concerning improvements on the designed lower bound $d \geqslant \deg G - 2g + 2$. Further we give several examples of our lower bound for some algebraic geometric codes coming from the Klein quartic, the Suzuki curve and the Hermitian curve.

The organization of the paper is as follows: we start in the first section with stating and proving the generalized order bound. As an illustration we consider some codes coming from the Klein quartic. In the second section we compare our bound to several known other bounds, namely the Goppa bound, the Kirfel–Pellikaan bound and the (generalized) floor bound. We discuss the lower bounds for some codes coming from the Suzuki curve. In the third and last section we consider two-point Hermitian codes. We derive a lower bound for the minimum distance of these codes.

2. The generalized order bound

In this section we will generalize the order bound in case of codes coming from curves. The order bound has been used to estimate minimum distance of one-point codes. A reference for the one-point case is [4].

We fix some terminology. For any rational point Q of $\mathcal{C}$ we denote by v_Q the valuation map at Q and for convenience we define $\rho_Q := -v_Q$. Given a rational divisor G we denote by $v_Q(G)$ the coefficient of the point Q in G. For any function f on $\mathcal{C}$ we have $v_Q(f) = v_Q((f))$, so there is no danger of confusing the map v_Q on functions with the map v_Q on divisors. For a point Q we denote by $H(Q)$ the Weierstrass semigroup of Q.

Definition 1. Let F be a rational divisor and Q a rational point. We define

$$H(Q; F) := \rho_Q\left(\bigcup_{i=-\deg F}^{\infty} L(F + iQ)\backslash\{0\}\right).$$

The set $H(Q; F)$ gives set of F-non-gaps at Q (see [2]). An integer $j \geqslant v_Q(F) - \deg F$ is called an F-gap at Q if $j \notin H(Q; F)$.

We now collect some facts which apart from the first two are mentioned in [9].

Remark 2.

(i) From Definition 1 one can directly derive that

$$H(Q; F) = H(Q; F + jQ)$$

for any $j \in \mathbb{Z}$. In particular we can always assume that the support of F does not contain Q by choosing $j = -v_Q(F)$.

(ii) Any F-non-gap j at Q satisfies $j \geqslant v_Q(F) - \deg F$. To see this we first choose a non-zero function f from the space $L(F + iQ)$. We then have $\rho_Q(f) = -v_Q(f) \geqslant v_Q(F) + i$. On the other hand, we have $i \geqslant -\deg F$, since otherwise $L(F + iQ) = \{0\}$.

(iii) An integer $j \leqslant -\deg F$ is an F-gap at Q if and only if $L(F + (j-1)Q) = L(F + jQ)$.

(iv) There are exactly g F-gaps at Q, where g is the genus of the curve $\mathcal{C}$.

(v) Any F-gap is contained in the interval $[-\deg F, 2g - 1 - \deg F]$.

We now define a set that is crucial for the definition of the generalized order bound. It followed by a key proposition concerning the weight of certain codewords.

Definition 3. Let F_1 and F_2 be two divisors of $\mathcal{C}$ and write $G := F_1 + F_2$. We define

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

The following proposition is a direct adaptation of [4, Proposition 4.11], although our proposition is more general. The proof of the proposition can also be derived from the proof of [9, Theorem 2.5]. Especially the decomposition of the syndrome-matrix into a suitable product of three matrices is established there.

Proposition 4. *Let $\mathcal{C}$ be a smooth algebraic curve defined over a finite field $\mathbb{F}_q$. Further let $\mathcal{P}$ be a collection of n rational points and F_1, F_2 be rational divisors whose supports are disjoint from $\mathcal{P}$. Finally let Q be a rational point of $\mathcal{C}$ not occurring in $\mathcal{P}$ and suppose that $C_{\mathcal{P}}(F_1 + F_2) \neq C_{\mathcal{P}}(F_1 + F_2 + Q)$. Any codeword $y \in C_{\mathcal{P}}(F_1 + F_2) \backslash C_{\mathcal{P}}(F_1 + F_2 + Q)$ has Hamming weight at least $\nu(Q, F_1, F_2)$.*

Proof. Denote the evaluation map $\varphi_{\mathcal{P}}$ corresponding to the set $\mathcal{P}$ by φ for convenience. We consider $\varphi(f)$ as a row vector with n entries. We start the proof by choosing a natural number $k > 0$ such that:

$$k > \max\{\deg F_1, \deg F_2\},$$
$$C_{\mathcal{P}}(F_1 + kQ) = \{0\}, \quad \text{and}$$
$$C_{\mathcal{P}}(F_2 + kQ) = \{0\}.$$

It is clear that this can always be done. Next we choose a basis $f_1, \ldots, f_N$ of $L(F_1 + kQ)$ such that $\rho_Q(f_i) < \rho_Q(f_j)$ for all $1 \leqslant i, j \leqslant N$ satisfying $i < j$. Similarly, we choose a basis $g_1, \ldots, g_M$ of $L(F_2 + kQ)$ such that $\rho_Q(g_i) < \rho_Q(g_j)$ for all $1 \leqslant i, j \leqslant M$ satisfying $i < j$.

For $y \in \mathbb{F}_q^n$ we define the $n \times n$ matrix $D(y)$ as the matrix with y on its diagonal and zeros elsewhere. Further we define the $N \times n$ matrix $H_1 := (\varphi(f_i))_i$ and the $M \times n$ matrix $H_2 := (\varphi(g_j))_j$. Most importantly we define the matrix of syndromes $S(y) := H_1 D(y) H_2^T$. We denote by $\mathrm{w}(y)$ the Hamming weight of a vector $y \in \mathbb{F}_q^n$. Note that $\operatorname{rank} S(y) = \operatorname{rank} D(y) = \mathrm{w}(y)$, since H_1 and H_2 both have full rank n.

Now let y be an arbitrary element of the set $C_{\mathcal{P}}(F_1 + F_2) \backslash C_{\mathcal{P}}(F_1 + F_2 + Q)$. Let (i_1, j_1) and (i_2, j_2) be two different elements of $N(Q, F_1, F_2)$ such that $i_1 < i_2$. Then we have $i_1 + j_1 = v_Q(F_1 + F_2) + 1$. Since $j_1 \geqslant v_Q(F_2) - \deg F_2$ by Remark 2, we derive that $i_1 = v_Q(F_1 + F_2) + 1 - j_1 \leqslant v_Q(F_1) + \deg F_2 + 1 \leqslant v_Q(F_1) + k$. Similarly one can show that $i_2 \leqslant v_Q(F_1) + k$ and, reversing the roles of F_1 and F_2, that $j_1 \leqslant v_Q(F_2) + k$ and $j_2 \leqslant v_Q(F_2) + k$. This implies that the space $L(F_1 + kQ)$ contains two functions with pole orders i_1, respectively i_2 at Q. Similarly the space $L(F_2 + kQ)$ contains two functions with pole orders j_1, respectively j_2 at Q.

By the above discussion and the choice of the basis $f_1, \dots, f_N$, it is clear that there exist indices k_1 and k_2 such that $\rho_Q(f_{k_1}) = i_1$ and $\rho_Q(f_{k_2}) = i_2$. Similarly there exist indices l_1 and l_2 such that $\rho_Q(g_{l_1}) = j_1$ and $\rho_Q(g_{l_2}) = j_2$. By definition the element $f_{k_1} g_{l_1}$ belongs to the set $L(F_1 + F_2 + Q) \backslash L(F_1 + F_2)$. This means that $S(y)_{k_1, l_1} = y \cdot \varphi(f_{k_1} g_{l_1}) \neq 0$, since $y \notin C_{\mathcal{P}}(F_1 + F_2 + Q)$. Similarly $S(y)_{k_2, l_2} \neq 0$. We claim $S(y)_{k_1, l_2} = 0$. To prove this we first note that the function $f_{k_1} g_{l_2} \in L(F_1 + F_2)$. Indeed for any point $R \neq Q$ we have $\rho_R(f_{k_1} g_{l_2}) = \rho_R(f_{k_1}) + \rho_R(g_{l_2}) \leqslant v_R(F_1 + F_2)$. Also we have $\rho_Q(f_{k_1} g_{l_2}) = i_1 + j_2 < i_1 + j_1 = v_Q(F_1 + F_2) + 1$, from which we deduce $\rho_Q(f_{k_1} g_{l_2}) \leqslant v_Q(F_1 + F_2)$. This implies that $S(y)_{k_1, l_2} = y \cdot \varphi(f_{k_1} g_{l_2}) = 0$, since $y \in C_{\mathcal{P}}(F_1 + F_2)$. It is now obvious that $\mathrm{w}(y) = \operatorname{rank} S(y) \geqslant \nu(Q, F_1, F_2)$. □

Remark 5. Let G be a rational divisor whose support is disjoint from the set $\mathcal{P}$. One can use the above proposition to obtain a lower bound for the minimum distance of a code $C_{\mathcal{P}}(G)$ in the following way:

(i) Choose an infinite sequence of rational points $Q_1, Q_2, \dots$ not in $\mathcal{P}$.

(ii) For every $i \geqslant 0$, choose divisors $F_1^{(i)}$ and $F_2^{(i)}$ with supports disjoint from $\mathcal{P}$ such that $F_1^{(i)} + F_2^{(i)} = G + \sum_{j=1}^{i} Q_j$ (in particular $F_1^{(0)} + F_2^{(0)} = G$).

(iii) For every $i \geqslant 0$, calculate the numbers $\nu(Q_{i+1}, F_1^{(i)}, F_2^{(i)})$. In fact one needs not do infinitely many calculations here, because one can show that

$$\nu\bigl(Q_{i+1}, F_1^{(i)}, F_2^{(i)}\bigr) = \deg\bigl(F_1^{(i)} + F_2^{(i)}\bigr) - 2g + 2$$

as soon as $\deg(F_1^{(i)} + F_2^{(i)}) \geqslant 4g - 1$ (compare with Lemma 9 and the discussion following it).

(iv) Calculate $d := \min \nu(Q_{i+1}, F_1^{(i)}, F_2^{(i)})$, where the minimum is taken over all $i \geqslant 0$ such that $C_{\mathcal{P}}(G + \sum_{j=1}^{i} Q_j) \neq C_{\mathcal{P}}(G + \sum_{j=1}^{i+1} Q_i)$.

The number d gives a lower bound for the minimum distance of the code, since

$$C_{\mathcal{P}}(G) \backslash \{0\} = \bigcup_{i=0}^{\infty} C_{\mathcal{P}}(G + Q_1 + \cdots + Q_i) \backslash C_{\mathcal{P}}(G + Q_1 + \cdots + Q_{i+1}).$$

Note that the condition that all points Q_i are rational is not vital. One can always extend the field of definition $\mathbb{F}_q$, because this does not influence the minimum distance of the codes we are investigating.

In practice it is not easy to go through all possibilities and determine the best one. One possibility, that gives good results in practice (see Section 4), is to choose $F_1^{(i)} = G + \sum_{j=1}^{i} Q_j$ and $F_2^{(i)} = 0$. Since we will use this bound later on, especially in Section 4, we will now define the bound obtained in this way.

Definition 6. Let a rational divisor G and a set $\mathcal{P}$ of rational points on $\mathcal{C}$ be given. Suppose that $\mathcal{P}$ is disjoint from the support of G. For any infinite sequence $S = Q_1, Q_2, \ldots$ of points on $\mathcal{C}\backslash\mathcal{P}$ we define

$$d_S(G) := \min\bigl\{\nu(Q_{i+1}, G + Q_1 + \cdots + Q_i, 0)\bigr\},$$

where the minimum is taken over all $i \geqslant 0$ such that $L(G + Q_1 + \cdots + Q_i) \neq L(G + Q_1 + \cdots + Q_{i+1})$. Further we define

$$d(G) := \max d_S(G),$$

where the maximum is taken over all infinite sequences S of points having entries in $\mathcal{C}\backslash\mathcal{P}$.

Similarly we define

$$d_{S,\mathcal{P}} := \min\bigl\{\nu(Q_{i+1}, G + Q_1 + \cdots + Q_i, 0)\bigr\},$$

where the minimum is taken over all $i \geqslant 0$ such that $C_{\mathcal{P}}(G + Q_1 + \cdots + Q_i) \neq C_{\mathcal{P}}(G + Q_1 + \cdots + Q_{i+1})$. We then also define

$$d_{\mathcal{P}}(G) := \max d_{S,\mathcal{P}}(G),$$

where as before the maximum is taken over all infinite sequences S of points having entries in $\mathcal{C}\backslash\mathcal{P}$.

The statement $L(G) = L(G + Q)$ is equivalent to $\nu(Q, G, 0) = 0$. Therefore we could also have defined $d_S(G)$ by taking the minimum of all the non-zero terms $\nu(Q_{i+1}, G + Q_1 + \cdots + Q_i, 0)$.

Theorem 7. *Let $\mathcal{C}$ be an algebraic curve and G a rational divisor. Let $\mathcal{P}$ be a set of rational points not occurring in the support of the divisor G. Then we have*

$$d\bigl(C_{\mathcal{P}}(G)\bigr) \geqslant d_{\mathcal{P}}(G) \geqslant d(G).$$

Proof. Clearly $d_{\mathcal{P}}(G) \geqslant d(G)$. Consider an infinite sequence $S = Q_1, Q_2, \ldots$. Corresponding to S we find a sequence of codes

$$C_{\mathcal{P}}(G) \supset C_{\mathcal{P}}(G + Q_1) \supset C_{\mathcal{P}}(G + Q_1 + Q_2) \supset \cdots.$$

Any codeword in the set $C_{\mathcal{P}}(G + Q_1 + \cdots + Q_i)\backslash C_{\mathcal{P}}(G + Q_1 + \cdots + Q_{i+1})$ has weight at least $\nu(Q_{i+1}, G + Q_1 + \cdots + Q_i, 0)$ by Proposition 4. Since $C_{\mathcal{P}}(G)\backslash\{0\} = \bigcup_{i=0}^{\infty} C_{\mathcal{P}}(G + Q_1 + \cdots + Q_i)\backslash C_{\mathcal{P}}(G + Q_1 + \cdots + Q_{i+1})$, we conclude that $d(C_{\mathcal{P}}(G)) \geqslant d_{S,\mathcal{P}}(G)$. Taking the maximum over all possible sequences then implies that $d(C_{\mathcal{P}}(G)) \geqslant d_{\mathcal{P}}(G)$. □

The significance of Theorem 7 and Remark 5 is that it gives an order bound type of result for general algebraic geometric codes, instead of just for one point codes. Although the results in [9] also apply for general algebraic geometric codes, we will see in Section 3 that their bound follows from ours by considering only constant sequences $S = (Q, Q, \ldots)$, but no other sequences. Moreover, in the one point case, it can happen that the generalized order bound is better than the (ordinary) order bound (see Example 8).

The bound described above is only useful if one can calculate it in a reasonable time. Therefore we would like to address this issue here. Suppose that we are explicitly given an algebraic curve $\mathcal{C}$, a divisor G, and a set $\mathcal{P}$ of rational points on $\mathcal{C}$. We wish to calculate a lower bound for the minimum distance of the code $C_{\mathcal{P}}(G)$. The first thing one needs to realize is that one obtains a lower bound of the minimum distance of a code $C_{\mathcal{P}}(G)$ for every sequence one chooses. Of course one would like to find a sequence that gives the best possible lower bound on the minimum distance, but such a sequence may be hard to find or even to determine theoretically. Therefore what one does in practice, is to choose a finite set $\mathcal{Q}$ containing points of $\mathcal{C}$ beforehand (disjoint from the set $\mathcal{P}$) and only consider sequences with entries in $\mathcal{Q}$. It makes sense to include the support of the divisor G in this set because of the disjointness condition, but $\mathcal{Q}$ could be larger than $\operatorname{supp} G$. The next step is to calculate the set $H(Q; G + E)$ for any $Q \in \mathcal{Q}$ and any effective divisor E such that $\operatorname{supp} E \subset \mathcal{Q}$ and $\deg E \leqslant 4g - 2 - \deg G$ (to understand this last condition see the discussion after Lemma 9). This is something that can be very hard, but a computer package like MAGMA can do it. A lot of computation time can be saved by noting that $H(Q; G + E_1) \subset H(Q; G + E_2)$ if $E_1 < E_2$. One can also delete some possibilities for the divisor E by using the properties mentioned in 2. Next one determines the values $\nu(Q, G + E, 0)$. This is a relatively straightforward computation once the sets $H(Q)$ and $H(Q; G + E)$ have been determined. Finally one can find a best possible sequence (with entries in $\mathcal{Q}$) using a backtracking algorithm.

Example 8. The Klein quartic is a curve of genus 3 defined over the finite field $\mathbb{F}_8$ by the homogeneous equation

$$X^3Y + Y^3Z + Z^3X = 0.$$

We define the points $P := (0 : 0 : 1)$, $Q := (0 : 1 : 0)$ and $R := (1 : 0 : 0)$. Moreover we define $\mathcal{P}$ to be the set of all affine points different from P, Q, or R. It is well known that $\#\mathcal{P} = 21$ (see e.g. [4, Example 2.20]). To calculate the bound from Definition 6, we need to do some calculations. We denote by x (respectively y) the function X/Z (respectively Y/Z). First note that

$$(x) = 3P - 2Q - R$$

and

$$(y) = P - 3Q + 2R.$$

Therefore for $m, n \in \mathbb{Z}$ we have

$$\left(x^m y^n\right) = (3m+n)P + (-2m-3n)Q + (-m+2n)R.$$

This enables one to explicitly calculate the sets $H(P; G)$, $H(Q; G)$ and $H(R; G)$ for any divisor G with support contained in $\{P, Q, R\}$. Say, for example, that we want to calculate $H(P; aP + bQ + cR)$. By Remark 2 we see directly that $H(P; aP + bQ + cR) = H(P; bQ + cR)$. Moreover, from the above divisor of $x^m y^n$ we deduce that

$$\{-3m - n \mid m, n \in \mathbb{Z},\ -2m - 3n \geqslant -b,\ -m + 2n \geqslant -c\} \subset H(P; bQ + cR).$$

Since in general for any divisor G the number of G-gaps at a point P is equal to the genus of the curve (see Remark 2), we have a criterion to determine if we have found all G-non-gaps or not. In this way one obtains for example:

$$\begin{array}{ll}
H(P;0) = \{0,3,5,6,7,\ldots\}, & H(Q;0) = \{0,3,5,6,7,\ldots\}, \\
H(P;Q) = H(P) \cup \{2\}, & H(Q;P) = H(Q) \cup \{4\}, \\
H(P;2Q) = H(P;Q) \cup \{4\}, & H(Q;2P) = H(Q;P) \cup \{1\}, \\
H(P;3Q) = H(P;2Q) \cup \{-1\}, & H(Q;3P) = H(Q;2P) \cup \{-2\}, \\
H(P;4Q) = H(P;3Q) \cup \{1\}, & H(Q;4P) = H(Q;3P) \cup \{2\}, \\
H(P;5Q) = H(P;4Q) \cup \{-4\}, & H(Q;5P) = H(Q;4P) \cup \{-1\}, \\
H(P;6Q) = H(P;5Q) \cup \{-2\}, & H(Q;6P) = H(Q;5P) \cup \{-4\}, \\
H(P;7Q) = H(P;6Q) \cup \{-7\}, & H(Q;7P) = H(Q;6P) \cup \{-7\}.
\end{array}$$

Note that $H(P; 7Q) = \{i - 7 \mid i \in H(P)\}$ (and more general $H(P; (i+7)Q) = \{i - 7 \mid i \in H(P; iQ)\}$). The reason for this is that $7(P - Q)$ is a principal divisor (namely the divisor of x^2y). Dividing with x^2y therefore gives a bijection from $\bigcup_{i=-\deg G-7}^{\infty} L(G + 7Q + iP)$ to $\bigcup_{i=-\deg G}^{\infty} L(G + iP)$. Similarly one has $(x^3y^{-2}) = 7(P - R)$ and $(xy^{-3}) = 7(Q - R)$. It is not a coincidence that $H(P; G + Q)\backslash H(P; G)$ consists of one number for all mentioned divisors G. Indeed, it follows from the Riemann–Roch theorem, that the space $\bigcup_{i=-\deg G-1}^{\infty} L(G + Q + iP)/\bigcup_{i=-\deg G}^{\infty} L(G + iP)$ is one-dimensional, say spanned by the function f. By taking a suitable function g from $\bigcup_{i=-\deg G}^{\infty} L(G + iP)$, we can make sure that $-v_P(f + g) \notin H(P; G)$. This is then the value in $H(P; G + Q)\backslash H(P; G)$ we are looking for.

The above information allows one to calculate the generalized order bound for the codes $C_{\mathcal{P}}(aP + bQ)$ if we restrict ourselves to sequences S with entries in $\{P, Q\}$. The ordinary order bound gives the lower bound 2 for the minimum distance of the code $C_{\mathcal{P}}(5P)$, while it is not hard to see that the minimum distance is 3 in this case (compare with Example 4.16 in [4]). We can improve upon the ordinary order bound in this case, since $d_S(5P) = 3$ if we choose for S the sequence $(P, Q, Q, Q, \ldots)$. The reason the ordinary order bound gives 2 as a lower bound is that $\nu(P, 6P, 0) = 2$. However, we can avoid this small value, by choosing the sequence S differently. In particular we have $\nu(Q, 6P, 0) = \#\{(1, 0), (-2, 3), (-4, 5)\} = 3$. We see that it can be useful to include points in the sequence S that do not occur in the support of the defining divisor. Another example of this phenomenon is the following: the ordinary order bound for the minimum distance of the code $C_{\mathcal{P}}(8P)$ is equal to 4. Choosing $S = (R, R, R, \ldots)$ we obtain $d_S(8P) = 5$.

If the divisor contains two points, it can also happen that one needs a third point to obtain the best possible sequence S. One can show that we obtain the lower bound 3 for the minimum distance of the code $C_{\mathcal{P}}(P+6Q)$ if we consider only sequences with entries in $\{P, Q\}$. However, $d_S(P+6Q)=4$ if we take the sequence $S:=(R, R, R, \ldots)$.

3. A comparison with other lower bounds

In this section we will compare the lower bounds described in Remark 5 and Definition 6 with several known lower bounds. We will first show that the lower bound $d(G)$ is at least as good as the Goppa bound. We start with a lemma.

Lemma 9. *Let C be an algebraic curve of genus g defined over a finite field $\mathbb{F}_q$. Further let G be a rational divisor and Q a rational point. Then*

$$\nu(Q, G, 0) \geqslant \deg(G) - 2g + 2.$$

Proof. For a given divisor G, define the Laurent series

$$p_{Q,G}(t) := \sum_{i \in H(Q;G)} t^i.$$

Since $1/(1-t) = \sum_{i \geqslant 0} t^i$ and $H(Q; G) \subset \mathbb{Z}_{\geqslant -\deg G}$, the Laurent series

$$q_{Q,G}(t) := \frac{1}{1-t} - t^{\deg G} \cdot p_{Q,G}(t)$$

is in fact a polynomial. This polynomial has degree at most $2g-1$. For $G=0$, this follows from the fact that a gap at Q is at most $2g-1$. In general it follows directly from the Riemann–Roch theorem. We also claim that $q_{Q,G}(1) = g$. This is equivalent to the fact that there are exactly g G-gaps (see Remark 2). Denoting the G-gaps by say $i_1, \ldots, i_g$, we obtain that

$$q_{Q,G}(t) = t^{\deg G} \sum_{j=1}^{g} t^{i_j}.$$

From Definition 3 we can deduce that $\nu(Q, G, 0)$ is equal to the coefficient of t in the Laurent series $p_{Q,G}(t) \cdot p_{Q,0}(t)$. However, by the above properties of $q_{Q,G}(t)$, this product is equal to

$$t^{-\deg(G)}\left(\frac{1}{(1-t)^2} - \frac{2g}{1-t} + \frac{q_{Q,G}(t)-g}{t-1} + \frac{q_{Q,0}(t)-g}{t-1} + q_{Q,G}(t) \cdot q_{Q,0}(t)\right). \tag{1}$$

The coefficient of t in $t^{-\deg(G)}(1/(1-t)^2 - 2g/(1-t))$ is $\deg G + 2 - 2g$, so by Eq. (1) we are done if we prove that $(q_{Q,G}(t)-g)/(t-1) + (q_{Q,0}(t)-g)/(t-1) + q_{Q,G}(t) \cdot q_{Q,0}(t)$ is a power series with nonnegative coefficients. The term $q_{Q,G}(t) \cdot q_{Q,0}(t)$ clearly is a polynomial with nonnegative coefficients. Both $q_{Q,G}(t)$ and $q_{Q,0}(t)$ are sums of g monomials t^i (with coefficient one). Moreover $(t^i - 1)/(t-1)$ is a polynomial with nonnegative coefficients. Therefore $(q_{Q,G}(t)-g)/(t-1)$ and $(q_{Q,0}(t)-g)/(t-1)$ are both power series (in fact polynomials) with nonnegative coefficients. □

From the above proof and the fact that the polynomials $q_{Q,G}(t)$ and $q_{Q,0}(t)$ have degree at most $2g-1$, one sees that $\nu(Q,G,0) > \deg G - 2g + 2$ can only hold if $\deg G \leqslant 4g-2$. Note that the statement of the above lemma is similar to that of [9, Theorem 3.8]. We proved the following proposition.

Proposition 10. *Let $\mathcal{C}$ be an algebraic curve of genus g defined over a finite field $\mathbb{F}$. Further let G be a divisor. Then*

$$d(G) \geqslant \deg G - 2g + 2.$$

Proof. This follows immediately from the definition of $d(G)$ and Lemma 9. □

Now we will compare the Kirfel–Pellikaan bound in [9] with the bound obtained in Remark 5. The Kirfel–Pellikaan bound is a bound similar to the ordinary order bound. In case of algebraic geometric codes, it arises by considering three sequences of L-spaces and their associated codes. The three sequences of L-spaces are an example of an error-correcting array [9, Definition 2.1, Example 3.3]. More precisely, one has three rational divisors F_1, F_2, G whose support is disjoint from a set $\mathcal{P}$ of rational points. One assumes that $F_1 + F_2 = G$ and that there exists a rational point Q not in $\mathcal{P}$. One then considers the F_1-non-gap sequence (μ_i) at Q, the F_2-non-gap sequence (ν_i) at Q, and the G-non-gap sequence (ρ_i) at Q. Next one defines the function $r(i,j)$ to be the index r occurring in ρ_r of the G-non-gap $\mu_i + \nu_j$. The Kirfel–Pellikaan bound for the minimum distance of the code $C_{\mathcal{P}}(G)$ is defined by

$$\min \#\bigl\{(i,j) \in \mathbb{N}^2 \bigm| r(i,j) = r+1\bigr\},$$

where the minimum is taken over all $r \geqslant 0$ such that $C_{\mathcal{P}}(G + rQ) \neq C_{\mathcal{P}}(G + (r+1)Q)$.

We will now use the terminology from Remark 5. We obtain a lower bound for the minimum distance of the code $C_{\mathcal{P}}(G)$ by choosing $F_1^{(i)} = F_1$ and $F_2^{(i)} = F_2 + iQ$ in Remark 5. This lower bound is exactly the Kirfel–Pellikaan bound and it arises from the sequence $(Q, Q, Q, \ldots)$. Therefore allowing more possible choices for the sequence, one might obtain a better lower bound. Allowing more possibilities for $F_1^{(i)}$ and $F_2^{(i)}$, could give an additional improvement as well. Indeed improvements on the Kirfel–Pellikaan bound can be obtained in this way. This was already apparent in Example 8. It is not clear that the bound $d_{\mathcal{P}}(G)$ in Definition 6 is always at least as good as the Kirfel–Pellikaan bound. We state the reformulation of the Kirfel–Pellikaan bound as a proposition.

Proposition 11. *Let $\mathcal{C}$ be an algebraic curve defined over a finite field $\mathbb{F}_q$ and let $\mathcal{P}$ be a set of rational points of $\mathcal{C}$. Further let F_1, F_2, G be divisors whose support is disjoint from the set $\mathcal{P}$. Assumes that $F_1 + F_2 = G$ and that there exists a rational point Q of $\mathcal{C}$ not in $\mathcal{P}$. Finally denote by (μ_i) the F_1-non-gap sequence at Q, by (ν_i) the F_2-non-gap sequence at Q, and by (ρ_i) the G-non-gap sequence at Q. The Kirfel–Pellikaan bound for the minimum distance of the code $C_{\mathcal{P}}(G)$ coming from the error-correcting array*

$$\bigl(\bigl(L(F_1 + \mu_i Q)\bigr), \bigl(L(F_2 + \nu_j Q)\bigr), \bigl(L(G + \rho_r Q)\bigr)\bigr),$$

is the same as the lower bound obtained in Remark 5 by choosing $F_1^{(i)} = F_1$ and $F_2^{(i)} = F_2 + iQ$.

Table 1
Lower bounds for the codes $C_{\mathcal{P}}(P + bQ)$

b	25	26	27	28	29	30	31	32	33	34	35	36	38	39
d_f	2	2	4	6	6	7	8	9	10	10	12	12	14	15
d_o	6	6	7	7	8	8	9	10	11	11	13	13	15	16

Table 2
Lower bounds for the codes $C_{\mathcal{P}}(2P + bQ)$

b	24	25	26	27	28
d_f	3	4	4	6	8
d_o	4	6	6	7	7

There exists another type of lower bound for the minimum distance of algebraic geometric codes: the generalized floor bound. This is a bound stated in [11]. It generalizes the floor bound mentioned in [12]. For the convenience of the reader we paraphrase their result.

Proposition 12. *Let $\mathcal{C}$ be a curve of genus g defined over a finite field $\mathbb{F}_q$. Let $\mathcal{P}$ be a collection of rational points and let A, B and $Z \geqslant 0$ be rational divisors whose support is disjoint from $\mathcal{P}$. Suppose that $L(A) = L(A - Z)$ and $L(B) = L(B + Z)$. Then the minimum distance of the code $C_{\mathcal{P}}(A + B)$ is at least* $\deg(A + B) - 2g + 2 + \deg Z$.

Using this result, lower bounds are derived in [11], for two-point codes coming from the Hermitian curve defined over $\mathbb{F}_{16}$ and the Suzuki curve defined over $\mathbb{F}_8$. In case of the Hermitian curves, the generalized order bound is at least as good (see Section 4). In case of the Suzuki curve the generalized floor bound is on one occasion better than the generalized order bound.

Before comparing the two bounds, we give some information about the Suzuki curve over $\mathbb{F}_8$ (see [3]). It is given by the equation $y^8 + y = x^{10} + x^3$ and has in total 65 rational points. The curve has genus 14 and a doubly transitive automorphism group. We write P for the (unique) point that is a common zero of x and y and Q for the (also unique) point that is a common pole of x and y. Also we define $\mathcal{P}$ to be the set of 63 rational points different from P and Q. In [11] a lower bound is calculated for codes $C_{\mathcal{P}}(aP + bQ)$ with $a + b \geqslant 26$ and $0 \leqslant a < 13$. The latter condition on a is not a restriction, since $13(P - Q)$ is a principal divisor (namely the divisor of the function $y^4x + (y^4 - x^5)^4$, see [13]). We consider the two point codes $C_{\mathcal{P}}(P + bQ)$ and $C_{\mathcal{P}}(2P + bQ)$ for $26 \leqslant a + b$, and compare the bounds (denoted by d_f) obtained in [11] with the generalized order bound from Definition 6 (denoted by d_o). We only give those values of b for which the bounds are different. We then obtain Tables 1, 2.

If $a = 1$ the generalized order bound is at least as good as the generalized floor bound. If $a = 2$ and $b = 28$, the bound in [11] is better, while if $a = 2$ and $24 \leqslant b \leqslant 27$ the generalized order bound is better. It turns out that the generalized order bound for a code on the Suzuki curve of the form $C_{\mathcal{P}}(aP + bQ)$, with $0 \leqslant a \leqslant 12$ as above, is only improved by the (generalized) floor bound in case $a = 2$ and $b = 28$. Also note that the generalized floor bound gives the same result as the floor bound for the code $C_{\mathcal{P}}(2P + 28Q)$.

To obtain the entries in the third rows of the above tables, we need to compute $H(Q; G)$ and $H(P; G)$ with G a divisor of the form $aP + bQ$. In order to achieve this, we can use results stated in [13]. There it is stated that $H(P) = H(Q)$ and that it is generated (as a semigroup) by the elements 8, 10, 12 and 13. The set of gaps is therefore given

Table 3

i	1	2	3	4	5	6	7	8	9	10	11	12
a_i	27	19	11	17	9	15	7	−1	5	−3	3	−5

by $\{1,2,3,4,5,6,7,9,11,14,15,17,19,27\}$. We claim that the set $H(Q;P)$ is given by $H(Q) \cup \{27\}$. This follows from the fact that there exists a function f_1 regular outside P and Q for which $v_P(f_1) = -1$ and $v_Q(f_1) = -27$ (see [13]). The claim follows, since $27 \notin H(Q)$. Since $H(Q;iP) \backslash H(Q;(i-1)P)$ consists of one number, say a_i, it suffices to specify this number in order to determine $H(Q;iP)$ from $H(Q;(i-1)P)$. All these numbers can be verified by finding functions f_i such that $v_P(f_i) = -i$ and $v_Q(f_i) = -a_i$. All these functions can be found from the ones given in [13]. Also note that $H(Q;13P) = \{i - 13 \mid i \in H(Q)\}$, since $13(P-Q)$ is a principal divisor. We give the a_i in Table 3.

Since the automorphism group of the Suzuki curve is doubly transitive, the role of P and Q can be interchanged. In particular we have $H(P;iQ) = H(Q;iP)$. This then gives in principle enough information to calculate the generalized order bound if we restrict our sequences to those with entries in $\{P, Q\}$.

As mentioned before, it is in practice not clear what the best choice of the sequence S is. However, under the restriction that its entries lie in the set $\{P, Q\}$, we can follow the procedure outlined before Example 8. The main computational problem, the determination of the sets $H(P;aP+bQ)$ and $H(Q;aP+bQ)$, has been solved above. A computer algorithm then determined a sequence S with entries in $\{P, Q\}$ giving the best lower bound.

4. The Hermitian curve

We will now study two-point codes coming from the Hermitian curve over $\mathbb{F}_{q^2}$. This curve is given by the equation

$$Y^q + Y = X^{q+1}. \tag{2}$$

The curve has $q^3 + 1$ rational points and genus $q(q-1)/2$. Therefore it attains the Hasse–Weil bound. We denote by P the point $(0,0)$ and by Q the point at infinity. Further we will in this section denote by $\mathcal{P}$ the set of all rational points different from P and Q. We will study codes $C_{\mathcal{P}}(G)$ with G a divisor of the form $G = aP + bQ$. Since the Hermitian curve has a doubly transitive automorphism group, our results extend to arbitrary two-point codes on the Hermitian curve. Since the divisor $(q+1)(P-Q)$ is principal (namely the divisor of the function y), we can assume without loss of generality that $-q \leqslant a \leqslant 0$. It is convenient to note that

$$C_{\mathcal{P}}(G) \cong E_{\mathcal{P}}\bigl(-G + \bigl(q^3 + q^2 - q - 2\bigr)Q - P\bigr). \tag{3}$$

This isomorphism follows from [15, Proposition II.2.10] using the differential form $(x^{q^2} - x)^{-1}\,dx$.

It is well known that the ordinary order bound gives the exact minimum distance of the codes $C_{\mathcal{P} \cup \{P\}}(bQ)$ (see [4,10,14]). This means that no improvements can be obtained as in Example 8, but we also see that, a fortiori, the generalized order bound gives the exact minimum distance of the codes $C_{\mathcal{P}}(bQ)$.

Recently, the exact minimum distance of the two-point Hermitian codes has been calculated (see [5–8]). In this section we will use the generalized order bound to determine a lower bound in

Theorem 17 on the minimum distance of the codes $C_{\mathcal{P}}(aP+bQ)$. Comparing this lower bound with the results in [8], one can see that this bound in fact gives the exact minimum distance in a large range.

Before deriving our lower bound for the minimum distance $d(C_{\mathcal{P}}(aP+bQ))$, we quote some results about the one-point case for future reference.

Fact 13. Let $m < q^2-1$ be an integer. Choose integers α and β such that $\alpha q+\beta(q+1)=m+1$ and $0 \leqslant \beta < q$. Then

$$\nu(Q,mQ,0)=\begin{cases} 0 & \text{if } \alpha<0,\\ (\alpha+1)(\beta+1) & \text{else.}\end{cases}$$

Moreover, for any integer $n \geqslant 0$, we have

$$\nu\big(Q,\big(q^2-q-2+n\big)Q,0\big)=n+\nu\big(Q,\big(q^2-q-2-n\big)Q,0\big).$$

The first formula is a special case of Lemma 5.27 in [4]. It actually holds as long as $m < q^2+q-1$. The second formula is not literally mentioned in [4], but it follows directly from [4, Theorem 5.24], using the fact that the semigroup $H(Q)$ is symmetric. More precisely, if $n > q^2-q-2$ the formula is true, since the genus of the Hermitian curve is $q(q-1)/2$. Therefore, suppose that $0 \leqslant n \leqslant q^2-q-2$. Theorem 5.24 in [4] implies that

$$\nu\big(Q,\big(q^2-q-2+n\big)Q,0\big)=n+\#\big\{(\alpha,\beta)\ \big|\ \alpha,\beta\in H(Q),\ \alpha+\beta=q^2-q-2+n+1\big\}.$$

Since $H(Q)$ is symmetric, the numbers α and β are gaps if and only if the numbers $q^2-q-2-\alpha$ and $q^2-q-2-\beta$ are non-gaps less than or equal to q^2-q-2. However, the latter two numbers add up to $(q^2-q-2-n)+1$. The result now follows.

We will now show how to calculate the numbers $\nu(Q,aP+bQ,0)$ using Fact 13.

Proposition 14. *Let $\mathcal{C}$ be the Hermitian curve over $\mathbb{F}_{q^2}$ defined by Eq.* (2) *and denote by P* (*respectively Q*) *the point* $(0,0)$ (*respectively the point at infinity*). *Further let $G=aP+bQ$ be a divisor satisfying $-q \leqslant a \leqslant 0$. Then we have*

$$\nu(Q,G,0)=\max\big\{\nu\big(Q,(b-q-1)Q,0\big),\nu(Q,bQ,0)+a\big\}.$$

Proof. For convenience we write $k=-a$. Let $G=-kP+bQ$ be a divisor satisfying $-k+b \geqslant 0$ and $0 \leqslant k \leqslant q+1$. We claim that

$$H(Q;G)=H(Q)\backslash\{iq \mid 0 \leqslant i \leqslant k-1\}.$$

First note that the functions x^iy^j with $j \geqslant 0$ and $0 \leqslant i \leqslant q$ are linearly independent. This follows, for example, because their evaluations at Q are all different. In fact, any given element of $H(Q)$ can be obtained as $v_P(x^iy^j)$ for a unique i and j. This implies that the above functions x^iy^j form a basis for the space $\bigcup_i L(iQ)$. We know that for any k with $0 \leqslant k \leqslant q$ the space $(\bigcup_i L(-(k+1)P+iQ))/(\bigcup_i L(-kP+iQ))$ is one-dimensional. Therefore a basis of $\bigcup_i L(-kP+iQ)$ is given by $\{x^i \mid k \leqslant i \leqslant q\} \cup \{x^iy^j \mid j \geqslant 1,\ 0 \leqslant i \leqslant q\}$. This implies the claim.

From now on we suppose that $k \leqslant q$. It follows that $H(Q; G) \supset H(Q; G - P)$ and that these sets differ exactly by the element kq. We also obtain that $N(Q, G) \supset N(Q, G - P)$ and that their cardinalities differ by at most one. From the fact that $(y) = (q + 1)(P - Q)$ we see that $H(Q; -(q + 1)P + bQ) = \{q + 1 + i \mid i \in H(Q))$. This implies that $\nu(Q, -(q + 1)P + bQ, 0) = \nu(Q, (b - q - 1)Q, 0)$.

We now claim that if $N(Q, G, 0) = N(Q, G - P, 0)$ and $k < q$, then also $N(Q, G - P, 0) = N(Q, G - 2P, 0)$. Indeed the equality $N(Q, G, 0) = N(Q, G - P, 0)$ is by definition equivalent to the statement that $b + 1$ cannot be written as a sum of kq and an element of $H(Q)$. However, this implies that $b + 1$ can certainly not be written as the sum of $(k + 1)q$ and an element of $H(Q)$. This implies in its turn that $N(Q, G - P, 0) = N(Q, G - 2P, 0)$. Using induction we can deduce from the above claim that if $N(Q, G, 0) = N(Q, G - P, 0)$, then $N(Q, G - iP, 0) = N(Q, -(q + 1)P + bQ, 0)$ for all i such that $0 \leqslant i \leqslant (q + 1) - k$. Or in other words that $\nu(Q, G - iP, 0) = \nu(Q, (b - q - 1)Q, 0)$ for all i with $0 \leqslant i \leqslant (q + 1) - k$.

We see that the sequence $(\nu(Q, bQ - iP, 0))_{0 \leqslant i \leqslant q+1}$ is non-increasing and that if two consecutive terms are equal, then it remains constant. Moreover two consecutive terms are either equal or differ by one. This implies the proposition. □

The above proposition enables one to compute the numbers $\nu(Q, aP + bQ, 0)$ from the numbers $\nu(Q, cQ, 0)$. Till now we have not discussed the numbers $\nu(P, aP + bQ, 0)$. However, the points P and Q play a symmetric role, which implies the following corollary.

Corollary 15. *Let $G = aP + bQ$ be a divisor as in Proposition* 14. *Write $b = \alpha + \beta$, with $-q \leqslant \alpha \leqslant 0$ and β divisible by $q + 1$. We have*

$$\nu(P, G, 0) = \max\bigl\{\nu\bigl(Q, (a + \beta - q - 1)Q, 0\bigr), \nu\bigl(Q, \alpha P + (a + \beta)Q, 0\bigr) + \alpha\bigr\}.$$

Proof. The isomorphism σ defined (on the function field) by $\sigma(x) = x/y$ and $\sigma(y) = 1/y$ interchanges the points P and Q. Therefore by symmetry we have $\nu(P, G, 0) = \nu(Q, bP + aQ, 0)$. Since the divisor $(q + 1)(P - Q)$ is principal, we get $\nu(Q, bP + aQ, 0) = \nu(Q, \alpha P + (a + \beta)Q, 0)$. After applying Proposition 14 the corollary follows. □

In the remainder of this section we will derive a lower bound for the minimum distance of the codes $C_{\mathcal{P}}(aP + bQ)$. We will start with the case that the divisor G has small degree.

Proposition 16. *Let $\mathcal{C}$ be the Hermitian curve over $\mathbb{F}_{q^2}$ defined by Eq.* (2) *and denote by P* (*respectively Q*) *the point* $(0, 0)$ (*respectively the point at infinity*). *Further let $G = aP + bQ$ be a divisor of nonnegative degree satisfying $-q \leqslant a < 0$ and $1 \leqslant b \leqslant q^2 - 1$. Then*

$$d\bigl(C_{\mathcal{P}}(G)\bigr) \geqslant 1 + \left\lfloor \frac{b}{q + 1} \right\rfloor.$$

Proof. From Fact 13 we can derive that:

$$d_S(bQ) = 2 + \left\lfloor \frac{b}{q + 1} \right\rfloor \quad \text{if } b \leqslant q^2 - 1, \tag{4}$$

where, as before, S denotes the constant sequence $(Q, Q, \ldots)$. This is very similar to Proposition 5.28 in [4]. Since $(q + 1)(Q - P)$ is a principal divisor, we have $d_S(-(q + 1)P +$

$bQ) = d_S((b-q-1)Q)$. However, $d_S((b-q-1)Q) = d_S(bQ) - 1$ by Eq. (4). This implies that $d(C_{\mathcal{P}}(aP+bQ)) \geqslant d_S(bQ) - 1$ for any $-q \leqslant a < 0$, since $C_{\mathcal{P}}(aP+bQ) \subset C_{\mathcal{P}}(-(q+1)P+bQ)$. □

Note that using this proposition, we obtain a lower bound for the minimum distance of the code $C_{\mathcal{P}}(aP+bQ)$ if $a+b \leqslant 2g-2$ and $a \neq 0$. Here $g = q(q-1)/2$ denotes the genus of the Hermitian curve. This is exactly the region where the designed minimum distance $\deg G - 2g + 2$ is trivial. The case $a = 0$ is not very interesting, since the one-point codes on the Hermitian codes have been well studied. We will now investigate the codes $C_{\mathcal{P}}(aP+bQ)$ with $a+b > 2g-2$.

Theorem 17. *Consider the Hermitian curve defined over the finite field $\mathbb{F}_{q^2}$ defined by the equation $X^{q+1} = Y^q + Y$. We denote by P the point $(0,0)$ and by Q the point at infinity. Moreover we denote by $\mathcal{P}$ the set consisting of the remaining q^3-1 rational points. Let $G = aP + bQ$ be a divisor satisfying $a+b > q^2-q-2$. Given a and b, we write $a = k\cdot(q+1)+l$ with k and l integers satisfying $-q \leqslant l \leqslant 0$. Also we write $b + k\cdot(q+1) = q^2-q-2+i(q+1)+j$ with i and j integers satisfying $i \geqslant 1$ and $-q \leqslant j \leqslant 0$. Then we have*

$$d\big(C_{\mathcal{P}}(G)\big) \geqslant \begin{cases} i(q+1)+l+j & \textit{if } l \geqslant -i \textit{ and } j \geqslant -i, \\ iq+l & \textit{if } l \geqslant -i \textit{ and } j < -i, \\ iq+j & \textit{if } l < -i \textit{ and } j \geqslant -i, \\ i(q-1) & \textit{if } l < -i,\ j < -i \textit{ and } (l,j) \neq (-q,-q), \\ (i-1)q & \textit{if } (l,j) = (-q,-q) \textit{ and } i < q. \end{cases}$$

Proof. It is no restriction to suppose that $-q \leqslant a \leqslant 0$. In other words, we can suppose that $k = 0$ and $l = a$. Moreover by Proposition 16 we can suppose that $b \geqslant q^2$. In other words, we can assume that $i \geqslant 2$. Note that the formulas for the minimum distance in the theorem are symmetric with respect to j and l. We claim that the codes $C_{\mathcal{P}}(lP + (q^2-q-2+i(q+1)+j)Q)$ and $C_{\mathcal{P}}(jP + (q^2-q-2+i(q+1)+l)Q)$ are equivalent. Indeed using the automorphism σ of the Hermitian curve defined by $\sigma(x) = x/y$ and $\sigma(y) = 1/y$ we see that the codes $C_{\mathcal{P}}(lP + (q^2-q-2+i(q+1)+j)Q)$ and $C_{\mathcal{P}}(lQ + (q^2-q-2+i(q+1)+l)P)$ are equivalent. Using the divisor $(y^{q-2+i}) = (q^2-q-2+i(q+1))(P-Q)$, we see that the codes $C_{\mathcal{P}}(lQ + (q^2-q-2+i(q+1)+l)P)$ and $C_{\mathcal{P}}(jP + (q^2-q-2+i(q+1)+l)Q)$ are equivalent. This proves the claim. Therefore it is no restriction to suppose that $j \leqslant l$. In the rest of the proof we will therefore assume that $k = 0$, $i \geqslant 2$ and $j \leqslant l$.

To prove the theorem we will distinguish four cases:

Case (1): $l \geqslant -i$ and $j \geqslant -i$.
Case (2): $l \geqslant -i$ and $j < -i$.
Case (3): $l < -i$, $j < -i$ and $(l,j) \neq (-q,-q)$.
Case (4): $(l,j) = (-q,-q)$ and $i < q$.

Case (1): From the Goppa bound we derive $d(C_{\mathcal{P}}(G)) \geqslant \deg G - q^2 + q + 2 = i(q+1)+l+j$.

Case (2): Using the second part of Fact 13 we find that $\nu(Q, (q^2-q-2+i(q+1)+j)Q, 0) = i(q+1)+j+\nu(Q, (q^2-q-2-i(q+1)-j)Q, 0)$. Since $q^2-q-2-(i(q+1)+j)+1 = (-i-j-1)(q+1)+(q+j)q$ we find using the first part of Fact 13 that $\nu(Q, (q^2-q-2-i(q+1)-j)Q, 0) = (-i-j)(q+j+1)$. Here we used that $j < -i$. Combining these equalities, we find that $\nu(Q,(q^2-q-2+i(q+1)+j)Q,0)=iq+(-i-j)(q+j)\geqslant iq$. By Proposition 14 we see that $\nu(Q,G,0)\geqslant iq+l$, independent of j, as long as $j<-i$. We now consider the sequence of codes

$$C_{\mathcal{P}}(G)\supset C_{\mathcal{P}}(G+Q)\supset\cdots\supset C_{\mathcal{P}}\bigl(G+(-i-j-1)Q\bigr)\supset C_{\mathcal{P}}\bigl(G+(-i-j)Q\bigr).$$

We use Proposition 4 to obtain the lower bound $iq+l$ for the Hamming weight for codewords in the difference of two consecutive codes in this sequence. Since $G+(-i-j)Q=lP+(q^2-q-2+i(q+1)-i)Q$, the minimum distance of the code $C_{\mathcal{P}}(G+(-i-j)Q)$ can be estimated by $i(q+1)+l-i=iq+l$ using case (1). In this way, we deduce that $d(C_{\mathcal{P}}(G)\geqslant iq+l$.

Case (3): Using Corollary 15 we deduce that $\nu(P,G,0)\geqslant\nu(Q,(l+q^2-q-2+(i-1)(q+1))Q,0)$. Further from Fact 13 we get, similarly as in case (2), after some calculations $\nu(Q,(l+q^2-q-2+(i-1)(q+1))Q,0)=i(q-1)+(-i-l)(q+l-1)\geqslant i(q-1)$. The last inequality holds, since $l\neq -q$. Indeed if $l=-q$, then from the assumptions $j\leqslant l$ and $j\geqslant -q$ we derive that $j=-q$. However, we excluded the pair $(j,l)=(-q,-q)$ from case (3).

Case (4): We may suppose that $2\leqslant i<q$, since for $i=1$ the condition $a+b>q^2-q-2$ is not satisfied. Note that in case (4) we have $G=-qP+(q^2+(i-2)(q+1))Q$. In case $i<q$, we can prove using Fact 13, that

$$\nu\bigl(Q,\bigl(q^2+(i-2)(q+1)\bigr)Q,0\bigr)=iq$$

and

$$\nu\bigl(Q,\bigl(q^2+(i-3)(q+1)\bigr)Q,0\bigr)=(i-1)q.$$

Therefore by Proposition 14 we have

$$\nu\bigl(Q,-qP+\bigl(q^2+(i-2)(q+1)\bigr)Q,0\bigr)=(i-1)q.$$

We claim that $\nu(Q,-qP+(q^2+(i-2)(q+1)+\lambda)Q,0)\geqslant(i-1)q$ for any $\lambda>0$. By Fact 13 and Proposition 14 we have

$$\nu\bigl(Q,-qP+\bigl(q^2+(i-2)(q+1)+\lambda\bigr)Q,0\bigr)\geqslant\nu\bigl(Q,\bigl(q^2+(i-2)(q+1)+\lambda\bigr)Q,0\bigr)-q$$

and

$$\nu\bigl(Q,\bigl(q^2+(i-2)(q+1)+\lambda\bigr)Q,0\bigr)=(i-1)q+i+\lambda+\nu\bigl(Q,\bigl(q^2-iq-(i+\lambda+2)\bigr)Q,0\bigr).$$

Hence if $\lambda\geqslant q-i$, the claim follows. If $0<\lambda<q-i-1$, then from Fact 13 we derive

$$\nu\bigl(Q,\bigl(q^2-iq-(i+\lambda+2)\bigr)Q,0\bigr)=(\lambda+2)(q-i-\lambda-1).$$

Then the claim also follows in this case after some calculations. We are left with the case that $\lambda=q-i-1$. By Proposition 14 we have

$$\begin{aligned}&\nu\bigl(Q,-qP+\bigl(q^2+(i-2)(q+1)+q-i-1\bigr)Q,0\bigr)\\&\quad\geqslant\nu\bigl(Q,\bigl(q^2+(i-3)(q+1)+q-i-1\bigr)Q,0\bigr)\end{aligned}$$

and by Fact 13

$$\nu\bigl(Q,\bigl(q^2+(i-3)(q+1)+q-i-1\bigr)Q,0\bigr)=(i-2)q+(q-2)+\nu\bigl(Q,q(q-i)Q\bigr).$$

Since $\nu(Q,q(q-i)Q)=2(q-i)$, we obtain that

$$\nu\bigl(Q,-qP+\bigl(q^2+(i-2)(q+1)+q-i-1\bigr)Q,0\bigr)\geqslant(i-1)q+2(q-i-1).$$

The claim now follows. It implies that $d(G)\geqslant d_S(G)=(i-1)q$, with $S=(Q,Q,\ldots)$. □

References

[1] G.L. Feng, T.R.N. Rao, Decoding algebraic geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 2398–3302.

[2] A. Garcia, R.F. Lax, Goppa codes and Weierstrass gaps, in: H. Stichtenoth, M.A. Tsfasman (Eds.), Coding Theory and Algebraic Geometry, Proceedings, Luminy 1991, in: Springer Lect. Notes Math., vol. 1518, 1992, pp. 33–42.

[3] J.P. Hansen, H. Stichtenoth, Group codes on certain algebraic curves with many rational points, Appl. Algebra Engrg. Comm. Comput. 1 (1990) 67–77.

[4] T. Høholdt, J.H. van Lint, R. Pellikaan, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. I, Elsevier, Amsterdam, 1998 (Chapter 10).

[5] M. Homma, S.J. Kim, Toward the determination of the minimum distance of two-point codes on a Hermitian curve, Des. Codes Cryptogr. 37 (2005) 111–132.

[6] M. Homma, S.J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance, Des. Codes Cryptogr. 38 (2006) 55–81.

[7] M. Homma, S.J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic, Des. Codes Cryptogr. 39 (2006) 375–386.

[8] M. Homma, S.J. Kim, The complete determination of the minimum distance of two-point codes on a Hermitian curve, Des. Codes Cryptogr. 40 (2006) 5–24.

[9] C. Kirfel, R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, IEEE Trans. Inform. Theory 41 (1995) 1720–1732.

[10] P.V. Kumar, K. Yang, On the true minimum distance of Hermitian codes, in: AGCT-3, in: Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 99–107.

[11] B. Lundell, J. McCullough, A generalized floor bound for the minimum distance of geometric Goppa codes, J. Pure Appl. Algebra 207 (2006) 115–164.

[12] H. Maharaj, G.L. Matthews, G. Pirsic, Riemann–Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, J. Pure Appl. Algebra 195 (2005) 261–280.

[13] G.L. Matthews, Codes from the Suzuki function field, IEEE Trans. Inform. Theory 50 (2004) 2398–3302.

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

[15] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.