

Delta sets for divisors supported in two points

Iwan M. Duursma ^{*} and Seungkook Park [†]

October 8, 2008 / March 23, 2009

Abstract

In [8], the authors formulate new coset bounds for algebraic geometric codes. The bounds give improved lower bounds for the minimum distance of algebraic geometric codes as well as improved thresholds for algebraic geometric linear secret sharing schemes. The coset bounds depend on the choice of a sequence of divisors and on its intersection with a given set of divisors called a delta set. In this paper, we give general properties of delta sets and we analyze sequences of divisors supported in two points on Hermitian and Suzuki curves.

Introduction

The best known lower bounds for the minimum distance of an algebraic geometric code are the floor bound and the order bound. Until recently the bounds were not comparable. In [8], the authors improve both the Lundell-McCullough floor bound [14] and the Beelen order bound [2]. The improvements are formulated separately but are such that the improved order bound is always at least equal to the improved floor bound. The order bound uses a partition of a code as a union of cosets of decreasing size and combines estimates for each of the cosets. Each estimate requires the choice of an increasing sequence of divisors. The Beelen order bound uses sequences that increase by the same point P at each step, with the possibility to choose the point P differently for different cosets. This choice is sufficient to give the actual minimum distance for Hermitian two-point codes [2], [17]; the actual minimum distance of Hermitian two-point codes was first obtained in [10] using different methods. The improved coset bounds in [8] allow more general sequences and in this way we obtain better lower bounds for the minimum distance of Suzuki two-point codes.

Another direction where our results have applications is the determination of thresholds for algebraic geometric linear secret sharing schemes [4]. In such schemes, an algebraic function $f \in L(G)$ is evaluated in distinct points P_1, \dots, P_n, P . The values $f(P_i)$, for $P_i \in A$, uniquely determine the value $f(P)$ if and only if $L(G - A) = L(G - A - P)$. To

^{*}Department of Mathematics, University of Illinois at Urbana-Champaign (duursma@math.uiuc.edu)

[†]Department of Mathematical Sciences, University of Cincinnati (seung-kook.park@uc.edu)

see how the choice of the divisor G affects the size of a set A that has access to the value $f(P)$ we write $G = K + C + P$, where K is the canonical divisor class. The condition for access to the value $f(P)$ then becomes $L(A - C) \neq L(A - C - P)$, and in particular $|A| \geq \deg C$. We may assume $P \notin A$ and thus $L(A) \neq L(A - P)$. The sets A disjoint from P that can recover the value $f(P)$ therefore belong to the semigroup ideal

$$\Gamma_P(C) = \{A : L(A) \neq L(A - P) \wedge L(A - C) \neq L(A - C - P)\}.$$

A delta set is defined as the complement. It contains sets A that can not recover the value $f(P)$.

$$\Delta_P(C) = \{A : L(A) \neq L(A - P) \wedge L(A - C) = L(A - C - P)\}.$$

The main theorem in [8] gives as a lower bound for $|A|$, for $A \in \Gamma_P(C)$, the length of a strictly increasing sequence $A_1 \leq A_2 \leq \dots \leq A_w \in \Delta_P(C)$.

In this paper, we give general properties of delta sets and we analyze sequences of divisors supported in two points on Hermitian and Suzuki curves. Algebraic geometric codes are defined in Section 1. Section 2 expresses properties of algebraic geometric codes in terms of semigroup ideals of divisors. Section 3 gives lower bounds for the minimum distance of algebraic geometric codes and for thresholds of algebraic geometric linear secret sharing schemes. The results in the first three sections summarize results in [8] where more details can be found. Section 4 gives basic relations among delta sets. In Section 5, we define a discrepancy, for given points P and Q , as a divisor $A \in \Delta_P(Q) = \Delta_Q(P)$. Discrepancies are our main tool for analyzing and improving lower bounds for two-point codes. In Section 6, we give two proofs, one due to Beelen [2] and Park [17], and one new, for lower bounds for the minimum distance of Hermitian two-point codes. The lower bounds meet the actual minimum distances in [10]. In Section 7, we determine discrepancies for Suzuki curves, and we give examples that show that our bounds improve known bounds for Suzuki two-point codes.

1 Algebraic geometric codes

Let X/\mathbb{F} be an algebraic curve (absolutely irreducible, smooth, projective) of genus g over a finite field \mathbb{F} . Let $\mathbb{F}(X)$ be the function field of X/\mathbb{F} and let $\Omega(X)$ be the module of rational differentials of X/\mathbb{F} . Given a divisor E on X defined over \mathbb{F} , let $L(E) = \{f \in \mathbb{F}(X) \setminus \{0\} : (f) + E \geq 0\} \cup \{0\}$ and let $\Omega(E) = \{\omega \in \Omega(X) \setminus \{0\} : (\omega) \geq E\} \cup \{0\}$. Let K represent the canonical divisor class. For n distinct rational points P_1, \dots, P_n on X and for disjoint divisors $D = P_1 + \dots + P_n$ and G , the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\begin{aligned} \alpha_L & : L(G) \longrightarrow \mathbb{F}^n, \quad f \mapsto (f(P_1), \dots, f(P_n)), \\ \alpha_\Omega & : \Omega(G - D) \longrightarrow \mathbb{F}^n, \quad \omega \mapsto (\text{res}_{P_1}(\omega), \dots, \text{res}_{P_n}(\omega)). \end{aligned}$$

The maps establish isomorphisms $L(G)/L(G - D) \simeq C_L(D, G)$ and $\Omega(G - D)/\Omega(G) \simeq C_\Omega(D, G)$. With the Residue theorem, the images are orthogonal subspaces of \mathbb{F}^n . With the Riemann-Roch theorem they are maximal orthogonal subspaces. The Goppa lower bound for the minimum distance of the codes is

$$\begin{aligned} d(C_L(D, G)) &\geq \max\{0, \deg(D - G)\}, \\ d(C_\Omega(D, G)) &\geq \max\{0, \deg(G - K)\}. \end{aligned}$$

To analyse the minimum distance of the codes we use the following characterization.

Proposition 1.1. (*[8, Proposition 2.1]*)

$$\begin{aligned} d(C_L(D, G)) &= \min\{\deg A : 0 \leq A \leq D \mid L(G - D + A) \neq L(G - D)\}, \\ d(C_\Omega(D, G)) &= \min\{\deg A : 0 \leq A \leq D \mid L(K - G + A) \neq L(K - G)\}. \end{aligned}$$

Proof. There exists a nonzero word in $C_L(D, G)$ with support in A , for $0 \leq A \leq D$, if and only if $L(G - D + A)/L(G - D) \neq 0$. There exists a nonzero word in $C_\Omega(D, G)$ with support in A , for $0 \leq A \leq D$, if and only if $\Omega(G - A)/\Omega(G) \neq 0$ if and only if $L(K - G + A)/L(K - G) \neq 0$. \square

For a point P disjoint from D , consider the dual extensions of codes $C_\Omega(D, G) \subseteq C_\Omega(D, G - P)$ and $C_L(D, G - P) \subseteq C_L(D, G)$. In [8], it is explained how the pair defines a pair of dual linear secret sharing schemes. For the secret sharing application it is important to know the weight of vectors that are contained in a code but not in a subcode. To obtain estimates for such weights we use the following refinement of the proposition.

Lemma 1.2. *A divisor A , for $0 \leq A \leq D$, supports a word in $C_L(D, G) \setminus C_L(D, G - P)$ if and only if*

$$A \in \{0 \leq A \leq D : L(G - D + A) \neq L(G - P - D + A)\}.$$

A divisor A , for $0 \leq A \leq D$, supports a word in $C_\Omega(D, G - P) \setminus C_\Omega(D, G)$ if and only if

$$A \in \{0 \leq A \leq D : L(K - G + P + A) \neq L(K - G + A)\}.$$

Denote the two sets in the lemma by Γ_ω and Γ_f , respectively.

$$\begin{aligned} \Gamma_\omega &= \{0 \leq A \leq D : L(G - D + A) \neq L(G - P - D + A)\} \\ \Gamma_f &= \{0 \leq A \leq D : L(K - G + P + A) \neq L(K - G + A)\} \end{aligned}$$

We sketch the interpretation of the sets for secret sharing. The value $f(P)$, for $f \in L(G)$, is uniquely determined by $\{f(P_i) : P_i \in A\}$ if and only if $L(G - A) = L(G - A - P)$ if and only if $A \in \Gamma_f$. The residue $\text{res}_P(\omega)$, for $\omega \in \Omega(G - D - P)$, is uniquely determined by $\{\text{res}_{P_i}(\omega) : P_i \in A\}$ if and only if $\Omega(G - D + A - P) = \Omega(G - D + A)$ if and only if $A \in \Gamma_\omega$. The sets Γ_ω and Γ_f are in duality via $A \in \Gamma_\omega$ if and only if $D - A \notin \Gamma_f$.

Proposition 1.3.

$$\begin{aligned} d(C_L(D, G)/C_L(D, G - P)) &= \min\{\deg A : A \in \Gamma_\omega\}, \\ d(C_\Omega(D, G - P)/C_\Omega(D, G)) &= \min\{\deg A : A \in \Gamma_f\}. \end{aligned}$$

2 Semigroup ideals

Let X/\mathbb{F} be a curve over a field \mathbb{F} and let $\text{Pic}(X)$ be the group of divisor classes. Let $\Gamma = \{A : L(A) \neq 0\}$ be the semigroup of effective divisor classes. For a given point $P \in X$, let $\Gamma_P = \{A : L(A) \neq L(A - P)\}$ be the semigroup of effective divisor classes with no base point at P . For a divisor class C , define the semigroup ideal

$$\Gamma_P(C) = \{A \in \Gamma_P : A - C \in \Gamma_P\}.$$

The ideal structure of the semigroup $\Gamma_P(C)$ amounts to the property $A + E \in \Gamma_P(C)$ whenever $A \in \Gamma_P(C)$ and $E \in \Gamma_P$. For $A \in \Gamma_P(C)$, we can express $C = A - (A - C)$ as the difference of two divisors $A, A - C \in \Gamma_P$. We ask how small the degree of A can be in such an expression and we define

$$\gamma_P(C) = \min\{\deg A : A \in \Gamma_P(C)\}.$$

Lemma 2.1. *For a divisor C , $\gamma_P(C) \geq \max\{0, \deg C\}$. Moreover,*

$$\begin{aligned} \gamma_P(C) > 0 & \Leftrightarrow 0 \notin \Gamma_P(C) \\ & \Leftrightarrow L(-C) = L(-C - P). \\ \gamma_P(C) > \deg C & \Leftrightarrow C \notin \Gamma_P(C) \\ & \Leftrightarrow L(C) = L(C - P). \end{aligned}$$

Proposition 2.2. *For a point $P \notin D$,*

$$\begin{aligned} d(C_L(D, G)/C_L(D, G - P)) & \geq \gamma_P(D - G). \\ d(C_\Omega(D, G)/C_\Omega(D, G + P)) & \geq \gamma_P(G - K). \end{aligned}$$

Moreover,

$$\begin{aligned} C_L(D, G) \neq C_L(D, G - P) & \Rightarrow \gamma_P(D - G) > 0. \\ C_\Omega(D, G) \neq C_\Omega(D, G + P) & \Rightarrow \gamma_P(G - K) > 0. \end{aligned}$$

Proof. The first part is a restatement of Proposition 1.3. For the second part, use

$$\begin{aligned} C_L(D, G) \neq C_L(D, G - P) & \Leftrightarrow \begin{cases} L(G) \neq L(G - P) \\ L(G - D) = L(G - D - P) \end{cases} \\ C_\Omega(D, G) \neq C_\Omega(D, G + P) & \Leftrightarrow \begin{cases} \Omega(G - D) \neq \Omega(G + P - D) \\ \Omega(G) = \Omega(G + P) \end{cases} \end{aligned}$$

and apply the lemma with $C = D - G$ and $C = G - K$, respectively. \square

With the lemma $\gamma_P(D - G) > \deg(D - G)$ only if P is a base point for the divisor $D - G$. If P is not a basepoint for $D - G$ then the lower bound $\gamma_P(D - G) = \deg(D - G)$ is equal to the Goppa lower bound for the minimum distance of $C_L(D, G)$. Similarly, $\gamma_P(G - K) > \deg(G - K)$ only if P is a base point for the divisor $G - K$. Repeated application of the proposition gives the following Feng-Rao type lower bound for the minimum distance.

Proposition 2.3. *For a point $P \notin D$,*

$$\begin{aligned} d(C_L(D, G)) &\geq \min\{\gamma_P(D - G + iP) : i \geq 0\} \setminus \{0\}. \\ d(C_\Omega(D, G)) &\geq \min\{\gamma_P(G - K + iP) : i \geq 0\} \setminus \{0\}. \end{aligned}$$

3 Lower bounds

Let $\Gamma_P(C) = \{A \in \Gamma_P : A - C \in \Gamma_P\}$ as defined in the previous section. For the lower bounds in Propositions 2.2 and 2.3 we need to estimate the minimal degree $\gamma_P(C)$ of a divisor $A \in \Gamma_P(C)$. Let

$$\Delta_P(C) = \{A \in \Gamma_P : A - C \notin \Gamma_P\}$$

denote the complement of $\Gamma_P(C)$ in Γ_P . All divisors of sufficiently large degree belong to $\Gamma_P(C)$ while the degree of a divisor in $\Delta_P(C)$ is bounded.

Lemma 3.1. *For a curve X of genus g with canonical divisor K ,*

$$A \in \Delta_P(C) \Leftrightarrow K + C + P - A \in \Delta_P(C).$$

For $A \in \Delta_P(C)$,

$$\min\{0, \deg C\} \leq \deg A \leq \max\{2g - 1, \deg C + 2g - 1\}.$$

Proof. This follows from the definition together with the Riemann-Roch theorem. \square

We obtain lower bounds for the degree of $A \in \Gamma_P(C)$ by constructing increasing sequences of divisors in $\Delta_P(C)$.

Theorem 3.2. *([8, Theorem 5.3]) Let $\{A_1 \leq A_2 \leq \dots \leq A_w\} \subset \Delta_P(C)$ be a sequence of divisors with $A_{i+1} \geq A_i + P$, for $i = 1, \dots, w - 1$. Then $\deg A \geq w$, for every divisor $A \in \Gamma_P(C)$ with support disjoint from $A_w - A_1$.*

For the construction of sequences we consider two special cases. First we assume that $\{A_1 \leq A_2 \leq \dots \leq A_w\}$ is a subsequence of $\{B + iP : i \in \mathbb{Z}\}$, for some divisor B . For a given divisor B , let $\Delta_P(B, C) = \{B + iP : i \in \mathbb{Z}\} \cap \Delta_P(C)$.

Corollary 3.3. *For any choice of divisor B ,*

$$\gamma_P(C) \geq \#\Delta_P(B, C).$$

Proof. Every increasing sequence $A_1, A_2, \dots, A_w \in \Delta_P(B, C)$ meets the conditions of the theorem. \square

The lower bound $\#\Delta_P(B, C)$ is at least as good as the trivial estimate $\max\{0, \deg C\}$ in Lemma 2.1.

Lemma 3.4. (*[8, Lemma 5.4]*) *In general, $\#\Delta_P(B, C) - \#\Delta_P(B - C, -C) = \deg C$, and therefore $\#\Delta_P(B, C) \geq \max\{0, \deg C\}$. Moreover,*

$$\#\Delta_P(B, C) = \begin{cases} \deg C, & \text{if } C \in \Gamma_P. \\ 0, & \text{if } -C \in \Gamma_P. \end{cases}$$

For the second special case, we assume that $\{A_1 \leq A_2 \leq \dots \leq A_w\}$ is a subsequence of $\{B + iP : i \leq 0\} \cup \{B + Z + iP : i > 0\}$, for some divisor B and for a divisor $Z \geq 0$. We write $\Delta_P(\leq B, C) = \{B + iP : i \leq 0\} \cap \Delta_P(C)$ and $\Delta_P(> B + Z, C) = \{B + Z + iP : i > 0\} \cap \Delta_P(C)$.

Theorem 3.5. (*ABZ bound for cosets [8, Theorem 6.6]*) *Let C be a divisor and let P be a point. Let $K + C = A + B + Z$, such that $Z \geq 0$. For a divisor $D' \in \Gamma_P(C)$ such that $D' \cap Z = \emptyset$,*

$$\deg D' \geq \#\Delta_P(\leq A, C) + \#\Delta_P(\leq B, C).$$

In the following sections we analyze the optimization of the bounds in Theorem 3.2 as well as the two special cases in Corollary 3.3 and Theorem 3.5. In each case we obtain lower bounds for the weight of words in a coset. The bounds have to be applied repeatedly to obtain lower bounds for the minimum distance of a code. The repeated application can be carried out for the same P , such as in Proposition 2.3, or with different choices for P at each iteration. Repeated application of Corollary 3.3 with $P = Q_0, Q_1, \dots, Q_{r-1}$ gives the Beelen order bound which can be stated as follows.

Theorem 3.6. (*Beelen Order bound [2]*) *Let $C_\Omega(D, G)$ be an algebraic geometric code, and let $G = K + C$. For a sequence of points Q_0, \dots, Q_{r-1} disjoint from D , let $C_0 = C$ and $C_{i+1} = C_i + Q_i$, for $i = 0, \dots, r-1$. For r large enough, and for a sequence of divisors B_0, \dots, B_{r-1} , such that $\#\Delta_{Q_i}(B_i, C_i) \geq \#\Delta_{Q_i}(0, C_i)$,*

$$d(C_\Omega(D, G)) \geq \min\{\#\Delta_{Q_i}(B_i, C_i)\} \setminus \{0\}$$

The exclusion of $\{0\}$ before taking the minimum is justified by $\gamma_{Q_i}(C_i) > 0$ when $C_\Omega(D, K + C_i) \neq C_\Omega(D, K + C_i + Q_i)$, as in Proposition 2.2, together with the observation $\gamma_{Q_i}(C_i) > 0$ if and only if $0 \in \Delta_{Q_i}(0, C_i)$ if and only if $\#\Delta_{Q_i}(0, C_i) > 0$. The following bound is the best known floor bound. In some cases it yields better results than the Beelen order bound.

Theorem 3.7. (*ABZ bound for codes [8, Theorem 2.4]*) *Let $G = K + C = A + B + Z$, for $Z \geq 0$. For D with $D \cap Z = \emptyset$, $d(C_\Omega(D, G)) \geq l(A) - l(A - C) + l(B) - l(B - C)$.*

If we replace Corollary 3.3 in the Beelen order bound with Theorem 3.5 then the resulting lower bound is at least the bound of Theorem 3.7. This follows with two applications of the inequality $\#\Delta_P(\leq B, C) \geq l(B) - l(B - C)$ [8, Lemma 6.5].

4 Delta sets

For a given divisor C and a point P , Theorem 3.2 gives a lower bound for $\deg A$, for $A \in \Gamma_P(C) = \{A \in \Gamma_P : A - C \in \Gamma_P\}$. The lower bound depends on properties of the complement $\Delta_P(C) = \{A \in \Gamma_P : A - C \notin \Gamma_P\}$. Corollary 3.3 and Theorem 3.5 are formulated in terms of the subsets $\Delta_P(B, C)$ and $\Delta_P(\leq B, C)$, respectively, for a suitable choice of divisor B . The computation of optimal lower bounds requires either a complete description of the delta set (for Theorem 3.2) or at least a description from which the size of the sets $\Delta_P(B, C)$ or $\Delta_P(\leq B, C)$ can be computed (for Corollary 3.3 and Theorem 3.5, respectively).

We collect some straightforward relations that can be used to construct delta sets, to compare delta sets, or to compare sizes of delta sets. Most relations come in pairs such that $A \in \Delta_P(C)$ (i.e., $A \in \Gamma_P, A - C \notin \Gamma_P$) corresponds to $A - C \in \Delta_P(-C)$ (i.e., $A \notin \Gamma_P, A - C \in \Gamma_P$). The proofs in this section are entirely straightforward, in most cases applying the definition of $\Delta_P(C)$ is enough, and no proofs are included.

In general, for $E \in \Gamma_P$, $\Delta_P(C) \subset \Delta_P(C + E)$. The following lemma gives a precise version and its dual.

Lemma 4.1. *Let C be a divisor and P a point. For $E \in \Gamma_P$,*

$$\begin{aligned} A \in \Delta_P(C) & \\ \Leftrightarrow A \in \Delta_P(C + E) \wedge A + E \in \Delta_P(C + E). & \\ A - C - E \in \Delta_P(-C - E) & \\ \Leftrightarrow A - C - E \in \Delta_P(-C) \wedge A - C \in \Delta_P(-C). & \end{aligned}$$

For the four relations on the right we describe when the reverse implication fails.

Lemma 4.2.

$$\begin{aligned} A \in \Delta_P(C + E) \wedge A \notin \Delta_P(C) & \\ \Leftrightarrow A \in \Delta_P(C + E) \wedge A + E \notin \Delta_P(C + E) & \\ \Leftrightarrow A \in \Delta_P(C + E) \wedge A - C \in \Gamma_P & \\ \Leftrightarrow A - C \in \Delta_P(E) \wedge A \in \Gamma_P. & \end{aligned}$$

$$\begin{aligned} A - C \in \Delta_P(-C) \wedge A - C - E \notin \Delta_P(-C - E) & \\ \Leftrightarrow A - C \in \Delta_P(-C) \wedge A - C - E \notin \Delta_P(-C) & \\ \Leftrightarrow A - C \in \Delta_P(-C) \wedge A - C - E \notin \Gamma & \\ \Leftrightarrow A - C \in \Delta_P(E) \wedge A \notin \Gamma_P. & \end{aligned}$$

The second group follows with a substitution $A \mapsto A - C - E, C \mapsto -C - E$.

Lemma 4.3.

$$\begin{aligned}
A - C - E \in \Delta_P(-C) \wedge A - C - E \notin \Delta_P(-C - E) \\
\Leftrightarrow A - C - E \in \Delta_P(-C) \wedge A - C \notin \Delta_P(-C) \\
\Leftrightarrow A - C - E \in \Delta_P(-C) \wedge A \in \Gamma_P \\
\Leftrightarrow A \in \Delta_P(E) \wedge A - C - E \in \Gamma_P.
\end{aligned}$$

$$\begin{aligned}
A \in \Delta_P(C + E) \wedge A - E \notin \Delta_P(C) \\
\Leftrightarrow A \in \Delta_P(C + E) \wedge A - E \notin \Delta_P(C + E) \\
\Leftrightarrow A \in \Delta_P(C + E) \wedge A - E \notin \Gamma \\
\Leftrightarrow A \in \Delta_P(E) \wedge A - C - E \notin \Gamma_P.
\end{aligned}$$

For divisors B and C and for a point P , let

$$\begin{aligned}
I_P(B, C) &= \{i \in \mathbb{Z} : B + iP \in \Delta_P(C)\} \\
&= \{i \in \mathbb{Z} : B + iP \in \Gamma_P, B - C + iP \notin \Gamma_P\}. \\
I_P^*(B, C) &= \{i \in \mathbb{Z} : B - C + iP \in \Delta_P(-C)\} \\
&= \{i \in \mathbb{Z} : B - C + iP \in \Gamma_P, B + iP \notin \Gamma_P\}.
\end{aligned}$$

We rephrase some of the previous relations.

Lemma 4.4.

$$\begin{aligned}
I_P(B, C) &= I_P(B, C + E) \cap I_P(B + E, C + E). \\
I_P^*(B, C + E) &= I_P^*(B - E, C) \cap I_P^*(B, C).
\end{aligned}$$

Lemma 4.5.

$$\begin{aligned}
i \in I_P(B, C + E) \setminus I_P(B, C) &\Leftrightarrow i \in I_P(B - C, E) \wedge B + iP \in \Gamma_P, \\
i \in I_P^*(B, C) \setminus I_P^*(B, C + E) &\Leftrightarrow i \in I_P(B - C, E) \wedge B + iP \notin \Gamma_P. \\
i \in I_P^*(B - E, C) \setminus I_P^*(B, C + E) &\Leftrightarrow i \in I_P(B, E) \wedge B - C + E + iP \in \Gamma_P, \\
i \in I_P(B, C + E) \setminus I_P(B - E, C) &\Leftrightarrow i \in I_P(B, E) \wedge B - C + E + iP \notin \Gamma_P.
\end{aligned}$$

For each of the sets $I_P(B - C, E)$ and $I_P(B, E)$ we obtain a partition into two subsets that are in duality.

Proposition 4.6.

$$\begin{aligned}
I_P(B, C + E) \setminus I_P(B, C) \cup I_P^*(B, C) \setminus I_P^*(B, C + E) &= I_P(B - C, E). \\
I_P(B, C + E) \setminus I_P(B - E, C) \cup I_P^*(B - E, C) \setminus I_P^*(B, C + E) &= I_P(B, E).
\end{aligned}$$

We describe the first partition for the following choice of divisors. For divisors B_0 and C_0 of degree zero, and for a point Q , let $B = B_0, C = C_0 - 2gQ, E = 4gQ$. Then

$$I_P(B_0, C_0 + 2gQ) \cup I_P(B_0 - C_0 + 2gQ, -C_0 + 2gQ) = I_P(B_0 - C_0 + 2gQ, 4gQ).$$

In general,

$$\{0, \dots, 2g - 1\} \subset I_P(B_0 - C_0 + 2gQ, 4gQ) \subset \{-2g, \dots, 4g - 1\}.$$

The first inclusion follows with the definition of $I_P(B, C)$. For the second inclusion, Lemma 3.1 gives $0 \leq i + 2g \leq 6g - 1$.

Proposition 4.7. *Let B_0 and C_0 be divisor classes of degree zero. Define partitions $\{-2g, \dots, -1\} = N_1 \cup G_1$, $\{0, \dots, 2g - 1\} = N_2 \cup G_2$, and $\{2g, \dots, 4g - 1\} = N_3 \cup G_3$, such that*

$$\begin{aligned} k \in N_1 &\Leftrightarrow B_0 - C_0 + 2gQ + kP \in \Gamma_P, \\ k \in N_2 &\Leftrightarrow B_0 + kP \in \Gamma_P, \\ k \in N_3 &\Leftrightarrow B_0 - C_0 - 2gQ + kP \in \Gamma_P. \end{aligned}$$

Then $\#N_i = \#G_i = g$, for $i = 1, 2, 3$. Moreover

$$I_P(B_0, C_0 + 2gQ) = N_2 \cup G_3 \quad \text{and} \quad I_P(B_0 - C_0 + 2gQ, -C_0 + 2gQ) = N_1 \cup G_2.$$

Proof.

	$\{-2g, \dots, -1\}$	$\{0, \dots, 2g - 1\}$	$\{2g, \dots, 4g - 1\}$
$\{k : B_0 + kP \in \Gamma_P \wedge B_0 - C_0 - 2gQ + kP \in \Gamma_P\}$	—	—	N_3
$\{k : B_0 + kP \in \Gamma_P \wedge B_0 - C_0 - 2gQ + kP \notin \Gamma_P\}$	—	N_2	G_3
$\{k : B_0 + kP \notin \Gamma_P \wedge B_0 - C_0 + 2gQ + kP \in \Gamma_P\}$	N_1	G_2	—
$\{k : B_0 + kP \notin \Gamma_P \wedge B_0 - C_0 + 2gQ + kP \notin \Gamma_P\}$	G_1	—	—

□

5 Discrepancies

We continue the description of a delta set $\Delta_P(C)$ in terms of other known delta sets. The results in the previous section show that differences between similar delta sets, such as $\Delta_P(C + E)$ and $\Delta_P(C)$, for $E \in \Gamma_P$, can be described in terms of the delta set $\Delta_P(E)$. In this section, we refine the results for the special case that $E = Q$ is a point different from P .

Lemma 5.1. For distinct points P and Q , $\Delta_P(Q) = \Delta_Q(P)$.

Proof.

$$\begin{aligned} A \in \Delta_P(Q) &\Leftrightarrow L(A) \neq L(A - P) \wedge L(A - Q) = L(A - Q - P) \\ &\Leftrightarrow L(A) \neq L(A - Q) \wedge L(A - P) = L(A - P - Q) \Leftrightarrow A \in \Delta_Q(P). \end{aligned}$$

□

Let $D(P, Q) = \Delta_P(Q) = \Delta_Q(P)$. We call a divisor $A \in D(P, Q)$ a discrepancy for the points P and Q .

Lemma 5.2. A divisor $A \in D(P, Q)$ is of degree $0 \leq \deg A \leq 2g$. The cases $\deg A = 0$ and $\deg A = 2g$ correspond to unique divisor classes $A = 0$ and $A = K + P + Q$, respectively. Furthermore,

$$A \in D(P, Q) \Leftrightarrow K + P + Q - A \in D(P, Q).$$

Proof. Use Lemma 3.1.

□

Lemma 5.3. For distinct points P and Q , and for a divisor B ,

$$\Delta_P(B, Q) = \{B + iP : i \in \mathbb{Z}\} \cap \Delta_P(Q) = \{B + kP\}$$

for k minimal such that $L(B + kP) \neq L(B + kP - Q)$. In general, $B + iP \in \Gamma_Q$ if and only if $i \geq k$.

Proof.

$$\begin{aligned} B + kP \in \Delta_P(Q) &\Leftrightarrow B + kP \in \Delta_Q(P) \\ &\Leftrightarrow B + kP \in \Gamma_Q \wedge B + (k - 1)P \notin \Gamma_Q. \end{aligned}$$

□

Define functions $\sigma = \sigma_B, \tau = \tau_B : \mathbb{Z} \rightarrow \mathbb{Z}$ such that

$$\begin{aligned} \Delta_P(B + jQ, Q) &= \{B + \tau(j)P + jQ\}, \\ \Delta_Q(B + iP, P) &= \{B + iP + \sigma(i)Q\}. \end{aligned}$$

So that

$$\begin{aligned} B + iP + jQ \in \Gamma_P &\Leftrightarrow j \geq \sigma(i), \\ B + iP + jQ \in \Gamma_Q &\Leftrightarrow i \geq \tau(j). \end{aligned}$$

Theorem 5.4. For distinct points P and Q , and for a divisor B ,

$$\begin{aligned} & \{B + iP + jQ : i, j \in \mathbb{Z}\} \cap D(P, Q) \\ &= \{B + iP + \sigma(i)Q : i \in \mathbb{Z}\} = \{B + \tau(j)P + jQ : j \in \mathbb{Z}\}. \end{aligned}$$

The functions $\sigma = \sigma_B$ and $\tau = \tau_B$ are mutual inverses and describe permutations of the integers. For a divisor B of degree zero, and for $i \in \mathbb{Z}$, $-i \leq \sigma(i), \tau(i) \leq 2g - i$. For m such that $mP \sim mQ$, the functions $i + \sigma(i), j + \tau(j)$ only depend on i, j modulo m . The functions σ, τ are determined by their images on a full set of representatives for $\mathbb{Z}/m\mathbb{Z}$.

Proof. For the second claim use Lemma 5.2. Finally, $B + iP + jQ \in D(P, Q)$ only depends on the divisor class of $B + iP + jQ$ and therefore

$$B + iP + jQ \in D(P, Q) \Leftrightarrow B + (i + m)P + (j - m)Q \in D(P, Q),$$

so that $\sigma(i + m) = \sigma(i) - m$. □

We write $D_B(P, Q)$ for the subset of discrepancies $\{B + iP + jQ : i, j \in \mathbb{Z}\} \cap D(P, Q)$. The discrepancies $D_B(P, Q)$ serve as an index set for a common basis of the vector spaces $L(B + aP + bQ)$, for $a, b \in \mathbb{Z}$.

Theorem 5.5.

$$\dim L(B + aP + bQ) = \#\{B + iP + jQ \in D(P, Q) : i \leq a \wedge j \leq b\}.$$

Proof. $\dim L(B + aP + bQ) \neq \dim L(B + aP + bQ - P)$ if and only if $B + aP + bQ \in \Gamma_P$ if and only if $B + aP + bQ \geq (B + aP)_P \in D_B(P, Q)$ if and only if there exists $B + iP + jP \in D_B(P, Q)$ with $i = a, j \leq b$. Use induction on a to complete the proof. □

For given distinct points P and Q and divisors B_0 and C_0 of degree zero, let

$$\begin{array}{llll} \sigma = \sigma_{B_0} & \tau = \tau_{B_0} & d_P(k) = k + \sigma(k) & d_Q(\ell) = \tau(\ell) + \ell. \\ \sigma' = \sigma_{B_0 - C_0} & \tau' = \tau_{B_0 - C_0} & d'_P(k) = k + \sigma'(k) & d'_Q(\ell) = \tau'(\ell) + \ell. \end{array}$$

For $mP \sim mQ$, the functions d_P, d_Q and d'_P, d'_Q are defined modulo m .

Theorem 5.6. Let $A = B_0 + kP + \ell Q$ and $C = C_0 + iP + jQ$. Then

$$A \in \Delta_P(C + Q) \Leftrightarrow \deg A \geq d_P(k) \wedge \deg(A - C) \leq d'_P(k - i).$$

Moreover,

$$\begin{aligned} d_P(k) = \deg A \leq d'_P(k - i) + \deg C &\Leftrightarrow A \in \Delta_P(C + Q) \wedge A - Q \notin \Delta_P(C + Q). \\ d_P(k) \leq \deg A = d'_P(k - i) + \deg C &\Leftrightarrow A \in \Delta_P(C + Q) \wedge A + Q \notin \Delta_P(C + Q), \\ &\Leftrightarrow A \in \Delta_P(C + Q) \wedge A \notin \Delta_P(C). \end{aligned}$$

Proof. $A \in \Gamma_P$ if and only if $\ell \geq \sigma(k)$, and $A-C-Q \notin \Gamma_P$ if and only if $\ell-j-1 < \sigma'(k-i)$. The last claims use Lemma 4.3 (part two) and Lemma 4.2 (part one), respectively. \square

Lemma 5.7. *Let $A = B_0 + kP + \ell Q$ and $C = C_0 + iP + jQ$.*

$$d_P(k) = \deg A \leq d'_P(k-i) + \deg C \Leftrightarrow \begin{cases} k = k^+ = d_Q(\ell) - \ell \wedge \\ d_Q(\ell) - d'_P(k^+ - i) \leq i + j. \end{cases}$$

$$d_P(k) \leq \deg A = d'_P(k-i) + \deg C \Leftrightarrow \begin{cases} k = k^- = d'_Q(\ell - j) - \ell + i + j \wedge \\ d_P(k^-) - d'_Q(\ell - j) \leq i + j. \end{cases}$$

We use the lemma to create tables for each of the three equivalences in Theorem 5.6. The tables N and K are used to compute the size of a delta set or to construct a delta set, respectively (Example 6.11). The tables N^+ and N^- are used in the optimization of the order bound (Example 7.5). The tables K^+ and K^- provide more information that can be used for further improvements with the ABZ bound (Example 7.6). In all cases, let $A = B_0 + kP + \ell Q$, and let $C = C_0 + iP + jQ$.

$$A \in \Delta_P(C + Q) \wedge A \notin \Delta_P(C).$$

$$K_\ell(i, j) = d'_Q(\ell - j) - \ell + i + j, \quad N_\ell(i, j) = \begin{cases} 1 & \text{if } d_P(k^-) - d'_Q(\ell - j) \leq i + j \\ 0 & \text{if } d_P(k^-) - d'_Q(\ell - j) > i + j \end{cases}$$

The table $N_\ell(i, j)$ indicates whether there exists $A \in \Delta_P(B_0 + \ell Q, C + Q) \setminus \Delta_P(B_0 + \ell Q, C)$. In the affirmative case ($N=1$), the table $K_\ell(i, j)$ gives $k = k^-$ such that $A = B_0 + kP + \ell Q$. The table N is sufficient for computing the size of a delta set, the table K moreover provides the elements of a delta set.

$$A \in \Delta_P(C + Q) \wedge A - Q \notin \Delta_P(C + Q).$$

$$K_i^+(j, \ell) = d_Q(\ell) - \ell, \quad N_i^+(j, \ell) = \begin{cases} 1 & \text{if } d_Q(\ell) - d'_P(k^+ - i) \leq i + j. \\ 0 & \text{if } d_Q(\ell) - d'_P(k^+ - i) > i + j. \end{cases}$$

The table $N_i^+(j, \ell)$ indicates whether there exists $A \in \Delta_P(B_0 + \ell Q, C + Q)$ with $A - Q \notin \Delta_P(B_0 + \ell Q - Q, C + Q)$. In the affirmative case ($N=1$), the table $K_i^+(j, \ell)$ gives $k = k^+$ such that $A = B_0 + kP + \ell Q$. The table N^+ is sufficient to obtain the size of the difference of two delta sets, the table K^+ moreover provides the elements for the difference $I_P(B_0 + \ell Q, C + Q) \setminus I_P(B_0 + \ell Q - Q, C + Q)$.

$$A \in \Delta_P(C + Q) \wedge A + Q \notin \Delta_P(C + Q).$$

$$K_i^-(j, \ell) = d'_Q(\ell - j) - \ell + i + j, \quad N_i^-(j, \ell) = \begin{cases} 1 & \text{if } d_P(k^-) - d'_Q(\ell - j) \leq i + j \\ 0 & \text{if } d_P(k^-) - d'_Q(\ell - j) > i + j \end{cases}$$

The table $N_i^-(j, \ell)$ indicates whether there exists $A \in \Delta_P(B_0 + \ell Q, C + Q)$ with $A + Q \notin \Delta_P(B_0 + \ell Q + Q, C + Q)$. In the affirmative case ($N=1$), the table $K_i^-(j, \ell)$ gives $k = k^-$ such that $A = B_0 + kP + \ell Q$. The table N^- is sufficient to obtain the size of the opposite difference of two delta sets, the table K^- moreover provides the elements for the difference $I_P(B_0 + \ell Q, C + Q) \setminus I_P(B_0 + \ell Q + Q, C + Q)$.

6 Hermitian curves

Let X be the Hermitian curve over \mathbb{F}_{q^2} defined by the equation $y^q + y = x^{q+1}$. The curve has $q^3 + 1$ rational points and genus $g = q(q-1)/2$. Let P and Q be two distinct rational points. We will give a description of the set

$$D_0(P, Q) = D(P, Q) \cap \{iP + jQ : i, j \in \mathbb{Z}\}.$$

We use this description to determine lower bounds for $\gamma_P(C)$, for $C \in \{iP + jQ : i, j \in \mathbb{Z}\}$. The only property of the two rational points that we use is that lines intersect the pair (P, Q) with one of the multiplicities

$$\begin{array}{ccc} (0, 0) & (0, 1) & (0, q+1) \\ (1, 0) & \underline{(1, 1)} & \\ (q+1, 0) & & \end{array}$$

The curve is a smooth plane curve and if H is the intersection divisor of a line then $K = (q-2)H$ represents the canonical class. We have $H \sim (q+1)P \sim (q+1)Q$ and $m(P-Q)$ is principal for $m = q+1$.

Proposition 6.1. *The m inequivalent divisor classes in $D_0(P, Q)$ are represented by the divisors*

$$dH - dP - dQ, \quad \text{for } d = 0, 1, \dots, q.$$

Proof. Since $m = q+1$ is minimal such that $mP \sim mQ$, the divisors are inequivalent. As multiples of $H - P - Q \in \Gamma_P$, each of the divisors $dH - dP - dQ \in \Gamma_P$, for $d = 0, 1, \dots, q$. A divisor $A \in \Gamma_P$ is a discrepancy if and only if $K + P + Q - A \in \Gamma_P$. Now use $K + P + Q = (q-2)H + P + Q = q(H - P - Q)$. \square

The function y has divisor $y = (q+1)(P_0 - P_\infty)$, where $P_0 = (0, 0)$ and $P_\infty = (0 : 1 : 0)$. Moreover $L(H - P_0 - P_\infty) = \langle x \rangle$.

Corollary 6.2. *The ring O of functions that are regular outside P_0 and P_∞ has a basis $\langle x^i y^j \mid 0 \leq i \leq q, j \in \mathbb{Z} \rangle$ as vector space over \mathbb{F}_{q^2} .*

Proof. Theorem 5.5. \square

Lemma 6.3. *Let $C = dH - aP - bQ$, for $0 \leq a \leq q, 0 \leq b \leq q+1$.*

$$C \in \Gamma_P \Leftrightarrow d > a \text{ or } d = a \geq b.$$

Proof. We use Lemma 5.3 together with Proposition 6.1. We may assume $H = (q+1)Q$. Then, $dH - aP - bQ \in \Gamma_P$ if and only if $dH - aP - bQ \geq aH - aP - aQ$ if and only if $d > a$ or $d = a \geq b$. \square

Proposition 6.4. *Let $C = dH - aP - bQ$, for $0 \leq a, b \leq q$. The set $\Delta_P(-C) = \{A \in \Gamma_P : A + C \notin \Gamma_P\}$ contains the following elements*

$$\begin{aligned} (q-1-d-r)H - (q-a)P, & \quad \text{for } d \leq d+r < a. \\ sH, & \quad \text{for } d \leq d+s < a. \\ sH - (d+s-a)P & \quad \text{for } d \leq a \leq d+s < b. \end{aligned}$$

Proof. With the lemma, $A = (q-1-d-r)H - (q-a)P \in \Gamma_P$ for $q-a \leq q-1-d-r$, and $A+C = (q-1-r)H - qP - bQ \notin \Gamma_P$ for $r \geq 0$. Clearly, $A = sH \in \Gamma_P$ for $s \geq 0$, and $A+C = (d+s)H - aP - bQ \notin \Gamma_P$ for $a > d+s$. Finally, $A = sH - (d+s-a)P \in \Gamma_P$ for $0 \leq d+s-a \leq s$, and $A+C = (d+s)H - (d+s)P - bQ \notin \Gamma_P$ for $b > d+s$. \square

Lemma 6.5. *Let $0 \leq a, b \leq q$. There exists a form of degree d that intersects the curve in (P, Q) with precise multiplicities (a, b) if and only if $0 \leq a, b \leq d$.*

Proof. Such a curve exists if and only if $dH - aP - bQ \in \Gamma_P \cap \Gamma_Q$. With Lemma 6.3, the latter holds if and only if $0 \leq a, b \leq d$. \square

Lemma 6.6. *For $d \geq 0$, let C be a divisor with $dH - dP - dQ \leq C \leq dH$. Then C has no base points and $\gamma_P(C) = \deg C$.*

Proof. Since C is equivalent to an effective divisor with support in P and Q , those two points are the only candidates for the base points. With Lemma 6.3, $C \in \Gamma_P \cap \Gamma_Q$, and therefore neither P nor Q is a base point. The last claim uses Proposition ???. \square

Proposition 6.7. *Let*

$$\begin{aligned} C &= dH - aP - bQ, & \text{for } d \in \mathbb{Z}, 0 \leq a, b \leq q, \\ A &= jH + i(H - P), & \text{for } j \in \mathbb{Z}, 0 \leq i \leq q. \end{aligned}$$

Then $A \in \Delta_P(C)$ if and only if

$$\begin{cases} 0 \leq j \leq (d-a+q-1), & \text{if } 0 \leq i < a-b \\ 0 \leq j \leq (d-a+q-2), & \text{if } a-b \leq i < a \\ 0 \leq j \leq (d-a-1), & \text{if } a \leq i < a-b+q+1 \\ 0 \leq j \leq (d-a-2), & \text{if } a-b+q+1 \leq i \leq q \end{cases}$$

Proof. For $A - C$ we write

$$\begin{cases} (j+i-d+1)H - (i-a)P - (q+1-b)Q, & \text{if } i-a \geq 0. \\ (j+i-d+2)H - (i-a+q+1)P - (q+1-b)Q, & \text{if } i-a < 0. \end{cases}$$

With Lemma 6.3, $A - C \notin \Gamma_P$ if and only if

$$\begin{cases} j < d-a-1, \text{ or } j = d-a-1, i-a < q+1-b, & \text{if } i-a \geq 0. \\ j < d-a-1+q \text{ or } j = d-a-1+q, i-a < -b, & \text{if } i-a < 0. \end{cases}$$

In combination with $A \in \Gamma_P$ if and only if $j \geq 0$, this proves the claim. \square

Corollary 6.8. Let $C = dH - aP - bQ$, for $0 \leq a, b \leq q$.

For $a - d < 0$,

$$\Delta_P(-C) = \emptyset, \quad \#\Delta_P(0, C) = \deg C.$$

For $0 \leq a - d \leq q - 1$,

$$\begin{aligned} \#\Delta_P(0, C) &= a(q - 1 - a + d) + \max\{0, a - b\}. \\ \#\Delta_P(0, -C) &= (q + 1 - a)(a - d) + \max\{0, b - a\}. \end{aligned}$$

For $a - d > q - 1$,

$$\Delta_P(C) = \emptyset, \quad \#\Delta_P(0, -C) = -\deg C.$$

Theorem 6.9. Let $C = dH - aP - bQ$, for $d \in \mathbb{Z}$, and for $0 \leq a, b \leq q$. Then

$$\begin{aligned} (\text{Case 1 : } a, b \leq d) & \quad \gamma_P(C) = \gamma_Q(C) = \deg C. \\ (\text{Case 2a : } b \leq d \leq a) & \quad \gamma_P(C) \geq \deg C + a - d. \\ (\text{Case 2b : } a \leq d \leq b) & \quad \gamma_Q(C) \geq \deg C + b - d. \\ (\text{Case 3a : } d \leq a \leq b, a < q) & \quad \gamma_P(C) \geq \deg C + a - d + b - d. \\ (\text{Case 3b : } d \leq b \leq a, b < q) & \quad \gamma_Q(C) \geq \deg C + a - d + b - d. \\ (\text{Case 4 : } d \leq a = b = q) & \quad \gamma_P(C) = \gamma_Q(C) \geq \deg C + q - d. \end{aligned}$$

Proof. (Case 1) uses Lemma 6.6. The lower bounds follow from Proposition 6.4 by using $\gamma_P(C) = \deg C + \gamma_P(-C)$. Or we can obtain the lower bounds from Corollary 6.8 in combination with $\gamma_P(C) \geq \#\Delta_P(0, C)$ (Corollary 3.3). For $0 \leq a - d \leq q - 1$,

$$\#\Delta_{P_\infty}(0, C) = a(q - 1 - a + d) + \max\{0, a - b\}.$$

(Case 2a: $b \leq d \leq a$) $a(q - 1 - a + d) + a - b - d(q - 1) + b - d = (a - d)(q - a) \geq 0$.

(Case 3a : $d \leq a \leq b$) $a(q - 1 - a + d) + 0 - d(q - 1) = (a - d)(q - 1 - a) \geq 0$.

(Case 4 : $d \leq a = b = q$) $q(d - 1) = d(q + 1) - q - q + (q - d)$. □

Theorem 6.10. For $G = K + C$, and for $D \cap S = \emptyset$, the algebraic geometric code $C_\Omega(D, G)$ has minimum distance $d \geq \gamma(C; S)$. Let $C = dH - aP - bQ$, for $d \in \mathbb{Z}$, and for $0 \leq a, b \leq q$. Then

$$\begin{aligned} (\text{Case 1 : } a, b \leq d) & \quad \gamma(C) \geq \deg C. \\ (\text{Case 2a : } b \leq d \leq a) & \quad \gamma(C; P) \geq \deg C + a - d. \\ (\text{Case 2b : } a \leq d \leq b) & \quad \gamma(C; Q) \geq \deg C + b - d. \\ (\text{Case 3a : } d \leq a \leq b, a < q) & \quad \gamma(C; P, Q) \geq \deg C + a - d + b - d. \\ (\text{Case 3b : } d \leq b \leq a, b < q) & \quad \gamma(C; P, Q) \geq \deg C + a - d + b - d. \\ (\text{Case 4 : } d \leq a = b = q) & \quad \gamma(C; P) = \gamma(C; Q) \geq \deg C + q - d. \end{aligned}$$

Proof. Use the order bound with

(Case 2a: $b \leq d \leq a$) $Q_0 = \dots = Q_{a-d-1} = P$.

(Case 3a : $d \leq a \leq b$) $Q_0 = \dots = Q_{a-d-1} = P, Q_{a-d} = \dots = Q_{a-d+b-d-1} = Q$.

(Case 4 : $d \leq a = b = q$) $Q_0 = \dots = Q_{q-d-1} = P$. □

The following example illustrates the use of the tables $K_\ell(i, j)$ and $N_\ell(i, j)$ for constructing a delta set $\Delta_P(\ell Q, iP + jQ + Q)$ (Lemma 5.7). In this case, the functions $d_P = d_Q = d'_P = d'_Q$ all agree and we can omit the index.

Example 6.11. For the Hermitian curve of degree four, the genus $g = 3$. The discrepancies $D_0(P, Q)$ are represented by the divisors $0, H - P - Q, 2H - 2P - 2Q, 3H - 3P - 3Q$. In particular, $d(k) = 0, 2, 4, 6$, for $k = 0, -1, -2, -3$ modulo 4, respectively.

$(\ell = 0, i = 1)$	j	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4
	$d(\ell - j)$	2	4	6	0	2	4	6	0	2	4	6	0
(K)	k	(-4)	(-1)	(2)	(-3)	0	3	6	(1)	4	7	10	(5)
	$d(k)$	0	2	4	6	0	2	4	6	0	2	4	6
	$d(k) - d(\ell - j)$	-2	-2	-2	6	-2	-2	-2	6	-2	-2	-2	6
(N)	$\leq i + j$	0	0	0	0	1	1	1	0	1	1	1	0

The value for $k = d(\ell - j) - \ell + i + j$. Row (K) gives the difference $\Delta_P(\ell Q, iP + jQ + Q) \setminus \Delta_P(\ell Q, iP + jQ) = \{kP + \ell Q\} \cap \Gamma_P$, with empty intersection if and only if k appears in parentheses. Row (N) has the decision whether the difference is empty (N=0) or nonempty (N=1). As a special case, we see that $\Delta_P(0, P + 2Q) = \{0, 3P, 6P, 4P\}$. The numbers in parentheses illustrate the duality in Proposition 4.7.

$$\begin{aligned} \Delta_P(0, P + 5Q) &= 0 + \{0, 3P, 6P, 4P, 7P, 10P\}, \\ \Delta_P(-P + 7Q, -P + 7Q) &= (-P + 7Q) + \{-4P, -P, 2P, -3P, P, 5P\}. \end{aligned}$$

With $-P + 7Q \sim 7P - Q$,

$$\Delta_P(-Q, -P + 7Q) = \{3P - Q, 6P - Q, 9P - Q, 4P - Q, 8P - Q, 9P - Q\}.$$

The partition of the interval $\{-2g, \dots, 4g - 1\}$ in Proposition 4.7 is given by

$$\begin{aligned} N_3 &= \{8, 9, 11\} \\ N_2 &= \{0, 3, 4\} & G_3 &= \{6, 7, 10\} \\ N_1 &= \{-4, -3, -1\} & G_2 &= \{1, 2, 5\} \\ G_1 &= \{-6, -5, -2\} \end{aligned}$$

7 Suzuki curves

The Suzuki curve over the field of $q = 2q_0^2$ elements is defined by the equation $y^q + y = x_0^q(x^q + x)$. The curve has $q^2 + 1$ rational points and genus $g = q_0(q - 1)$. The semigroup of Weierstrass nongaps at a rational point is generated by $\{q, q + q_0, q + 2q_0, q + 2q_0 + 1\}$. For any two rational points P and Q there exists a function with divisor $(q + 2q_0 + 1)(P - Q)$. Let $m = q + 2q_0 + 1 = (q_0 + 1)^2 + q_0^2$, and let H be the divisor class containing $mP \sim mQ$.

The divisor H is very ample and gives an embedding of the Suzuki curve in P^4 as a smooth curve of degree m . The canonical divisor $K \sim 2(q_0 - 1)H$. A hyperplane H intersects (P, Q) with one of the following multiplicities.

$$\begin{array}{cccccc} (0, 0) & (0, 1) & (0, q_0 + 1) & (0, 2q_0 + 1) & (0, q + 2q_0 + 1) & \\ (1, 0) & (1, 1) & (1, q_0 + 1) & (1, 2q_0 + 1) & & \\ (q_0 + 1, 0) & (q_0 + 1, 1) & \underline{(q_0 + 1, q_0 + 1)} & & & \\ (2q_0 + 1, 0) & \underline{(2q_0 + 1, 1)} & & & & \\ (q + 2q_0 + 1, 0) & & & & & \end{array}$$

Let

$$D_0 = H - (2q_0 + 1)P - Q, \quad D_1 = H - (q_0 + 1)(P + Q), \quad D_2 = H - P - (2q_0 + 1)Q.$$

Then $L(D_i) \neq 0$, and $L(D_i - P) = \dim L(D_i - Q) = 0$, for $i = 0, 1, 2$. And $D_i \in D(P, Q)$, for $i = 0, 1, 2$.

Lemma 7.1. *For any nonnegative integer q_0 ,*

$$\{-q_0(q_0 + 1), \dots, +q_0(q_0 + 1)\} = \{a(q_0 + 1) + bq_0 : |a| + |b| \leq q_0\}.$$

Theorem 7.2. *The m inequivalent divisor classes in $D_0(P, Q)$ are represented by*

$$\begin{aligned} iD_0 + jD_2, & \quad \text{for } 0 \leq i, j \leq q_0, \text{ and} \\ D_1 + i'D_0 + j'D_2, & \quad \text{for } 0 \leq i', j' \leq q_0 - 1. \end{aligned}$$

The given representatives correspond one-to-one to the m divisors

$$D(a, b) = (a + q_0)H - ((a + q_0)(q_0 + 1) + bq_0)P - ((a + q_0)(q_0 + 1) - bq_0)Q,$$

for $|a| + |b| \leq q_0$.

Proof.

$$\begin{aligned} & iD_0 + jD_2 \\ &= i(H - (2q_0 + 1)P - Q) + j(H - P - (2q_0 + 1)Q), \\ &= (i + j)H - (i + j)(q_0 + 1)(P + Q) - (i - j)q_0(P - Q). \end{aligned}$$

Moreover, $0 \leq i, j \leq q_0$ if and only if $|i + j - q_0| + |i - j| \leq q_0$. Thus

$$\{iD_0 + jD_2 : 0 \leq i, j \leq q_0\} = \{D(a, b) : |a| + |b| \leq q_0, a - b \equiv 0 \pmod{2}\}$$

$$\begin{aligned} & H - (q_0 + 1)(P + Q) + i'D_0 + j'D_2 \\ &= (i' + j' + 1)H - (i' + j' + 1)(q_0 + 1)(P + Q) - (i' - j')q_0(P - Q). \end{aligned}$$

Similarly, $0 \leq i', j' \leq q_0 - 1$ if and only if $|i' + j' + 1 - q_0| + |i' - j'| \leq q_0 - 1$. And

$$\begin{aligned} & \{H - (q_0 + 1)(P + Q) + i'D_0 + j'D_2 : 0 \leq i', j' \leq q_0 - 1\} \\ &= \{D(a, b) : |a| + |b| \leq q_0, a - b \equiv 1 \pmod{2}\} \end{aligned}$$

We have constructed m inequivalent divisors in Γ_P . A divisor $A \in \Gamma_P$ is a discrepancy if and only if $K + P + Q - A \in \Gamma_P$. With $K = 2(q_0 - 1)H$, we see that

$$\begin{aligned} D(a, b) + D(-a, -b) &= (2q_0)H - (2q_0(q_0 + 1)P - 2q_0(q_0 + 1)Q) \\ &= (2q_0 - 2)H + P + Q = K + P + Q. \end{aligned}$$

□

As an illustration, we give the discrepancies for the Suzuki curve $y^8 + y = x^{10} + x^3$ over the field of eight elements ($q_0 = 2, q = 8, g = 14, N = 65, m = 13 = 3^2 + 2^2$).

$$\begin{array}{ccccc} 0 & \cdot & H - 5P - Q & \cdot & 2H - 10P - 2Q \\ \cdot & H - 3P - 3Q & \cdot & 2H - 8P - 4Q & \cdot \\ H - P - 5Q & \cdot & 2H - 6P - 6Q & \cdot & 3H - 11P - 7Q \\ \cdot & 2H - 4P - 8Q & \cdot & 3H - 9P - 9Q & \cdot \\ 2H - 2P - 10Q & \cdot & 3H - 7P - 11Q & \cdot & 4H - 12P - 12Q \end{array}$$

With $H \sim 13Q$, we obtain the following multiplicities for the discrepancies at (P, Q) .

$$\begin{array}{ccccc} (0, 0) & \cdot & (-5, 12) & \cdot & (-10, 24) \\ \cdot & (-3, 10) & \cdot & (-8, 22) & \cdot \\ (-1, 8) & \cdot & (-6, 20) & \cdot & (-11, 32) \\ \cdot & (-4, 18) & \cdot & (-9, 30) & \cdot \\ (-2, 16) & \cdot & (-7, 28) & \cdot & (-12, 40) \end{array}$$

For the given Suzuki curve, Beelen [2] gives an example of a two-point code for which the floor bound exceeds the order bound. The example generalizes to any Suzuki curve. For both the Suzuki curve over \mathbb{F}_8 and over \mathbb{F}_{32} (for which $q_0 = 4, q = 32, g = 124, N = 1025, m = 41 = 5^2 + 4^2$), the example is the only two-point code for which the floor bound exceeds the order bound.

Example 7.3. Let $A = B = K - H, Z = 2P + 2Q$. With $\dim L(H) - \dim L(H - 2P - 2Q) = 4$, it follows that $L(A + Z) = L(A)$ and $L(B + Z) = L(B)$. For the code $C_\Omega(D, G) = C_L(D, G)^\perp$ with $G = K + C = A + B + Z = 2K - 2H + 2P + 2Q$, the threshold divisor $C = K - 2H + Z$. The floor bound gives minimum distance $d \geq \deg C + \deg Z = d^* + 4$. This is one better than the order bound.

We give an example of the ABZ bound for codes that improves both the floor bound and the order bound.

Example 7.4. Let $A = B = K - H, Z = (q_0 + 2)P + 2Q$. For the code $C_\Omega(D, G) = C_L(D, G)^\perp$ with $G = K + C = A + B + Z = 2K - 2H + (q_0 + 2)P + 2Q$, the threshold divisor $C = K - 2H + Z$. For the ABZ bound we use $\dim L(A) - \dim L(A - C) + \dim L(B) - \dim L(B - C) = 2(\dim L(K - H) - \dim L(H - Z)) = 2 \deg(K - H) - \deg K + 2 \dim L(H)$. The bound $d \geq 10$ for $q_0 = 2$ is one better than both the floor bound and the order bound.

We illustrate the use of tables $K_i^\pm(j, \ell)$ and $N_i^\pm(j, \ell)$ for the comparison of delta sets $\Delta_P(\ell Q, iP + jQ + Q)$ and $\Delta_P(\ell Q \mp Q, iP + jQ + Q)$ (Lemma 5.7). The functions $d_P = d_Q = d'_P = d'_Q$ all agree and we can omit the index. The functions are defined on residue classes modulo m . With Lemma 7.1 and Theorem 7.2, for $|a| + |b| \leq q_0$,

$$d(k) = (q_0 - a)(q - 1), \quad \text{for } k = a(q_0 + 1) + bq_0 - q_0(q_0 + 1) \pmod{m}$$

Example 7.5. For the Suzuki curve over \mathbb{F}_{32} , let $C = 55P + 31Q$. In this case there is a unique choice $B = -5Q$ such that $\Delta_P(B, C) \geq 90$. The improvement over the choice $B = 0$ can be seen as follows.

$(i = 55, j = 30)$	ℓ	= 0	-1	-2	-3	-4	-5
	$d(\ell)$	0	31	62	93	124	·
(K^+)	k^+	0	32	64	(96)	(128)	·
	$d(k^+ - i)$	62	93	124	0	31	·
	$d(\ell) - d(k^+ - i)$	-62	-62	-62	93	93	·
(N^+)	$\leq i + j$	1	1	1	0	0	·

$(i = 55, j = 30)$	ℓ	= 0	-1	-2	-3	-4	-5
	$d(\ell - j)$	·	217	124	155	186	217
(K^-)	k^-	·	303	(211)	243	275	307
	$d(k^-)$	·	155	217	93	124	155
	$d(k^-) - d(\ell - j)$	·	-62	93	-62	-62	-62
(N^-)	$\leq i + j$	·	1	0	1	1	1

The tables use $k^+ = d(\ell) - \ell$ and $k^- = d(\ell - j) - \ell + i + j$.

From the tables we obtain

$$\begin{aligned} I_P(0, C) \setminus I_P(-5Q, C) &= \{k^+ \in I_P(-5Q, 5Q) : k^+P \in \Gamma_P\} \\ &= \{0, 32, 64, (96), (128)\}. \\ I_P(-5Q, C) \setminus I_P(0, C) &= \{k^- \in I_P(-C, 5Q) : -5Q + k^-P \notin \Gamma_P\} \\ &= \{307, 275, 243, (211), 303\}. \end{aligned}$$

The net gain is therefore $4 - 3 = 1$. To reach this conclusion it is sufficient to consult the rows (N^+) and (N^-) .

$$\begin{aligned} \Delta_P(55P + 31Q) \supseteq & \{A_1 = 36P - 5Q, \dots, A_{45} = 163P - 5Q\} \\ & \cup \{A_{46} = 180P - 5Q, \dots, A_{90} = 307P - 5Q\} \end{aligned}$$

Example 7.6. We illustrate the improvement of the ABZ bound for cosets over the order bound. Both $\#\Delta_P(0, 9P + 9Q) = \#\Delta_P(9Q, 9P + 9Q) = 40$. This is the optimum for the order bound. For $r \geq 0$,

$$\#\Delta_P(0, C) = \#\Delta_P(\leq rP, C) + \#\Delta_P(\geq rP + P, C).$$

For $r, s \geq 0$ such that

$$\#\Delta_P(\geq rP + P + sQ, C) > \#\Delta_P(\geq rP + P, C)$$

we obtain an improvement using the ABZ bound with choices $B = rP, Z = sQ$ (Theorem 3.5). As in the previous example we compare delta sets and find

$$\begin{aligned} I_P(0, 9P + 9Q) \setminus I_P(9Q, 9P + 9Q) &= \{k^- \in I_P(-9P, 9Q) : k^- P \in \Gamma_P\} \\ &= \{141, 109, 77, (45), 137, 105, 73, 41, (9)\}. \end{aligned}$$

$$\begin{aligned} I_P(9Q, 9P + 9Q) \setminus I_P(0, 9P + 9Q) &= \{k^+ \in I_P(9Q, 9Q) : 9Q + k^+ P \notin \Gamma_P\} \\ &= \{115, 147, 179, (211), 119, 151, 183, 215, (247)\}. \end{aligned}$$

The information shows that although the delta sets $\Delta_P(0, 9P + 9Q)$ and $\Delta_P(9Q, 9P + 9Q)$ have the same size, the first contains more divisors of small degree and the latter more divisors of high degree. For $Z = 9Q$ and for $141 \leq r \leq 146$ (or $109 \leq r \leq 114$) we see that

$$\#\Delta_P(\geq rP + P + sQ, C) - \#\Delta_P(\geq rP + P, C) = 5.$$

The order bound gives minimum distance $d \geq 40$ for the AG code with $C = 9P + 9Q$ and $d \geq 50$ for the AG code with $C = 10P + 9Q$. Thus we improve the minimum distance for $C = 9P + 9Q$ from $d \geq 40$ to $d \geq 45$.

$$\begin{aligned} \Delta_P(9P + 9Q) \supseteq & \{A_1 = 0, \dots, A_{18} = 109P\} \\ & \cup \{A_{19} = 112P + 9Q, \dots, A_{45} = 256P + 9Q\} \end{aligned}$$

Example 7.7. The ABZ bound, while more general than the order bound, is still only a special case of the main theorem. The following choice of divisors in $\Delta_P(12P + 12Q)$ gives $\gamma_P(12P + 12Q) \geq 56$. This improves both the order bound and the ABZ bound (for all possible choices of A, B , and Z as integer combinations of P and Q).

$$\begin{aligned} \Delta_P(12P + 12Q) \supseteq & \{A_1 = 0, \dots, A_{24} = 116P\} \\ & \cup \{A_{25} = 118P + 6Q, \dots, A_{32} = 141P + 6Q\} \\ & \cup \{A_{33} = 143P + 12Q, \dots, A_{56} = 259P + 12Q\} \end{aligned}$$

References

- [1] Maria Bras-Amorós. Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements. *IEEE Trans. Inform. Theory*, 50(6):1282–1289, 2004.
- [2] Peter Beelen. The order bound for general algebraic geometric codes. *Finite Fields Appl.*, 13(3):665–680, 2007.
- [3] Peter Beelen and Nesrin Tutaş. A generalization of the Weierstrass semigroup. *J. Pure Appl. Algebra*, 207(2):243–260, 2006.
- [4] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. In *Advances in cryptology—CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.*, pages 521–536. Springer, Berlin, 2006.
- [5] Antonio Campillo, José Ignacio Farrán, and Carlos Munuera. On the parameters of algebraic-geometry codes related to Arf semigroups. *IEEE Trans. Inform. Theory*, 46(7):2634–2638, 2000.
- [6] Cícero Carvalho and Fernando Torres. On Goppa codes and Weierstrass gaps at several points. *Des. Codes Cryptogr.*, 35(2):211–225, 2005.
- [7] Iwan M. Duursma. Algebraic geometry codes: general theory. In C. Munuera E. Martinez-Moro and D. Ruano, editors, *Advances in Algebraic Geometry Codes*, Series on Coding Theory and Cryptography. World Scientific, to appear.
- [8] Iwan M. Duursma and Seungkook Park. Coset bounds for algebraic geometric codes. Short version containing the first half of the original preprint arXiv:0810.2789, 2008. The results of the current paper form the second half of that preprint.
- [9] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*. (Princeton University Press, Princeton, 2008)
- [10] Masaaki Homma and Seon Jeong Kim. The complete determination of the minimum distance of two-point codes on a Hermitian curve. *Des. Codes Cryptogr.*, 40(1):5–24, 2006.
- [11] Johan P. Hansen and Henning Stichtenoth. Group codes on certain algebraic curves with many rational points. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):67–77, 1990.
- [12] Seon Jeong Kim. On the index of the Weierstrass semigroup of a pair of points on a curve. *Arch. Math. (Basel)*, 62(1):73–82, 1994.

- [13] Christoph Kirfel and Ruud Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory*, 41(6, part 1):1720–1732, 1995. Special issue on algebraic geometry codes.
- [14] Benjamin Lundell and Jason McCullough. A generalized floor bound for the minimum distance of geometric Goppa codes. *J. Pure Appl. Algebra*, 207(1):155–164, 2006.
- [15] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Des. Codes Cryptogr.*, 22(2):107–121, 2001.
- [16] Gretchen L. Matthews. Codes from the Suzuki function field. *IEEE Trans. Inform. Theory*, 50(12):3298–3302, 2004.
- [17] Seungkook Park. *Applications of algebraic curves to cryptography*. Dissertation, University of Illinois, Urbana, 2007.
- [18] Oliver Pretzel. *Codes and algebraic curves*, volume 8 of *Oxford Lecture Series in Mathematics and its Applications*. The Clarendon Press Oxford University Press, New York, 1998.
- [19] Serguei A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999.
- [20] Henning Stichtenoth. *Algebraic function fields and codes*. Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.
- [21] Michael Tsfasman, Serge Vlăduț, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.