Coset bounds for algebraic geometric codes

Iwan M. Duursma* and Seungkook Park†

October 8, 2008 / Reformatted February 16, 2009

Abstract

We develop new coset bounds for algebraic geometric codes. The bounds have a natural interpretation as an adversary threshold for algebraic geometric secret sharing schemes and lead to improved bounds for the minimum distance of an AG code. Our bounds improve both floor bounds and order bounds and provide for the first time a connection between the two types of bounds.

Introduction

This paper deals with coset bounds for algebraic geometric codes and their applications to lower bounds for the minimum distance of AG codes as well as for thresholds of algebraic geometric secret sharing schemes. The work was motivated by two important recent results. The first is the complete description of the minimum distance of Hermitian two-point codes by Homma and Kim [HK06]. The second is the introduction of algebraic geometric linear secret sharing schemes by Chen and Cramer [CC06].
For algebraic geometric codes, the actual value of the minimum distance is not a priori known and needs to be determined or estimated from the data used in the construction. The best known lower bounds for the minimum distance of an algebraic geometric code are the order bound and the floor bound. Beelen [Bee07], and independently the second author [Par], have shown that the order bound agrees, for Hermitian two-point codes, with the actual minimum distances found by Homma and Kim. In this paper we improve both the order bound and the floor bound.

An important application of secret sharing schemes is secure multi-party computation, which requires linear secret sharing schemes with a multiplicative property [CDM00], [CDG+05]. Chen and Cramer proposed to use one-point algebraic geometric codes for secret sharing and they have shown that the obtained algebraic geometric linear secret sharing schemes can be used for efficient secure computation over small fields [CC06].

*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)

Parties can reconstruct a secret uniquely from their shares only if the total number of shares exceeds the adversary threshold of the secret sharing scheme. The algebraic geometric construction of a linear secret sharing scheme guarantees a lower bound for the adversary threshold. The precise value of the threshold is in general not known. We show that the adversary threshold corresponds to the minimum distance between cosets of a code. Our results give improved lower bounds for distances between cosets of an algebraic geometric code, and therefore improved lower bounds for adversary thresholds of algebraic geometric linear secret sharing schemes.

As our main results, we formulate an *ABZ bound for codes* and an *ABZ bound for cosets*. The bounds improve and generalize the floor bound and the order bound, respectively. The bounds can be used as tools for constructing improved codes as well as improved secret sharing schemes. Our *Main theorem* is an even more general bound. Its main advantage is that it has a short proof and that all other bounds can be obtained as special cases.
The floor bound is independent of the order bound. Algorithms are available for decoding up to half the order bound but not for decoding up to half the floor bound. Beelen [Bee07] gives an example where the floor bound exceeds the order bound. For our generalizations there is a strict hierarchy. The improved order bound, obtained with the ABZ bound for cosets, is at least the ABZ bound for codes, which improves the floor bound. We show that decoding is possible up to half the bound in our main theorem, and therefore up to half of all our bounds. In particular, we obtain for the first time an approach to decode up to half the floor bound.

In Section 1, we describe the use of linear codes for secret sharing and the relation between coset distances and adversary thresholds. Theorem 1.2 gives a general coset bound for linear codes. Appendix A gives a coset decoding procedure that decodes up to half the bound. Algebraic geometric codes are defined in Section 2. Theorem 2.4 gives the ABZ bound for algebraic geometric codes with a first proof based on the AB bound for linear codes. Section 3 gives a geometric characterization of coset distances for algebraic geometric codes. In Section 4 we define, for a divisor C and for a point P, a semigroup ideal

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

such that the minimal degree for a divisor A in $\Gamma_P(C)$ is a lower bound for the coset distance of an algebraic geometric code. In Section 5, the main theorem gives a lower bound for the degree of a divisor in the semigroup ideal (Theorem 5.3). The bound is formulated in terms of properties of the complement

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

In Section 6, we explain the role of the divisor C for optimizing the order bound (Proposition 6.4). We formulate the ABZ bound for cosets (Theorem 6.6) and we describe its

relation to both the order bound (Theorem 6.3) and the floor bound (Theorem 2.3). The material in this paper forms the first half of the preprint [DP08].

1 Cosets of linear codes

Let $\mathbb{F}$ be a finite field. A $\mathbb{F}$-linear code $\mathcal{C}$ of length n is a linear subspace of $\mathbb{F}^n$. The Hamming distance between two vectors $x, y \in \mathbb{F}^n$ is $d(x,y) = |\{i : x_i \neq y_i\}|$. The minimum distance of a nontrivial linear code $\mathcal{C}$ is

$$\begin{aligned} d(\mathcal{C}) &= \min\{d(x,y) : x, y \in \mathcal{C}, x \neq y\} \\ &= \min\{d(x,0) : x \in \mathcal{C}, x \neq 0\}. \end{aligned}$$

If $d(\mathcal{C}) \geq 2t+1$ and if $y \in \mathbb{F}^n$ is at distance at most t from $\mathcal{C}$ then there exists a unique word $c \in \mathcal{C}$ with $d(c,y) \leq t$.

The Hamming distance between two nonempty subsets $X, Y \subset \mathbb{F}^n$ is the minimum of $\{d(x,y) : x \in X, y \in Y\}$. For a proper subcode $\mathcal{C}' \subset \mathcal{C}$, the minimum distance of the collection of cosets $\mathcal{C}/\mathcal{C}'$ is

$$\begin{aligned} d(\mathcal{C}/\mathcal{C}') &= \min\{d(x+\mathcal{C}', y+\mathcal{C}') : x, y \in \mathcal{C}, x-y \notin \mathcal{C}'\} \\ &= \min\{d(x,0) : x \in \mathcal{C}, x \notin \mathcal{C}'\}. \end{aligned}$$

Lemma 1.1. *If $d(\mathcal{C}/\mathcal{C}') \geq 2t+1$ and if $y \in \mathbb{F}^n$ is at distance at most t from $\mathcal{C}$ then there exists a unique coset $c+\mathcal{C}' \in \mathcal{C}/\mathcal{C}'$ with $d(c+\mathcal{C}', y+\mathcal{C}') \leq t$.*

The dual code $\mathcal{D}$ of $\mathcal{C}$ is the maximal subspace of $\mathbb{F}^n$ that is orthogonal to $\mathcal{C}$ with respect to the standard inner product. To the extension of codes $\mathcal{C}/\mathcal{C}'$ corresponds an extension of dual codes $\mathcal{D}'/\mathcal{D}$ with distance parameter $d(\mathcal{D}'/\mathcal{D})$. For two vectors $x, y \in \mathbb{F}^n$, let $x * y \in \mathbb{F}^n$ denote the Hadamard or coordinate-wise product of the two vectors.

Theorem 1.2. *(Shift bound or Coset bound) Let $\mathcal{C}/\mathcal{C}_1$ be an extension of $\mathbb{F}$-linear codes with corresponding extension of dual codes $\mathcal{D}_1/\mathcal{D}$ such that $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$. If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that*

$$\begin{cases} a_i * b_j \in \mathcal{D} & \text{for } i+j \leq w, \\ a_i * b_j \in \mathcal{D}_1 \backslash \mathcal{D} & \text{for } i+j = w+1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geq w$.

Proof. For all $c \in \mathcal{C}\backslash\mathcal{C}_1$ and $a * b \in \mathcal{D}_1\backslash\mathcal{D}$, $\sum_i a_i b_i c_i \neq 0$. To show the nonexistence of a vector $c \in \mathcal{C}\backslash\mathcal{C}_1$ with $d(c,0) < w$, it suffices to show, for any choice of $w-1$ coordinates, the existence of a vector $a * b \in \mathcal{D}_1\backslash\mathcal{D}$ that is zero in those coordinates. The conditions show that the vectors $a_1, \ldots, a_w$ are linearly independent, and there exists a nonzero linear combination a of the vectors $a_1, \ldots, a_w$ vanishing at $w-1$ given coordinates. If i is maximal such that a_i has a nonzero coefficient in the linear combination a then $a * b_{w+1-i} \in \mathcal{D}_1\backslash\mathcal{D}$ is zero in the $w-1$ coordinates. □

Let $y \in \mathbb{F}^n$ be a word at distance at most t from $\mathcal{C}$. For given vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that $w > 2t$, the unique coset $c + \mathcal{C}_1 \in \mathcal{C}/\mathcal{C}_1$ with $d(c + \mathcal{C}_1, y + \mathcal{C}_1) \leq t$ can be computed efficiently with the coset decoding procedure in Appendix A. Theorem 1.2 can be used to estimate the minimum distance $d(\mathcal{C}/\mathcal{C}')$ of an extension $\mathcal{C}/\mathcal{C}'$ with $\dim \mathcal{C}/\mathcal{C}' > 1$, after dividing $\mathcal{C}/\mathcal{C}'$ into subextensions.

Lemma 1.3. *Let $\mathcal{C}/\mathcal{C}'$ be an extension of $\mathbb{F}$-linear codes of length n. For $\mathcal{C} \supset \mathcal{C}'' \subset \mathcal{C}'$,*

$$d(\mathcal{C}/\mathcal{C}') = \min\{d(\mathcal{C}/\mathcal{C}''), d(\mathcal{C}''/\mathcal{C}')\}.$$

We will now describe the use of code extensions for secret sharing. Our description focuses on the connection between secret sharing thresholds and coset distances that will be established in Corollary 1.7. The main properties that we need are described in the following two lemmas.

Lemma 1.4. *Let $\{1, 2, \ldots, n\} = I \cup J$ be a partition of the coordinates. There exists a word $r \in \mathcal{C}\backslash\mathcal{C}_1$ with support in I if and only if there exists no word $s \in \mathcal{D}_1\backslash\mathcal{D}$ with support in J.*

Proof. Let E_I (resp. E_J) be the subspace of $\mathbb{F}^n$ of all vectors with support in I (resp. J). The exact sequences

$$0 \longrightarrow \mathcal{C} \cap E_I/\mathcal{C}_1 \cap E_I \longrightarrow \mathcal{C}/\mathcal{C}_1 \longrightarrow \mathcal{C} + E_I/\mathcal{C}_1 + E_I \longrightarrow 0,$$
$$0 \longrightarrow \mathcal{D}_1 \cap E_J/\mathcal{D} \cap E_J \longrightarrow \mathcal{D}_1/\mathcal{D} \longrightarrow \mathcal{D}_1 + E_J/\mathcal{D} + E_J \longrightarrow 0,$$

are in duality via $V \mapsto V^* = \mathrm{Hom}(V, \mathbb{F})$. And

$$(\dim \mathcal{C} \cap E_I/\mathcal{C}_1 \cap E_I) + (\dim \mathcal{D}_1 \cap E_J/\mathcal{D} \cap E_J) = \dim \mathcal{C}/\mathcal{C}_1 = 1.$$

□

Lemma 1.5. *Let $y_1 \in \mathcal{D}_1\backslash\mathcal{D}$. For a given vector $s \in \mathcal{D}_1 = \mathcal{D} \oplus \langle y_1 \rangle$, the projection of s on $\langle y_1 \rangle$ is uniquely determined by the subset of coordinates $\{s_i : i \in A\}$ if and only if $\mathcal{D}_1\backslash\mathcal{D}$ contains no word that is zero in the positions A.*

Proof. The only if part is clear. For the if part we may assume with the previous lemma that there exists $r \in \mathcal{C}\backslash\mathcal{C}_1$ with support in A. For any such r, and for $s = y + \lambda y_1$, $y \in \mathcal{D}$,

$$r \cdot s = r \cdot (y + \lambda y_1) = \lambda (r \cdot y_1).$$

Since $(r \cdot y_1) \neq 0$, we obtain $\lambda = (r \cdot s)/(r \cdot y_1)$. □

Let $y_1 \in \mathcal{D}_1\backslash\mathcal{D}$. For a secret $\lambda \in \mathbb{F}$, and for a random vector $y \in \mathcal{D}$, the vector $s = y + \lambda y_1$ is called a vector of shares for λ. A subset $A \subset \{1, 2, \ldots, n\}$ is called qualified if the shares $\{s_i : i \in A\}$ determine λ uniquely. Whether A is qualified depends on $\mathcal{D}_1/\mathcal{D}$ but not on the vector of shares $s \in \mathcal{D}_1$. Let $\Gamma(\mathcal{D}_1/\mathcal{D})$ denote the collection of all subsets $A \subset \{1, 2, \ldots, n\}$ that are qualified for $\mathcal{D}_1/\mathcal{D}$ and let $\Delta(\mathcal{D}_1/\mathcal{D})$ denote the collection of all subsets $A \subset \{1, 2, \ldots, n\}$ that are not qualified for $\mathcal{D}_1/\mathcal{D}$. For the definition and main properties of a general linear secret sharing scheme we refer to [CDG+05].

Theorem 1.6. *Let $\mathcal{C}/\mathcal{C}_1$ and $\mathcal{D}_1/\mathcal{D}$ be dual extensions of $\mathbb{F}$-linear codes of length n. Let E_A be the subset of $\mathbb{F}^n$ of all vectors with support in A.*

$$\Gamma(\mathcal{D}_1/\mathcal{D}) = \{A : \mathcal{C} \cap E_A \neq \mathcal{C}_1 \cap E_A\},$$
$$\Delta(\mathcal{D}_1/\mathcal{D}) = \{A : \mathcal{C} \cap E_A = \mathcal{C}_1 \cap E_A\}.$$

Moreover, for $\bar{A} = \{1, 2, \ldots, n\} \backslash A$,

$$\Gamma(\mathcal{C}/\mathcal{C}_1) = \{A : \bar{A} \in \Delta(\mathcal{D}_1/\mathcal{D})\},$$
$$\Delta(\mathcal{C}/\mathcal{C}_1) = \{A : \bar{A} \in \Gamma(\mathcal{D}_1/\mathcal{D})\}.$$

Proof. Lemma 1.5 and Lemma 1.4. □

Corollary 1.7. *The smallest qualified subset for $\mathcal{D}_1/\mathcal{D}$ is of size*

$$\min\{|A| : A \in \Gamma(\mathcal{D}_1/\mathcal{D})\} = d(\mathcal{C}/\mathcal{C}_1).$$

The largest unqualified subset for $\mathcal{D}_1/\mathcal{D}$ is of size

$$\max\{|A| : A \in \Delta(\mathcal{D}_1/\mathcal{D})\} = n - d(\mathcal{D}_1/\mathcal{D}),$$

2 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 $L(E)$ denote the vector space over $\mathbb{F}$ of functions $f \in \mathbb{F}(X)\backslash\{0\}$ with $(f) + E \geq 0$ together with the zero function. Let $\Omega(E)$ denote the vector space over $\mathbb{F}$ of differentials $\omega \in \Omega(X)\backslash\{0\}$ with $(\omega) \geq E$ together with the zero differential. Let K represent the canonical divisor class.

For n distinct rational points $P_1, \ldots, P_n$ on X and for disjoint divisors $D = P_1 + \cdots + P_n$ and G, the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\alpha_L \ : \ L(G) \ \longrightarrow \ \mathbb{F}^n, \ \ f \mapsto (\, f(P_1), \ldots, f(P_n)\,),$$
$$\alpha_\Omega \ : \ \Omega(G - D) \ \longrightarrow \ \mathbb{F}^n, \ \ \omega \mapsto (\, \mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)\,).$$

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.

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 $L(K - G + A)/L(K - G) \neq 0$.

Proposition 2.1.

$$d(C_L(D,G)) = \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(-C)\}, \quad \textit{for } C = D - G.$$
$$d(C_\Omega(D,G)) = \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(-C)\}, \quad \textit{for } C = G - K.$$

Theorem 2.2. *(Goppa bound) A nonzero word in $C_L(D,G)$ has weight $w \geq \deg(D-G)$. A nonzero word in $C_\Omega(D,G)$ has weight $w \geq \deg(G-K)$.*

The following bound improves on the Goppa bound in special cases.

Theorem 2.3. *(Floor bound) Let $G = K + C = A + B + Z$, for $Z \geq 0$ such that $L(A+Z) = L(A)$ and $L(B+Z) = L(B)$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D,G)$ has weight at least* $\deg C + \deg Z$.

Most algebraic bounds for the minimum distance of a linear code rely on one of two basic arguments. In the paper [vLW86] on cyclic codes they were named the AB bound and the Shift bound. We obtain the following bound, which includes the floor bound, using the AB bound argument in combination with the Goppa bound.

Theorem 2.4. *(ABZ bound for codes) Let $G = K+C = A+B+Z$, for $Z \geq 0$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D,G)$ has weight $w \geq l(A)-l(A-C)+l(B)-l(B-C)$.*

Proof. We may assume that A and B are disjoint from D. Since $Z \geq 0$ and $D \cap Z = \emptyset$, the code $C_L(D,G)$ contains the code $C_L(D,A+B)$ as a subcode. Thus, for a word $c \in C_\Omega(D,G)$, and for words $a \in C_L(D,A)$ and $b \in C_L(D,B)$, if c has support D' then $\sum_{P \in D'} a_P b_P c_P = 0$. The last orthogonality holds for all $a \in C_L(D',A)$ and $b \in C_L(D',B)$, so that $\dim C_L(D',A) + \dim C_L(D',B) \leq \deg D'$, and $\deg D' \geq l(A) - l(A-D') + l(B) - l(B-D')$. Together with $L(D'-C) \neq 0$, $\deg D' \geq l(A)-l(A-C)+l(B)-l(B-C)$. □

It is easy to see, using the Riemann-Roch theorem, that the choice $Z = 0$ returns the Goppa bound. Improvements of the Goppa bound are obtained only if the divisors A, B, and Z, are carefully chosen. For the special case $L(A+Z) = L(A)$ and $L(B+Z) = L(B)$, we recover the floor bound. In that case, for $K + C = A + B + Z$,

$$\begin{aligned} & l(A) - l(A-C) + l(B) - l(B-C) \\ = \; & l(A+Z) - l(K-B-Z) + l(B+Z) - l(K-A-Z) \\ = \; & \deg(A+Z) + \deg(B+Z) + 2 - 2g = \deg C + \deg Z. \end{aligned}$$

3 Cosets of algebraic geometric codes

Let $\mathcal{D} = C_\Omega(D,G)$ and $\mathcal{C} = C_L(D,G)$ be dual algebraic geometric codes. For a point P disjoint from D, let

$$\mathcal{D}_1/\mathcal{D} = C_\Omega(D, G-P)/C_\Omega(D,G),$$
$$\mathcal{C}/\mathcal{C}_1 = C_L(D,G)/C_L(D,G-P),$$

be dual extensions of codes. When $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$, the extensions can be used for secret sharing as described in Section 1. Theorem 1.6 describes the parties that can recover the secret for the extension $\mathcal{D}_1/\mathcal{D}$ as the subsets $0 \le A \le D$ that support a word in $\mathcal{C}/\mathcal{C}_1$. The formulation in terms of divisors is given in Proposition 3.2, with a similar result for the extension $\mathcal{C}/\mathcal{C}_1$ in Proposition 3.4. As additional motivation, we give a natural choice for the secret for each of the extensions $\mathcal{D}_1/\mathcal{D}$ and $\mathcal{C}/\mathcal{C}_1$, and we describe directly the qualified parties that can determine the secret, in Lemma 3.1 and Lemma 3.3, respectively. The propositions can then also be obtained from the lemmas.

Let P have multiplicity e in G, and let t be a fixed local parameter for P. For $\dim \mathcal{D}_1/\mathcal{D} = 1$, there exists a natural isomorphism $\Omega(G-D-P)/\Omega(G-D) \simeq \mathcal{D}_1/\mathcal{D} \simeq \mathbb{F}$ that maps $\omega \in \Omega(G-D-P)/\Omega(G-D)$ to $\mathrm{res}_P(t^{-e}\omega)$. For $\dim \mathcal{C}/\mathcal{C}_1 = 1$, there exists a natural isomorphism $L(G)/L(G-P) \simeq \mathcal{C}/\mathcal{C}_1 \simeq \mathbb{F}$, that maps $f \in L(G)/L(G-P)$ to $(ft^e)(P)$.

Lemma 3.1. *For $\omega \in \Omega(G-D-P)$, the residue $\mathrm{res}_P(t^{-e}\omega)(P)$ is uniquely determined by the values $\{f(P) : P \in A\}$, for $0 \le A \le D$, if and only if $\Omega(G-D+A-P) = \Omega(G-D+A)$.*

Proposition 3.2. *For the extension of codes $\mathcal{D}_1/\mathcal{D} = C_\Omega(D, G-P)/C_\Omega(D,G)$, where $D = P_1 + \cdots + P_n$ is a sum of n distinct points, G is a divisor disjoint from D, and P is a point disjoint from D,*

$$\begin{aligned}
\Gamma(\mathcal{D}_1/\mathcal{D}) &= \{0 \le A \le D : \mathcal{C} \cap E_A \ne \mathcal{C}_1 \cap E_A\},\\
&= \{0 \le A \le D : L(G-D+A) \ne L(G-D+A-P)\}.\\
\Delta(\mathcal{D}_1/\mathcal{D}) &= \{0 \le A \le D : \mathcal{C} \cap E_A = \mathcal{C}_1 \cap E_A\},\\
&= \{0 \le A \le D : L(G-D+A) = L(G-D+A-P)\}.
\end{aligned}$$

Proof. In each case, the two descriptions are clearly equivalent. The first description of $\Gamma(\mathcal{D}_1/\mathcal{D})$ uses Theorem 1.6. The second description uses Lemma 3.1. □

Lemma 3.3. *For $f \in L(G)$, the value $(t^e f)(P)$ is uniquely determined by the values $\{f(P) : P \in A\}$, for $0 \le A \le D$, if and only if $L(G-A) = L(G-A-P)$.*

Proposition 3.4. *For the extension of codes $\mathcal{C}/\mathcal{C}_1 = C_L(D,G)/C_L(D,G-P)$, where $D = P_1 + \cdots + P_n$ is a sum of n distinct points, G is a divisor disjoint from D, and P is a point disjoint from D,*

$$\begin{aligned}
\Gamma(\mathcal{C}/\mathcal{C}_1) &= \{0 \le A \le D : \mathcal{D}_1 \cap E_A \ne \mathcal{D} \cap E_A\},\\
&= \{0 \le A \le D : \Omega(G-A-P) \ne \Omega(G-A)\}.\\
\Delta(\mathcal{C}/\mathcal{C}_1) &= \{0 \le A \le D : \mathcal{D}_1 \cap E_A = \mathcal{D} \cap E_A\},\\
&= \{0 \le A \le D : \Omega(G-A-P) = \Omega(G-A)\}.
\end{aligned}$$

Proof. As in Proposition 3.2 but use Lemma 3.3. □

The propositions are related via the dualities $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ if and only if $D - A \in \Delta(\mathcal{C}/\mathcal{C}_1)$ and $A \in \Gamma(\mathcal{C}/\mathcal{C}_1)$ if and only if $D - A \in \Delta(\mathcal{D}_1/\mathcal{D})$ (as Theorem 1.6). The minimal degree of a divisor $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ or $A \in \Gamma(\mathcal{C}/\mathcal{C}_1)$ is given by the coset distance $d(\mathcal{C}/\mathcal{C}_1)$ or $d(\mathcal{D}_1/\mathcal{D})$, respectively (as in Corollary 1.7).

Proposition 3.5.

$$d(\mathcal{C}/\mathcal{C}_1) = \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(A-C-P)\}, \quad \textit{for } C = D - G,$$
$$d(\mathcal{D}_1/\mathcal{D}) = \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(A-C-P)\}, \quad \textit{for } C = G - K - P.$$

For a given divisor C and a point P, let

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

and let $\gamma_P(C)$ be the minimal degree for a divisor $A \in \Gamma_P(C)$. So that $\gamma_P(C) \geq \max\{0, \deg C\}$.

Theorem 3.6. *For the extensions of codes $\mathcal{D}_1/\mathcal{D} = C_\Omega(D, G-P)/C_\Omega(D,G)$ and $\mathcal{C}/\mathcal{C}_1 = C_L(D,G)/C_L(D,G-P)$,*

$$\begin{aligned} A \in \Gamma(\mathcal{D}_1/\mathcal{D}) &\Rightarrow \deg A \geq \gamma_P(D-G) \geq n - \deg G. \\ A \in \Delta(\mathcal{D}_1/\mathcal{D}) &\Rightarrow \deg A \leq n - \gamma_P(G-K-P) \leq n - \deg G + 2g - 1. \\ A \in \Gamma(\mathcal{C}/\mathcal{C}_1) &\Rightarrow \deg A \geq \gamma_P(G-K-P) \geq \deg G - 2g + 1. \\ A \in \Delta(\mathcal{C}/\mathcal{C}_1) &\Rightarrow \deg A \leq n - \gamma_P(D-G) \leq \deg G. \end{aligned}$$

The lower bounds for $\deg A$ that are obtained with $\gamma_P(D-G)$ and $\gamma_P(G-K-P)$ use the assumption $L(A) \neq L(A-P)$ instead of the stronger assumption $0 \leq A \leq D$. Thus, when the bound for $\deg A$ is not attained by divisors A of the form $0 \leq A \leq D$, the bounds will not be optimal. Essentially, we separate the problem of finding a small $A \in \Gamma(\mathcal{D}_1/\mathcal{D})$ into two parts: a geometric part that considers all effective divisors A not containing P, and an arithmetic part that verifies if A can be represented by a divisor with $0 \leq A \leq D$. Only the first part is considered in this paper. In other words, the bounds that we obtain apply to a different and more general problem, that of recovering local data at a point P from given local data at a divisor A, for any divisor A with no base point at P. We briefly outline this setting.

Definition 3.7. *Let $X/\mathbb{F}$ be a curve, and let C be a divisor on X. For a given point P on X define the collection $\Sigma_P(C) = \{\pi_A : A \geq 0\}$ of surjective maps*

$$\pi_A : \Omega(-C-P) \longrightarrow \Omega(-C-P)/\Omega(A-C-P), \quad A \geq 0.$$

The map π_A assigns to a differential $\omega \in \Omega(-C-P)$ the local information ω modulo $\Omega(A-C-P)$, in short the local information of ω at A. Given that $\omega \in \Omega(-C-P)$, any sufficiently large amount of local information determines ω uniquely. Indeed, for any

divisor A of sufficiently large degree, $\Omega(A-C-P) = 0$ and π_A is a bijection. For a divisor A with the weaker property $\Omega(A-C-P) = \Omega(A-C)$, the maps $\pi_A = \pi_{A+P}$ agree. In that case, the local information of ω at A determines uniquely the local information of ω at $A+P$. If P occurs in the support of A then this means that the local information can be determined with increased precision. For secret sharing we assume that the secret corresponds to a fixed map π_P. Then the parties that do not know π_P a priori are those with $L(A) \neq L(A-P)$. Among those, the parties that can determine π_P from π_A are those that satisfy $\Omega(A-C-P) = \Omega(A-C)$, or, equivalently, $L(A-C) \neq L(A-C-P)$. Together the conditions define the set $\Gamma_P(C)$. In this setting, the access structure $\Gamma_P(C)$ can be analyzed without further assumptions on the representation of the maps π_A. The image under π_A of a differential $\omega \in \Omega(-C-P)$ might be written out explicitly in terms of local parameters and residues, much like an algebraic geometric code, or it might simply be given as a differential $\omega + \eta$ for $\eta \in \Omega(A-C-P)$.

4 Semigroup ideals

Let $X/\mathbb{F}$ be a curve over a field $\mathbb{F}$ and let $\mathrm{Pic}(X)$ 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. Call $A \in \Gamma_P$ a P-denominator for the divisor class $C \in \mathrm{Pic}(X)$ if $A - C \in \Gamma_P$. So that $A - (A-C)$ expresses C as the difference of two effective divisor classes without base point at P. The P-denominators for C form the Γ_P-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 $E \in \Gamma_P$. The Γ_P-ideal of P-numerators for C is the ideal

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

Clearly, A is a P-denominator for C if and only if $A - C$ is a P-numerator for C, that is

$$A \in \Gamma_P(C) \;\Leftrightarrow\; A - C \in \Gamma_P(-C),$$

The minimal degree $\gamma_P(C)$ of a P-denominator for C is defined as

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

The minimal degrees satisfy

$$\gamma_P(C) - \gamma_P(-C) = \deg C.$$

The denominator and numerator terminology is borrowed from the ideal interpretation of divisors. Let O be the ring of rational functions in $\mathbb{F}(X)$ that are regular outside P. For

effective divisors A and B disjoint from P, the fractional O-ideal $\cup_{i\geq 0} L(iP-(B-A)) = JI^{-1}$ is the quotient of the integral O-ideals $J = \cup_{i\geq 0} L(iP-B)$ and $I = \cup_{i\geq 0} L(iP-A)$. To a denominator A of smallest degree corresponds an ideal I of smallest norm.

If either $C \in \Gamma_P$ or $-C \in \Gamma_P$ then the conditions $A \in \Gamma_P$ and $A - C \in \Gamma_P$ are dependent.

Proposition 4.1. *For a divisor C on a curve X of genus g, $\gamma_P(C) \geq \max\{0, \deg C\}$. Moreover,*

$$\gamma_P(C) = 0 \;\Leftrightarrow\; -C \in \Gamma_P \;\Leftrightarrow\; \Gamma_P(C) = \Gamma_P.$$
$$\gamma_P(C) = \deg C \;\Leftrightarrow\; C \in \Gamma_P \;\Leftrightarrow\; \Gamma_P(-C) = \Gamma_P.$$

The inequality is strict if and only if $C, -C \notin \Gamma_P$ only if $|\deg C| < 2g$.

For suitable choices of the divisor C, the parameter $\gamma_P(C)$ gives a lower bound for the coset distance of an algebraic geometric code (Proposition 3.5) and therefore bounds for the access structure of an algebraic geometric linear secret sharing scheme (Theorem 3.6). Proposition 4.1 shows that we can expect improvements over the trivial lower bound $\gamma_P(C) \geq \deg C$ that is used for Theorem 3.6 only if P is a base point for the divisor C.

Let S be a finite set of rational points that includes P. For $\Gamma_S = \cap_{P\in S}\Gamma_P$, let $\Gamma_P(C;S) = \Gamma_P(C) \cap \Gamma_S = \{A \in \Gamma_S : A - C \in \Gamma_P\}$, and let $\gamma_P(C;S)$ be the minimal degree for a divisor $A \in \Gamma_P(C;S)$.

Lemma 4.2. *For a given set of rational points S that includes P, and for extensions of algebraic geometric codes $C_\Omega(D, G-P)/C_\Omega(D,G)$ and $C_L(D,G)/C_L(D,G-P)$ defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S,*

$$d(C_L(D,G)/C_L(D,G-P)) \geq \gamma_P(C;S), \quad \text{for } C = D - G,$$
$$d(C_\Omega(D,G-P)/C_\Omega(D,G)) \geq \gamma_P(C;S), \quad \text{for } C = G - K - P.$$

Proof. Proposition 3.5. □

To obtain similar estimates for the minimum distance of an algebraic geometric code, we use Proposition 2.1. Define the Γ_S-ideals $\Gamma^*(C;S) \subseteq \Gamma(C;S)$,

$$\Gamma^*(C;S) = \{A \in \Gamma_S : L(A-C) \neq L(-C)\},$$
$$\Gamma(C;S) = \{A \in \Gamma_S : L(A-C) \neq 0\}.$$

Let $\gamma^*(C;S)$ (resp. $\gamma(C;S)$) denote the minimal degree for a divisor $A \in \Gamma^*(C;S)$ (resp. $A \in \Gamma(C,S)$).

Lemma 4.3. *For a given set of rational points S, and for algebraic geometric codes $C_L(D,G)$ and $C_\Omega(D,G)$ defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S,*

$$d(C_L(D,G)) \geq \gamma^*(C;S) \geq \gamma(C;S), \quad \text{for } C = D - G,$$
$$d(C_\Omega(D,G)) \geq \gamma^*(C;S) \geq \gamma(C;S), \quad \text{for } C = G - K.$$

For $L(-C) = 0$, $\gamma^*(C;S) = \gamma(C;S)$.

Proof. Proposition 2.1. □

The condition $L(-C) = 0$ holds in all cases where the Goppa lower bound $d \geq \deg C$ (Theorem 2.2) is positive. We give lower bounds for $\gamma(C;S)$ using lower bounds for $\gamma_P(C;S)$. With a minor modification, we obtain lower bounds for $\gamma^*(C;S)$.

Lemma 4.4. *Let S be a finite set of rational points. For a divisor C, and for a point $P \in S$,*

$$\Gamma(C;S) = \Gamma_P(C;S) \cup \Gamma(C+P;S).$$
$$\Gamma^*(C;S) \subseteq \Gamma_P(C;S) \cup \Gamma^*(C+P;S).$$

Moreover, for $-C \in \Gamma_P$,

$$\Gamma^*(C;S) \subseteq \Gamma^*(C+P;S).$$

Proof. For the equality, $L(A-C) \neq 0$ if and only if $L(A-C) \neq L(A-C-P)$ or $L(A-C-P) \neq 0$. For the inclusion, $L(A-C) \neq L(-C)$ only if $L(A-C) \neq L(A-C-P)$ or $L(A-C-P) \neq L(-C-P)$. Finally, for $A \in \Gamma^*(C;S)$ such that $-C \in \Gamma_P$, we have $\dim L(A-C)/L(-C-P) > 1$, and thus $L(A-C-P) \neq L(-C-P)$. So that $A \in \Gamma^*(C+P;S)$. □

Proposition 4.5.

$$\gamma(C;S) \geq \min\{\gamma_P(C;S), \gamma(C+P;S)\}.$$
$$\gamma^*(C;S) \geq \min\{\gamma_P(C;S), \gamma^*(C+P;S)\}\backslash\{0\}.$$

Proof. In general $\gamma^*(C;S) > 0$. And $\gamma_P(C;S) = 0$ only if $\gamma_P(C) = 0$ if and only if $-C \in \Gamma_P$, in which case we can omit $\gamma_P(C;S)$ before taking the minimum. □

5 Main theorem

For a given curve $X/\mathbb{F}$, let $C \in \mathrm{Pic}(X)$ be a divisor class and let P be a point on X. For the semigroup $\Gamma_P = \{A : L(A) \neq L(A-P)\}$ and the Γ_P-ideal

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

define the complement

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

Lemma 5.1.

$$\Delta_P(C) = \emptyset \;\Leftrightarrow\; \Gamma_P(C) = \Gamma_P \;\Leftrightarrow\; -C \in \Gamma_P.$$

Let X be of genus g and let K represent the canonical divisor class.

Lemma 5.2. *In general,*

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

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. □

The following is the analogue of Theorem 1.2 in the language of divisors.

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

$$\gamma_P(C; A_w - A_1) \geq w.$$

Proof. After replacing the sequence with an equivalent sequence if necessary, we may assume that $A_1, A_2, \ldots, A_w$ are disjoint from A. We obtain two sequences of subspaces.

$$L(A_w) \supsetneq L(A_w - P) \supseteq L(A_{w-1}) \supsetneq L(A_{w-1} - P) \supseteq \cdots$$
$$\cdots \supseteq L(A_2) \supsetneq L(A_2 - P) \supseteq L(A_1) \supsetneq L(A_1 - P).$$

$$\Omega(A_w - C) \subsetneq \Omega(A_w - C - P) \subseteq \Omega(A_{w-1} - C) \subsetneq \Omega(A_{w-1} - C - P) \subseteq \cdots$$
$$\cdots \subset \Omega(A_2 - C) \subsetneq \Omega(A_2 - C - P) \subseteq \Omega(A_1 - C) \subsetneq \Omega(A_1 - C - P).$$

For $i = 1, 2, \ldots, w$, choose

$$f_i \in L(A_i) \backslash L(A_i - P) \;\text{ and }\; \eta_i \in \Omega(A_i - C - P) \backslash \Omega(A_i - C).$$

Let $A \in \Gamma_P$ be of degree $\deg A < w$. Then there exists a linear combination f of $f_1, f_2, \ldots, f_w$ that vanishes on A. If f_i is the leading function in the linear combination then $f \in L(A_i - A) \backslash L(A_i - A - P)$ and $f\eta_i \in \Omega(-C - P + A) \backslash \Omega(-C + A)$. Thus $A - C \notin \Gamma_P$ and $A \notin \Gamma_P(C)$. □

For a divisor B, let

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

Lemma 5.4. *To the set $\Delta_P(B,C)$ corresponds a dual set*

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

such that $\#\Delta_P(B,C)-\#\Delta_P(B-C,-C)=\deg C$. Furthermore,

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

In particular,

$$\#\Delta_P(B,C)=\begin{cases}\deg C, & \text{if } \deg C\geq 2g.\\ 0, & \text{if } \deg C\leq -2g.\end{cases}$$

Proof. For i_0 large enough,

$$\begin{aligned}&\#\Delta_P(B,C)-\#\Delta_P(B-C,-C)\\ =\ &\#\{i\leq i_0 : B+iP\in\Gamma_P, B-C+iP\notin\Gamma_P\}\\ &\quad-\#\{i\leq i_0 : B+iP\notin\Gamma_P, B-C+iP\in\Gamma_P\}\\ =\ &\sum_{i\leq i_0}(l(B+iP)-l(B+iP-P))-(l(B-C+iP)-l(B-C+iP-P))\\ =\ &\dim L(B+i_0P)-\dim L(B-C+i_0P)=\deg C.\end{aligned}$$

For the remainder use Lemma 5.1. □

Corollary 5.5. *For any choice of divisor B, there is a pair of equivalent bounds*

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

Proof. For the first inequality, the elements $A_1,A_2,\ldots,A_w\in\Delta_P(B,C)$, ordered from lowest to highest degree, meet the conditions of the theorem. Similar for the second inequality. Equivalence follows from $\gamma_P(C)-\gamma_P(-C)=\deg C$ and the previous lemma. □

Lemma 5.6. *If $A\in\Gamma_P(E)$ and $E\in\Gamma_P(C)$ then $A\in\Gamma_P(C)$. For $E\in\Gamma_P(C)$,*

$$\Delta_P(C)\subset\Delta_P(E).$$

Proof. The first claim is immediate from the definitions, in particular $A-E\in\Gamma_P$ and $E-C\in\Gamma_P$ implies $A-C\in\Gamma_P$. For $E\in\Gamma_P(C)$, the first claim shows that $A\notin\Gamma_P(E)$ whenever $A\notin\Gamma_P(C)$. □

6 Order bound and floor bound

We unify and improve two known lower bounds for the minimum distance of an algebraic geometric code. Let S be a given set of rational points, and let $C_L(D,G)$ and $C_\Omega(D,G)$ be algebraic geometric codes defined with a divisor $D = P_1 + \cdots + P_n$ disjoint from S. With Lemma 4.3,

$$\begin{aligned} d(C_L(D,G)) &\geq \gamma^*(C;S), \quad \text{for } C = D - G, \\ d(C_\Omega(D,G)) &\geq \gamma^*(C;S), \quad \text{for } C = G - K. \end{aligned}$$

Proposition 6.1. *For points $Q_0, \ldots, Q_{r-1} \in S$, define divisors $C_0 \leq C_1 \leq \cdots \leq C_r$ such that $C_0 = C$ and $C_{i+1} = C_i + Q_i$, for $i = 0, \ldots, r-1$. Then*

$$\gamma^*(C;S) \geq \min\{\gamma_{Q_0}(C_0;S), \gamma_{Q_1}(C_1;S), \ldots, \gamma_{Q_{r-1}}(C_{r-1};S), \gamma^*(C_r;S)\}\backslash\{0\},$$

In general, $\gamma^*(C_r;S) \geq \deg C + r$.

Proof. Proposition 4.5 gives $\gamma^*(C_i;S) \geq \min\{\gamma_{Q_i}(C_i;S), \gamma^*(C_{i+1};S)\}\backslash\{0\}$. □

We give a formulation of the order bound for an algebraic geometric code $C_\Omega(D,G)$.

Theorem 6.2. *(Order bound [Bee07, 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*

$$d(C_{\mathcal{P}}(G)) \geq d_{\mathcal{P}}(G) \geq d(G).$$

Using [Bee07, Remark 5, Definition 6], we expand the theorem in the notation of the current paper. In comparison with the original theorem, we have removed the condition that the divisors $B_0, \ldots, B_r$ are disjoint from D.

Theorem 6.3. *(Order bound [Bee07]) Let $C_\Omega(D,G)$ be an algebraic geometric code, and let $G = K + C$. For a sequence of points $Q_0, \ldots, Q_{r-1}$ disjoint from D, let $C_0 = C$ and $C_{i+1} = C_i + Q_i$, for $i = 0, \ldots, r-1$.*

$$\mathcal{C}_0 = C_\Omega(D, K+C) \supseteq \mathcal{C}_1 = C_\Omega(D, K+C_1) \supseteq \cdots \supseteq \mathcal{C}_r = C_\Omega(D, K+C_r).$$

If $\mathcal{C}_i \neq \mathcal{C}_{i+1}$ then a word in $\mathcal{C}_i \backslash \mathcal{C}_{i+1}$ has weight $w \geq \#\Delta_{Q_i}(0, C_i)$. For r large enough,

$$d(C_\Omega(D,G)) \geq \min\{\#\Delta_{Q_i}(0,C_i) : \mathcal{C}_i \neq \mathcal{C}_{i+1}\}.$$

Moreover, for a sequence of divisors $B_0, \ldots, B_{r-1}$,

$$d(C_\Omega(D,G)) \geq \min\{\#\Delta_{Q_i}(B_i,C_i) : \mathcal{C}_i \neq \mathcal{C}_{i+1}\}.$$

Proof. The order bound for the minimum distance combines Proposition 6.1 with the estimates $\gamma_{Q_i}(C_i;S) \geq \gamma_{Q_i}(C_i) \geq \#\Delta_{Q_i}(B_i,C_i)$ in Corollary 5.5. □

We analyze the choice of the points $Q_0, Q_1, \ldots, Q_{r-1}$. In [Bee07], the choice of the points is unrestricted, and an example is given where the optimal lower bound is obtained with a choice of Q_i outside G. On the other hand, Proposition 4.1 shows that $\gamma_{Q_i}(C_i) \geq \deg C_i$. Thus, we may assume that the minimum $\min\{\gamma_{Q_i}(C_i)\}\backslash\{0\}$ is taken over an interval $i = 0, 1, \ldots, r$ such that, for all i in the interval, either $\gamma_{Q_i}(C_i) = 0$ or $\gamma_{Q_i}(C_i) > \deg C_i$. With Proposition 4.1 this implies that either $-C_i \in \Gamma_{Q_i}$ or $C_i \notin \Gamma_{Q_i}$. In both cases, we can conclude, for $C_i \neq 0$, that $C_i \notin \Gamma_{Q_i}$, i.e. that $L(C_i) = L(C_i - Q_i)$. The same conclusion can be reached with Lemma 5.4 if the argument is repeated for $\Delta_{Q_i}(B_i, C_i)$ instead of $\gamma_{Q_i}(C_i)$. The following stronger result holds.

Proposition 6.4. *The maximum in the order bound is attained for a choice of points $Q_0, Q_1, \ldots, Q_{r-1}$ such that, for $i = 0, 1, \ldots, r-1$, either $C_i = 0$, or $Q_i, \ldots, Q_{r-1}$ are base points of the divisor C_i. In particular, if C_i is a nonzero effective divisor, we may restrict the choice for $Q_i, \ldots, Q_{r-1}$ to points in the support of C_i.*

Proof. For $Q \in \{Q_i, \ldots, Q_{r-1}\}$, let j be minimal in $\{i, \ldots, r-1\}$ such that $Q_j = Q$. If $C_j \neq 0$, we may assume as explained above, that $C_j \notin \Gamma_Q$. With $E = Q_i + \cdots + Q_{j-1} \in \Gamma_Q$ and $C_j = C_i + E$ it follows that $C_i \notin \Gamma_Q$. If $C_j = 0$ then either $i = j$, in which case $C_i = 0$, or $i < j$, in which case $\deg C_i < 0$ and $C_i \notin \Gamma_Q$. □

In [Bee07, Example 8], the minimum distance lower bound for a code $C_\Omega(D, 5P)$ on the Klein curve is improved with a choice $Q_0 = P, Q_1 = Q \neq P$. For the example, $5P = K + 2P - Q$ and $6P = K + Q + R$, so that $C_0 = 2P - Q$ and $C_1 = Q + R$. Indeed, with the proposition, we can expect improvements only with $Q_1 = Q$ or with $Q_1 = R$.

To improve the order bound we apply the main theorem with a different format for the divisors $A_1, \ldots, A_w$. Let

$$\Delta_P(\leq B, C) = \{B + iP \in \Gamma_p : B - C - iP \notin \Gamma_P \ \wedge \ i \leq 0\},$$
$$\Delta_P(\geq B + P, C) = \{B + iP \in \Gamma_p : B - C - iP \notin \Gamma_P \ \wedge \ i \geq 1\},$$

be a partition of the set $\Delta_P(B, C)$ into divisors of small and large degree.

Lemma 6.5.

$$\#\Delta_P(\leq B, C) = \dim L(B) - \dim L(B - C) + \#\Delta_P(\leq B - C, -C).$$

Proof. Similar to the proof of Lemma 5.4, but use $i_0 = 0$. □

Theorem 6.6. *(ABZ bound for cosets) Let C be a divisor and let P be a point. For $G = K + C = A + B + Z$, $Z \geq 0$,*

$$\gamma_P(C; Z \cup P) \geq \#\Delta_P(\leq A, C) + \#\Delta_P(\leq B, C).$$

Proof. With Lemma 5.2, a divisor $A' \in \Delta_P(C)$ if and only if $K + C + P - A' \in \Delta_P(C)$. And $A' \leq A$ if and only if $K + C + P - A' \geq K + C + P - A = B + P + Z$. The elements $A_1, A_2, \ldots, A_w \in \Delta_P(\leq B, C) \cup \Delta_P(\geq B + P + Z, C)$, ordered from lowest to highest degree, meet the conditions of Theorem 5.3, with $w = \#\Delta_P(\leq A, C) + \#\Delta_P(\leq B, C)$. □

The lower bound $\#\Delta_P(B, C)$ that is used for the order bound takes into account only the number of divisors in a delta set $\Delta_P(B, C)$. The improved bounds in Theorem 6.6 are possible by considering also the degree distribution of divisors in the delta set. For $Z = 0$, the bounds in the theorem include those used in the order bound (Theorem 6.3). The floor bound (Theorem 2.3) sometimes exceeds the order bound. The ABZ bound for codes (Theorem 2.4) gives an improvement and generalization of the floor bound. We show that the bounds in the theorem not only include those obtained with the order bound but also those obtained with the ABZ bound for codes. In each case, the coset decoding procedure in the appendix decodes efficiently up to half the bound.

Theorem 6.7. *(ABZ bound for codes) Let $G = K+C = A+B+Z$, for $Z \geq 0$. For D with $D \cap Z = \emptyset$, a nonzero word in $C_\Omega(D, G)$ has weight $w \geq l(A)-l(A-C)+l(B)-l(B-C)$.*

Proof. Let P be a point on the curve not in the support of D, if necessary it can be chosen over an extension field. We use Proposition 6.1 with $S = Z \cup P$ and $Q_0 = Q_1 = \ldots = Q_{r-1} = P$.

$$\gamma^*(C; S) \geq \min\{\gamma_P(C; S), \gamma_P(C + P; S), \ldots, \gamma_P(C + (r-1)P; S), \gamma^*(C + rP; S)\} \backslash \{0\}.$$

Now use Theorem 6.6 with $K + C + iP = A + B + (Z + iP)$,

$$\gamma_P(C + iP; S) \geq \#\Delta_P(\leq A, C + iP) + \#\Delta_P(\leq B, C + iP).$$

With Lemma 6.5,

$$\begin{aligned} \gamma_P(C + iP; S) &\geq l(A) - l(A - C - iP) + l(B) - l(B - C - iP) \\ &\geq l(A) - l(A - C) + l(B) - l(B - C). \end{aligned}$$

Hence, by taking r large enough, $\gamma^*(C; S) \geq l(A) - l(A - C) + l(B) - l(B - C)$. □

Neither the ABZ bound for codes, nor the ABZ bound for cosets gives an improvement in general. For $Z = 0$, both bounds return previously known bounds, namely the Goppa bound and the order bound, respectively. For carefully chosen nontrivial Z, there are possible improvements. If we apply Lemma 6.5 with both A and B,

$$\begin{aligned} \#\Delta_P(\leq A, C) &= \dim L(A) - \dim L(A - C) + \#\Delta_P(\leq A - C, -C), \\ \#\Delta_P(\leq B, C) &= \dim L(B) - \dim L(B - C) + \#\Delta_P(\leq B - C, -C), \end{aligned}$$

and add the two equations, then we see that the improvement of the ABZ coset bound applied to $G = K+C = A+B+Z$ over the floor bound applied to $G = K+C = A+B+Z$

is given by the ABZ coset bound applied to the dual decomposition $G' = K - C = (A - C) + (B - C) + Z$. For $Z = 0$, we recover that the improvement of the order bound applied to $G = K + C$ over the Goppa bound $\deg C$ is given by the order bound applied to $G' = K - C$ (Lemma 5.4 and Corollary 5.5).

We consider the special case of the order bound with $B_0 = \cdots = B_{r-1} = 0$ and $Q_0 = \cdots = Q_{r-1} = P$. For codes of the form $C_L(D, \rho P)^\perp = C_\Omega(D, \rho P)$ or of the form $C_L(D, K + P + \rho P)^\perp = C_\Omega(D, K + P + \rho P)$ the resulting bound can be formulated entirely in terms of the numerical semigroup S of Weierstrass P-nongaps. For the first code use $C = \rho P - K$, and for the second $C = \rho P + P$. For the delta sets we obtain

$$\begin{aligned} pP \in \Delta_P(\rho P - K) &\Leftrightarrow pP \in \Gamma_P \wedge K + pP - \rho P \notin \Gamma_P. \\ &\Leftrightarrow p \in S \wedge \rho - p + 1 \in S, \\ pP \in \Delta_P(\rho P) &\Leftrightarrow pP \in \Gamma_P \wedge pP - \rho P - P \notin \Gamma_P. \\ &\Leftrightarrow p \in S \wedge p - \rho - 1 \notin S. \end{aligned}$$

The first of the two bounds in the following theorem is the Feng-Rao bound [FR93], [CFM00]. The second bound is different when the canonical divisor $K \not\sim (2g-2)P$.

Theorem 6.8. *(Feng-Rao bound) Let S be the semigroup of Weierstrass P-nongaps.*

$$d(C_L(D, \rho P)^\perp) \geq \min\{\#A[\rho'] : \rho' > \rho\} \backslash \{0\},$$

where $A[\rho] = \{p \in S | \rho - p \in S\}$.

$$d(C_L(D, K + \rho P)^\perp) \geq \min\{\#B[\rho'] : \rho' > \rho\} \backslash \{0\},$$

where $B[\rho] = \{p \in S | p - \rho \notin S\}$.

Proof. Apply Proposition 6.1 with the given delta sets. □

7 Concluding remark

Both problems of finding the lower bound for the adversary threshold of an algebraic geometric linear secret sharing scheme and the lower bound for the minimum distance of an algebraic geometric code can be approached as a geometric approximation problem : Given a divisor on an algebraic curve, represent the divisor as a difference of two effective divisors such that the effective divisors are each disjoint from a given set S and find lower bounds for the degrees of the effective divisors in such a representation. In other words, for a given curve X and divisor class C, find the lower bounds on the degree of a divisor A such that A and $A - C$ belong to specified semigroups of divisors. For suitable choices of the semigroups we obtain (1) lower bounds for the size of a party A that can recover the secret in an algebraic geometric linear secret sharing scheme with adversary threshold C, and (2) lower bounds for the support A of a codeword in a geometric Goppa code with designed minimum support C.

A Coset decoding

For a given vector $y \in \mathbb{F}^n$, and for an extension of linear codes $\mathcal{C}' \subset \mathcal{C} \subset \mathbb{F}^n$, coset decoding determines the cosets of $\mathcal{C}'$ in $\mathcal{C}$ that are nearest to the vector y. If y is at distance $d(y, \mathcal{C}) \leq t$ from $\mathcal{C}$ and the minimum distance $d(\mathcal{C}/\mathcal{C}')$ between distinct cosets is at least $w > 2t$ then there exists a unique nearest coset $c + \mathcal{C}'$ with $d(y, c + \mathcal{C}') \leq t$. We describe a coset decoding procedure that returns the unique coset when the estimate $d(\mathcal{C}/\mathcal{C}') \geq w$ is obtained with Theorem 1.2. The procedure follows the majority coset decoding procedure in [Duu], [Duu93].

Shift bound or Coset bound (Theorem 1.2): Let $\mathcal{C}/\mathcal{C}_1$ be an extension of $\mathbb{F}$-linear codes with corresponding extension of dual codes $\mathcal{D}_1/\mathcal{D}$ such that $\dim \mathcal{C}/\mathcal{C}_1 = \dim \mathcal{D}_1/\mathcal{D} = 1$. If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

$$\begin{cases} a_i * b_j \in \mathcal{D} & \text{for } i + j \leq w, \\ a_i * b_j \in \mathcal{D}_1 \backslash \mathcal{D} & \text{for } i + j = w + 1, \end{cases}$$

then $d(\mathcal{C}/\mathcal{C}_1) \geq w$.

For a given $x \in \mathcal{D}_1 \backslash \mathcal{D}$, we may assume, after rescaling if necessary, that $a_i * b_{w+1-i} \in x + \mathcal{D}$, for $i = 1, \ldots, w$. Define the following cosets of a_i and b_{w+1-i}, for $i = 1, \ldots, w$,

$$A_i = a_i + \langle a_1, \ldots, a_{i-1} \rangle,$$
$$B_{w+1-i} = b_{w+1-i} + \langle b_1, \ldots, b_{w-i} \rangle.$$

For $c \in \mathcal{C}$, the coset $c + \mathcal{C}_1$ is uniquely determined by $x \cdot c$. For a given $y \in \mathbb{F}^n$ such that $d(y, \mathcal{C}) \leq t$, the decoding procedure will look for a pair $a' \in A_i, b' \in B_{w+1-i}$ such that, for all $c \in \mathcal{C}$ with $d(y, c) \leq t$, $(a' * b') \cdot y = x \cdot c$. The vector $a' * b'$ is defined as the Hadamard or coordinate-wise product of the vectors a' and b'. We use $(a' * b') \cdot y = (a' * y) \cdot b'$.

Theorem A.1. *(Decoding up to half the coset bound) Let $2t < w \leq d(\mathcal{C}/\mathcal{C}_1)$, for $\mathcal{C}/\mathcal{C}_1$ and w as in Theorem 1.2. For $y \in \mathbb{F}^n$ such that $d(y, \mathcal{C}) \leq t$, let*

$$I = \{1 \leq i \leq w : \ (\exists a'_i \in A_i)\ (a'_i * b_j) \perp y, 1 \leq j \leq w - i \ \},$$
$$I^* = \{1 \leq j \leq w : \ (\exists b'_j \in B_{w+1-j})\ (a_i * b'_j) \perp y, 1 \leq i \leq j - 1 \ \}.$$

For every $c \in \mathcal{C}$ with $d(y, c) \leq t$, $x \cdot c = (a'_i * b'_i) \cdot y$, for a majority of $i \in I \cap I^*$.

Proof. For $c \in \mathcal{C}$, let $a'_i \in A_i$ be such that $a'_i * y = a'_i * c$. The vector a'_i, if it exists, satisfies $(a'_i * b_j) \cdot y = 0$, for $j = \{1, \ldots, w - i\}$. Moreover, for any $b' \in B_{w+1-i}$, $(a'_i * b') \cdot y = (a'_i * b') \cdot c = (a_i * b_{w+1-i}) \cdot c = x \cdot c$. Let

$$\Gamma = \{1 \leq i \leq w : \ (\exists a'_i \in A_i)\ a'_i * y = a'_j * c \ \}, \qquad \Delta = \{1 \leq i \leq w\} \backslash \Gamma,$$
$$\Gamma^* = \{1 \leq j \leq w : \ (\exists b'_j \in B_{w+1-j})\ b'_j * y = b'_j * c\}, \qquad \Delta^* = \{1 \leq j \leq w\} \backslash \Gamma^*.$$

We know a priori only the sets I and I^*. Clearly, $\Gamma \subset I$ and $\Gamma^* \subset I^*$. Moreover, for $c \in \mathcal{C}$ with $d(y,c) \leq t$, $|\Delta|, |\Delta^*| \leq t$. For $i \in I \cap I^*$, $(a'_i * b'_i) \cdot y = x \cdot c$ if either $i \in \Gamma$ or $i \in \Gamma^*$. Regardless of the actual sets I and I^*, this is certainly the case if $i \in \Gamma \cap \Gamma^*$ and it fails only when $i \in \Delta \cap \Delta^*$. Now

$$|\Gamma \cap \Gamma^*| - |\Delta \cap \Delta^*| = w - |\Gamma \cap \Delta^*| - |\Gamma^* \cap \Delta| \geq w - 2t > 0.$$

Thus, the majority of $i \in I \cap I^*$ will give a value $(a'_i * b'_i) \cdot y = x \cdot c$. □

If $\dim \mathcal{C}/\mathcal{C}' > 1$ then the procedure can be applied iteratively to a sequence of extensions $\mathcal{C}' = \mathcal{C}_r \subset \mathcal{C}_{r-1} \subset \cdots \mathcal{C}_1 \subset \mathcal{C}_0 = \mathcal{C}$ such that $\dim \mathcal{C}_i/\mathcal{C}_{i-1} = 1$, for $i = 1, \ldots, r$. For given $y_0 \in \mathbb{F}^n$ with $d(y_0, \mathcal{C}_0) \leq t$, the procedure returns the unique coset $c_0 + \mathcal{C}_1$ such that $d(y_0, c_0 + \mathcal{C}_1) \leq t$. At the next iteration, for $y_1 = y_0 - c_0 \in \mathbb{F}^n$ with $d(y_1, \mathcal{C}_1) \leq t$, the procedure returns the unique coset $c_1 + \mathcal{C}_2$ such that $d(y_1, c_1 + \mathcal{C}_2) \leq t$, and so on.

Let $\mathcal{A} = \{A_1 \leq A_2 \leq \cdots \leq A_w\} \subset \Delta_P(C)$ be a sequence of divisors with $A_{i+1} \geq A_i + P$, for $i = 1, \ldots, w-1$. Theorem 5.3 (Main theorem) together with Lemma 4.2 shows that $d(C_\Omega(D, G-P)/C_\Omega(D,G)) \geq w$, for G such that $C = G - K - P$, and for $D \cap (A_w - A_1) = \emptyset$. We show how the coset decoding procedure applies to the given extension. For a divisor $A_i \in \Delta_P(C)$, also $K + C + P - A_i = G - A_i \in \Delta_P(C)$. Thus, there exist functions $f_i \in L(A_i) \backslash L(A_i - P)$ and $g_i \in L(G - A_i) \backslash L(G - A_i - P)$. Let $(a_i * b_{w+1-j}) = ((f_i g_j)(P_n), \ldots, (f_i g_j)(P_n))$, for $i \leq j$. Then

$$\begin{cases} a_i * b_j \in C_L(D,G) & \text{for } i + j \leq w, \\ a_i * b_j \in C_L(D,G) \backslash C_L(D, G-P) & \text{for } i + j = w + 1, \end{cases}$$

Moreover, we have the following interpretation for the sets $\Gamma, \Gamma^*, \Delta, \Delta^*$.

$$\begin{array}{llll} i \in \Gamma & \Leftrightarrow A_i \in \Gamma_P(Q), & i \in \Delta & \Leftrightarrow A_i \in \Delta_P(Q), \\ i \in \Gamma^* & \Leftrightarrow A_i \in \Delta_P(C-Q), & i \in \Delta^* & \Leftrightarrow A_i \in \Gamma_P(C-Q). \end{array}$$

The order bound (Theorem 6.3) and the floor bound (Theorem 2.3) as well as their generalizations the ABZ bound for cosets (Theorem 6.6) and the ABZ bound for codes (Theorem 6.7) are all obtained in this paper as special cases of the main theorem. Thus, in each case coset decoding can be performed with Theorem A.1.

References

[BA04] 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.

[Bee07] Peter Beelen. The order bound for general algebraic geometric codes. *Finite Fields Appl.*, 13(3):665–680, 2007.

[BT06] Peter Beelen and Nesrin Tutaş. A generalization of the Weierstrass semigroup. *J. Pure Appl. Algebra*, 207(2):243–260, 2006.

[CC06] 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.

[CDG+05] Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. In *Advances in cryptology—CRYPTO 2005*, volume 3621 of *Lecture Notes in Comput. Sci.*, pages 327–343. Springer, Berlin, 2005.

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 316–334. Springer, Berlin, 2000.

[CFM00] 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.

[CT05] Cícero Carvalho and Fernando Torres. On Goppa codes and Weierstrass gaps at several points. *Des. Codes Cryptogr.*, 35(2):211–225, 2005.

[Duu] Iwan M. Duursma. *Decoding codes from curves and cyclic codes*. Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1993.

[Duu93] Iwan M. Duursma. Majority coset decoding. *IEEE Trans. Inform. Theory*, 39(3):1067–1070, 1993.

[Duuar] 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.

[DP08] Iwan M. Duursma and Seungkook Park. Coset bounds for algebraic geometric codes. arXiv:0810.2789, 2008.

[FR93] Gui Liang Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inform. Theory*, 39(1):37–45, 1993.

[GKL93] Arnaldo García, Seon Jeong Kim, and Robert F. Lax. Consecutive Weierstrass gaps and minimum distance of Goppa codes. *J. Pure Appl. Algebra*, 84(2):199–207, 1993.

[HK06] 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.

[HP03] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[Kim94] 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.

[KP95] 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.

[LM06] 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.

[Mat01] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Des. Codes Cryptogr.*, 22(2):107–121, 2001.

[MM06] Hiren Maharaj and Gretchen L. Matthews. On the floor and the ceiling of a divisor. *Finite Fields Appl.*, 12(1):38–55, 2006.

[O'S01] Michael E. O'Sullivan. New codes for the Berlekamp-Massey-Sakata algorithm. *Finite Fields Appl.*, 7(2):293–317, 2001.

[Par] Seungkook Park. *Applications of algebraic curves to cryptography*. Dissertation, University of Illinois, Urbana, 2007.

[Pre98] 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.

[Ste99] Serguei A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes*. Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.

[TVN07] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[vL99] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

[vLW86] Jacobus H. van Lint and Richard M. Wilson. On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory*, 32(1):23–40, 1986.