Minimum weights of two-point algebraic geometry codes

Boran Kim
(joint work with Yoonjin Lee)

Institute of Mathematical Sciences
Ewha Womans University

July 5, 2018

Outline

Previous Works

Previous Works

- Algebraic geometry code (AG code) is constructed by Goppa.
- The order bound is a certain type of bound of the minimum weights for AG code.
- The original order bound for minimum weights of AG code was introduced by Feng et al.
- Geil and Ruano considered the special case of the order bound, and it is called order-like bound. They studied the order-like bound for only one-point AG codes.

Our Goal

Our Goal

- We find the order-like bound of the minimum weights of two-point AG codes on algebraic curves.
- We prove that this order-like bound is better than the Goppa bound.
- We explicitly determine the order-like bounds for one-point AG codes and two-point AG codes on norm-trace curves over $\mathbb{F}_{2^r}$.

Preliminaries

- An *algebraic function field F/K of one variable over K* is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some $x \in F$, which is transcendental over K.
- A *valuation ring $\mathcal{O}$* of the function field F/K is a ring with the following properties:

$$(1) K \subsetneq \mathcal{O} \subsetneq F,$$
$$(2) \forall z \in F,\ z \in \mathcal{O} \text{ or } z^{-1} \in \mathcal{O}.$$

- A *place P* of a function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$.

- A *divisor* is a formal sum

$$D = \sum_{p \in \mathbb{P}_F} n_P P$$

  with $n_P \in \mathbb{Z}$, almost all $n_P = 0$.
- *supp* D:=$\{P \in \mathbb{P}_F \mid n_P \neq 0\}$.
- Let $0 \neq x \in F$
  - $\mathbb{P}_F$: the set of all places of an algebraic function field F
  - v_P: the valuation of P with $P \in \mathbb{P}_F$
  - Z: the set of zeros of x in $\mathbb{P}_F$ (that is, $Z = \{P \in \mathbb{P}_F : v_P(x) > 0\}$)
  - N: the set of poles of x in $\mathbb{P}_F$ (that is, $N = \{P \in \mathbb{P}_F : v_P(x) < 0\}$)

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \quad \textit{the zero divisor of } x$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P, \quad \textit{the pole divisor of } x$$

$$(x) := (x)_0 - (x)_\infty, \quad \textit{the principal divisor of } x$$

- For a divisor A, we set $\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}$.
- The *Weierstrass semigroup* at P is

$$H(P) := \{h \in \mathbb{N}_0 : \exists f \in F \text{ with } (f)_\infty = hP\}.$$

- $G(P) := \mathbb{N}_0 \setminus H(P)$: the *gap set* at P
- $H(Q_1, Q_2) := \{(h_1, h_2) \in \mathbb{N}_0^2 : \exists f \in F \text{ with } (f)_\infty = h_1 Q_1 + h_2 Q_2\}$
- $G(Q_1, Q_2) := \mathbb{N}_0^2 \setminus H(Q_1, Q_2)$

The algebraic geometry code (AG code)

- $\mathcal{L}$-construction: $C_{\mathcal{L}}(D, G)$
- Ω-construction: $C_{\Omega}(D, G)$

The codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ are dual to each other, that is,

$$C_{\Omega}(D, G) = C_{\mathcal{L}}(D, G)^{\perp}.$$

- $F/\mathbb{F}_q$: an algebraic function field of genus g
- $P_0, \cdots, P_{n-1}$: pairwise distinct places of $F/\mathbb{F}_q$ of degree 1
- $D = P_0 + \cdots + P_{n-1}$
- G: a divisor of $F/\mathbb{F}_q$ such that $supp\ G \cap supp\ D = \emptyset$

The *algebraic geometry code (AG code)* $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is defined by

$$\begin{aligned} C_{\mathcal{L}}(D, G) &:= \{(x(P_0), \cdots, x(P_{n-1})) \mid x \in \mathcal{L}(G)\} \subset \mathbb{F}_q^n \\ &:= \{ev(x) \mid x \in \mathcal{L}(G)\}, \end{aligned}$$

where ev is the evaluation map such that $ev : x \mapsto (x(P_0), \cdots, x(P_{n-1}))$.

- If the divisor G consists of only one place, then $C_{\mathcal{L}}(D, G)$ is called *one-point AG code*.
- If the divisor G consists of two places, then $C_{\mathcal{L}}(D, G)$ is called *two-point AG code*.

- *The Goppa bound:* Any AG code $C = C(D, G)$ on an algebraic curve χ has the parameters $[n, k, d]$ such that

$$k = \ell(G) - \ell(G - D) \text{ and } d \geq n - deg(G),$$

where n is the length of C, k is the dimension of C and d is the minimum weight of C.

The norm-trace curve

The *norm-trace curve* over $\mathbb{F}_{q^r}$ with $r \geq 2$ has the defining equation

$$y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y = x^{a+1}, \tag{1}$$

where $a = \frac{q^r - 1}{q-1} - 1$ (if $r = 2$, then it is called the *Hermitian curve*).

- the curve has a single rational point at infinity, $P_\infty = (0:1:0)$ and q^{2r-1} affine rational points.
- the genus of $F/\mathbb{F}_{q^r}$ is $g = \frac{a(q^{r-1}-1)}{2}$ with $a = \frac{q^r-1}{q-1} - 1$.
- $|G(P_\infty)| = g$
- $H(P_{00}) =$
  $\langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)\rangle$,
  where $\lambda = q^{r-2} + q^{r-3} + \ldots + q - 1$.
- $H(P_\infty) = \langle q^{r-1}, (q^r-1)/(q-1)\rangle$

- $H(Q_1, Q_2) = \{lub(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(Q_1, Q_2) \cup (H(Q_1) \times \{0\}) \cup (\{0\} \times H(Q_2))\}$, where $lub(\mathbf{x}, \mathbf{y}) := (max\{(\alpha_1, \alpha_2), max\{\beta_1, \beta_2\}\})$ with $\mathbf{x} = (\alpha_1, \beta_1)$ and $\mathbf{y} = (\alpha_2, \beta_2)$.
  - Given two different rational points Q_1, Q_2, for $\alpha \in G(Q_1)$, we define
    $$\beta_\alpha := min\{\beta \in \mathbb{N}_0 : (\alpha, \beta) \in H(Q_1, Q_2)\}.$$
  - $\{\beta_\alpha : \alpha \in G(Q_1)\} = G(Q_2)$
  - for $\alpha_1 < \alpha_2 < \ldots < \alpha_g \in G(Q_1)$, $\beta_1 < \beta_2 < \ldots < \beta_g \in G(Q_2)$
    $$\Gamma(Q_1, Q_2) := \{(\alpha_i, \beta_{\alpha_i}) : i = 1, 2, \ldots, g\}.$$
- (On norm-trace curves) for every s and (i, j) such that
  - $1 \leq s \leq q^{r-2} + \ldots + q + 1$
  - $1 \leq j \leq i \leq a - s$
  - $(s-1)q - (s-1) \leq i - j \leq sq - (s+1)$

  we have
  $$\beta_{(i-j)(a+1)+j} = (q^{r-1} - (i - j + 1))(a + 1) - jq^{r-1}.$$

The order-like bound for a one-point AG code

- χ: a (projective, non-singular, geometrically irreducible) algebraic curve over a finite field $\mathbb{F}_p$
- P_∞: the point at infinity $(0:1:0)$ of χ
- f_j: an element of F such that $v_{P_\infty}(f_j) = m_j$ for $1 \leq j \leq n$
- $B = \{ev(f_1), \ldots, ev(f_n)\}$: a basis of $\mathbb{F}_p^n$
- $C_i = \langle ev(f_1), \ldots, ev(f_i) \rangle = C(D, m_i P_\infty)$ $(1 \leq i \leq n)$: a one-point AG code of length n on χ for $1 \leq i \leq n$
- $C_1 \subsetneq C_2 \subsetneq \ldots \subsetneq C_n$

– the map $\nu : \mathbb{F}_p^n \to \{1 \ldots, n\}$ such that

$$\nu(\mathbf{v}) = min\{i : \mathbf{v} \in C_i\}.$$

- the order $(r, s) \prec (i, j)$ in $\{1, \ldots, n\}^2$ if and only if $r \leq i$, $s \leq j$ and $(r, s) \neq (i, j)$.

The order-like bound for a one-point AG code

- A pair $(ev(f_i), ev(f_j))$ is called *well-behaving* if

$$\nu(ev(f_r) * ev(f_s)) < \nu(ev(f_i) * ev(f_j))$$

for all $(r, s) \prec (i, j)$, where $*$ is the component-wise product.

- Define

$$\Lambda_i^* = \{ev(f_j) \in B : (ev(f_i), ev(f_j)) \text{ is well-behaving}\}$$

for $i = 1, \ldots, n$.

- If $\mathbf{c} \neq 0$ and $\mathbf{c} \in C_i \setminus C_{i-1}$, then $wt(\mathbf{c}) \geq |\Lambda_i^*|$.
- The *order-like bound for a one-point AG code* $C(D, m_i P_\infty)$ is defined as follows:

$$d^*(C(D, m_i P_\infty)) := min\{|\Lambda_r^*| : r \leq m_i\}.$$

$(C_1 \subsetneq C_2 \subsetneq \ldots \subsetneq C_n)$

Two-point AG codes on algebraic curves and their order-like bound

P_∞ (resp. P_0)	the point at infinity $(0:1:0)$ of χ (resp. the zero point $(0:0:1)$ of χ)
$P_1, \cdots, P_{n-1}$	pairwise distinct rational points of χ except for P_0 and P_∞
D_0	the divisor $D - P_0$ of an algebraic curve χ over $\mathbb{F}_p$ (that is, $deg(D_0) = n-1$)
k	the smallest positive pole number at P_0 of χ
$H_k(P_\infty)$	$\{m \in \mathbb{N}_0 : (m,k) \in H(P_\infty, P_0)\}$
$\widetilde{G}$	$H_k(P_\infty) \setminus H(P_\infty)$
$G_k(P_\infty)$	$\mathbb{N}_0 \setminus H_k(P_\infty)$
$H^*(P_\infty, P_0)$	$\{(m,k) \in H(P_\infty, P_0) : C(D_0, (m-1)P_\infty + kP_0) \subsetneq C(D_0, mP_\infty + kP_0)\}$
$H_k^*(P_\infty)$	$\{m \in \mathbb{N}_0 : (m,k) \in H^*(P_\infty, P_0)\}$

- $m_1, \ldots, m_{n-2} \in H_k^*(P_\infty)$ such that $m_1 < \ldots < m_{n-2}$
- C_{m_i}: a two-point AG code $C(D_0, m_i P_\infty + kP_0)$ of length $n-1$
- $\Lambda_{m_i}^* := \{(m,k) : m = m_i + m_j \in H_k^*(P_\infty) \text{ for } m_j \in H_k^*(P_\infty)\}$

(i) $\widetilde{G} \cap H_k^*(P_\infty) = \emptyset$. Then

$$d(C_{m_i}) \geq d^*(C_{m_i}) := min\{|\Lambda_{m_r}^*| : m_r \leq m_i\}.$$

This bound $d^*(C_{m_i})$ is greater than or equal to the Goppa bound.

(ii) $\widetilde{G} \cap H_k^*(P_\infty) \neq \emptyset$. Then

$$d(C_{m_i}) \geq d^*(C_{m_i}) := \min\{|\widehat{\Lambda^*_{m_r}}| : m_r \leq m_i\},$$

where $\alpha \in \widetilde{G}$, $\delta_\alpha = max\{d_G(C(D_0, \alpha P_\infty + kP_0)),\ |\Lambda^*_\alpha|\}$ and

$$|\widehat{\Lambda^*_{m_i}}| := \begin{cases} \delta_\alpha & \text{if } m_i = \alpha, \\ |\Lambda^*_{m_i}| & \text{if } m_i \neq \alpha. \end{cases}$$

Furthermore, if $m_i \neq \alpha$, this bound is better than the Goppa bound.

The order-like bound for one-point AG codes on norm-trace curves

- over $\mathbb{F}_{2^r}$, $r \geq 3$ and $s = 2^{r-1} - 1$
- $a = js + t \in H^*(P_\infty)$, where $0 \leq j \leq 2^r - 1$ and $\left\lceil \frac{j}{2} \right\rceil \leq t \leq j$
- $C(D, aP_\infty)$: a one-point AG code on the norm-trace curve over $\mathbb{F}_{2^r}$ of length $n = deg(D) = 2^{2r-1}$

Then we have that

$$d(C(D, aP_\infty)) \geq d^*(C(D, aP_\infty)) := \begin{cases} 2^{2r-1} - js - \left\lceil \frac{j}{2} \right\rceil & \text{if } \left\lceil \frac{j}{2} \right\rceil \leq t \leq j-1, \\ 2^{2r-1} - js - j & \text{if } t = j. \end{cases}$$

Moreover, this bound is greater than or equal to the Goppa bound.

Lemma 1

Let g: the genus of the norm-trace curve χ over $\mathbb{F}_{2^r}$ with $r \geq 3$.

(i) Any pole number h at P_∞ with $h \leq 2^{2r-1} - 2^{r-1}$ on the norm-trace curve over $\mathbb{F}_{2^r}$ with $r \geq 3$ can be written uniquely as

$$h = j(2^{r-1} - 1) + t,$$

where j and t are non-negative integers, $0 \leq j \leq 2^r - 1$ and $\left\lceil \frac{j}{2} \right\rceil \leq t \leq j$.

(ii) The largest element of $G(P_\infty)$ is equal to $2g - 1$.

(iii) Any element $m \in H^*(P_\infty)$ satisfies $0 \leq m \leq (2^r - 1)^2$.

The order-like bound for two-point AG codes on norm-trace curves

- $k = 2^r - 2$ and $n = deg(D_0) + 1$
- C_m: a two-point AG code $C(D_0, mP_\infty + kP_0)$ on the norm-trace curve over $\mathbb{F}_{2^r}$ of length $n-1$, where $m \in H_k^*(P_\infty)$

The order-like bound $d^*(C_m)$ for C_m is computed as follows:
Suppose that $r = 2$. Then $m \in \{0, 1, 2, 3, 4, 6\}$, and

$$d^*(C_m) = \begin{cases} 6 & \text{if } m = 0, \\ 4 & \text{if } m = 1, 2, \\ 3 & \text{if } m = 3, \\ 2 & \text{if } m = 4, \\ 1 & \text{if } m = 6. \end{cases}$$

Now, suppose that $r \geq 3$.

- j: an integer with $0 \leq j \leq 2^r - 4$
- $m = a(j,t) = js + t$, where $s = 2^{r-1} - 1$ and $\left\lceil \frac{j}{2} \right\rceil \leq t \leq j + 1$

We consider the following three cases.

Case 1. If $j = 0$ and $t = 0$, then $d^*(C_{a(0,0)}) = |H_k^*(P_\infty)| = n - 2$.

Case 2. If $1 \leq j \leq 2^{r-1} - 2$ and $\left\lceil \frac{j}{2} \right\rceil \leq t \leq j$, then

$$d^*(C_{a(j,t)}) = 2^{2r-1} - 2^r + 1 - (j-1)(2^{r-1} - 1) - j.$$

Case 3. In the following cases, $2^{r-1}-1 \le j \le 2^r-4$.

Subcase 3.1. If $\lceil \frac{j}{2} \rceil \le t \le j-1$, then we have

$$d^*(C_{a(j,t)}) = 2^{2r-1} - 3\cdot 2^{r-1} + 3 - (2^{r-1}-2)j.$$

Subcase 3.2. If $t = j$, then we have

$$d^*(C_{a(j,t)}) = \begin{cases} 2^{2r-1} - 3\cdot 2^{r-1} + 3 - (2^{r-1}-2)j & \text{if } 2^{r-1}-1 \le j \le 3\cdot 2^{r-2}-3, \\ 2^{2r-1} - 2 - a(j,t) & \text{if } 3\cdot 2^{r-2}-2 \le j \le 2^r-4. \end{cases}$$

Subcase 3.3. If $t = j+1$, then we have

$$d^*(C_{a(j,t)}) = \begin{cases} 2^{2r-1} - 3\cdot 2^{r-1} + 3 - (2^{r-1}-2)(j+1) & \text{if } 2^{r-1}-1 \le j \le 2^r-5, \\ 2^{2r-1} - 3\cdot 2^{r-1} + 2 - (2^{r-1}-2)(j+1) & \text{if } j = 2^r-4. \end{cases}$$

Lemma 2

Let

- $k = 2^r - 2$
- P_∞: the point at infinity of the norm-trace curve over $\mathbb{F}_{2^r}$ with $r \geq 2$

(i) Every element h of $H_k(P_\infty)$ with $h \leq 2^{2r-1} - 2^{r+1} + 1$ can be written uniquely as

$$h = j(2^{r-1} - 1) + t$$

where j and t are non-negative integers such that $0 \leq j \leq 2^r - 4$ and $\left\lceil \frac{j}{2} \right\rceil \leq t \leq j + 1$.

(ii) The largest element of $G_k(P_\infty)$ is equal to

$$(2^r - 6)(2^{r-1} - 1) + (2^r - 4).$$

(iii) Let $\delta = js + t$ be an integer with $\delta \leq 2^{2r-1} - 2^{r+1} + 1$, where j and t are non-negative integers and $s = 2^{r-1} - 1$. If there exists an integer l such that

$$\left\lceil \frac{j+l}{2} \right\rceil + ls \leq t \leq j + l + ls + 1,$$

then δ is contained in $H_k(P_\infty)$.

(iv) Any element $m \in H_k^*(P_\infty)$ satisfies $0 \leq m \leq (2^{r+1} - 2)(2^{r-1} - 1)$.

(v) The set $H_k^*(P_\infty)$ consists of non-negative integers m such that

$$\begin{cases} m \in H_k(P_\infty) & \text{if } 0 \le m \le 2^{2r-1} - 2^r, \\ m \in H_k(P_\infty) \setminus M_k & \text{if } 2^{2r-1} - 2^r + 1 \le m \le (2^{r+1} - 2)(2^{r-1} - 1), \end{cases}$$

where $M_k = \{m \in H_k(P_\infty) : m - 2^{2r-1} + 2^r - 1 \in H(P_\infty)\}$.

(vi) Every element of $H_k(P_\infty) \setminus H(P_\infty)$ is expressed by

$$j(2^{r-1} - 1) + j + 1$$

for all $0 \le j \le 2^r - 4$.

(v) $H_k(P_\infty) \setminus H(P_\infty) \subseteq H_k^*(P_\infty)$

One-point AG codes and Two-point AG codes

- $r \geq 3$
- j: a positive integer such that $2 \leq j \leq 2^r - 4$
- t: a positive integer such that

$$t \in \left\{ i \in \mathbb{Z} : \left\lceil \frac{j+2}{2} \right\rceil \leq i \leq j \right\} \text{ or } \quad t \in \left\{ j+1 \in \mathbb{Z} : j + \left\lceil \frac{j}{2} \right\rceil > 2^r - 4 \right\}.$$

  - The two-point AG codes $C(D_0, ((j(2^{r-1}-1)+t)P_\infty + kP_0))$ and the one-point AG codes $C(D_0, ((j+2)(2^{r-1}-1)+t)P_\infty)$ have the same length and the same dimension on the norm-trace curve over $\mathbb{F}_{2^r}$.
  - But $d^*(C(D_0, ((js+t)P_\infty + kP_0)))$ is larger than $d^*(C(D_0, ((j+2)s+t)P_\infty))$ in terms of their order-like bounds.

References I


P. Beelen, *The order bound for general algebraic geometric codes*, Finite Fields Appl., **13**, (2007), 665-680.


C. Carvalho, F. Torres, *On Goppa codes and Weierstrass gaps at several points*, Des. Codes Cryptogr., **35**, (2005), 211-225.


I. Duursma, R. Kirov, S. Park, *Distance bounds for algebraic geometric codes*, J. Pure Appl. Algebra, **215**, (2011), 1863-1878.


O. Geil, D. Ruano, *On the order bounds for one-point AG codes*, Adv. Math. Commun., **5**, (2011), 489-504.


B. Kim, Y. Lee, *The minimum weights of two-point AG codes on norm-trace curves*, Finite Fields Appl., **53**, (2018), 113-139.


G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes Cryptogr., **22**, (2001), 107-121.


C. Munuera, G. C. Tizziotti, F. Torres, *Two point codes on norm-trace curves*, Coding Theory and Applications, Second International Castle Meeting, ICMCTA 2008 (A. Barbero Ed.), Lecture Notes in Comput. Sci., **5228**, (2008), 128-136.


W. Olaya-Leon, C. Munuera, *On the minimum distance of Castle codes*, Finite Fields Appl., **20**, (2013), 55-63.

Thank you

Example

- χ: the norm-trace curve $X^{15} - Y^8Z^7 - Y^4Z^{11} - Y^2Z^{13} - YZ^{14}$ over $\mathbb{F}_{2^4}$
- $g = 49$
- the number of rational points (including P_∞) $= 129$
- $P_\infty = (0:1:0)$, $P_0 = (0:0:1)$
- $D_0 = P_1 + \cdots + P_{127}$, where P_i are pairwise distinct rational points.

We consider the sequence of two-point AG codes $(C_i)_{i\in\{1,\cdots,127\}}$ such that $C_1 = C(D_0, 0)$ and $C_i = C(D_0, m_iP_\infty + 14P_0)$ for $2 \le i \le 127$, where $2^r - 2 = 14$ is the smallest positive pole number at P_0 and $m_i \in H_k^*(P_\infty)$.

For example, if $a(t) = 7 \cdot 9 + t$, where $j = 9$ and $\lceil \frac{9}{2} \rceil = 5 \leq t \leq 10$, then we have the order-like bound for the two-point AG codes $C_{a(t)}$ by the main result as follows:

(i) If $5 \leq t \leq 9$, then we have

$$d^*(C_{a(t)}) = 2^{2r-1} - 3 \cdot 2^{r-1} + 3 - (2^{r-1} - 2)j = 53.$$

(ii) If $t = j + 1 = 10$, then we obtain

$$d^*(C_{a(t)}) = 2^{2r-1} - 3 \cdot 2^{r-1} + 3 - (2^{r-1} - 2)(j + 1) = 47.$$

Now, we consider the one-point AG codes of length 127 on the same norm-trace curve χ. The two-point AG codes $C(D_0, (js+t)P_\infty + 14P_0)$ have better order-like bound than the bound for

$$C(D_0, ((j+2)s+t)P_\infty), \text{ where } 2 \leq j \leq 12$$

and

$$t \in \left\{ i \in \mathbb{Z} : \lceil \frac{j+2}{2} \rceil \leq i \leq j \right\} \cup \left\{ j+1 : j + \lceil \frac{j}{2} \rceil > 12 \right\};$$

in this case, both codes have the same dimension and the same length.

For instance, when $j = 9$ and $t = 10$, the two-point AG code $C_{2t} = C(D_0, 73P_\infty + 14P_0)$ and the one-point AG code $C_{1t} = C(D_0, 87P_\infty)$ have the same dimension and the same length 127, and we have

$$d^*(C_{2t}) = 47 > d^*(C_{1t}) = 45.$$