Delta sets for divisors supported in two points

Seungkook Park

Sookmyung Women's University

2012 KIAS International Conference on Coding Theory and Applications, November 16, 2012

Joint work with Iwan Duursma

Goal

Goal :

- Give motivation for the delta sets.
- Improve the bounds for the minimum distance of AG codes.

Code

- $\mathbb{F}$: finite field
- $\mathbb{F}$-linear code $\mathcal{C}$ of length n : linear subspace of $\mathbb{F}^n$
- Hamming distance of $x, y \in \mathbb{F}^n$: $d(x, y) = |\{i : x_i \neq y_i\}|$
- Minimum distance of $\mathcal{C}$:

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

- $x * y$: coordinate-wise product of x and y

Algebraic geometric code

- $X/\mathbb{F}$: algebraic curve (absolutely irreducible, smooth, projective) of genus g over finite field $\mathbb{F}$
- $\mathbb{F}(X)$: function field of $X/\mathbb{F}$
- $L(A) := \{f \in \mathbb{F}(X)\backslash\{0\} \ : \ (f) + A \geq 0 \ \} \cup \{0\}$
- $\Omega(A) := \{\omega \in \Omega(X)\backslash\{0\} \ : \ (\omega) \geq A \ \} \cup \{0\}$
- K : canonical divisor
- $P_1, \ldots, P_n$: n distinct rational points on X
- $D = P_1 + \cdots + P_n$
- G : divisor, $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$

Example

$(f) = 5P - 3Q$

- f has zeros of order 5 at P
- f has poles of order 3 at Q
- $\deg(\ (f)\ ) = 5 - 3 = 2$

If $A = 4P - 2Q$ then $L(A) := \{f \in \mathbb{F}(X)\backslash\{0\}\ :\ (f) + A \geq 0\ \} \cup \{0\}$ consists of all elements $f \in \mathbb{F}(X)$ such that

- f has zeros of order at least 2 at Q
- f may have a pole at P of order at most 4

Algebraic geometric code :

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

Algebraic geometric code $C_L(D, G)$:

$$C_L(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\} \subseteq \mathbb{F}^n$$

Algebraic geometric code $C_\Omega(D, G)$:

$$C_\Omega(D, G) := \{(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega) \mid \omega \in \Omega(G - D)\} \subseteq \mathbb{F}^n$$

Algebraic geometric code

- $C_L(D, G)$ and $C_\Omega(D, G)$ are dual to each other
- $C_L(D, G)^\perp = C_\Omega(D, G) = C_L(D, K + D - G)$
- For $a, b \in \mathbb{Z}$ and $P, Q \in X(\mathbb{F})$,

$$G = aP \quad : \quad \text{one-point code}$$
$$G = aP + bQ \quad : \quad \text{two-point code}$$

Order bounds of the minimum distance

- Hamming distance between two nonempty subsets $X, Y \subset \mathbb{F}^n$:

$$\text{minimum of } \{d(x,y) : x \in X, y \in Y\}$$

- For a proper subcode $\mathcal{C}' \subset \mathcal{C}$, the minimum distance of the collection of cosets $\mathcal{C}/\mathcal{C}'$ is

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

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

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

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

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

Hermitian curve $X/\mathbb{F}_{q^2} : y^q + y = x^{q+1}$

- Number of rational points : $q^3 + 1$
- Genus : $g = q(q-1)/2$
- P_∞ : the point at infinity of X
- P_0 : the point $(0, 0)$
- $K = (q-2)H$, where $H \sim (q+1)P_\infty \sim (q+1)P_0$

Example of one-point Hermitian code :

$X : y^4 + y = x^5$ over $\mathbb{F}_{16}$

Number of rational points $= 65$: $P_1, \ldots, P_{64}, P_\infty$

$g = 6$

Canonical divisor : $K = 10P_\infty$

For $f \in \mathbb{F}_{16}(X)\backslash\{0\}$,

$(f)_\infty$: the pole divisor of f

$(f)_0$: the zero divisor of f

$(f) = (f)_0 - (f)_\infty$

Weierstrass semigroup of the point P_∞:

$$H(P_\infty) = \{n \in \mathbb{N}_0 : \exists\ f \in \mathbb{F}_{16}(X) \ \text{ with } \ (f)_\infty = nP_\infty\}$$

$(x)_\infty = 4P_\infty$

$(y)_\infty = 5P_\infty$

Gap numbers : 1,2,3,6,7,11

$$H(P_\infty) = \langle 4, 5\rangle = \{0,\ 4,\ 5,\ 8,\ 9,\ 10,\ 12,\ 13,\ 14,\ 15,\ 16, \ldots\}$$

Question :

For $G = 17P_\infty$ and $D = P_1 + \cdots + P_{64}$,

$d(C_\Omega(D, G))= ?$

$$\mathcal{C}/\mathcal{C}_1 = C_\Omega(D, 17P_\infty)/C_\Omega(D, 18P_\infty) \longleftrightarrow \mathcal{D}_1/\mathcal{D} = C_L(D, 18P_\infty)/C_L(D, 17P_\infty)$$

If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

$$\begin{cases} a_i * b_j \in \mathcal{D} = C_L(D, 17P_\infty) & \text{for } i + j \leq w, \\ a_i * b_j \in \mathcal{D}_1 \backslash \mathcal{D} = C_L(D, 18P_\infty) \backslash C_L(D, 17P_\infty) & \text{for } i + j = w + 1, \end{cases}$$

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

- In other words, if there exist rational functions $f_1,\ f_2, \ldots, f_w$ and $g_1,\ g_2, \ldots, g_w$ such that

$$\begin{cases} f_i g_j \in L(17P_\infty) & \text{for } i+j \leq w, \\ f_i g_j \in L(18P_\infty) \backslash L(17P_\infty) & \text{for } i+j = w+1, \end{cases}$$

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

- $f_i g_j \in L(18P_\infty) \backslash L(17P_\infty)$ means that $f_i g_j$ has a pole only at P_∞ with exact pole order 18, that is, $(f_i g_j)_\infty = 18P_\infty$.

Hermitian curve

			f_1	f_2	f_3	f_4	f_5	f_6		f_7	f_8				f_9
			1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2
			0	4	5	8	9	10	12	13	14	15	16	17	18
g_1	1	0													18
g_2	x	4									18				
g_3	y	5								18					
g_4	x^2	8						18							
g_5	xy	9					18								
g_6	y^2	10				18									
	x^3	12													
g_7	x^2y	13			18										
g_8	xy^2	14		18											
	y^3	15													
	x^4	16													
	x^3y	17													
g_9	x^2y^2	18	18												

It follows from the figure that

$$\begin{cases} f_i g_j \in L(17P_\infty) & \text{for } i+j \leq 9, \\ f_i g_j \in L(18P_\infty) \backslash L(17P_\infty) & \text{for } i+j = 10. \end{cases}$$

Thus $d(\mathcal{C}/\mathcal{C}_1) \geq 9$.

✓				✓	✓			✓	✓	✓			✓	✓				✓
0	~~1~~	~~2~~	~~3~~	4	5	~~6~~	~~7~~	8	9	10	~~11~~	12	13	14	15	16	17	18
18	17	16	15	14	13	12	~~11~~	10	9	8	~~7~~	~~6~~	5	4	~~3~~	~~2~~	~~1~~	0

Applying the same method to $C_\Omega(D, 18P_\infty)/C_\Omega(D, 19P_\infty)$ we have

$$d(C_\Omega(D, 18P_\infty)/C_\Omega(D, 19P_\infty)) \geq 8.$$

≥ 9	$C_\Omega(D, 17P_\infty) \setminus C_\Omega(D, 18P_\infty)$
≥ 8	$C_\Omega(D, 18P_\infty) \setminus C_\Omega(D, 19P_\infty)$
≥ 9	$C_\Omega(D, 19P_\infty) \setminus C_\Omega(D, 20P_\infty)$
≥ 10	$C_\Omega(D, 20P_\infty) \setminus C_\Omega(D, 21P_\infty)$
	$\vdots$

By taking the minimum of the weights of the codewords, we have

$$d(C_\Omega(D, G)) \geq 8.$$

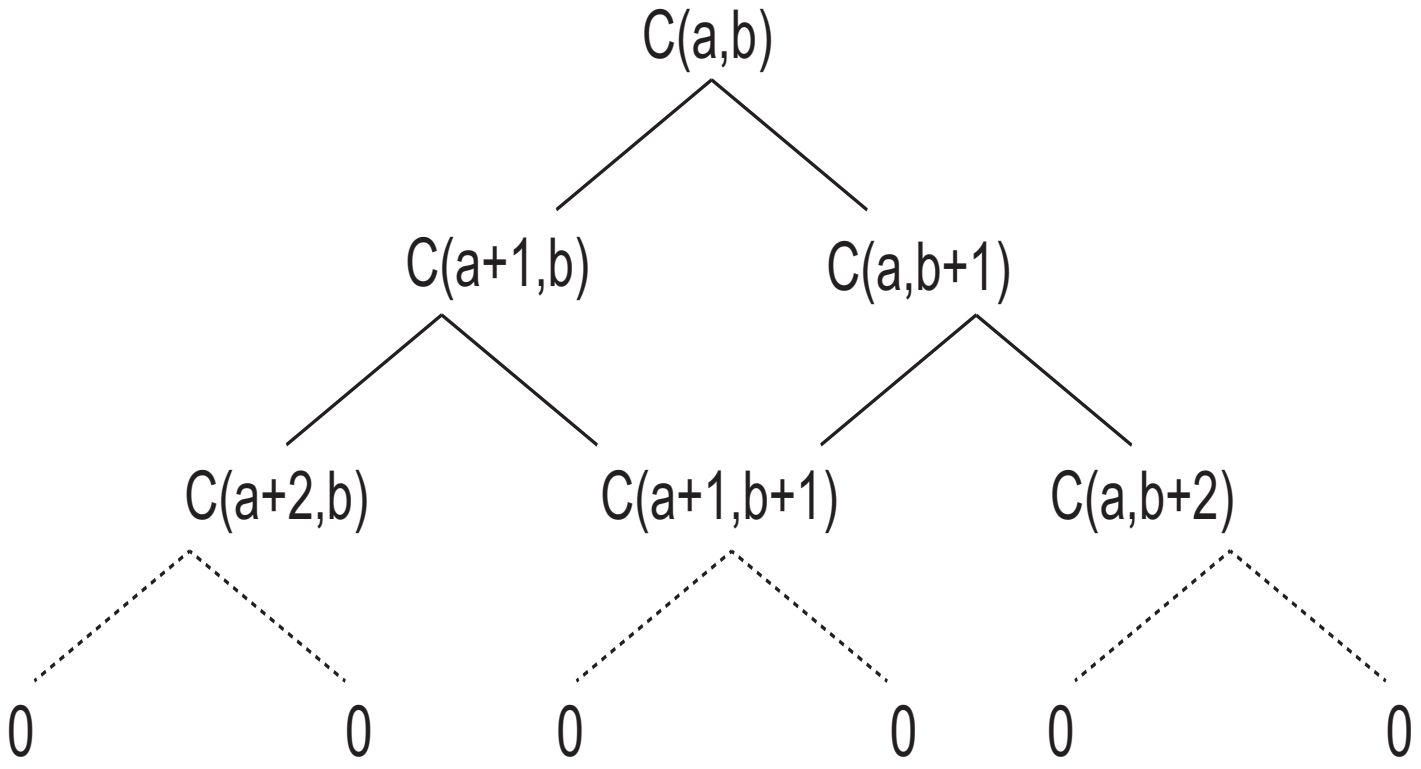
Notation : $C_\Omega(D, G) = C(a, b)$, where $G = aP_\infty + bP_0$

In two-point Hermian code with $q = 4$:

If $G = 20P_\infty + P_0$ then what is $d(C(20P_\infty + P_0))$?

$C(20P_\infty + P_0) \longrightarrow C(21P_\infty + P_0)$

$C(20P_\infty + P_0) \longrightarrow C(20P_\infty + 2P_0)$


C(a,b)
C(a+1,b)
C(a,b+1)
C(a+2,b)
C(a+1,b+1)
C(a,b+2)
0
0
0
0
0
0

Order bounds for the minimum distance

- For the Feng-Rao bound the filtration is determined by the choice of a point P and takes the form

$$C_\Omega(D, G) \supset C_\Omega(D, G + P) \supset C_\Omega(D, G + 2P) \supset \cdots \supset \{0\}$$

- Beelen allows the addition of different points at different steps in the filtration.

$$d(C_L(D,G)) = \min\{\deg A : 0 \leq A \leq D \mid L(G-D+A) \neq L(G-D)\}$$

$$= \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(-C)\}, \quad \text{for } C = D-G$$

$$d(C_\Omega(D,G)) = \min\{\deg A : 0 \leq A \leq D \mid \Omega(G-A) \neq \Omega(G)\}$$

$$= \min\{\deg A : 0 \leq A \leq D \mid L(K-G+A) \neq L(K-G)\}$$

$$= \min\{\deg A : 0 \leq A \leq D \mid L(A-C) \neq L(-C)\}, \quad \text{for } C = G-K$$

Notation

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

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

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

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

$P \notin D$ and $0 \leq A \leq D \Longrightarrow L(A) \neq L(A - P)$

This motivates the following definition :

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

Definition :

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

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

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

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

Theorem :

For a rational point $P \notin D$,

$$d(C_L(D, G)/C_L(D, G - P)) \geq \gamma_P(D - G).$$

$$d(C_\Omega(D, G)/C_\Omega(D, G + P)) \geq \gamma_P(G - K).$$

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

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

For $A \in \Delta_P(C)$, $0 \leq \deg A \leq \deg C + 2g - 1$.

Theorem (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 $A_w - A_1$

Sketch of Proof :

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

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

For a given divisor B,

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

Corollary :

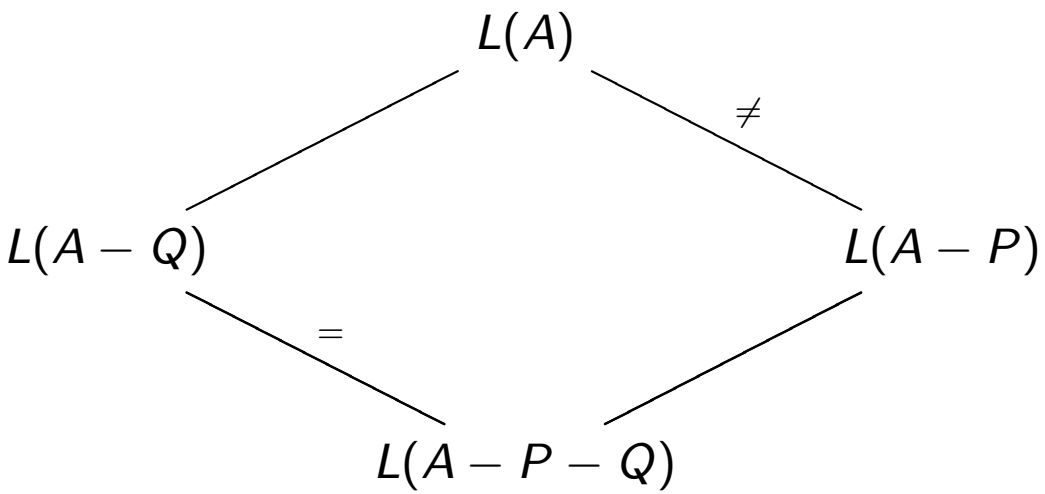
For any choice of divisor B,

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

Lemma :

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

Sketch of Proof :



Definition :

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

Theorem :

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

Definition :

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

Theorem :

For distinct points P and Q, and for a given divisor B, there exist functions $\sigma = \sigma_B$ and $\tau = \tau_B$ such that

$$D_B(P, Q) = \{B + \tau(j)P + jQ : j \in \mathbb{Z}\} = \{B + iP + \sigma(i)Q : i \in \mathbb{Z}\}.$$

$\sigma = \sigma_B$, $\tau = \tau_B$: mutual inverses and describe permutations of the integers. For m minimal such that $mP \sim mQ$, the functions σ, τ are determined by their images on a full set of representatives for $\mathbb{Z}/m\mathbb{Z}$. and $D_B(P, Q)$ consists of m distinct divisor classes.

Hermitian Curve over $\mathbb{F}_{q^2}$:

$$X/\mathbb{F}_{q^2} : y^q + y = x^{q+1}$$

- For $P, Q \in X(\mathbb{F}_{q^2})$, $mP \sim mQ$ for $m = q + 1$
- The m inequivalent divisor classes in $D_0(P, Q)$ with support in P and Q are represented by the divisors

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

- $D_0(P, Q) = \{d(qQ - P) + j(q + 1)(P - Q) : d = 0, 1, \ldots, q, j \in \mathbb{Z}\}$.

Suzuki Curve over $\mathbb{F}_q$:

$$y^q + y = x^{q_0}(x^q + x), \qquad q_0 = 2^n, \qquad q = 2q_0^2 = 2^{2n+1}$$

- Number of rational points : $q^2 + 1$
- Genus : $g = q_0(q-1)$
- P_∞ : the unique pole of x
- P_0 : the unique zero of both x and y
- Semigroup of Weierstrass nongaps at P_∞
  $= \langle q, q+q_0, q+2q_0, q+2q_0+1 = m \rangle$
- $K \sim 2(q_0-1)H$, where $H \sim (q+2q_0+1)P_\infty \sim (q+2q_0+1)P_0$

Theorem :

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

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

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 $|a| + |b| \le q_0$.

Suzuki curve over $\mathbb{F}_8$:

$X/\mathbb{F}_8 : y^8 + y = x^{10} + x^3$

$g = 14, N = 65,, m = 13$

The m inequivalent divisor classes in $D(P, Q)$ with support in P and Q are represented by the divisors

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

Theorem :

Let $A = kP + \ell Q$ and $C = iP + jQ$. Let

$$k^- + \ell = d_Q(\ell - j) + i + j, \qquad d^- = d_P(k^-) - d_Q(\ell - j).$$
$$k^+ + \ell = d_Q(\ell), \qquad d^+ = d_Q(\ell) - d_P(k^+ - i).$$

Then

$$(1)\ \ A \notin \Delta_P(C) \ \wedge\ A - Q \in \Delta_P(C) \ \Leftrightarrow\ k = k^- \ \wedge\ i + j > d^-.$$
$$(2)\ \ A \in \Delta_P(C) \ \wedge\ A - Q \notin \Delta_P(C) \ \Leftrightarrow\ k = k^+ \ \wedge\ i + j > d^+.$$

$kP + \ell Q \in \Gamma_P \Longleftrightarrow k + \ell \geq d_P(k)$
$kP + \ell Q \in \Gamma_Q \Longleftrightarrow k + \ell \geq d_Q(\ell)$
For $mP \sim mQ$, the functions d_P and d_Q are defined modulo m.
$d_p(k) = k + \sigma(k)$ and $d_Q(\ell) = \ell + \tau(\ell)$

Example :

For the Suzuki curve over $\mathbb{F}_{32}$, let $C = 55P + 31Q$. The full grid contains a unique maximal sequence of length 90 in row $\ell = -5$,

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

THANK YOU!