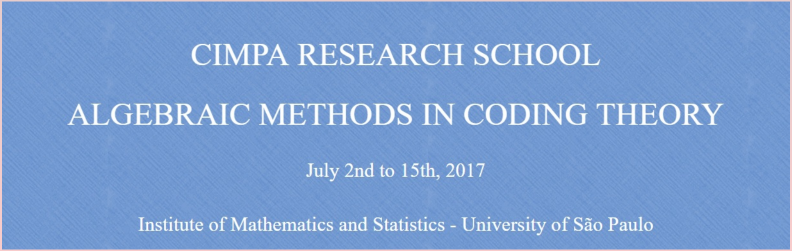
Weierstrass Semigroup over Kummer Extensions

Alonso Sepúlveda Castellanos[1]
with G. Tizziotti



[1]Universidade Federal de Uberlândia - FAPEMIG

Table of Contents

1. Weierstrass Semigroup
2. Weierstrass semigroup and Discrepancy
3. Weierstrass Semigroup $H(P_1, \ldots, P_m)$ for certain types of curves
4. Example

Weierstrass Semigroup

- Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible, algebraic curve of genus g over a finite field $\mathbb{F}_q$.

Weierstrass Semigroup

- Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible, algebraic curve of genus g over a finite field $\mathbb{F}_q$.
- $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions and $Div(\mathcal{X})$ be the set of divisors on $\mathcal{X}$

Weierstrass Semigroup

- Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible, algebraic curve of genus g over a finite field $\mathbb{F}_q$.
- $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions and $Div(\mathcal{X})$ be the set of divisors on $\mathcal{X}$
- For $f \in \mathbb{F}_q[\mathcal{X}]$, the divisor of f will be denoted by (f) and the divisor of poles of f by $(f)_\infty$. We denote $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

Weierstrass Semigroup

- Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible, algebraic curve of genus g over a finite field $\mathbb{F}_q$.
- $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions and $Div(\mathcal{X})$ be the set of divisors on $\mathcal{X}$
- For $f \in \mathbb{F}_q[\mathcal{X}]$, the divisor of f will be denoted by (f) and the divisor of poles of f by $(f)_\infty$. We denote $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- Let $P_1, \ldots, P_m$ be distinct rational points on $\mathcal{X}$. The set

$$H(P_1, \ldots, P_m) = \left\{ (a_1, \ldots, a_m) \in \mathbb{N}_0^m \; ; \exists f \in \mathbb{F}_q[\mathcal{X}] \text{ with } (f)_\infty = \sum_{i=1}^{m} a_i P_i \right\}$$

  is called the *Weierstrass semigroup* at the points $P_1, \ldots, P_m$.
- The set $G(P_1, \ldots, P_m) = \mathbb{N}_0^m \setminus H(P_1, \ldots, P_m)$ is called *gap set* of $P_1, \ldots, P_m$.

- The case $m = 1$, It was observed that to using the arithmetical structure of the Weierstrass semigroup we can improvements in the bounds for minimal distance in Algebraic Geometric One-point-Codes by Garcia, Kim, Lax.

- The case $m = 1$, It was observed that to using the arithmetical structure of the Weierstrass semigroup we can improvements in the bounds for minimal distance in Algebraic Geometric One-point-Codes by Garcia, Kim, Lax.
- The case $m = 2$, started to be studied by Kim and Homma, where several properties were presented. A similar result for Two-point-Codes was obtained by Homma and Kim using the notion of pure gaps that they introduced.

- The case $m = 1$, It was observed that to using the arithmetical structure of the Weierstrass semigroup we can improvements in the bounds for minimal distance in Algebraic Geometric One-point-Codes by Garcia, Kim, Lax.
- The case $m = 2$, started to be studied by Kim and Homma, where several properties were presented. A similar result for Two-point-Codes was obtained by Homma and Kim using the notion of pure gaps that they introduced.
- For $m > 2$, this semigroup has been studied for some specific curves as Hermitian and Norm-trace curves by Gretchen.
- With increasing interest in this semigroup, many results have been produced with several applications in coding theory by Torres and Carvalho, Garcia, Kim, Lax, Homma, Gretchen, and others.

- The case $m = 1$, It was observed that to using the arithmetical structure of the Weierstrass semigroup we can improvements in the bounds for minimal distance in Algebraic Geometric One-point-Codes by Garcia, Kim, Lax.
- The case $m = 2$, started to be studied by Kim and Homma, where several properties were presented. A similar result for Two-point-Codes was obtained by Homma and Kim using the notion of pure gaps that they introduced.
- For $m > 2$, this semigroup has been studied for some specific curves as Hermitian and Norm-trace curves by Gretchen.
- With increasing interest in this semigroup, many results have been produced with several applications in coding theory by Torres and Carvalho, Garcia, Kim, Lax, Homma, Gretchen, and others.

- For $\mathbf{u}_1, \ldots, \mathbf{u}_t \in \mathbb{N}_0^m$, where, for all k, $\mathbf{u}_k = (u_{k_1}, \ldots, u_{k_m})$, we define the *least upper bound* (*lub*) by:

$$lub\{\mathbf{u}_1, \ldots, \mathbf{u}_t\} = (\max\{u_{1_1}, \ldots, u_{t_1}\}, \ldots, \max\{u_{1_m}, \ldots, u_{t_m}\}) \in \mathbb{N}_0^m.$$

Proposition (Gretchen)

Suppose that $1 \leq t \leq m \leq q$ and $\mathbf{u}_1, \ldots, \mathbf{u}_t \in H(P_1, \ldots, P_m)$. Then $lub\{\mathbf{u}_1, \ldots, \mathbf{u}_t\} \in H(P_1, \ldots, P_m)$.

- For $\mathbf{u}_1, \ldots, \mathbf{u}_t \in \mathbb{N}_0^m$, where, for all k, $\mathbf{u}_k = (u_{k_1}, \ldots, u_{k_m})$, we define the *least upper bound* (*lub*) by:

$$lub\{\mathbf{u}_1, \ldots, \mathbf{u}_t\} = (\max\{u_{1_1}, \ldots, u_{t_1}\}, \ldots, \max\{u_{1_m}, \ldots, u_{t_m}\}) \in \mathbb{N}_0^m.$$

Proposition (Gretchen)

Suppose that $1 \leq t \leq m \leq q$ and $\mathbf{u}_1, \ldots, \mathbf{u}_t \in H(P_1, \ldots, P_m)$. Then $lub\{\mathbf{u}_1, \ldots, \mathbf{u}_t\} \in H(P_1, \ldots, P_m)$.

Definition: (Minimal Generating Set)

Let $\Gamma(P_1) = H(P_1)$ and, for $m \geq 2$, define

$$\Gamma(P_1, \ldots, P_m) := \{\mathbf{n} \in \mathbb{N}^m : \text{ for some } i, 1 \leq i \leq m, \mathbf{n} \text{ is minimal in } \nabla_i(\mathbf{n})\}.$$

where $\nabla_i(\mathbf{n}) := \{(p_1, \ldots, p_m) \in H(P_1, \ldots, P_m) \; ; \; p_i = n_i\}$.

$$H(P_1, P_2) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

Discrepancy

Duursma and Park introduced the concept of discrepancy as follows.

Discrepancy

Duursma and Park introduced the concept of discrepancy as follows.

Definition

A divisor $A \in Div(\mathcal{X})$ is called a *discrepancy* for two rational points P and Q on $\mathcal{X}$ if $\mathcal{L}(A) \neq \mathcal{L}(A-P) = \mathcal{L}(A-P-Q)$ and $\mathcal{L}(A) \neq \mathcal{L}(A-Q) = \mathcal{L}(A-P-Q)$.

Discrepancy

Duursma and Park introduced the concept of discrepancy as follows.

Definition

A divisor $A \in Div(\mathcal{X})$ is called a *discrepancy* for two rational points P and Q on $\mathcal{X}$ if $\mathcal{L}(A) \neq \mathcal{L}(A-P) = \mathcal{L}(A-P-Q)$ and $\mathcal{L}(A) \neq \mathcal{L}(A-Q) = \mathcal{L}(A-P-Q)$.

The next result relates the concept of discrepancy with the set $\Gamma(P_1, \ldots, P_m)$.

Discrepancy

Duursma and Park introduced the concept of discrepancy as follows.

Definition

A divisor $A \in Div(\mathcal{X})$ is called a *discrepancy* for two rational points P and Q on $\mathcal{X}$ if $\mathcal{L}(A) \neq \mathcal{L}(A-P) = \mathcal{L}(A-P-Q)$ and $\mathcal{L}(A) \neq \mathcal{L}(A-Q) = \mathcal{L}(A-P-Q)$.

The next result relates the concept of discrepancy with the set $\Gamma(P_1, \ldots, P_m)$.

Lemma

Let $\mathbf{n} = (n_1, \ldots, n_m) \in H(P_1, \ldots, P_m)$. Then $\mathbf{n} \in \Gamma(P_1, \ldots, P_m)$ if and only if the divisor $A = n_1 P_1 + \cdots + n_m P_m$ is a discrepancy with respect to P and Q for any two rational points $P, Q \in \{P_1, \ldots, P_m\}$.

Weierstrass Semigroup $H(P_1,\ldots,P_m)$

- Consider a curve $\mathcal{X}$ over $\mathbb{F}_q$ given by affine equation

$$f(y) = g(x)$$

Weierstrass Semigroup $H(P_1, \ldots, P_m)$

- Consider a curve $\mathcal{X}$ over $\mathbb{F}_q$ given by affine equation

$$f(y) = g(x)$$

- $\deg(f(y)) = a$ and $\deg(g(x)) = b$, with $gdc(a, b) = 1$, and genus $g = (a-1)(b-1)/2$.

Weierstrass Semigroup $H(P_1,\ldots,P_m)$

- Consider a curve $\mathcal{X}$ over $\mathbb{F}_q$ given by affine equation

$$f(y) = g(x)$$

- $\deg(f(y)) = a$ and $\deg(g(x)) = b$, with $gdc(a,b) = 1$, and genus $g = (a-1)(b-1)/2$.
- Let $P_1, P_2, \ldots, P_{a+1}$ be $a+1$ distinct rational points such that

$$aP_1 \sim P_2 + \cdots + P_{a+1}\,, \tag{1}$$

and

$$bP_i \sim bP_j, \text{ for all } i,j \in \{1,2,\ldots,a+1\}, \tag{2}$$

- Note that $H(P_1) = \langle a, b\rangle$.

- Let $1 \leq m \leq a+1 \leq q$. For

$$t + \sum_{j=2}^{m} s_j = a + 1 - m\,, \qquad 0 < ia < tb, \qquad s_j \geq 0\,. \qquad (3)$$

- Let $1 \leq m \leq a+1 \leq q$. For

$$t + \sum_{j=2}^{m} s_j = a + 1 - m \,, \qquad 0 < ia < tb, \qquad s_j \geq 0 \,. \qquad (3)$$

- Equivalence of the divisors and the before conditions, we have

$$(tb - ia)P_1 + (sb + i)P_2 + i(P_3 + \cdots + P_m) \sim \sum_{j=m+1}^{a+1} (b - i)P_j \quad (4)$$

- Let $1 \leq m \leq a+1 \leq q$. For

$$t + \sum_{j=2}^{m} s_j = a + 1 - m \,, \qquad 0 < ia < tb, \qquad s_j \geq 0 \,. \qquad (3)$$

- Equivalence of the divisors and the before conditions, we have

$$(tb - ia)P_1 + (sb + i)P_2 + i(P_3 + \cdots + P_m) \sim \sum_{j=m+1}^{a+1} (b - i)P_j \quad (4)$$

Proposition

Let a, b, t, i, $s_2, \ldots, s_m$ be as above. Then, the divisor $(tb - ia)P_1 + \sum_{j=2}^{m}(s_j b + i)P_j$ is a discrepancy with respect to P and Q for any two distinct points $P, Q \in \{P_1, \ldots, P_m\}$.

Main Theorem

Let $\mathcal{X}$ and $P_1, P_2, \ldots, P_{a+1}$ be as above. For $2 \leq m \leq a+1$, let

$$S_m = \left\{ (tb - ia, s_2 b + i, \ldots, s_m b + i);\ t + \sum_{j=2}^{m} s_j = a + 1 - m,\ 0 < ia < tb,\ s_j \geq 0 \right\}$$

Then, $\Gamma(P_1, \ldots, P_m) = S_m$.

Kummer Extension

- Let a Kummer extensions over $\mathbb{F}_q$

$$y^b = g(x) = \prod_{i=1}^{a}(x - \alpha_i)$$

$\gcd(a, b) = 1$, genus $(b-1)(a-1)/2$.

1. $(x - \alpha_i) = bP_i - bP_1$ for every i, $2 \leq i \leq a+1$,
2. $(y) = P_2 + \cdots + P_{a+1} - aP_1$,

- For $a = 5$ and $b = 7$ we have that

$$\begin{aligned}
\Gamma(P_1, P_2) &= \{(23,1),(18,2),(13,3),(8,4),(3,5),(16,8),\\
&\quad (11,9),(6,10),(1,11),(9,15),(4,16),(2,22)\}\ .\\
\Gamma(P_1, P_2, P_3) &= \{(2,8,8),(2,15,1),(2,0,15),(9,8,1),(9,1,8),\\
&\quad (4,9,2),(4,2,9),(16,1,1),(11,2,2),(6,3,3),(1,4,4)\}\ .\\
\Gamma(P_1, P_2, P_3, P_4) &= \{(2,8,1,1),(2,1,8,1),(2,1,1,8),(9,1,1,1),(4,2,2,2)\}\ .\\
\Gamma(P_1, P_2, P_3, P_4, P_5) &= \{(2,1,1,1,1)\}\ .
\end{aligned}$$

Other Applications

We apply the same idea in:

The *GK curve* over $\mathbb{F}_{q^2}$ is the curve of $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$ with affine equations

$$\begin{cases} Z^{n^2-n+1} = Yh(X) \\ X^n + X = Y^{n+1} \end{cases}, \tag{5}$$

where $h(X) = \sum_{i=0}^{n} (-1)^{i+1} X^{i(n-1)}$.

Other Applications

We apply the same idea in:
The *GK* curve over $\mathbb{F}_{q^2}$ is the curve of $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$ with affine equations

$$\begin{cases} Z^{n^2-n+1} = Yh(X) \\ X^n + X = Y^{n+1} \end{cases}, \qquad (5)$$

where $h(X) = \sum_{i=0}^{n} (-1)^{i+1} X^{i(n-1)}$.

$$H(P_\infty) = \langle n^3 - n^2 + n, n^3, n^3 + 1 \rangle$$

Bibliography

I. Duursma and S. Park, *Delta sets for divisors supported in two points*, Finite Fields and Their Applications, 18 (5), 2012, 865-885.

A.S. Castellanos and G. Tizziotti, *On Weierstrass semigroup at m points on curves of the type $f(y) = g(x)$*. To appear in Journal Pure on Applied Algebra (2017).

Muchas Gracias !!!

Muito Obrigado !!!

God Bless You