Weierstrass semigroup and Automorphism group of the curves $\mathcal{X}_{n,r}$

Guilherme Chaud Tizziotti
Based on joint work with H. Borges and A. Sepúlveda

FAMAT - Universidade Federal de Uberlândia

XXICLA - Buenos Aires

Motivation

- Applications on Goppa codes.

Weierstrass semigroup

For a rational point $P \in \mathcal{X}$, the *Weierstrass semigroup* of $\mathcal{X}$ at P is defined by

$$H(P) := \{n \in \mathbb{N}_0 : \exists f \in \mathbb{F}_q(\mathcal{X}) \text{ with } div_\infty(f) = nP\},$$

and the set $G(P) = \mathbb{N}_0 \setminus H(P)$ is called *Weierstrass gap set* of P.

• $G(P) = \{\alpha_1, \ldots, \alpha_g\}$ and $1 = \alpha_1 < \cdots < \alpha_g \leq 2g - 1$.

• The semigroup $H(P)$ is called symmetric if $\alpha_g = 2g - 1$.

• The curve $\mathcal{X}$ is called *Castle curve* if $H(P) = \{0 = m_1 < m_2 < \cdots\}$ is symmetric and $\#\mathcal{X}(\mathbb{F}_q) = m_2 q + 1$.

Definition

Let $(a_1, \ldots, a_m)$ be a sequence of positive integers whose greatest common divisor is 1. Set $d_0 = 0$, and define $d_i := gcd(a_1, \ldots, a_i)$ and $A_i := \{\frac{a_1}{d_i}, \ldots, \frac{a_i}{d_i}\}$ for $i = 1, \ldots, m$. If $\frac{a_i}{d_i}$ lies in the semigroup generated by A_i, for $i = 2, \ldots, m$, then the sequence $(a_1, \ldots, a_m)$ is called *telescopic*. A semigroup is called telescopic if it is generated by a telescopic sequence.

For a semigroup S, the number of gaps and the largest gap of S will be denoted by $g(S)$ and $l_g(S)$, respectively. The following result will be a significant factor in determining the semigroup $H(P_\infty)$ of the curves $\mathcal{X}_{n,r}$.

Lemma (C. Kirfel and R. Pellikaan)

If S_m is the semigroup generated by a telescopic sequence $(a_1, \ldots, a_m)$, then

- $l_g(S_m) = d_{m-1} l_g(S_{m-1}) + (d_{m-1} - 1)a_m = \sum_{i=1}^{m} (\frac{d_{i-1}}{d_i} - 1)a_i$
- $g(S_m) = d_{m-1} g(S_{m-1}) + (d_{m-1} - 1)(a_m - 1)/2 = (l_g(S_m) + 1)/2,$

where $d_0 = 0$. In particular, telescopic semigroups are symmetric.

Let $\mathrm{Aut}(\mathcal{X})$ be the automorphism group of $\mathcal{X}$ and $\mathbb{G} \subseteq \mathrm{Aut}(\mathcal{X})$ be a finite subgroup. For a rational point $P \in \mathcal{X}$, the stabilizer of P in $\mathbb{G}$, denoted by $\mathbb{G}_P$, is the subgroup of $\mathbb{G}$ consisting of all elements fixing P. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $\mathbb{G}_P^{(i)}$ and defined by

$$\mathbb{G}_P^{(i)} = \{\alpha \in \mathbb{G}_P : \; v_P(\alpha(t) - t) \geq i + 1\} ,$$

where t is a local parameter at P. Here $\mathbb{G}_P^{(0)} = \mathbb{G}_P$ and $\mathbb{G}_P^{(1)}$ is the unique Sylow p-subgroup of $\mathbb{G}_P$. Moreover, $\mathbb{G}_P^{(1)}$ has a cyclic complement H in $\mathbb{G}_P$, i.e.,

$$\mathbb{G}_P = \mathbb{G}_P^{(1)} \rtimes H \tag{1}$$

where H is a cyclic group of order coprime to p.

Theorem (M. Giulietti and G. Korchmáros)

Let $\mathcal{X}$ be a curve of genus $g \geq 2$ over $\mathbb{F}_q$, where q is a prime power, and let $\mathbb{G}$ be an automorphism group of $\mathcal{X}$ such that $\mathcal{X}$ has a $\mathbb{F}_q$-rational point P satisfying the condition $|\mathbb{G}_P^{(1)}| > 2g + 1$. Then one of the following cases occurs:

1) $\mathbb{G} = \mathbb{G}_P$.

2) *$\mathcal{X}$ is birationally equivalent to one of the following curves:*

(i) the Hermitian curve $\mathbf{v}(Y^n + Y - X^{n+1})$ with $n = q^t \geq 2$ and $g = \frac{1}{2}(n^2 - n)$

(ii) the DLS curve (the Deligne-Lusztig curve arising from the Suzuki group) $\mathbf{v}(X^{n_0}(X^n + X) - (Y^n + Y))$ with $p = 2$, $q = n$, $n_0 = 2^r$, $r \geq 1$, $n = 2n_0^2$ and $g = n_0(n-1)$

(iii) the DLR curve (the Deligne-Lusztig curve arising from the Ree group) $\mathbf{v}(Y^{n^2} - (1 + (X^n - X)^{n-1})Y^n + (X^n - X)^{n-1}Y - X^n(X^n - X)^{n+3n_0}$ with $p = 3$, $q = n$, $n_0 = 3^r$, $n = 3n_0^2$ and $g = \frac{3}{2}n_0(n-1)(n + n_0 + 1)$.

Where $\mathbf{v}(F(X, Y))$ is the plane projective curve with affine equation $F(X, Y) = 0$.

• Family of curves introduced by H. Borges and R. Conceição - paper "Minimal value set polynomials and a generalization of the Hermitian curve", to appear.

• An example is the following curve over $\mathbb{F}_{q^n}$:

$$\mathcal{H}: \quad \mathrm{T_n}(y) = \mathrm{T_n}(x^{q^r+1}) \qquad \pmod{x^{q^n} - x}$$

where, for a symbol z,

$$\mathrm{T_n}(z) := z^{q^{n-1}} + z^{q^{n-2}} + \ldots + z\,,$$

and $r = r(n) \geq n/2$ is the smallest positive integer such that $\gcd(n, r) = 1$.

• We consider a set of curves $\mathcal{X}_{n,r}$ (which includes the curve $\mathcal{H}$).

The curves $\mathcal{X}_{n,r}$

Fix integers $n \geq 2$ and $r \in \{\lceil \frac{n}{2} \rceil, \ldots, n-1\}$, with $\gcd(n,r) = 1$. Consider the polynomial

$$f_r(x) := T_n\left(x^{1+q^r}\right) \mod (x^{q^n} - x), \tag{2}$$

where $T_n(x) = x + x^q + \ldots + x^{q^{n-1}}$, and define the curve $\mathcal{X}_{n,r}$ by affine equation

$$T_n(y) = f_r(x). \tag{3}$$

It is easy to check that the polynomial f_r satisfies $f_r(a) \in \mathbb{F}_q$ for all $a \in \mathbb{F}_{q^n}$, and that if $n > 2$, then $f_r(x)$ can written as

$$f_r(x) = \sum_{i=0}^{n-r-1} (x^{1+q^r})^{q^i} + \sum_{i=0}^{r-1} (x^{1+q^{n-r}})^{q^i}. \tag{4}$$

Theorem (H. Borges and R. Conceição)

The following holds:
1) The curve $\mathcal{X}_{n,r}$ has degree $d = q^{n-1} + q^{r-1}$, genus $g = q^r(q^{n-1} - 1)/2$ and $N = q^{2n-1} + 1$ $\mathbb{F}_{q^n}$-rational points.
2) In the projective closure of $\mathcal{X}_{n,r}$, the point $P_\infty = (0 : 1 : 0)$ is the only singular point.

The Weierstrass semigroup $H(P_\infty)$

- $P_\infty = (0:1:0) \in \mathcal{X}_{n,r}$

Lemma

Let $z_0 := y^{q^{n-r}} - x^{q^{n-r}+1}$ *and* $z := z_0^{q^{2r-n}} - x^{q^r+1} + x^{q^{2r-n}-1}y$. *For the functions* $x, y, z \in F_{n,r}$ *we have that*

1) $div_\infty(x) = q^{n-1}P_\infty$
2) $div_\infty(y) = (q^{n-1} + q^{r-1})P_\infty$
3) $div_\infty(z) = (q^{2r-1} + q^{n-r-1})P_\infty$.

Proposition

Let α and β be positive integers such that $(n-r)\alpha - \beta n = 1$, and consider the following functions in $F_{n,r}$:

$$w := \sum_{i=0}^{\alpha-1} {z_0}^{q^{(n-r)i}} - \sum_{i=1}^{\beta} \left(x^{q^{n-r}+1} + x^{q^n+q^{n-r}}\right)^{q^{n(\beta-i)+1}} \tag{5}$$

and

$$t := x^{q^{2r-n+1}-q} w + z^q + x^{q^{2r-n+1}-q^{2r-n}-q+1} z. \tag{6}$$

Then $div_\infty(w) = (q^n + q^{n-r})P_\infty$, and
$div_\infty(t) = (q^{2r} - q^n + q^r + 1)P_\infty$.

Proposition

The curve $\mathcal{X}_{n,r}$ has a plane model given by

$$y^{q^{n-1}} + \cdots + y^q + y = x^{q^{n-r}+1} - x^{q^n+q^{n-r}}. \qquad (7)$$

Theorem

Let $H(P_\infty)$ be the Weierstrass semigroup at P_∞. Then

$$H(P_\infty) = \langle q^{n-1}, q^{n-1}+q^{r-1}, q^n+q^{n-r}, q^{2r-1}+q^{n-r-1}, q^{2r}-q^n+q^r+1\rangle$$

Moreover, $H(P_\infty)$ is a telescopic semigroup and, in particular, symmetric.

Corollary

The curves $\mathcal{X}_{n,r}$ are Castle curves.

Automorphism group

Let us consider the q^{2n-1} affine points $P := (\delta, \mu) \in \mathcal{X}_{n,r}(\mathbb{F}_{q^n})$ and all the elements $\gamma \in \mathbb{F}_{q^n}$ such that

$$\begin{cases} \gamma^{q-1} = 1 & \text{if } n \text{ is odd} \\ \gamma^{q^2-1} = 1 & \text{if } n \text{ is even} \end{cases} .$$

Automorphism group

Using that $\mathcal{X}_{n,r}$ is given by $T_n(y) = f_r(x)$, where $f_r(x) = \sum_{i=0}^{n-r-1}(x^{1+q^r})^{q^i} + \sum_{i=0}^{r-1}(x^{1+q^{n-r}})^{q^i}$, one can easily check that the set G of maps on $F_{n,r}$, given by

$$\alpha_{\gamma,P} : (x, y) \longrightarrow (\gamma x + \delta, \gamma^{1+q} y + (\delta^{q^{n-r}} + \delta^{q^r})\gamma x + \mu), \quad (8)$$

is a subgroup of $\mathrm{Aut}(\mathcal{X}_{n,r})$, whose elements fix P_∞, i.e., $G \subseteq \mathrm{Aut}_{P_\infty}(\mathcal{X}_{n,r})$. Based on the above definition, note that the following subgroups of G:
$N = \{\alpha_{\gamma,P} \in G : \gamma = 1\}$ and
$H = \{\alpha_{\gamma,P} \in G : P = (0,0)\} \cong \mathbb{F}^*_{q^{2-(n \mod 2)}}$
have order q^{2n-1} and $q^{2-(n \mod 2)} - 1$, repectively.

Theorem

The group G is the full group of automorphisms of $\mathcal{X}_{n,r}$. Moreover, $N = Aut_{P_\infty}(\mathcal{X}_{n,r})^{(1)}$ and

$$G = Aut_{P_\infty}(\mathcal{X}_{n,r}) = N \rtimes H.$$

Lemma

$Aut_{P_\infty}(\mathcal{X}_{n,r}) = G.$

Lemma

$Aut_{P_\infty}(\mathcal{X}_{n,r})^{(1)} = N$ *and* $Aut_{P_\infty}(\mathcal{X}_{n,r}) = N \rtimes H.$

Obrigado!