A Class of Artin-Schreier Curves With Many Automorphisms

Renate Scheidler

UNIVERSITY OF CALGARY

Joint work with **Irene Bouw**, **Wei Ho**, **Beth Malmskog**,
Padmavathi Srinivasan and **Christelle Vincent**

In *Directions in Number Theory - Proceedings of the 2014 WIN3 Workshop*, AWM Series, vol. 3, Springer 2016, 87-124
Thanks to *WIN3* — 3rd *Women in Numbers*, BIRS, April 20-24, 2014

Alberta Number Theory Days
March 19, 2017
Banff International Research Station

Artin-Schreier Curves

Let p be a prime.

Artin-Schreier Curves

Let p be a prime.

Artin-Schreier curve over $\mathbb{F} \supset \mathbb{F}_p$:

$$C : y^p - y = F(x) \quad \text{with } F(x) \in \mathbb{F}(x) \text{ non-constant} .$$

Artin-Schreier Curves

Let p be a prime.

Artin-Schreier curve over $\mathbb{F} \supset \mathbb{F}_p$:

$$C : y^p - y = F(x) \quad \text{with } F(x) \in \mathbb{F}(x) \text{ non-constant} .$$

Standard examples: elliptic and hyperelliptic curves for $p = 2$.

Artin-Schreier Curves

Let p be a prime.

Artin-Schreier curve over $\mathbb{F} \supset \mathbb{F}_p$:

$$C : y^p - y = F(x) \quad \text{with } F(x) \in \mathbb{F}(x) \text{ non-constant} .$$

Standard examples: elliptic and hyperelliptic curves for $p = 2$.

The extension $\mathbb{F}(x, y)/\mathbb{F}(x)$ is cyclic Galois of degree p with Galois group generated by the $\mathbb{F}(x)$-automorphism

$$y \longrightarrow y + 1 .$$

Artin-Schreier Curves

Let p be a prime.

Artin-Schreier curve over $\mathbb{F} \supset \mathbb{F}_p$:

$$C : y^p - y = F(x) \quad \text{with } F(x) \in \mathbb{F}(x) \text{ non-constant} .$$

Standard examples: elliptic and hyperelliptic curves for $p = 2$.

The extension $\mathbb{F}(x, y)/\mathbb{F}(x)$ is cyclic Galois of degree p with Galois group generated by the $\mathbb{F}(x)$-automorphism

$$y \longrightarrow y + 1 .$$

So Artin-Schreier extensions are the wild analogues of (tame cyclic) Kummer extensions $\mathbb{F}(x, y)/\mathbb{F}(x)$ where $\mu_n \subset \mathbb{F}$ and

$$y^n = F(x) \quad \text{with} \quad p \nmid n .$$

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Equivalently, all monomials appearing in $R(x)$ are of the form x^{p^i}.

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Equivalently, all monomials appearing in $R(x)$ are of the form x^{p^i}.

Most prominent example: **Hermitian curve** $y^p - y = x^{p+1}$ $(R(x) = x^p)$.

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Equivalently, all monomials appearing in $R(x)$ are of the form x^{p^i}.

Most prominent example: **Hermitian curve** $y^p - y = x^{p+1}$ $(R(x) = x^p)$.

Another surprisingly important case: $y^p - y = mx^2$ $(R(x) = mx)$.

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Equivalently, all monomials appearing in $R(x)$ are of the form x^{p^i}.

Most prominent example: **Hermitian curve** $y^p - y = x^{p+1}$ $(R(x) = x^p)$.

Another surprisingly important case: $y^p - y = mx^2$ $(R(x) = mx)$.

C_R has one point at infinity, denoted ∞.

Our Main Protagonist

For p odd, we consider the family of Artin-Schreier curves

$$C_R : y^p - y = xR(x)$$

where $R(x)$ is an **additive** polynomial, i.e. $R(x+z) = R(x) + R(z)$.

Equivalently, all monomials appearing in $R(x)$ are of the form x^{p^i}.

Most prominent example: **Hermitian curve** $y^p - y = x^{p+1}$ $(R(x) = x^p)$.

Another surprisingly important case: $y^p - y = mx^2$ $(R(x) = mx)$.

C_R has one point at infinity, denoted ∞.

The genus of C_R is $g(C_R) = \dfrac{\deg(R)(p-1)}{2}$.

Why Study C_R?

Why are these curves of interest?

Why Study C_R?

Why are these curves of interest?

- Connection to weight enumerators of subcodes of Reed-Muller codes
  (Case $p = 2$ in van der Geer & van der Vlugt, *Comp. Math.* **84**, 1992)

Why Study C_R?

Why are these curves of interest?

- Connection to weight enumerators of subcodes of Reed-Muller codes
  (Case $p = 2$ in van der Geer & van der Vlugt, *Comp. Math.* **84**, 1992)

- Maximal over suitable fields and hence a good source for algebraic geometry codes.

Why Study C_R?

Why are these curves of interest?

- Connection to weight enumerators of subcodes of Reed-Muller codes
  (Case $p = 2$ in van der Geer & van der Vlugt, *Comp. Math.* **84**, 1992)
- Maximal over suitable fields and hence a good source for algebraic geometry codes.
- Other cool geometric and algebraic properties:
  - Very large and interesting automorphism group.
  - Supersingular family (Jacobian is isogenous to a product of supersingular elliptic curves).

Outline

For odd p, this is our protagonist's story:

1. Point counts
2. Zeta function (almost)
3. Automorphism group, including fields of definition
4. Zeta function
5. Examples

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Let

- W its set of roots;

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Let

- W its set of roots;
- $\mathbb{F}_q$ its splitting field.

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Let

- W its set of roots;
- $\mathbb{F}_q$ its splitting field.

Remarks:

- W is the kernel of the bilinear form $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(y) + yR(x))$.

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Let

- W its set of roots;
- $\mathbb{F}_q$ its splitting field.

Remarks:

- W is the kernel of the bilinear form $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(y) + yR(x))$.
- W is an $\mathbb{F}_p$-vector space of dimension $2h$.

Two Magic Structures

Consider $C_R : y^p - y = xR(x)$ with $R(x)$ additive, and write

$$R(x) = \sum_{i=0}^{h} a_i x^{p^i} \ .$$

Define an additive polynomial associated to $R(x)$:

$$E(x) = R(x)^{p^h} + \sum_{i=0}^{h} (a_i x)^{p^{h-i}} \ .$$

Let

- W its set of roots;
- $\mathbb{F}_q$ its splitting field.

Remarks:

- W is the kernel of the bilinear form $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xR(y) + yR(x))$.
- W is an $\mathbb{F}_p$-vector space of dimension $2h$.
- We have a very explicit description of the elements of W (later).

UNIVERSITY OF CALGARY

Proposition

Let

$$C_R : y^p - y = xR(x)$$

with $R(x) \in \mathbb{F}_q[x]$ *additive of degree* p^h. *Then for any extension* $\mathbb{F}_{p^n}$ *of* $\mathbb{F}_q$, *the number of* $\mathbb{F}_{p^n}$*-rational points is*

$$\#C_R(\mathbb{F}_{p^n}) = \begin{cases} p^n + 1 & \text{for } n \text{ odd,} \\ p^n + 1 \pm (p-1)p^{h+n/2} & \text{for } n \text{ even.} \end{cases}$$

Point Counts

Proposition

Let

$$C_R : y^p - y = xR(x)$$

with $R(x) \in \mathbb{F}_q[x]$ *additive of degree* p^h*. Then for any extension* $\mathbb{F}_{p^n}$ *of* $\mathbb{F}_q$*, the number of* $\mathbb{F}_{p^n}$*-rational points is*

$$\#C_R(\mathbb{F}_{p^n}) = \begin{cases} p^n + 1 & \text{for } n \text{ odd,} \\ p^n + 1 \pm (p-1)p^{h+n/2} & \text{for } n \text{ even.} \end{cases}$$

Corollary

C_R *is either maximal* $(+)$ *or minimal* $(-)$ *for* n *even.*

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Now count:

- N_n elements $\overline{x} \in \mathbb{F}_{p^n}/W$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Now count:

- N_n elements $\overline{x} \in \mathbb{F}_{p^n}/W$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each yields $|W| = p^{2h}$ values $x \in F_{p^n}$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Now count:

- N_n elements $\overline{x} \in \mathbb{F}_{p^n}/W$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each yields $|W| = p^{2h}$ values $x \in F_{p^n}$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each of those yields p values $y \in \mathbb{F}_{p^n}$ with $y^p - y = xR(x)$.

Idea of the Proof

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Now count:

- N_n elements $\overline{x} \in \mathbb{F}_{p^n}/W$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each yields $|W| = p^{2h}$ values $x \in F_{p^n}$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each of those yields p values $y \in \mathbb{F}_{p^n}$ with $y^p - y = xR(x)$.
- One point at infinity ∞.

Idea of the Proof

UNIVERSITY OF CALGARY

$$(x, y) \in \#C_R(\mathbb{F}_{p^n}) \iff \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0 \ .$$

The zero locus of the quadratic form

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) \ ,$$

projected down onto $\mathbb{F}_{p^n}/W$, is a smooth quadric whose cardinality N_n is known (Joly, *Enseignement Math.* **19**, 1973).

Now count:

- N_n elements $\overline{x} \in \mathbb{F}_{p^n}/W$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each yields $|W| = p^{2h}$ values $x \in F_{p^n}$ with $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xR(x)) = 0$.
- Each of those yields p values $y \in \mathbb{F}_{p^n}$ with $y^p - y = xR(x)$.
- One point at infinity ∞.

Total count: $\#C_R(\mathbb{F}_{p^n}) = p^{2h+1}N_n + 1$.

Zeta Function

The *zeta function* of a curve C of genus g over a finite field $\mathbb{F}_q$ is

$$Z_C(t) = \exp\left(\sum_{n \in \mathbb{N}} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right) .$$

Zeta Function

The *zeta function* of a curve C of genus g over a finite field $\mathbb{F}_q$ is

$$Z_C(t) = \exp\left(\sum_{n\in\mathbb{N}} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right) .$$

Then the L-polynomial of C over $\mathbb{F}_{q^n}$ is $L_{C,q^n}(t) = (1-t)(1-q^n t)Z_C(t)$.

Zeta Function

The *zeta function* of a curve C of genus g over a finite field $\mathbb{F}_q$ is

$$Z_C(t) = \exp\left(\sum_{n \in \mathbb{N}} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right) .$$

Then the L-polynomial of C over $\mathbb{F}_{q^n}$ is $L_{C,q^n}(t) = (1-t)(1-q^n t)Z_C(t)$.

It is a polynomial of degree $2g$ with integer coefficients.

Zeta Function

The *zeta function* of a curve C of genus g over a finite field $\mathbb{F}_q$ is

$$Z_C(t) = \exp\left(\sum_{n \in \mathbb{N}} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right) .$$

Then the L-polynomial of C over $\mathbb{F}_{q^n}$ is $L_{C,q^n}(t) = (1-t)(1-q^n t) Z_C(t)$.

It is a polynomial of degree $2g$ with integer coefficients.

If we write $L_{C,q^n}(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$, then $\sum_{i=1}^{2g} \alpha_i = \#C(\mathbb{F}_{q^n}) - q^n - 1$.

The *zeta function* of a curve C of genus g over a finite field $\mathbb{F}_q$ is

$$Z_C(t) = \exp\left(\sum_{n\in\mathbb{N}} \frac{\#C(\mathbb{F}_{q^n})}{n} t^n\right).$$

Then the L-polynomial of C over $\mathbb{F}_{q^n}$ is $L_{C,q^n}(t) = (1-t)(1-q^n t)Z_C(t)$.

It is a polynomial of degree $2g$ with integer coefficients.

If we write $L_{C,q^n}(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, then $\sum_{i=1}^{2g} \alpha_i = \#C(\mathbb{F}_{q^n}) - q^n - 1$.

Applying this to C_R, we obtain for all i:

$$\alpha_i = \begin{cases} \pm q^n & \text{when } n \text{ is odd,} \\ \pm q^{n/2} & \text{when } n \text{ is even.} \end{cases}$$

L-Polynomial of C_R (Almost)

Proposition

Let $C_R : y^p - y = xR(x)$ with $R(x) \in \mathbb{F}_q[x]$ additive of degree p^h. Then for any extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_q$, we have

$$L_{C_R,p^n}(t) = \begin{cases} (1 \pm p^n t^2)^g & \text{when } n \text{ is odd,} \\ (1 \pm p^{n/2} t)^{2g} & \text{when } n \text{ is even.} \end{cases}$$

L-Polynomial of C_R (Almost)

Proposition

Let $C_R : y^p - y = xR(x)$ with $R(x) \in \mathbb{F}_q[x]$ additive of degree p^h. Then for any extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_q$, we have

$$L_{C_R,p^n}(t) = \begin{cases} (1 \pm p^n t^2)^g & \text{when } n \text{ is odd,} \\ (1 \pm p^{n/2} t)^{2g} & \text{when } n \text{ is even.} \end{cases}$$

Since all the slopes of the Newton polygon of the L-polynomial are equal to $1/2$, we obtain:

Corollary

The Jacobian of C_R is isogenous to a product of supersingular elliptic curves. So C_R is supersingular.

L-Polynomial of C_R (Almost)

Proposition

Let $C_R : y^p - y = xR(x)$ with $R(x) \in \mathbb{F}_q[x]$ additive of degree p^h. Then for any extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_q$, we have

$$L_{C_R,p^n}(t) = \begin{cases} (1 \pm p^n t^2)^g & \text{when } n \text{ is odd,} \\ (1 \pm p^{n/2} t)^{2g} & \text{when } n \text{ is even.} \end{cases}$$

Since all the slopes of the Newton polygon of the L-polynomial are equal to $1/2$, we obtain:

Corollary

The Jacobian of C_R is isogenous to a product of supersingular elliptic curves. So C_R is supersingular.

Unfortunately, the "$\pm$" is surprisingly hard to resolve.

Automorphism Group of C_R

Follows Lehr & Matignon, *Compositio Math.* **141**, 2005.

Automorphism Group of C_R

Follows Lehr & Matignon, *Compositio Math.* **141**, 2005.

Proposition

Assume without loss of generality that $R(x)$ is monic.

- *If $R(x) = x$, then $\mathrm{Aut}(C_R) \cong SL_2(\mathbb{F}_p)$.*
- *If $R(x) = x^p$, then $\mathrm{Aut}(C_R) \cong PGU_3(\mathbb{F}_p)$ (Hermitian case).*
- *If $R(x) \notin \{x, x^p\}$, then every element of $\mathrm{Aut}(C_R)$ fixes ∞.*

Automorphism Group of C_R

Follows Lehr & Matignon, *Compositio Math.* **141**, 2005.

Proposition

Assume without loss of generality that $R(x)$ is monic.

- *If $R(x) = x$, then $\mathrm{Aut}(C_R) \cong SL_2(\mathbb{F}_p)$.*
- *If $R(x) = x^p$, then $\mathrm{Aut}(C_R) \cong PGU_3(\mathbb{F}_p)$ (Hermitian case).*
- *If $R(x) \notin \{x, x^p\}$, then every element of $\mathrm{Aut}(C_R)$ fixes ∞.*

It therefore suffices to compute the group

$$\mathrm{Aut}^{\infty}(C_R)$$

of automorphisms that fix ∞.

The group $\mathrm{Aut}^\infty(C_R)$

We have the following commutative diagram:

$$\begin{tikzcd} C_R \arrow[r, "\varphi"] \arrow[d, "{(x,y) \mapsto x}"'] & C_R \arrow[d, "{(x,y) \mapsto x}"] \\ \mathbb{P}^1 \arrow[r, "\tilde{\varphi}"] & \mathbb{P}^1 \end{tikzcd}$$

The group $\mathrm{Aut}^{\infty}(C_R)$

We have the following commutative diagram:

$$\begin{tikzcd} C_R \arrow[r, "\varphi"] \arrow[d, "(x,y)\mapsto x"'] & C_R \arrow[d, "(x,y)\mapsto x"] \\ \mathbb{P}^1 \arrow[r, "\tilde{\varphi}"] & \mathbb{P}^1 \end{tikzcd}$$

As a result, all automorphisms in $\mathrm{Aut}^{\infty}(C_R)$ have the form

$$\varphi(x, y) = (ax + c, dy + B(x))$$

with $a, c, d, B(x)$ live in some extension of $\mathbb{F}_p$.

The group $\mathrm{Aut}^\infty(C_R)$

We have the following commutative diagram:

$$\begin{tikzcd} C_R \arrow[r, "\varphi"] \arrow[d, "{(x,y)\mapsto x}"'] & C_R \arrow[d, "{(x,y)\mapsto x}"] \\ \mathbb{P}^1 \arrow[r, "\tilde{\varphi}"] & \mathbb{P}^1 \end{tikzcd}$$

As a result, all automorphisms in $\mathrm{Aut}^\infty(C_R)$ have the form

$$\varphi(x, y) = (ax + c, dy + B(x))$$

with $a, c, d, B(x)$ live in some extension of $\mathbb{F}_p$.

Structure of $\mathrm{Aut}^\infty(C_R)$: We have $\mathrm{Aut}^\infty(C_R) = P \rtimes H$ where

- H is a boring group of dilations.
- P is an interesting group of translations.

The Group H in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

H consists of all the automorphisms of the form

$$\tau_{a,d}(x, y) = (ax, dy)$$

The Group H in $\mathrm{Aut}^\infty(C_R) = P \rtimes H$

H consists of all the automorphisms of the form

$$\tau_{a,d}(x, y) = (ax, dy)$$

where

- $d \in \mathbb{F}_p^*$.

The Group H in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

H consists of all the automorphisms of the form

$$\tau_{a,d}(x, y) = (ax, dy)$$

where

- $d \in \mathbb{F}_p^*$.
- $a^{p^i+1} = d$ whenever $a_i \neq 0$.

The Group H in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

H consists of all the automorphisms of the form

$$\tau_{a,d}(x, y) = (ax, dy)$$

where

- $d \in \mathbb{F}_p^*$.
- $a^{p^i+1} = d$ whenever $a_i \neq 0$.

H is cyclic, and its order can be easily determined from $R(x)$.

The group P in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

The group P in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$

The group P in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$, or equivalently, there exists a unique additive polynomial $B_c(x) \in \mathbb{F}_q[x]$ such that

$$B_c(x)^p - B_c(x) = cR(x) + R(c)x \ .$$

The group P in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$, or equivalently, there exists a unique additive polynomial $B_c(x) \in \mathbb{F}_q[x]$ such that

$$B_c(x)^p - B_c(x) = cR(x) + R(c)x \ .$$

- $b = B_c(c)/2 + i$ with $i \in \mathbb{F}_p$.

The group P in $\mathrm{Aut}^\infty(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$, or equivalently, there exists a unique additive polynomial $B_c(x) \in \mathbb{F}_q[x]$ such that

$$B_c(x)^p - B_c(x) = cR(x) + R(c)x \ .$$

- $b = B_c(c)/2 + i$ with $i \in \mathbb{F}_p$.

Remarks:

- All automorphisms in P are defined over $\mathbb{F}_q$.

The group P in $\mathrm{Aut}^{\infty}(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$, or equivalently, there exists a unique additive polynomial $B_c(x) \in \mathbb{F}_q[x]$ such that
$$B_c(x)^p - B_c(x) = cR(x) + R(c)x \ .$$
- $b = B_c(c)/2 + i$ with $i \in \mathbb{F}_p$.

Remarks:

- All automorphisms in P are defined over $\mathbb{F}_q$.
- $\sigma_{1,0}$ is the *Artin-Schreier operator* $(x, y) \mapsto (x, y + 1)$.

The group P in $\mathrm{Aut}^\infty(C_R) = P \rtimes H$

P consists of all the automorphisms of the form

$$\sigma_{b,c}(x, y) = (x + c, y + B_c(x) + b)$$

where

- $c \in W$, or equivalently, there exists a unique additive polynomial $B_c(x) \in \mathbb{F}_q[x]$ such that
$$B_c(x)^p - B_c(x) = cR(x) + R(c)x \ .$$
- $b = B_c(c)/2 + i$ with $i \in \mathbb{F}_p$.

Remarks:

- All automorphisms in P are defined over $\mathbb{F}_q$.
- $\sigma_{1,0}$ is the *Artin-Schreier operator* $(x, y) \mapsto (x, y + 1)$.
- Every pair (c, b) is a point on C_R.

Structure of P

Wow, what a group!

Structure of P

Wow, what a group!

- P is normal in $\mathrm{Aut}^{\infty}(C_R)$.

Structure of P

Wow, what a group!

- P is normal in $\mathrm{Aut}^\infty(C_R)$.
- The centre of P is $Z(P) = \langle \sigma_{1,0} \rangle$.

Structure of P

Wow, what a group!

- P is normal in $\mathrm{Aut}^{\infty}(C_R)$.
- The centre of P is $Z(P) = \langle \sigma_{1,0} \rangle$.
- P is the unique Sylow p-subgroup of $\mathrm{Aut}^{\infty}(C_R)$.

Structure of P

Wow, what a group!

- P is normal in $\mathrm{Aut}^\infty(C_R)$.
- The centre of P is $Z(P) = \langle \sigma_{1,0} \rangle$.
- P is the unique Sylow p-subgroup of $\mathrm{Aut}^\infty(C_R)$.
- P has exponent p and order p^{2h+1}.

Wow, what a group!

- P is normal in $\mathrm{Aut}^\infty(C_R)$.
- The centre of P is $Z(P) = \langle \sigma_{1,0} \rangle$.
- P is the unique Sylow p-subgroup of $\mathrm{Aut}^\infty(C_R)$.
- P has exponent p and order p^{2h+1}.
- P is extraspecial (so its structure is completely understood).

Wow, what a group!

- P is normal in $\mathrm{Aut}^{\infty}(C_R)$.
- The centre of P is $Z(P) = \langle \sigma_{1,0} \rangle$.
- P is the unique Sylow p-subgroup of $\mathrm{Aut}^{\infty}(C_R)$.
- P has exponent p and order p^{2h+1}.
- P is extraspecial (so its structure is completely understood).
- The map $P \to W$ via $\sigma_{b,c} \mapsto c$ is a homomorphism with kernel $Z(P) = \langle \sigma_{1,0} \rangle$.

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.
- Any such M is the union of $Z(P)$ and p subgroups $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, and all these $p+1$ subgroups intersect trivially. Chose A as any A_i.

Strategy for Resolving $\pm$ in $L_{C_{R,p^n}}(t)$

Find a large subgroup A of $\mathrm{Aut}^{\infty}(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c,c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.
- Any such M is the union of $Z(P)$ and p subgroups $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, and all these $p+1$ subgroups intersect trivially. Chose A as any A_i.
- The curves C_R/A_i are all isomorphic and are $\mathbb{F}_q$-isomorphic to $C_{m_M x} : y^p - y = m_M x^2$ with $m_M \in \mathbb{F}_q$.

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.
- Any such M is the union of $Z(P)$ and p subgroups $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, and all these $p+1$ subgroups intersect trivially. Chose A as any A_i.
- The curves C_R/A_i are all isomorphic and are $\mathbb{F}_q$-isomorphic to $C_{m_M x} : y^p - y = m_M x^2$ with $m_M \in \mathbb{F}_q$. We have a formula for m_M that depends only on a_h and W_M, not on any A_i.

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.
- Any such M is the union of $Z(P)$ and p subgroups $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, and all these $p+1$ subgroups intersect trivially. Chose A as any A_i.
- The curves C_R/A_i are all isomorphic and are $\mathbb{F}_q$-isomorphic to $C_{m_M x} : y^p - y = m_M x^2$ with $m_M \in \mathbb{F}_q$. We have a formula for m_M that depends only on a_h and W_M, not on any A_i.
- This yields $\mathrm{Jac}(C_R) \sim_{\mathbb{F}_q} \mathrm{Jac}(C_R/A)^{p^h}$, so $L_{C_R,\mathbb{F}_{p^n}}(t) = L_{C_R/A,\mathbb{F}_{p^n}}(t)^{p^h}$ (Kani & Rosen, *Math. Ann.* **284**, 1989)

Strategy for Resolving $\pm$ in $L_{C_R,p^n}(t)$

Find a large subgroup A of $\mathrm{Aut}^\infty(C_R)$ such that the L-polynomial of the *quotient curve* C_R/A is easily computable and is related to $L_{C_R,\mathbb{F}_{p^n}}(t)$.

Avoid groups with $\sigma_{1,0} \in A$ as $C_R/A \cong \mathbb{P}^1$ (no help there).

Road map:

- The map $\epsilon(c, c') = B_c(c') - B_{c'}(c)$ is a symplectic pairing on W.
- Under the homomorphism $\sigma_{b,c} \mapsto c$, every maximal abelian subgroup M of P is the pre-image of a maximal isotropic subspace $W_M \subset W$. We have $M \cong (Z/p\mathbb{Z})^{h+1}$ and $\sigma_{1,0} \in M$.
- Any such M is the union of $Z(P)$ and p subgroups $A_i \cong (\mathbb{Z}/p\mathbb{Z})^h$, and all these $p+1$ subgroups intersect trivially. Chose A as any A_i.
- The curves C_R/A_i are all isomorphic and are $\mathbb{F}_q$-isomorphic to $C_{m_M x} : y^p - y = m_M x^2$ with $m_M \in \mathbb{F}_q$. We have a formula for m_M that depends only on a_h and W_M, not on any A_i.
- This yields $\mathrm{Jac}(C_R) \sim_{\mathbb{F}_q} \mathrm{Jac}(C_R/A)^{p^h}$, so $L_{C_R,\mathbb{F}_{p^n}}(t) = L_{C_R/A,\mathbb{F}_{p^n}}(t)^{p^h}$ (Kani & Rosen, *Math. Ann.* **284**, 1989)
- Compute $L_{C_R/A,\mathbb{F}_{p^n}}(t)$ directly.

Resolving $\pm$ in $L_{C_R,p^n}(t)$

Theorem

Let $m = a_h$ if $h = 0$ and $m = m_M$ when $h > 0$.

If $p \equiv 1 \pmod 4$, then

$$L_{C_R,\mathbb{F}_{p^n}}(t) = \begin{cases} (1-p^n t^2)^g & \text{when } n \text{ is odd}, \\ (1-p^{n/2}t)^{2g} & \text{when } n \text{ is even and } m_M = \square \text{ in } \mathbb{F}_{p^n}, \\ (1+p^{n/2}t)^{2g} & \text{when } n \text{ is even and } m_M \neq \square \text{ in } \mathbb{F}_{p^n}. \end{cases}$$

If $p \equiv 3 \pmod 4$, then

$$L_{C_R,\mathbb{F}_{p^n}}(t) = \begin{cases} (1+p^n t^2)^g & \text{when } n \text{ is odd}, \\ (1-p^{n/2}t)^{2g} & \text{when } n \equiv 0 \pmod 4 \text{ and } m_M = \square \text{ in } \mathbb{F}_{p^n} \\ & \text{or } n \equiv 2 \pmod 4 \text{ and } m_M \neq \square \text{ in } \mathbb{F}_{p^n}, \\ (1+p^{n/2}t)^{2g} & \text{when } n \equiv 0 \pmod 4 \text{ and } m_M \neq \square \text{ in } \mathbb{F}_{p^n} \\ & \text{or } n \equiv 2 \pmod 4 \text{ and } m_M = \square \text{ in } \mathbb{F}_{p^n}, \end{cases}$$

Some Examples

Examples with $h = 0$, i.e. $R(x) = mx$

The following two maximal curves are additions to the database www.manYPoints.org:

- The genus 5 curve $y^{11} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{11^4}$, is maximal over $\mathbb{F}_{11^4}$.
- The genus 9 curve $y^{19} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{19^4}$, is maximal over $\mathbb{F}_{19^4}$.

Some Examples

Examples with $h = 0$, i.e. $R(x) = mx$

The following two maximal curves are additions to the database www.manYPoints.org:

- The genus 5 curve $y^{11} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{11^4}$, is maximal over $\mathbb{F}_{11^4}$.
- The genus 9 curve $y^{19} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{19^4}$, is maximal over $\mathbb{F}_{19^4}$.

The main difficulty of finding examples of minimal or maximal curves with $h > 0$ is to construct suitable elements $m = m_M$.

Examples with $h = 0$, i.e. $R(x) = mx$

The following two maximal curves are additions to the database www.manYPoints.org:

- The genus 5 curve $y^{11} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{11^4}$, is maximal over $\mathbb{F}_{11^4}$.
- The genus 9 curve $y^{19} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{19^4}$, is maximal over $\mathbb{F}_{19^4}$.

The main difficulty of finding examples of minimal or maximal curves with $h > 0$ is to construct suitable elements $m = m_M$.

Families of examples with $h > 0$ and $R(x) = mx^{p^h}$

- The curve $y^p - y = x^{p^h}$ is minimal over $\mathbb{F}_q = \mathbb{F}_{p^{4h}}$.

Examples with $h = 0$, i.e. $R(x) = mx$

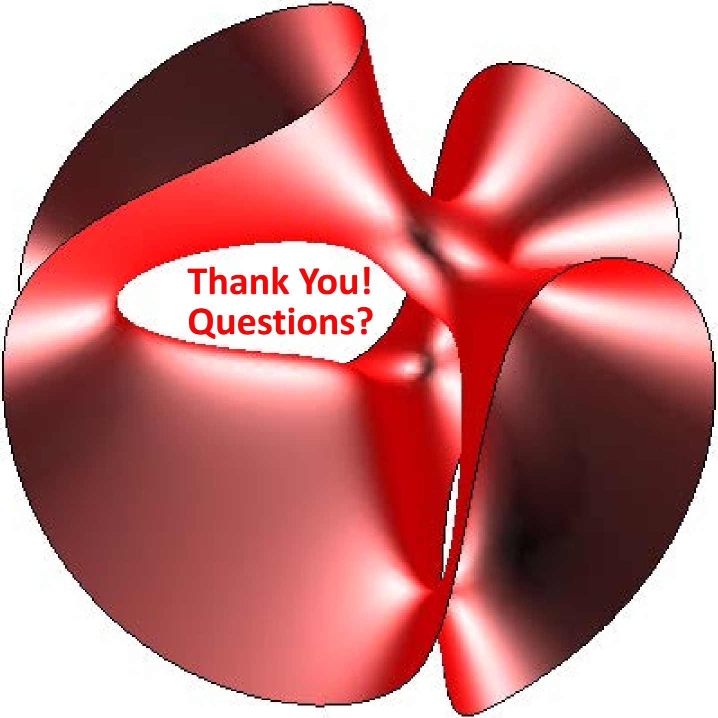
The following two maximal curves are additions to the database www.manYPoints.org:

- The genus 5 curve $y^{11} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{11^4}$, is maximal over $\mathbb{F}_{11^4}$.
- The genus 9 curve $y^{19} - y = mx^2$, with m a nonsquare in $\mathbb{F}_{19^4}$, is maximal over $\mathbb{F}_{19^4}$.

The main difficulty of finding examples of minimal or maximal curves with $h > 0$ is to construct suitable elements $m = m_M$.

Families of examples with $h > 0$ and $R(x) = mx^{p^h}$

- The curve $y^p - y = x^{p^h}$ is minimal over $\mathbb{F}_q = \mathbb{F}_{p^{4h}}$.
- The curve $y^p - y = mx^{p^h}$ defined over $\mathbb{F}_{p^{2h}}$, with $m^{p^h - 1} = -1$, is maximal over $\mathbb{F}_q = \mathbb{F}_{p^{2h}}$ (an example of unusually small genus).


Thank You!
Questions?