Curves with Many Automorphisms

Christelle Vincent

Stanford University

Joint work with I. Bouw, W. Ho, B. Malmskog, R. Scheidler, and P. Srinivasan

Project started at Women in Numbers 3

The set-up

Let p be an odd prime.

The set-up

Let p be an odd prime.

Let $R(X) \in \mathbb{F}_{p^r}[X]$ be an additive polynomial of degree p^h for $h \geq 1$.

The set-up

Let p be an odd prime.

Let $R(X) \in \mathbb{F}_{p^r}[X]$ be an additive polynomial of degree p^h for $h \geq 1$.

Let

$$C_R : Y^p - Y = XR(X).$$

Things we will do to C_R

1. Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$

Things we will do to C_R

1. Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$
2. Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined

Things we will do to C_R

1. Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$
2. Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined
3. Give the structure of this (sub)group of automorphisms

Things we will do to C_R

1. Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$
2. Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined
3. Give the structure of this (sub)group of automorphisms
4. Compute the zeta function of C_R

Zeta function of a curve

For C a curve over a finite field $\mathbb{F}_{p^s}$, we define

$$Z_{C,\mathbb{F}_{p^s}}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{p^{ns}})T^n}{n}\right).$$

Zeta function of a curve

For C a curve over a finite field $\mathbb{F}_{p^s}$, we define

$$Z_{C,\mathbb{F}_{p^s}}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{p^{ns}})T^n}{n}\right).$$

Then

$$Z_{C,\mathbb{F}_{p^s}}(T) = \frac{L_{C,\mathbb{F}_{p^s}}(T)}{(1-T)(1-p^sT)} = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-p^sT)}.$$

But first some notation

Let

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

But first some notation

Let

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

Then we can write an **explicit** polynomial associated to R:

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

But first some notation

Let

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

Then we can write an **explicit** polynomial associated to R:

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

Its zero locus is

$$W = \{c \in \overline{\mathbb{F}}_{p^r} : E(c) = 0\}$$

But first some notation

Let

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

Then we can write an **explicit** polynomial associated to R:

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

Its zero locus is

$$W = \{c \in \overline{\mathbb{F}}_{p^r} : E(c) = 0\}$$

and its splitting field is $\mathbb{F}_q$.

The magical space W

Proposition

1. *$c \in W$ if and only if there exists a polynomial $B(X) \in \mathbb{F}_q[X]$ such that*

$$B(X)^p - B(X) = cR(X) + R(c)X.$$

The magical space W

Proposition

1. *$c \in W$ if and only if there exists a polynomial $B(X) \in \mathbb{F}_q[X]$ such that*

$$B(X)^p - B(X) = cR(X) + R(c)X.$$

2. *Every such $B(X)$ is of the form*

$$B(X) = B_c(X) + \frac{B_c(c)}{2} + i$$

as i ranges over $\mathbb{F}_p$ and where $B_c(X) \in X\mathbb{F}_q[X]$ is unique.

1. Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$

Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined

Give the structure of this (sub)group of automorphisms

Compute the zeta function of C_R

Point counting

Proposition

Let $\mathbb{F}_{p^s}$ be an extension of $\mathbb{F}_q$. The number of $\mathbb{F}_{p^s}$-rational points on C_R is

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

Idea of the proof

Define the bilinear form

$$Q(x, y) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)).$$

Idea of the proof

Define the bilinear form

$$Q(x,y) = \frac{1}{2}\operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)).$$

This is a non-degenerate bilinear form on $\mathbb{F}_{p^s}/W \times \mathbb{F}_{p^s}/W$.

Idea of the proof

Define the bilinear form

$$Q(x, y) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)).$$

This is a non-degenerate bilinear form on $\mathbb{F}_{p^s}/W \times \mathbb{F}_{p^s}/W$.

The zero locus of the associated quadratic form is a smooth quadric whose cardinality we know.

Idea of the proof

Define the bilinear form

$$Q(x, y) = \frac{1}{2} \operatorname{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(xR(y) + yR(x)).$$

This is a non-degenerate bilinear form on $\mathbb{F}_{p^s}/W \times \mathbb{F}_{p^s}/W$.

The zero locus of the associated quadratic form is a smooth quadric whose cardinality we know.

Each of these zeroes gives p^{2h+1} points on C_R. □

This is almost enough

From this easy point count we can get

Proposition

Let $\mathbb{F}_{p^s}$ be an extension of $\mathbb{F}_q$. The L-polynomial of C_R over $\mathbb{F}_{p^s}$ is

$$L_{C_R,\mathbb{F}_{p^s}}(T) = \begin{cases} (1 \pm p^s T^2)^g & \text{if } s \text{ is odd,} \\ (1 \pm p^{s/2} T)^{2g} & \text{if } s \text{ is even.} \end{cases}$$

Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$

2. Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined

Give the structure of this (sub)group of automorphisms

Compute the zeta function of C_R

Many automorphisms of C_R

Theorem (Stichtenoth, Lehr-Matignon)

Let $R(X)$ be monic. If $R(X) \notin \{X, X^p\}$, then all automorphisms of C_R defined over $\overline{\mathbb{F}}_{p^r}$ fix the unique point at ∞ of C_R.

Many automorphisms of C_R

Theorem (Stichtenoth, Lehr-Matignon)

Let $R(X)$ be monic. If $R(X) \notin \{X, X^p\}$, then all automorphisms of C_R defined over $\overline{\mathbb{F}}_{p^r}$ fix the unique point at ∞ of C_R.

We denote the subgroup of automorphisms that fix ∞ by $\mathrm{Aut}^0(C_R)$.

Many/all automorphisms of C_R

Lemma

Every automorphism in $\mathrm{Aut}^0(C_R)$ *is of the form*

$$\begin{aligned}\sigma_{a,b,c,d} \colon C_R &\to C_R \\ (x,y) &\mapsto (ax+c, dy+b+B_c(ax)),\end{aligned}$$

where $c \in W$ *and* $b = \frac{B_c(c)}{2} + i$ *for some* $i \in \mathbb{F}_p$.

What we want

Our goal now will be to find a large subgroup A of $\mathrm{Aut}^0(C_R)$ so that C_R/A

What we want

Our goal now will be to find a large subgroup A of $\mathrm{Aut}^0(C_R)$ so that C_R/A

- is easily computable and its L-polynomial can be computed,

What we want

Our goal now will be to find a large subgroup A of $\mathrm{Aut}^0(C_R)$ so that C_R/A

- is easily computable and its L-polynomial can be computed,
- and its L-polynomial is related to the L-polynomial of C_R.

What we want

Our goal now will be to find a large subgroup A of $\mathrm{Aut}^0(C_R)$ so that C_R/A

- is easily computable and its L-polynomial can be computed,
- and its L-polynomial is related to the L-polynomial of C_R.

One thing to avoid is for $\rho = \sigma_{1,1,0,1}$ ($\rho(x,y) = (x, y+1)$) to be in A. In that case $C_R/A \cong \mathbb{P}^1$.

Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$

Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined

3. Give the structure of this (sub)group of automorphisms

Compute the zeta function of C_R

The structure of the automorphism group of C_R

Theorem

- *The group* $\mathrm{Aut}^0(C_R)$ *has a unique Sylow p-subgroup, which we denote by* P*. It consists of all automorphisms* $\sigma_{1,b,c,1}$.

The structure of the automorphism group of C_R

Theorem

- *The group* $\mathrm{Aut}^0(C_R)$ *has a unique Sylow p-subgroup, which we denote by* P*. It consists of all automorphisms* $\sigma_{1,b,c,1}$.
- *The automorphisms* $\sigma_{a,0,0,d}$ *form a cyclic subgroup* H *of* $\mathrm{Aut}^0(C_R)$*, whose cardinality we know.*

The structure of the automorphism group of C_R

Theorem

- *The group* $\mathrm{Aut}^0(C_R)$ *has a unique Sylow p-subgroup, which we denote by* P. *It consists of all automorphisms* $\sigma_{1,b,c,1}$.
- *The automorphisms* $\sigma_{a,0,0,d}$ *form a cyclic subgroup* H *of* $\mathrm{Aut}^0(C_R)$, *whose cardinality we know.*
- $\mathrm{Aut}^0(C_R) = P \rtimes H$.

Zooming in on P

Because we have such an explicit description of the elements of P, we can deduce the following facts:

Zooming in on P

Because we have such an explicit description of the elements of P, we can deduce the following facts:

Theorem

- *P has center generated by $\rho = \sigma_{1,1,0,1}$ $(\rho(x, y) = (x, y + 1))$.*

Zooming in on P

Because we have such an explicit description of the elements of P, we can deduce the following facts:

Theorem

- *P has center generated by $\rho = \sigma_{1,1,0,1}$ ($\rho(x, y) = (x, y + 1)$).*
- *$P/Z(P) \cong W$.*

Important consequence of $P/Z(P) \cong W$

In P, we have

$$[\sigma_{1,b_1,c_1,1}, \sigma_{1,b_2,c_2,1}] = \rho^{-\epsilon(c_1,c_2)},$$

where

$$\epsilon(c_1, c_2) = B_{c_1}(c_2) - B_{c_2}(c_1).$$

Important consequence of $P/Z(P) \cong W$

In P, we have

$$[\sigma_{1,b_1,c_1,1}, \sigma_{1,b_2,c_2,1}] = \rho^{-\epsilon(c_1,c_2)},$$

where

$$\epsilon(c_1, c_2) = B_{c_1}(c_2) - B_{c_2}(c_1).$$

Since $c_i \in W$, this gives a symplectic pairing on W.

Maximal isotropic subspaces

Fact

Every maximal abelian subgroup $\mathcal{A}$ of P is the inverse image of a maximal isotropic subspace of W. Such an $\mathcal{A} \cong (\mathbb{Z}/p\mathbb{Z})^{h+1}$, and contains $Z(P)$.

Maximal isotropic subspaces

Fact

Every maximal abelian subgroup $\mathcal{A}$ of P is the inverse image of a maximal isotropic subspace of W. Such an $\mathcal{A} \cong (\mathbb{Z}/p\mathbb{Z})^{h+1}$, and contains $Z(P)$.

The subgroup A we seek is any subgroup A of $\mathcal{A}$ such that $A \cong (\mathbb{Z}/p\mathbb{Z})^h$ and $A \cap Z(P) \cong \{1\}$.

Consequences for the curve C_R

Theorem

Any two subgroups A, A' of $\mathcal{A}$ of order p^h which trivially intersect $Z(P)$ are conjugate inside P.

Consequences for the curve C_R

Theorem

Any two subgroups A, A' of $\mathcal{A}$ of order p^h which trivially intersect $Z(P)$ are conjugate inside P.

This immediately implies

Proposition

For any such A, A', $C_R/A \cong C_R/A'$.

Consequences for the curve C_R

Theorem

For a fixed $\mathcal{A}$ and any subgroup $A \cong (\mathbb{Z}/p\mathbb{Z})^h \subset \mathcal{A}$ intersecting $Z(P)$ trivially, there exist subgroups $A_1, \ldots, A_{p-1}$ of $\mathcal{A}$ such that

$$\mathcal{A} = Z(P) \cup A_1 \cup \ldots \cup A_{p-1} \cup A,$$

$$A_i \cong (\mathbb{Z}/p\mathbb{Z})^h, \quad A_i \cap Z(P) = \{1\}, \quad A_i \cap A_j = \{1\}.$$

Consequences for the curve C_R

Theorem

For a fixed $\mathcal{A}$ and any subgroup $A \cong (\mathbb{Z}/p\mathbb{Z})^h \subset \mathcal{A}$ intersecting $Z(P)$ trivially, there exist subgroups $A_1, \ldots, A_{p-1}$ of $\mathcal{A}$ such that

$$\mathcal{A} = Z(P) \cup A_1 \cup \ldots \cup A_{p-1} \cup A,$$

$$A_i \cong (\mathbb{Z}/p\mathbb{Z})^h, \quad A_i \cap Z(P) = \{1\}, \quad A_i \cap A_j = \{1\}.$$

Using a theorem of Kani and Rosen, from this decomposition we get as an immediate consequence

Consequences for the curve C_R

Theorem

For a fixed $\mathcal{A}$ and any subgroup $A \cong (\mathbb{Z}/p\mathbb{Z})^h \subset \mathcal{A}$ intersecting $Z(P)$ trivially, there exist subgroups $A_1, \ldots, A_{p-1}$ of $\mathcal{A}$ such that

$$\mathcal{A} = Z(P) \cup A_1 \cup \ldots \cup A_{p-1} \cup A,$$
$$A_i \cong (\mathbb{Z}/p\mathbb{Z})^h, \quad A_i \cap Z(P) = \{1\}, \quad A_i \cap A_j = \{1\}.$$

Using a theorem of Kani and Rosen, from this decomposition we get as an immediate consequence

Theorem

$\mathrm{Jac}(C_R) \sim_{\mathbb{F}_q} \mathrm{Jac}(C_R/A)^{p^h}$.

Almost count the number of points of C_R over certain field extensions of $\mathbb{F}_{p^r}$

Exhibit many automorphisms (and in most cases all) of C_R as well as determine the field over which these automorphisms are defined

Give the structure of this (sub)group of automorphisms

4. Compute the zeta function of C_R

Reducing to a simpler problem

Because of facts about L-polynomials and isogenies, the upshot of this last theorem is that

$$L_{C_R}(T) = L_{C_R/A}(T)^{p^h}.$$

The curve C_R/A

Theorem

Let $A \subset \mathcal{A}$. Then C_R/A is isomorphic over $\mathbb{F}_q$ to the curve

$$Y^p - Y = a_{\mathcal{A}} X^2,$$

where

$$a_{\mathcal{A}} = \frac{a_h}{2} \prod_{c \in \overline{A} \setminus \{0\}} c,$$

where $\overline{A}$ is the maximal isotropic subspace of W that is the image of $\mathcal{A}$ under the quotient map $P \to W$.

The curve C_R/A

A curve with equation

$$Y^p - Y = aX^2$$

is simple enough that we can count its points explicitly and compute the zeta function directly.

The L-polynomial

Theorem

1. *If* $p \equiv 1 \pmod 4$, *then the L-polynomial of* C_R *over* $\mathbb{F}_{p^s}$ *is given by*

$$L_{C_R,\mathbb{F}_{p^s}}(T) = \begin{cases} (1 - p^s T^2)^g & \text{if } s \text{ is odd,} \\ (1 - p^{s/2} T)^{2g} & \text{if } s \text{ is even and } a_{\mathcal{A}} \text{ is a square in } \mathbb{F}_{p^s}^*, \\ (1 + p^{s/2} T)^{2g} & \text{if } s \text{ is even and } a_{\mathcal{A}} \text{ is a non-square in } \mathbb{F}_{p^s}^*. \end{cases}$$

The L-polynomial

Theorem

2. *If* $p \equiv 3 \pmod 4$, *then the* L*-polynomial of* C_R *over* $\mathbb{F}_{p^s}$ *is given by*

$$L_{C_R,\mathbb{F}_{p^s}}(T) = \begin{cases} (1+p^sT^2)^g & \text{if } s \text{ is odd,} \\ (1-p^{s/2}T)^{2g} & \text{if } s \equiv 0 \pmod 4 \text{ and } a_{\mathcal{A}} \\ & \text{is a square in } \mathbb{F}_{p^s}^*, \\ (1+p^{s/2}T)^{2g} & \text{if } s \equiv 0 \pmod 4 \text{ and } a_{\mathcal{A}} \\ & \text{is a nonsquare in } \mathbb{F}_{p^s}^*, \\ (1+p^{s/2}T)^{2g} & \text{if } s \equiv 2 \pmod 4 \text{ and } a_{\mathcal{A}} \\ & \text{is a square in } \mathbb{F}_{p^s}^*, \\ (1-p^{s/2}T)^{2g} & \text{if } s \equiv 2 \pmod 4 \text{ and } a_{\mathcal{A}} \\ & \text{is a nonsquare in } \mathbb{F}_{p^s}^*. \end{cases}$$

For all of this and more, please visit my website, `math.stanford.edu/~cvincent`.

Thank you!