Automorphism groups of algebraic curves in positive characteristic

Maria Montanucci

Technical University of Denmark (DTU)

Arithmetic, Geometry, Cryptography and Coding Theory

09-13 June, 2025

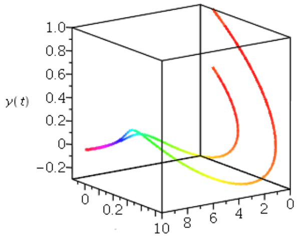
DTU Compute
Department of Applied Mathematics and Computer Science

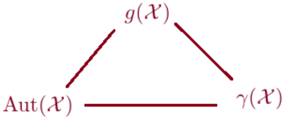
Outline

- Preliminaries
  - Notation and terminology
- Open Problem 1: d-group of automorphisms, $d \neq p$ prime number
  - (Korchmáros-M., 2020)
- Open Problem 2: Automorphism groups of ordinary curves
  - (Korchmáros-M., 2019)
  - (Korchmáros-M.-Speziali, 2018)
  - (M.-Zini, 2018)
  - (M.-Speziali, 2019)
- Open Problem 3: large automorphism groups imply p-rank zero
  - (M., 2023)
- Applications of automorphism groups and future work

Algebraic curves and birational invariants

- K: algebraically closed field of characteristic p
- $\mathcal{X} \subseteq \mathbb{P}^r = \mathbb{P}^r(K)$: projective, geometrically irreducible, non-singular algebraic curve
- Algebraic function field F/K: $F = K(\mathcal{X})$
- $g = g(\mathcal{X}) \geq 0$: genus of $\mathcal{X}$ $\rightarrow$ $\mathrm{Aut}(\mathcal{X})$ is infinite, if $g \leq 1$
- $\gamma = \gamma(\mathcal{X})$: p-rank (Hasse-Witt invariant) of $\mathcal{X}$ $\rightarrow$ $0 \leq \gamma \leq g$
- $\mathrm{Aut}(\mathcal{X})$: (full) automorphism group of $\mathcal{X}$ over K





Automorphism groups and quotient curves

$G :=$ finite automorphism group of $\mathcal{X}$

- G acts faithfully on $\mathcal{X}$
- G has a finite number of short orbits $\theta_1, ..., \theta_k$
- $\exists$ curve $\mathcal{Y}$ whose points are the G-orbits of $\mathcal{X}$
- $\mathcal{Y} := \mathcal{X}/G$ is called quotient curve of $\mathcal{X}$ by G
- $N_{\mathrm{Aut}(\mathcal{X})}(G)/G \leq Aut(\mathcal{Y})$

Riemann-Hurwitz Formula:

$$2g(\mathcal{X}) - 2 = |G|(2g(\mathcal{Y}) - 2) + \mathrm{Diff}(\mathcal{X}|\mathcal{Y})$$

Deuring-Shafarevic Formula: If $|G| = p^h$ then

$$\gamma(\mathcal{X}) - 1 = |G|(\gamma(\mathcal{Y}) - 1) + \sum_{i=1}^{k}(|G| - |\theta_i|)$$

How many automorphisms?

[Schmid (1938), Iwasawa-Tamagawa (1951), Roquette (1952), Rosenlicht (1954), Garcia (1993)]

If $g \geq 2$ then $Aut(\mathcal{X})$ is a finite group

Classical Hurwitz bound (1892)

If $p = 0$ and $g \geq 2$ then $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$

Example: Klein quartic

$\mathcal{K} : X^3 + Y + XY^3 = 0$, $g(\mathcal{K}) = 3$, $|Aut(\mathcal{K})| = |PSL(2,7)| = 84(3-1)$

- If $gcd(p, |\mathrm{Aut}(\mathcal{X})|) = 1$ then $|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1)$
- If $gcd(p, |\mathrm{Aut}(\mathcal{X})|) > 1$ interesting behaviours can occur

What if p divides $|\mathrm{Aut}(\mathcal{X})|$?

- Hermitian curve $\mathcal{H} : X^{q+1} = Y^q + Y$, $q = p^h$, $|\mathrm{Aut}(\mathcal{H})| = |PGU(3,q)| \geq 16g(\mathcal{H})^4$

Stichtenoth (1973)

If $g = g(\mathcal{X}) \geq 2$ and $|\mathrm{Aut}(\mathcal{X})| \geq 16g^4$ then $\mathcal{X}$ is the Hermitian curve $\mathcal{H}$ (up to isomorphism). In particular $\gamma(\mathcal{X}) = 0$.

Henn (1976)

If $g = g(\mathcal{X}) \geq 2$ and $|\mathrm{Aut}(\mathcal{X})| > 8g^3$ then $\gamma(\mathcal{X}) = 0$ and $\mathcal{X}$ is one of the following curves (up to isomorphism):

- $\mathcal{Y} : Y^2 + Y + X^{2^k+1} = 0$, $p = 2$, $g = 2^{k-1}$ and $|\mathrm{Aut}(\mathcal{Y})| = 2^{2k+1}(2^k+1)$.
- The Roquette curve $\mathcal{R} : Y^2 - (X^q - X) = 0$ with $p > 2$, $g = (q-1)/2$. Also $\mathrm{Aut}(\mathcal{R})/M \cong PSL(2,q), PGL(2,q)$, where $q = p^r$ and $|M| = 2$;
- The Hermitian curve $\mathcal{H} : X^{q+1} = Y^q + Y$, $q = p^h$, p prime.
- The Suzuki curve $\mathcal{S} : X^{q_0}(X^q + X) + Y^q + Y = 0$, with $p = 2$, $q_0 = 2^r \geq 2$, $q = 2q_0^2$, $g(\mathcal{S}) = q_0(q-1)$, and $\mathrm{Aut}(\mathcal{S}) = Sz(q)$ (Suzuki group).

The link between $\mathrm{Aut}(\mathcal{X})$ and $\gamma(\mathcal{X})$

Theorem (Nakajima, 1987)

1. If $\mathcal{X}$ is ordinary, then $|\mathrm{Aut}(\mathcal{X})| \leq 84(g^2-g) \rightarrow$ no extremal examples provided!
2. Let S be a p-subgroup of $\mathrm{Aut}(\mathcal{X})$. Then

$$|S| \leq \begin{cases} g(\mathcal{X})-1, \text{ if } \gamma(\mathcal{X})=1, \\ 4(\gamma(\mathcal{X})-1), \text{ if } \gamma(\mathcal{X}) \geq 2, \\ \max\{g(\mathcal{X}), 4p/(p-1)^2 g(\mathcal{X})^2\}, \text{ if } \gamma(\mathcal{X})=0. \end{cases}$$

3. If $|S| > \frac{2p}{p-1} g(\mathcal{X})$ then $\gamma(\mathcal{X})=0$.

- Open Problem 1: What if S is a d-group where $d \neq p$ is a prime?
- Open Problem 2: Can Nakajima's bound 1 be improved?
- Open Problem 3: Find an optimal $f(g)$ such that if $|\mathrm{Aut}(\mathcal{X})| > f(g)$ then $\gamma(\mathcal{X})=0$ (clearly $f(g) \leq 8g^3$), e.g. can $f(g) \sim g^2$?

What if the classical Hurwitz bound does not hold? Classification results

Let G automorphism group of a curve $\mathcal{X}$ of genus $g \geq 2$. A consequence of the Riemann-Hurwitz Formula:

- If G has more than 4 short orbits, then $|G| \leq 4(g-1)$
- If $G = G_P$ and p does not divide $|G|$, then $|G| \leq 4g+2$

Exceptions to the classical Hurwitz bound, for a group $|G| > 84(g-1)$, occur only in the following cases:

1. G has two short orbits and both are non-tame; here $|G| \leq 16g^2$
2. G has three short orbits with precisely one non-tame orbit; here $|G| \leq 24g^2$
3. G has a unique short orbit which is non-tame; here $|G| \leq 8g^3$
4. G has two short orbits and one short orbit is tame, one non-tame

$\rightarrow$ IDEA: What about bounds for $|G|$ in Case 3? All the curves in Henn's result satisfy case 4

Our contributions to Open Problem 1

Let G be a d-group of automorphisms of a curve $\mathcal{X}$ of genus $g \geq 2$.

1. How large is $|G|$ with respect to g?
2. Structure in terms of generators and relations of extremal groups G
3. Is the bound sharp? Explicit construction of extremal examples $(\mathcal{X}, G)$

Zomorrodian (1985-1987): the case Char$(K) = 0$

$|G| \leq 9(g-1)$ and the bound is sharp if and only if $g - 1 = 3^k$ and $g \geq 10$

- (Giulietti-Korchmáros 2010-2017, Stichtenoth 1973) Nakajima extremal curves

Our results:

- Zomorrodian's result holds also when $\mathrm{Char}(K) = p \neq 0$ and $d \neq 2, p$

For the interesting case $d = 3$:

- the group structure of G is uniquely determined
- two general methods to construct extremal examples $(\mathcal{X}, G)$.

Theorem (Korchmáros-M., 2020)

Let $g(\mathcal{X}) \geq 2$. If G is a d-subgroup of $\mathrm{Aut}(\mathcal{X})$ with $d \neq p$ and d odd then

$$|G| \leq \begin{cases} 9(g-1), & \text{if } d=3, \\ \frac{2d}{d-3}(g-1), & \text{if } d>3. \end{cases}$$

For $d=3$ if equality holds then G is not abelian and $g \neq 2$.

Remark: the bound is sharp for $d \geq 5$ (abelian groups)

Fermat curve $\mathcal{F}_d : x^d + y^d + 1 = 0$ has genus $(d-1)(d-2)/2$,
$C_d \times C_d \cong G < \mathrm{Aut}(\mathcal{F}_d)$ of order $d^2 = 2d(g-1)/(d-3)$:

$$G = \{(x,y) \mapsto (\lambda x, \mu y) \mid \lambda^d = \mu^d = 1\}$$

- known: G abelian then $|G| \leq 4g+4 \implies$ if G is extremal and $d=3$ then G is non-abelian (interesting case)

Improvements of the bound for non-abelian groups

Theorem (Korchmáros-M., 2020)

Let G be a non-abelian d-subgroup of $\mathrm{Aut}(\mathcal{X})$. If Z is an order d subgroup of $Z(G)$ such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/Z$ has genus at most 1 then $\bar{\mathcal{X}}$ is elliptic and

$$|G| \leq \frac{2d}{d-1}(g-1)$$

apart from the case where $d = 3$ and $|G| = 9(g-1)$.

- $g(\mathcal{X}/Z) \geq 2 \implies \mathcal{X}/Z$ is still extremal as $G/Z \leq \mathrm{Aut}(\mathcal{X}/\mathrm{Z})$
- "Minimal" extremal examples are those for which $g(\mathcal{X}/Z) \leq 1$
- Interesting case: $d = 3$ ($d \geq 5$ G is abelian)
- An Extremal 3-Zomorrodian curve is a curve $\mathcal{X}$ of genus $g \geq 2$ admitting $G \leq \mathrm{Aut}(\mathcal{X})$ with $|G| = 9(g-1)$

Minimal Extremal 3-Zomorrodian curves: structure of G

Proposition (Korchmáros-M., 2020)

Let G be a Sylow 3-subgroup of a curve of an Extremal 3-Zomorrodian curve of elliptic type and genus $g = 3^h + 1$, $h \geq 3$. Then

- either $Z(G) \cong C_3$ or $Z(G) \cong C_3 \times C_3$,
- G has 3 short orbits θ, σ, Ω of sizes $|G|/3$, $|G|/3$ and $|G|/9$
- G can be generated by 2 elements $\implies [G : \Phi(G)] = 9$;
- maximal subgroups of G are normal of index 3. Exactly one of them is either abelian or minimal non-abelian.

- Minimal non-abelian case: Qu Haipeng, Yang Sushan, Xu Mingyao, and An Lijian, Finite p-groups with a minimal non-abelian subgroup of index p (I), J. Algebra 358 (2012), 178-188.
- Abelian case: N. Blackburn, On a special class of p-groups, Acta Math. 100 (1958), 45-92.

Elliptic type: structure of G

Theorem (Korchmáros-M., 2020)

If $|Z(G)| = 3$ then G has no abelian maximal subgroups of index 3 and

- $|G| = 3^{2e}$ and $G = \langle s_1, s_2, s \mid s_1^{3^e} = s_2^{3^{e-1}} = 1, s^3 = s_1^{\delta 3^{e-1}}, [s_1, s] = s_2, [s_2, s] = s_2^{-3} s_1^{-3}, [s_2, s_1] = s_1^{3^{e-1}} \rangle$ where $\delta = 0, 1, 2$;
- $|G| = 3^{2e+1}$ and $G = \langle s_1, s_2, s \mid s_1^{3^e} = s_2^{3^e} = 1, s^3 = s_2^{\delta 3^{e-1}}, [s_1, s] = s_2, [s_2, s] = s_2^{-3} s_1^{-3}, [s_2, s_1] = s_2^{3^{e-1}} \rangle$ where $\delta = 0, 1, 2$.

If $|Z(G)| = 9$ then G has no abelian subgroups of index 3 and

- $G = \langle s_1, s_2, \beta, x \mid s_1^{3^n} = s_2^{3^{n-1}} = x^3 = 1, \beta^3 = x^2, [s_1, \beta] = s_2, [s_2, \beta] = s_2^{-3} s_1^{-3}, [s_1, s_2] = x, [x, s_1] = [x, s_2] = 1 \rangle$, for $|G| = 3^{2n+1}$, $e \geq 3$;
- $G = \langle s_1, s_2, \beta, x \mid s_1^{3^n} = s_2^{3^n} = x^3 = 1, \beta^3 = x^2, [s_1, \beta] = s_2, [s_2, \beta] = s_2^{-3} s_1^{-3}, [s_1, s_2] = x, [x, s_1] = [x, s_2] = 1 \rangle$, for $|G| = 3^{2n+2}$, $n \geq 2$.

Can we construct infinite families of Extremal 3-Zomorrodian curves?

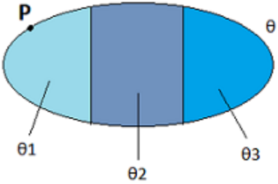
Construction of Elliptic type Extremal 3-Zomorrodian curves for every $(g, |G|) = (3^h + 1, 3^{h+2})$

- Elliptic curve $\mathcal{E} : X^3 + Y^3 + Z^3 = 0$ ($J(\mathcal{E})$ = Jacobian group)
- $P = (-1, 0, 1)$ is an inflection point of $\mathcal{E}$, and $\bar{\alpha} : (X, Y, Z) \mapsto (X, \epsilon Y, Z)$ with $\epsilon^3 = 1$ primitive, is an order 3 automorphism of $\mathcal{E}$ fixing P
- $\bar{\alpha}$ has two more fixed points on $\mathcal{E}$, namely $P_1 = (-\epsilon, 0, 1)$ and $P_2 = (-\epsilon^2, 0, 1)$ $\implies \bar{\alpha} \notin J(\mathcal{E})$

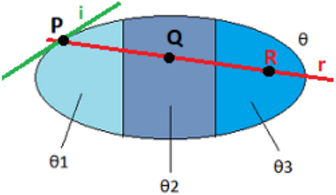
Theorem (Korchmáros-M. 2020)

A 3-group $\bar{G}$ of automorphisms of $\mathcal{E}$ can be written up to conjugation as $\bar{G} = \bar{H} \rtimes \langle \bar{\alpha} \rangle = \bar{H} \rtimes \bar{G}_P$ where $\bar{H} = \bar{G} \cap J(\mathcal{E})$ and $\bar{G}$ can be generated by 2 elements

- let $\bar{G} = \bar{H} \rtimes \langle\bar{\alpha}\rangle \leq \mathrm{Aut}(\mathcal{E})$ with $|\bar{G}| = 3^{h+1}$, $h \geq 2$
- Since $\bar{G}$ can be generated by 2 elements, $\bar{G}/\Phi(\bar{G})$ is elementary abelian of order 9
- since $\bar{H}$ is maximal, $\Phi(\bar{G}) \leq \bar{H}$
- $\theta_1 = \Phi(\bar{G})-$orbit containing $P \implies |\theta_1| = 3^{h-1}$
- $\Phi(\bar{G})$ is a normal subgroup of $\bar{H}$, the $\bar{H}$-orbit θ containing P is partitioned into three $\Phi(\bar{G})$-orbits which may be parameterized by $\Phi(\bar{G})$ together with its two cosets in $\bar{H}$

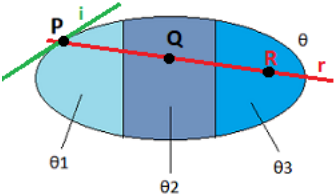


- (Korchmáros-Nagy-Pace, 2014) If $Q \in \theta_2$ then the line through P and Q meets $\mathcal{E}$ in a point $R \in \theta_3$



- r has homogenous equation $mX - Y + mZ = 0$ for some $m \in K$
- (inflectional) tangent to $\mathcal{E}$ at P is $i : X + Z = 0$

- in $K(\mathcal{E}) = K(x,y)$ with $x^3 + y^3 + 1 = 0$ define $t = \frac{mx-y+m}{x+1}$ then $(t) = Q + R - 2P$



- let $w = \prod_{f\in\Phi(\bar{G})} f(t)$. Then $(w) = -2\theta_1 + \theta_2 + \theta_3$ and $\bar{g} \in \bar{G}$ acts on $\{\theta_1, \theta_2, \theta_3\}$.

$$\begin{cases} (1)\ \bar{g}(w)/w = \lambda,\ \ for\ some\ \lambda \in K \\ (2)\ (\bar{g}(w)/w) = -2\theta_1 + \theta_2 + \theta_3 - (-2\theta_3 + \theta_1 + \theta_2) = -3\theta_1 + 3\theta_3 \end{cases}$$

In any case

(key property) $\bar{g}(w)/w = v^3$, for some $v \in K(x,y)$

- We define

$$\mathcal{X} : \begin{cases} x^3 + y^3 + 1 = 0, \\ z^3 = w \end{cases} \implies g(\mathcal{X}) = 3^h + 1$$

- Also every $\bar{g} \in \bar{G}$ can be lifted in three ways creating a group $G \leq \mathrm{Aut}(\mathcal{X})$ of order $3|\bar{G}| = 3^{h+2} = 9(g-1)$
- Indeed for $\bar{g} \in \bar{G}$ we define,

$$g : (x, y, z) \mapsto (\bar{g}(x), \bar{g}(y), vz),$$

where $v^3 = \bar{g}(w)/w$. Then

$$g(z^3) = v^3 z^3 = \frac{\bar{g}(w)}{w} w = \bar{g}(w) = g(w) \implies \mathcal{X} \textit{ is preserved!}$$

Explicit examples using MAGMA

- $g = 10,\ |G| = 81$

$$\begin{cases} x^3 + y^3 + 1 = 0; \\ z^3 = \frac{x}{y^2}. \end{cases}$$

- $g = 28,\ |G| = 729$

$$\begin{cases} x^3 + y^3 + 1 = 0; \\ z^3 = (y^{18} + 3y^{15} + 52y^{12} + 26y^9 + 52y^6 + 3y^3 \\ +1)/(y^{17} + 3y^{14} + 5y^{11} + 5y^8 + 3y^5 + y^2)x. \end{cases}$$

- $g = 82,\ |G| = 2187$

$$\begin{cases} x^3 + y^3 + 1 = 0; \\ z^3 = (y^{54} + 9y^{51} + 151y^{48} + 191y^{45} + 243y^{42} + 21y^{39} + 86y^{36} \\ +184y^{33} + y^{30} + 153y^{27} + y^{24} + 184y^{21} + 86y^{18} + 21y^{15} \\ +243y^{12} + 191y^9 + 151y^6 + 9y^3 + 1)/(y^{53} + 9y^{50} + 261y^{47} \\ +258y^{44} + 138y^{41} + 146y^{38} + 206y^{35} + 24y^{32} + 12y^{29} + 12y^{26} \\ +24y^{23} + 206y^{20} + 146y^{17} + 138y^{14} + 258y^{11} \\ +261y^8 + 9y^5 + y^2)x. \end{cases}$$

Ordinary algebraic curves with many automorphisms

$\mathcal{X}$ is ordinary if $g(\mathcal{X}) = \gamma(\mathcal{X})$

- Nakajima (1987): $|Aut(\mathcal{X})| \leq 84(g(\mathcal{X})-1)g(\mathcal{X}) \to$ **can this bound be improved?**

Theorem (Korchmáros-M., 2019)

Let $\mathcal{X}$ be an ordinary curve of genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field of odd characteristic p. If $G \leq Aut(\mathcal{X})$ is solvable then

$$|G| \leq 34(g(\mathcal{X})+1)^{3/2} < 68\sqrt{2}g(\mathcal{X})^{3/2}$$

- This is the best bound known for automorphism groups of ordinary curves
- (Korchmáros-M.-Speziali, 2018) Extremal example up to the constant term: a generalized Artin-Schreier extension of the Artin-Mumford curve
- (M.-Zini, 2018) An infinite family of extrermal examples: Generalized Artin-Mumford curves
- $\implies$ Our bound **cannot be improved!**

Why is the hypothesis G solvable relevant/useful?

- First observation: if $g(\mathcal{X}) = 2$ then $|G| \leq 48$ (known), so the statement is true. We assume $g(\mathcal{X}) \geq 3$.
- By contradiction: $(G, g(\mathcal{X}))$ is a **minimal counterexample**, that is, $|G| > 34(g(\mathcal{X}) + 1)^{3/2}$ and if $g(\mathcal{Y}) < g(\mathcal{X})$, $\mathcal{Y}$ is ordinary and $H \leq Aut(\mathcal{Y})$ is solvable then $|H| \leq 34(g(\mathcal{Y}) + 1)^{3/2}$
- Since G is solvable, it admits a minimal normal subgroup S which is elementary abelian.
- **Two cases are treated separately:** either S is a p-group, or it has order prime to p.
- In both cases we try to construct a quotient curve which is still ordinary and gives a contradiction to the minimality of $(G, g(\mathcal{X}))$.

Our bound is sharp (up to the constant term)

$q = p^h$, $h \geq 1$ and $K = \overline{\mathbb{F}}_q$. For $(m, p) = 1$ let

$$\mathcal{Y} : y^q + y = x^m + 1/x^m$$

and $F = K(\mathcal{Y})$ its function field. Let $t = x^{m(q-1)}$. $F|K(t)$ is not Galois

Theorem (Korchmáros-M.-Speziali, 2018)

The Galois closure of $F|K(t)$ is $L = K(x, y, z)$ where $y^q + y = x^m + 1/x^m$ and $z^a + z = x^m$. Also

- $g(L) = (q-1)(q^m - 1)$, $\gamma(L) = (q-1)^2$,
- $|Aut(L)| \geq m(q-1)$,
- if $m = 1$, L is ordinary and $|Aut(\mathcal{X})| > 2g^{3/2}$.

- (M.-Zini, 2018): infinite family of extremal examples (**Generalized Artin-Mumford curves**) $\mathcal{X}_{L_1,L_2} : L_1(x) \cdot L_2(y) = 1$, where L_1 and L_2 are linearized polynomials.

Large automorphism groups of ordinary curves

Natural questions:

- What if $p = 2$ and G is solvable?
- What if p is odd but G is not solvable?

Theorem (M.-Speziali, 2019)

Let $\mathcal{X}$ be an ordinary curve of even genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field of odd characteristic 2. If $G \leq Aut(\mathcal{X})$ is solvable then

$$|G| \leq 35(g(\mathcal{X})+1)^{3/2}$$

Theorem (M.-Speziali, 2019)

Let $\mathcal{X}$ be an ordinary curve of genus $g(\mathcal{X}) \geq 2$ defined over an algebraically closed field of odd characteristic p. If $G \leq Aut(\mathcal{X})$ is not solvable then

$$|G| \leq 822g(\mathcal{X})^{7/4}$$

- A general and sharp refinement of Nakajima's bound is still an open problem!

The third open problem: improving Henn's result

If $G \leq \mathrm{Aut}(\mathcal{X})$ is such that $|G| > 84(g(\mathcal{X}) - 1)$ then one of the following occurs:

1. G has two short orbits and both are non-tame; here $|G| \leq 16g^2$
2. G has three short orbits with precisely one non-tame orbit; here $|G| \leq 24g^2$
3. G has a unique short orbit which is non-tame; here $|G| \leq 8g^3$
4. G has two short orbits and one short orbit is tame, one non-tame (if $|G| \geq 8g^3$ then G is known and $\gamma(\mathcal{X}) = 0$).

Open Problem 3

Is it possible to find a (optimal) function $f(g)$ such that the existence of an automorphism group G of $\mathcal{X}$ with $|G| > f(g)$ implies that $\mathcal{X}$ has p-rank zero?

- we already see that if $|Aut(\mathcal{X})| > 24g^2$ then either Case 3 or 4 occurs.
- $\longrightarrow$ Natural idea: improve the bounds in 3 and/or 4 to obtain (up to finite exceptions) a function $f(g) = cg^2$ for some constant c

The result: An improvement of the Henn's result, Case 3

Theorem (M., 2023)

Let $G \leq Aut(\mathcal{X})$, where $g = g(\mathcal{X}) \geq 2$ and $\mathcal{X}$ is defined over an algebraically closed field of characteristic $p > 0$.

1. If G satisfies Case 3 then $|G| \leq 336g(\mathcal{X})^2$.
2. If $|G| \geq 60g^2$ and Case 3 is satisfied than $\gamma(\mathcal{X})$ is positive and congruent to zero modulo p.
3. If $|G| \geq 900g^2$ then Case 4 is satisfied. If $\gamma(\mathcal{X}) \neq 0$ then $g(\mathcal{X})$ is odd. Furthermore, if for $P, R \in O_1$ (non-tame short orbit) one has $g(\mathcal{X}/G_P^{(1)}) = 0$ and $G_{P,R}$ is either a p-group or a prime to p group then $\gamma(\mathcal{X}) = 0$.

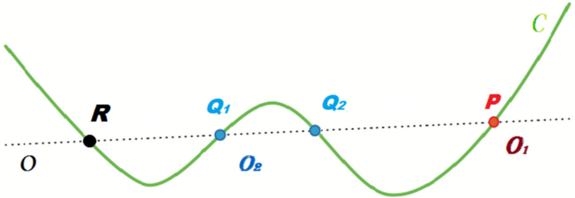
Work in progress: Is it true that if $|G| \geq 900g^2$ then $\gamma(\mathcal{X}) = 0$?

Sketch of the proof of the first item

- By contradiction $|G| > 336g^2$
- Let $O := P^G$ be the unique short orbit of G
- **[Case 1: $\mathbf{O} = \{\mathbf{P}\}$]** Thus, $G = G_P$. Let $\mathcal{X}_1 := \mathcal{X}/G_P^{(1)}$
- If $\mathcal{X}_1$ is not rational $\longrightarrow |G| = |G_P| = |G_P^{(1)} \rtimes H| \leq g(4g+2) < 5g^2$, a contradiction
- Let $\mathcal{X}_1$ be rational. Thus, $G_P = G_P^{(1)} \rtimes H$. If $\alpha \in H$ then α induces an automorphism α' on $\mathcal{X}_1$
- Since every automorphism of a rational function field whose order is prime to p has exactly 2 fixed places $\rightarrow \alpha'$ fixes a place $Q \neq P$
- This implies that Q^G is short and $Q^G \neq O$, a contradiction
- This shows that if $G = G_P$ and Case 3 is satisfied then $|G| < 5g^2$

Sketch of the proof of the first item

- **[Case 2: $\mathbf{O} \supset \{\mathbf{P}\}$]**
- $g(\mathcal{X}/G_P) = 0$ and either $\gamma(\mathcal{X}) = 0$ or $\gamma(\mathcal{X}) > 0$ and G_P, $G_P^{(1)}$ have the same two (non-tame) short orbits
- **First aim**: To prove that the case $\gamma = \gamma(\mathcal{X}) > 0$ is impossible
- If $\gamma > 0$ then G_P has 2 short orbits $O_1 = \{P\}$ and O_2
- $O = \{P\} \cup O_2$
- Since G_P acts transitively on $O_2 = O \setminus \{P\} \longrightarrow G$ acts 2-transitively on O
- **Idea**: Use the complete list of finite 2-transitive groups to exclude the case $\gamma > 0$
- **Second aim**: the case $\gamma = 0$ is not possible from the Deuring-Shafarevic formula



Examples: Curves satisfying case 4

- **Example 1: GK Curve**:

$$\mathcal{C}_n : Y^{n^3+1} + (X^n + X)(\sum_{i=0}^{n}(-1)^{i+1}X^{i(n-1)})^{n+1}) = 0$$

1. $|Aut(\mathcal{C}_n)| = (n^3+1)n^3(n-1) \sim 4g^2$

- **Example 2: Skabelund curves**

$$\tilde{S} : \begin{cases} y^q + y = x^{q_0}(x^q + x), \\ t^m = x^q + x \end{cases}$$

where $q = 2q_0^2 = 2^{2s+1}$ and $m = q - 2q_0 + 1$

1. (Giulietti-M.-Quoos-Zini, 2017) $|Aut(\tilde{S})| = m(q^2+1)q^2(q-1) \sim 4g^2$

Automorphism groups as a tool: classifications and constructions

- Coding theory:
  - (Bartoli-M.-Quoos, 2021) Locally recoverable codes (LRC) from curves of genus $g \geq 1$
  - (Bartoli-M.-Zini, 2021) Construction of self-orthogonal AG codes (quantum codes)
- Classification of maximal curves
  - (Bartoli-M.-Torres, 2021) Classification of $\mathbb{F}_{p^2}$-maximal curves with many automorphisms
- Construction of maximal curves
  - (Giulietti-Kawakita-Lia-M., 2021) Construction of maximal curves of low genus (Kani-Rosen)
  - (Beelen-M.-Niemann-Quoos, 2025) A family of non-isomorphic maximal curves
  - (Beelen-Drue-M.-Zini, 2025) New maximal function fields (as subcovers of the BM maximal curves)

What's next? Some possible interesting questions

- Find a sharp bound for non-solvable automorphism groups of ordinary curves
- Link between automorphism groups and a-number
- For p-rank zero complete the proof $f(g) \sim g^2$
- Classification results for extremal ordinary curves
- Classify maximal curves based on their automorphisms

Maria Montanucci
Department of Applied Mathematics and Computer Science
Technical University of Denmark (DTU)

Building 303B, Room 150
2800 Kgs. Lyngby, Denmark
marimo@dtu.dk