Algebraic curves and their applications

Marco Timpanella

University of Perugia

Young researchers@DMI:

V Workshop of the Department of Mathematics and Computer Science

8 February 2023

Theoretical problems:

1. Automorphism groups of algebraic curves;
2. Curves with many rational points;
3. Castle curves, Frobenius non-classical curves, Galois points...;

Applications:

1. AG codes, locally recoverable codes, PIR codes...;
2. Permutation polynomials, planar functions, APN functions...;
3. Cryptography (ECC, isogeny-based cryptography).

Theoretical problems:

1. Automorphism groups of algebraic curves;
2. Curves with many rational points;
3. Castle curves, Frobenius non-classical curves, Galois points...;

Applications:

1. AG codes, locally recoverable codes, PIR codes...;
2. Permutation polynomials, planar functions, APN functions...;
3. Cryptography (ECC, isogeny-based cryptography).

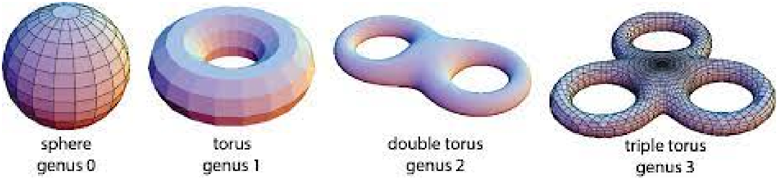
Notation and terminology

$\mathbb{K}$ algebraically closed field of characteristic $p > 0$.

Algebraic curve $\mathcal{X}$: projective (absolutely irreducible, non-singular) algebraic variety of dimension 1 in a projective space $PG(r, \mathbb{K})$.

- Birational geometry $\rightarrow$ curves up to birational maps
- Any algebraic curve $\mathcal{X}$ is birationally equivalent to a (possibly singular) plane curve $\mathcal{C} : F(X, Y, Z) = 0 \longrightarrow$ a plane model of $\mathcal{X}$.

Birational invariants: the genus



$\mathcal{C} : F(X, Y, Z) = 0$ a plane model of $\mathcal{X}$.
The genus $g(\mathcal{X})$ of $\mathcal{X}$ is

$$g(\mathcal{X}) := \frac{1}{2}(\deg(F) - 1)(\deg(F) - 2) - \delta$$

- Lines (and irreducible conics) have genus 0
- Non-singular plane cubics (elliptic curves) have genus 1

Birational invariants: the automorphism group

- $\mathrm{Aut}(\mathcal{X}) = \{\phi : \mathcal{X} \to \mathcal{X} \mid \phi \text{ birational}\}$

Example: the Fermat curve

$$\mathcal{F}_n : X^n + Y^n + Z^n = 0, \quad n \neq p^r.$$

1. $\alpha_1 : (X, Y, Z) \mapsto (X, \lambda Y, \mu Z)$, $\lambda, \mu \in \mathbb{K}$ n-th roots of unity;
2. $\alpha_2 : (X, Y, Z) \mapsto (Y, Z, X)$;
3. $\alpha_3 : (X, Y, Z) \mapsto (X, Z, Y)$.

$$\langle \alpha_1, \alpha_2, \alpha_3 \rangle \leq \mathrm{Aut}(\mathcal{F}_n).$$

Some motivations

"Whatever you have to do with a structure-endowed entity Sigma try to determine its group of automorphisms.
You can expect to gain a deep insight into the constitution of Sigma in this way."
(H. Weyl, *Symmetry*)

- Construction of linear codes with many automorphisms.
- $G \leq \mathrm{Aut}(\mathcal{X})$, G finite. There exists a curve $\mathcal{Y}$ whose points correspond to the G-orbits of $\mathcal{X}$.

  $\mathcal{Y} := \mathcal{X}/G$ is the quotient curve of $\mathcal{X}$ by G.

How many automorphisms?

- If $g(\mathcal{X}) \geq 2$, $\mathrm{Aut}(\mathcal{X})$ is a finite group [Schmid (1938), Iwasawa-Tamagawa (1951), Roquette (1952), Rosentlich (1955), Garcia (1993)]
- Hurwitz bound (1892): If $\mathbb{K} = \mathbb{C}$ and $g(\mathcal{X}) \geq 2$,

$$|\mathrm{Aut}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$$

Example: Klein quartic

$$\mathcal{K} : X^3Z + YZ^3 + XY^3 = 0$$

- $g(\mathcal{K}) = 3$
- $\mathrm{Aut}(\mathcal{K}) = PSL(2, 7)$
- $|\mathrm{Aut}(\mathcal{K})| = 168 = 84(3 - 1) \rightarrow \mathcal{K}$ attains the Hurwitz bound.

The genus 4 case

Klein-Wiman-Edge-..

The maximum size for the automorphism group of a genus 4 complex curve is 120 $\rightarrow$ there is no Hurwitz curve of genus 4!

Example: the Bring's curve

Let $\mathcal{V}$ be the algebraic curve defined by

$$\begin{cases} X_1 + X_2 + X_3 + X_4 + X_5 = 0; \\ X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0; \\ X_1^3 + X_2^3 + X_3^3 + X_4^3 + X_5^3 = 0. \end{cases}$$

- $\mathcal{V}$ is an algebraic curve of genus 4 embedded in $\mathrm{PG}(4, \mathbb{C})$;
- The automorphism group of $\mathcal{V}$ is Sym_5.

A generalization of Bring's curve in any characteristic

Let $\mathcal{V}$ be the algebraic variety of $\mathrm{PG}(m-1,\mathbb{K})$ defined by

$$\begin{cases} X_1 + X_2 + \ldots + X_m = 0; \\ X_1^2 + X_2^2 + \ldots + X_m^2 = 0; \\ \ldots\ldots \\ \ldots\ldots \\ X_1^{m-2} + X_2^{m-2} + \ldots + X_m^{m-2} = 0; \end{cases}$$

- $\mathcal{V}$ is an algebraic curve;
- If $\mathbb{K}$ has zero characteristic, or the characteristic p does not divide $|\mathrm{Aut}(\mathcal{V})|$, then $\mathrm{Aut}(\mathcal{V}) = Sym_m$;
- Examples of maximal curves, connections with the work of Redei, regular sequences.

G. Korchmáros, S. Lia, and M. Timpanella, *A generalization of Bring's curve in any characteristic*, submitted to Mathematische Zeitschrift.

The case of positive characteristic

- Hurwitz bound II: If $p > 0$ and $gcd(p, |\mathrm{Aut}(\mathcal{X})|) = 1$, then

$$|\mathrm{Aut}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$$

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

Example: Hermitian curve

$$\mathcal{H}_q : X^{q+1} + Y^{q+1} + Z^{q+1} = 0, \quad q = p^h$$

- $g(\mathcal{H}_q) = \frac{1}{2}q(q-1)$
- $|\mathrm{Aut}(\mathcal{H}_q)| = |PGU(3,q)| = q^3(q^3+1)(q^2-1)$.

- $|\mathrm{Aut}(\mathcal{X})| \leq 16g(\mathcal{X})^4$ up to one exception (the Hermitian curve) [Stichtenoth (1973)]

A further improvement

Henn (1978): $|\mathrm{Aut}(\mathcal{X})| \leq 8g(\mathcal{X})^3$ up to four exceptions, namely:

- $p = 2$, $\mathcal{X}$ a non-singular model of

$$Y^2 + Y = X^{2^k+1}, \quad k > 1$$

- $p > 2$, $\mathcal{X}$ a non-singular model of

$$Y^2 = X^n - X, \quad n = p^h, \quad h > 0$$

- The Hermitian curve
- The Suzuki curve: $p = 2$, $\mathcal{X}$ a non-singular model of

$$X^{n_0}(X^n + X) = Y^n + Y, \quad n_0 = 2^r, \quad r \geq 1, \quad n = 2n_0^2.$$

Birational invariants: the p-rank

- $\mathcal{X}$ algebraic curve of genus $g \to J_{\mathcal{X}}$ Jacobian variety of dimension g;

  For any prime m,

  $$G_m := \{Q \in J_{\mathcal{X}} \mid [m]Q = 0\}$$

- $m \neq p \longrightarrow |G_m| = m^{2g}$
- $m = p \longrightarrow |G_p| = p^{\gamma} \longrightarrow \gamma =: \gamma(\mathcal{X})$ is the p-rank of $\mathcal{X}$
- $0 \leq \gamma(\mathcal{X}) \leq g(\mathcal{X})$. If $\gamma(\mathcal{X}) = g(\mathcal{X}) \to \mathcal{X}$ is ordinary.

Back to Henn

Henn (1978): $|\mathrm{Aut}(\mathcal{X})| \leq 8g(\mathcal{X})^3$ up to four exceptions, namely:

- $p = 2$, $\mathcal{X}$ a non-singular model of

$$Y^2 + Y = X^{2^k+1}, \quad k > 1$$

- $p > 2$, $\mathcal{X}$ a non-singular model of

$$Y^2 = X^n - X, \quad n = p^h, \quad h > 0$$

- The Hermitian curve
- The Suzuki curve: $p = 2$, $\mathcal{X}$ a non-singular model of

$$X^{n_0}(X^n + X) = Y^n + Y, \quad n_0 = 2^r, \quad r \geq 1, \quad n = 2n_0^2.$$

All these exceptions have zero p-rank!

Links between $\gamma(\mathcal{X})$ and $\text{Aut}(\mathcal{X})$

Theorem (Nakajima, 1987)

- If $\mathcal{X}$ is ordinary ($\gamma(\mathcal{X}) = g(\mathcal{X})$) then

$$|\text{Aut}(\mathcal{X})| \leq 84g(\mathcal{X})(g(\mathcal{X}) - 1)$$

- Let S be a p-subgroup of $\text{Aut}(\mathcal{X})$. If

$$|S| > \frac{2p}{p-1} g(\mathcal{X}),$$

then $\gamma(\mathcal{X}) = 0$

The Hurwitz bound may even fail on $\mathrm{Aut}(\mathcal{X})_P$ for some $P \in \mathcal{X}$, i.e $|\mathrm{Aut}(\mathcal{X})_P| > 84(g(\mathcal{X})-1)$.

- Singh (1974):

$$|\mathrm{Aut}(\mathcal{X})_P| \leq \frac{4pg(\mathcal{X})^2}{p-1}\left(\frac{2g(\mathcal{X})}{p-1}+1\right)$$

- Giulietti, Korchmáros (2018): p odd$\longrightarrow$ if $|\mathrm{Aut}(\mathcal{X})_P| > 30(g(\mathcal{X})-1)$ then either $\mathcal{X}$ is ordinary, or $\mathcal{X}$ has zero p-rank.

- Korchmáros, Montanucci (2018): p odd and $\mathcal{X}$ ordinary $\longrightarrow$ if $|\mathrm{Aut}(\mathcal{X})_P| > 12(g(\mathcal{X})-1)$ then either
  - (i) $|\mathrm{Aut}(\mathcal{X})_P| = 3p^h$, $3 \nmid p$, or
  - (ii) if $\bar{\mathcal{X}} = \mathcal{X}/Q$, Q normal p-subgroup of $\mathrm{Aut}(\mathcal{X})_P$, then $\bar{\mathcal{X}}$ is rational and Q has exactly two short orbits.

Let G be an automorphism group of an ordinary curve $\mathcal{X}$. If

$$|G_P| > 12(g(\mathcal{X}) - 1)$$

then, up to birational equivalence, one of the following holds.

(i) $\mathcal{X}$ has affine equation $L_1(y) = ax + 1/x$, where $a \in \mathbb{K}^*$ and $L_1(T) \in \mathbb{K}[T]$ is a separable p-linearized polynomial of degree q. Furthermore, $\mathcal{X}$ is ordinary.

(ii) $p \neq 3$ and $\mathcal{X}$ has affine equation $L_2(y) = x^3 + bx$, where $b \in \mathbb{K}$ and $L_2(T) \in \mathbb{K}[T]$ a separable p-linearized polynomial of degree q. Furthermore the p-rank of $\mathcal{X}$ is equal to zero.

In Case (i) $\rightarrow$ $\mathcal{X}$ is an ordinary curve
In Case (ii) $\rightarrow$ $\mathcal{X}$ has zero p-rank and $p \neq 3$.

S. Lia and M. Timpanella, *Bound on the order of the decomposition groups of an algebraic curve in positive characteristic*, Finite Fields and Their Applications vol. 69, 101771 (2021)

An alternative proof of Nakajima's bound

Theorem (Lia, T., 2021)

Let $\mathcal{X}$ be a curve of genus $g(\mathcal{X}) \geq 2$ with positive p-rank and let G be a subgroup of $\mathrm{Aut}(\mathcal{X})$. If for every $P \in \mathcal{X}$, $G_P^{(2)} = \{1\}$ then

$$|G| \leq 48(g(\mathcal{X}) - 1)^2. \tag{1}$$

Open problem

Is this bound sharp? (at least for sufficiently large g, up to the constant 48)

- Closest known example: DGZ curve.

M. Giulietti, G. Korchmáros and M. Timpanella, *On the Dickson-Guralnick-Zieve curve*, Journal of Number Theory vol. 196, 114-138 (2019).

The DGZ curve

- $\mathbb{F}_q$ finite field of order $q = p^h$.

$$D_1(x,y,z) = \begin{vmatrix} x & x^q & x^{q^3} \\ y & y^q & y^{q^3} \\ z & z^q & z^{q^3} \end{vmatrix}, \quad D_2(x,y,z) = \begin{vmatrix} x & x^q & x^{q^2} \\ y & y^q & y^{q^2} \\ z & z^q & z^{q^2} \end{vmatrix};$$

- $A \in GL(3,q)$, and $(\bar{x},\bar{y},\bar{z})^t = A(x,y,z)^t$. Then

  $D_1(\bar{x},\bar{y},\bar{z}) = \det(A) D_1(x,y,z)$, and $D_2(\bar{x},\bar{y},\bar{z}) = \det(A) D_2(x,y,z)$.

- The rational function

$$F(x,y,z) = \frac{D_1(x,y,z)}{D_2(x,y,z)}$$

  is $GL(3,q)$-invariant.

The DGZ curve

- $\mathbb{F}_q$ finite field of order $q = p^h$.

$$D_1(x,y,z) = \begin{vmatrix} x & x^q & x^{q^3} \\ y & y^q & y^{q^3} \\ z & z^q & z^{q^3} \end{vmatrix}, \quad D_2(x,y,z) = \begin{vmatrix} x & x^q & x^{q^2} \\ y & y^q & y^{q^2} \\ z & z^q & z^{q^2} \end{vmatrix};$$

- $A \in GL(3,q)$, and $(\bar{x},\bar{y},\bar{z})^t = A(x,y,z)^t$. Then

  $D_1(\bar{x},\bar{y},\bar{z}) = \det(A) D_1(x,y,z)$, and $D_2(\bar{x},\bar{y},\bar{z}) = \det(A) D_2(x,y,z)$.

- The rational function

$$F(x,y,z) = \frac{D_1(x,y,z)}{D_2(x,y,z)}$$

  is $GL(3,q)$-invariant.

The DGZ curve

- $F(x, y, z)$ is an absolutely irreducible (homogeneous) polynomial of degree $q^3 - q^2$.
- The Dickson-Guralnick-Zieve (DGZ) curve is the (absolutely irreducible) plane curve with homogeneous equation $\mathcal{D} : F(x, y, z) = 0$.
- The DGZ curve has genus $g = \frac{1}{2}q(q-1)(q^3 - 2q - 2) + 1$.
- Several properties: (unique) double Frobenius non-classical curve over $\mathbb{F}_q$ and $\mathbb{F}_{q^3}$, combinatorial properties of $\mathcal{D}(\mathbb{F}_{q^3})$, very large automorphism group.

The DGZ curve

- $F(x,y,z)$ is an absolutely irreducible (homogeneous) polynomial of degree q^3-q^2.
- The Dickson-Guralnick-Zieve (DGZ) curve is the (absolutely irreducible) plane curve with homogeneous equation
$\mathcal{D} : F(x,y,z)=0.$
- The DGZ curve has genus $g=\frac{1}{2}q(q-1)(q^3-2q-2)+1$.
- Several properties: (unique) double Frobenius non-classical curve over $\mathbb{F}_q$ and $\mathbb{F}_{q^3}$, combinatorial properties of $\mathcal{D}(\mathbb{F}_{q^3})$, very large automorphism group.

Theorem (Giulietti, Korchmáros, T., 2019)

- $|\mathrm{Aut}(\mathcal{D})| = |PGL(3,q)| = q^3(q^3-1)(q^2-1)$.
- $|\mathrm{Aut}(\mathcal{D})| \approx g^{8/5}$.
- If $q = p$, $\mathcal{D}$ is ordinary.

Guralnick, Zieve (conjecture): Nakajima's bound is not sharp $\rightarrow g^{8/5}$

Theorem (Giulietti, Korchmáros, Lia, T., in preparation)

For a point $P \in \mathcal{X}$, let S_P be the Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})_P$. If $g(\mathcal{X}/S_P) = 0$ and $|\mathrm{Aut}(\mathcal{X})| > 10(g(\mathcal{X})-1)(2\gamma(\mathcal{X})+3)$, then either

- $\gamma(\mathcal{X}) = 0$;
- there exists $g \in \mathrm{Aut}(\mathcal{X})$ such that $S_P \cap S_R = \{1\}$, where $R = g(P)$ and $S_R = gS_Pg^{-1}$.

THANK YOU FOR YOUR ATTENTION