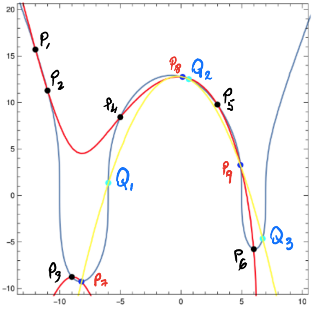
A geometrical interpretation of addition on Jacobian varieties

T. Shaska

(joint work with Y. Kopeliovich)



Outline

Low genus curves

- Conics
- Elliptic curves
- Genus 2 curves
- Hyperelliptic curves

General curves

- Max Noether's Fundamental Theorem
- Noether's Gap Theorem
- Adopted basis at $P \in \mathcal{C}$

Superelliptic curves

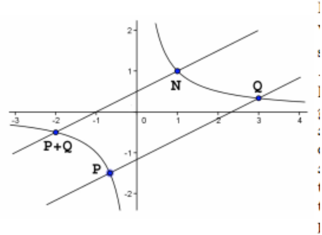
- Hyperelliptic
- Trigonal curves

Further questions

Conics as groups

Lemma

A conic $\mathcal{C}$ has a k-rational point if and only if its discriminant is a square in k.



Lemma

Assume that exists $\mathcal{O} \in \mathcal{C}(\mathbb{Q})$. Then,

- *Fix $\mathcal{O}$ in $\mathcal{C}$. This will be the group identity.*
- *For every two points P and Q in $\mathcal{C}$, from $\mathcal{O}$ draw the parallel line with PQ. This line intersects the conic $\mathcal{C}$ in another point $R \in \mathcal{C}(\mathbb{Q})$.*
- *Define $P \oplus Q := R$.*

Then, $(\mathcal{C}(\mathbb{Q}), \oplus)$ is an Abelian group.

Corollary

Given the conic $\mathcal{C}$ with equation

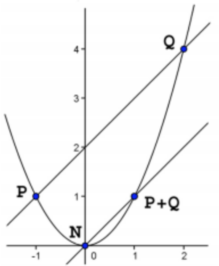
$$ax^2 + bxy + cy^2 + dx + ey = 0,$$

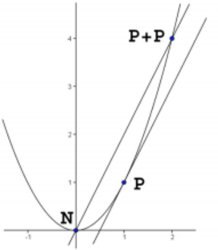
and the point $\mathcal{O}(0,0)$ on it. For every two points $P(\alpha_1, \beta_1)$ and $Q(\alpha_2, \beta_2)$ the formula to compute the coordinates of $P \oplus Q$ is given by

$$P \oplus Q = \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a}, \lambda \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a} \right) \right),$$

where

$$\lambda = \begin{cases} \dfrac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}, & \textit{kur } P \neq Q \\ -\dfrac{2\,a\beta_1 + b\beta_1 + d}{b\alpha_1 + 2\,c\beta_1 + c}, & \textit{if } P = Q \end{cases}$$





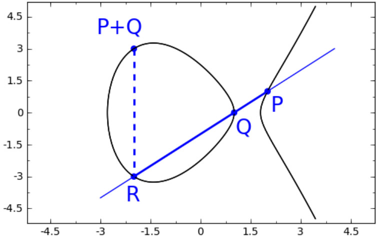
Elliptic curves

A genus 1 curve defined over a field k has equation

$$\mathcal{C}: \quad y^2 = f(x),$$

where $\deg f = 3, 4$. (char $k \neq 2$). We take $\mathcal{O} = \infty$. Hence, $\deg f = 3$. Then we can define a group structure as follows:

- For any two points P, Q, construct the line l going through P and Q.
- From Bezout's theorem, l will intersect $\mathcal{C}$ in a third point R. Take as $P \oplus Q$ the symmetrical of R with respect to the x-axis.



A genus 1 curve with a group structure is called an **elliptic curve**.

Genus 2

Let $\mathcal{C}$ be a genus 2 curve defined over a field k. If $\mathrm{char}\, k \neq 2, 3$ the $\mathcal{C}$ is isomorphic to a curve with equation

$$y^2 = a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0. \tag{1}$$

Thus, infinity is a Weierstrass point of $\mathcal{C}$.
$\mathcal{C}$ can NOT be made into a group. However, it can be embedded into a group, called the **Jacobian** of $\mathcal{C}$,

$$\mathcal{C} \hookrightarrow \mathrm{Jac}\, \mathcal{C} \hookrightarrow \mathcal{C} \times \mathcal{C}$$

So elements of Jac $\mathcal{C}$ are ordered pairs $(P_1, P_2) \in \mathcal{C} \times \mathcal{C}$ (up to some equivalence).
More later ...
So let $D_1, D_2 \in \mathrm{Jac}\, \mathcal{C}$ such that

$$D_1 = (P_1, P_2), \qquad D_2 = (P_3, P_4),$$

where $P_1, P_2, P_3, P_4 \in \mathcal{C}$ and $P_i(x_i, y_i$, for $i = 1, .., 4$.

How can we define $D_1 \oplus D_2$?

We determine a curve $\mathcal{C}'$

$$y = x^3 + b_1 x^2 + b_2 x + b_3, \tag{2}$$

going through the points $P_1, P_2(x_2, y_2), Q_1, Q_2 \in \mathcal{C}$. This cubic will intersect the curve $\mathcal{C}$ at exactly 6 points (Bezout's theorem).

Well ....., no Bezout's theorem is needed here, substitute y from Eq. (2) into Eq. (1). Hence, we have two new points $P_5, P_6 \in \mathcal{C} \cap \mathcal{C}'$.

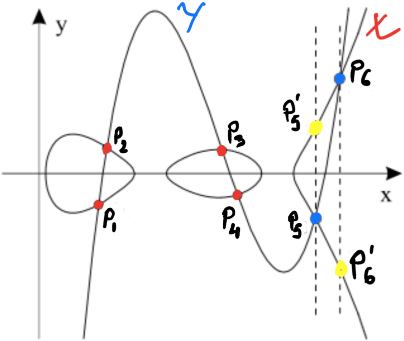
$$x^2 + s_1 x + (b_3^2 - a_5)\frac{1}{s_4} = 0.$$

where $s_1 = x_1 + x_2 + x_3 + x_4$ and $s_4 = x_1 x_2 x_3 x_4$.

$$D_1 = (P_1 + P_2) - 2\infty$$

$$D_2 = (P_3 - P_4) - 2\infty$$

$$D_1 + D_2 = (P_5' + P_6') - 2\infty$$



$D_1 \oplus D_2$ is not (P_5, P_6), but it is (P_5', P_6'), where P_5', P_6' are the symmetric points of P_5, P_6 with respect to the y-axis.

Does this work for higher genii?

Hyperelliptic Jacobians

Consider a genus $g > 2$ hyperelliptic curve with equation

$$y^2 = f(x),$$

where $\deg f = 2g + 1$. Let $D_1, D_2 \in \mathcal{C}^g$, say

$$D_1 = (P_1, \dots, P_g), \qquad D_2 = (P_{g+1}, \dots, P_{2g}) \tag{3}$$

for $P_i(x_1, y_1) \in \mathcal{C}$, $i = 1, \dots, 2g$.
We follow a similar approach and define a curve $\mathcal{C}'$ such that it goes through $P_1, \dots, P_{2g}$ and $\mathcal{C} \cap \mathcal{C}'$ intersect in exactly g new points.
Let $\mathcal{C}'$ be the unique curve going through the points P_i

$$b(x) - yc(x) = 0. \tag{4}$$

In (Cantor, 1987) are determined the degrees of $b(x)$ and $c(x)$ such that $\mathcal{C}'$ intersects $\mathcal{C}$ in $3g$ points. Let $P_{2g+1}, \dots, P_{3g}$ be the new points of intersection and $P_{3g+1}, \dots, P_{4g}$ their symmetrical points with respect to the x-axis. Then,

$$D_1 \oplus D_2 = (P_{3g+1}, \dots, P_{4g}),$$

see (Frey and Shaska, 2019) for details.

Extending to a general curve

Can we extend the above geometrical method to define the group law in Jac $\mathcal{C}$ for a general curve?

Here is what we have:

- A divisor in Jac $\mathcal{C}$ still can be presented by a tuple of points $(P_1, \dots P_g) \in \mathcal{C}^g$.
- How to define the curve $\mathcal{C}'$ that intersects $\mathcal{C}$ in precisely $3g$ points.
- What taking symmetric points with respect to the x-axis would actually mean now? After all a general curve is not symmetric to the x-axis, since its equation is not $y^2 = f(x)$.

We will give a general approach in the remaining of this talk.

There are two main concepts that we will use repeatedly:

- intersection of curves
- Weierstrass points

both of which closely related to Max Noether (1844-1921). (also known for Brill-Noether theory, blowups, rationality of algebraic surfaces,etc)

Max Noether's Fundamental Theorem

Theorem (Noether Fundamental Theorem)

Let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ be three projective plane curves with equations

$$\mathcal{C}_1 : f(x,y,z) = 0, \quad \mathcal{C}_2 : g(x,y,z) = 0, \quad \mathcal{C}_3 : h(x,y,z) = 0,$$

such that $\mathcal{C}_1$ and $\mathcal{C}_2$ have no common components. There exists $A(x,y,z)$ and $B(x,y,z)$ such that

$$h(x,y,z) = A(x,y,z)f(x,y,z) + B(x,y,z)g(x,y,z),$$

with $deg\ A = deg\ g - deg\ f$ and $deg\ B = deg\ h - deg\ g$ if and only if one of the following is satisfied at every $P \in \mathcal{C}_1 \cap \mathcal{C}_2$.

i) *$\mathcal{C}_1$ and $\mathcal{C}_2$ meet transversally at P and $P \in \mathcal{C}_3$.*

ii) *P is simple on $\mathcal{C}_1$ and $(\mathcal{C}_1 \cap \mathcal{C}_3)_P \geq (\mathcal{C}_1 \cap \mathcal{C}_2)_P$*

iii) *$\mathcal{C}_1$ and $\mathcal{C}_2$ have distinct tangents at P, and*

$$mult_P(\mathcal{C}_3) \geq mult_P(\mathcal{C}_1) + mult_P(\mathcal{C}_2) - 1.$$

See (Fulton, 1989, pg. 61) for details. Conditions i), ii), iii) are called Noether conditions. There are many applications of Noether's fundamental theorem, but we are especially interested in the following.

Addition on a cubic

Let $\mathcal{C}$ be a smooth cubic defined over a field k. Fix $\mathcal{O} \in \mathcal{C}(k)$. For $P, Q \in \mathcal{C}(k)$ there is a unique line $\mathcal{C}_1$ such that $\mathcal{C} \bullet \mathcal{C}_1 = P + Q + R$, for some $R \in \mathcal{C}$. Define the function $\varphi : \ \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, such that $(P, Q) \to R$.
Define the addition as

$$P \oplus Q = \varphi(\mathcal{O}, \varphi(P, Q)).$$

Use the figure to show associative property

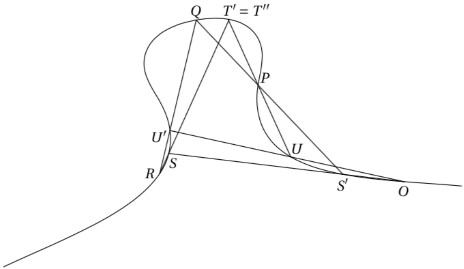


Figure: Associative property: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

We would like to generalize this construction to higher genii.

Noether Gap theorem

Let $P_1, P_2, \dots,$ be a sequence of (not necessarily distinct) points on $\mathcal{C}$. Let

$$D_0 = 0 \quad \text{and } D_k = P_1 + \cdots + P_k.$$

One can ask the following question: **For each nonnegative k, does there exist e meromorphic function f on $\mathcal{C}$ whose polar divisor $(f)_\infty$ satisfies $(f)_\infty \le D_k$ and $(f)_\infty \not\le D_{k-1}$?**

If the answer for a given k is ”No” then we say that k is a **Noether gap** for the sequence $P_1, P_2, \dots,$ otherwise is a **non-gap**.

Theorem (Noether Gap Theorem)

*For any sequence $P_1, P_2, \dots,$ there are **exactly** g Noether gap numbers n_i with*

$$1 = n_1 < n_2 < \cdots < n_g \le 2g - 1.$$

The Weierstrass Gap Theorem is a special case of the Noether Gap theorem, taking $P_i = P$ for all i. It is a direct application of the Riemann-Roch theorem.

Meromorphic function at a point $P \in \mathcal{C}$.

Fix a point $P \in \mathcal{C}$ such that P is a Weierstrass point. We have the following theorem.

Theorem
Any generic collection of points

$$P_1, \dots, P_{g+s} \in \mathcal{C},$$

where $s \geq 0$, can be realized uniquely as zeros of a meromorphic function $\Phi(x, y)$ or order at most $2g + s$ and this function is unique up to multiplication by a constant.

Proof.
A meromorphic function $\Phi(x, y)$ belongs to the function field $k(\mathcal{C})$.

We can consider a basis of $k(\mathcal{C})$ at a Weierstrass point $P \in \mathcal{C}$.

By the Weierstrass gap theorem for a function of order $2g + s$ we will have at most $g + s$ orders at P (as there are no functions at the gaps) and hence this function will be determined uniquely by the $g + s$ points $P_1, \dots, P_{g+s}$.

□

A basis of $k(\mathcal{C})$ adopted to $P \in \mathcal{C}$.

Fix $P \in \mathcal{C}$ and let (x_P, y_P) be a local coordinate around P. By a **basis adapted to** P, we mean a basis

$$\mathcal{B} := \{1, \varphi_1, \varphi_2, \cdots, \varphi_m, \dots\},$$

of the of the function field $k(\mathcal{C})/k$ ordered according to their order at P,

$$\mathrm{ord}_P(\varphi_1) < \dots < \mathrm{ord}_P(\varphi_i) < \dots < \mathrm{ord}_P(\varphi_m).$$

Such basis $\mathcal{B}$ adapted to P is not unique. To make it unique consider the Taylor series expansion of φ_i at P, say

$$\varphi_i(t) = \sum_{j=0}^{\infty} a_{i,j}(t-P)^j$$

and require that $a_{i,j} = 1$ for $i = j$ and $a_{i,j} = 0$ otherwise. The **weight of** P **with respect to** $\mathcal{B}$ is defined as

$$\tau(P) = \sum_{i=1}^{m} (\mathrm{ord}_P(\varphi_i) - i + 1)$$

If P is the place at infinity, then we can assume that $\mathcal{B}$ is a monomial basis. In this case $\mathcal{B}$ is unique.

From now on $P = \infty$ and $\mathcal{B}$ is an adopted monomial basis at P.

Main theorem

Theorem (Kopeliovich-Sh)

Let $\mathcal{C} : F_1(x,y,z) = 0$ be a smooth, projective, genus $g \geq 1$ curve defined over k, $P \in \mathcal{C}(k)$, and $\mathcal{B} = \{1, \varphi_1, \varphi_2, \cdots, \varphi_m, \dots\}$ a basis adapted to P. For any generic set of points $P_1, \dots, P_m \in \mathcal{C}(k)$, for $m \leq 2g$, there exist unique curves $\mathcal{C}'$ and $\mathcal{C}^{"}$ such that:

i) *$\mathcal{C}' : \ F_2(x,y,z) = 0$ is a degree $d_1 = deg\ (\varphi_{m+g})$ curve which meets $\mathcal{C}$ transversally at $(m+g)$ points, say $\mathcal{C} \bullet \mathcal{C}' = \sum_{i=1}^{m+g} P_i$. Then deg $\mathcal{C} \bullet \mathcal{C}' \leq m+g$.*

ii) *$\mathcal{C}^{"} : \ F_3(x,y,z) = 0$ is a degree $d_2 = deg\ \varphi_g$ curve which meets $\mathcal{C}$ transversally at $m+2g$ points and*

$$\mathcal{C} \bullet \mathcal{C}^{"} = \left(\sum_{i=m+1}^{m+g} P_i \right) + \sum_{i=1}^{g} Q_i,$$

for some $Q_1, \dots, Q_g \in \mathcal{C}$.

iii) *There exists polynomials $A, B \in k[x,y,z]$ such that*

$$F_3(x,y,z) = F_1(x,y,z)\, A(x,y,z) + F_2(x,y,z)\, B(x,y,z), \tag{5}$$

with deg $A =$ deg $F_2 -$ deg F_1 and deg $B =$ deg $F_3 -$ deg F_2 .

iv) *If $m = 2g$ then the sum of the zero-cycles $D_1 = \sum_{i=1}^{g} P_i$ and $D_2 = \sum_{j=g+1}^{2g} P_j$ is given by the formula $D_1 + D_2 = \sum_{i=1}^{g} Q_i$.*

Sketch of the proof

For a point $P \in \mathcal{C}$, let $\mathcal{B}$ be a basis $\mathcal{B}$ adapted to P. Given points $P_1, P_2, \ldots, P_m \in \mathcal{C}$, we take the first $(m+1)$ functions $\varphi_1, \ldots, \varphi_{m+1}$ of $\mathcal{B}$ (i.e., the ones with smallest order at P). Define the interpolating matrix A as

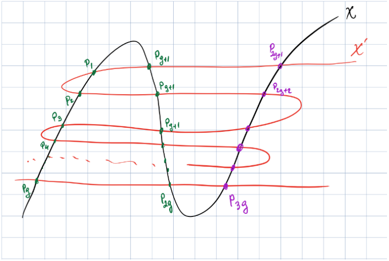
$$A_P(P_1, \ldots P_m) := \begin{bmatrix} \varphi_1(x,y) & \varphi_2(x,y) & \cdots & \varphi_{m+1}(x,y) \\ \varphi_1(x_1,y_1) & \varphi_2(x_1,y_1) & \cdots & \varphi_{m+1}(x_1,y_1) \\ \vdots & \vdots & \cdots & \vdots \\ \varphi_1(x_m,y_m) & \varphi_2(x_m,y_m) & \cdots & \varphi_{m+1}(x_m,y_m) \end{bmatrix} \tag{6}$$

which depends only on the base point $P \in \mathcal{C}$ and the zero-cycle $D = \sum_{i=1}^m P_i$.
Let $\mathcal{C}'$ be the curve defined by

$$\mathcal{C}' : \quad \det A_P(P_1, \ldots P_m) = 0. \tag{7}$$

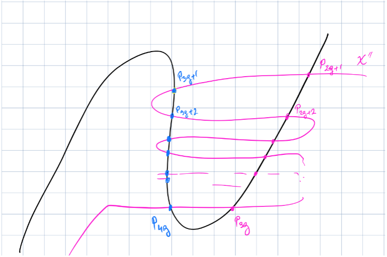
To show that $P_i \in \mathcal{C}'$ for $i = 1, \ldots, m$ it is enough to show that when we substitute (x, y) by (x_i, y_i) in Eq. (6), then $\det A_P(P_1, \ldots P_m) = 0$. But this is obvious since in this case the matrix A_P has two identical rows.

Consider det A. The coefficient of φ_i is $(-1)^{1+j}B_{1j}$, where B_{1j} is the minor. Recall that the poles of $\varphi_1, \ldots, \varphi_m$ have at most order g. Thus we can view the det A as a polynomial in x and y of degree $m+g$, since by clearing out denominators we can only have degree g monomials.



The intersection cycle $\mathcal{C} \bullet \mathcal{C}'$ is principal and generated by the monomials of $\varphi_1, \ldots, \varphi_m$. Since all the monomials have degree $\leq m+g$, this divisor will have degree $\leq m+g$. This completes the proof of i).

To prove part ii) we start with the points $P_{m+1}, \ldots, P_{m+g} \in \mathcal{C}$ and apply part i) to these points. Hence we have a new curve $\mathcal{C}''$ such that it intersects $\mathcal{C}$ in exactly $m + 2g$ points, from which $P_{m+1}, \ldots, P_{m+g}$ are already points of intersection. Denote the new points of intersection by $Q_1, \ldots, Q_g$. Then $\mathcal{C} \bullet \mathcal{C}''$ as claimed.



Part iii) follows from the Thm. 1. Take curves $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ as $\mathcal{C}, \mathcal{C}'$, and $\mathcal{C}''$ respectively. Since $\mathcal{C}$ and $\mathcal{C}'$ meet transversally at all $P \in \mathcal{C} \cap \mathcal{C}'$ then conditions of the Noether's theorem are satisfied. Hence, exist $A, B \in k[x, y, z]$ such that Eq. (5) is satisfied. Let D_1 and D_2 as in the hypothesis of part iv). From Bezout's theorem, $\mathcal{C}_1 \cap \mathcal{C}_2$ is a principal divisor. Hence, $D_1 + D_2 = -\sum_{i=2g+1}^{3g} P_i$. By the same argument, since $\mathcal{C}' \cap \mathcal{C}''$ is a principal divisor then $-\sum_{i=2g+1}^{3g} P_i = \sum_{i=1}^{g} Q_i$.

□

Further details can be found in (Kopeliovich and Shaska, 2019).

Superelliptic curves

Let $\mathcal{C}$ be a genus $g \geq 2$ defined over k such that there exists an order $n > 1$ automorphism $\sigma \in \mathrm{Aut}(\mathcal{C})$ with the following properties:

- σ is central in $\mathrm{Aut}(\mathcal{C})$,
- $\mathcal{C}/\langle\sigma\rangle$ has genus zero.

Such curves are called superelliptic curves and their Jacobians superelliptic Jacobians. They have affine equation

$$\mathcal{C}: \; y^n = f(x) = \prod_{i=1}^{d}(x - \alpha_i) \tag{8}$$

Proposition (Towse)

Let $\mathcal{C}$ be a superelliptic curve with equation Eq. (8), s.t. $\Delta(f) \neq 0$, $\deg f = d > n$, and let $d = sn - e$, for $0 < e < n$. Then a basis for the space of holomorphic differentials is

$$\left\{ x^i \frac{dx}{y^j} \mid 1 \leq j \leq n, \; 1 \leq i \leq b_j \right\},$$

where $b_j = sj - 1 - \left\lfloor \frac{e}{n} j \right\rfloor$.

Proposition (Kopeliovich-Sh)

For every order j at ∞ such that $2g \leq j \leq 3g$ we have a monomial $x^m y^{m_j}$ such that the order of this monomial at ∞ is exactly j.

Let $L(k\infty)$ denote the space of meromorphic functions on $\mathcal{C}$ which are holomorphic on $\mathcal{C} \setminus \{\infty\}$ and have poles of order at most k at ∞. From the Riemann-Roch we have

$$\dim(L(N+g-1)\infty) = N, \quad \text{for} \quad N \geq g.$$

Consider the space

$$L(\star\infty) := \cup_{k=1}^{\infty} L(k\infty),$$

of meromorphic functions on $\mathcal{C}$ which are holomorphic on $\mathcal{C} \setminus \{\infty\}$. This is the space of polynomials on x and y. Then we have the following.

Lemma

A basis of $L(k\infty)$ over k is given by

$$\mathcal{B} := \left\{ x^i y^j, \ 0 \leq i \leq d, \ 0 \leq j \leq n-1, \right\}$$

which is the adopted monomial basis of $P = \infty$.

We can put these monomials in a matrix $B = [b_{i,j}]$ such that $b_{i,j} = x^i y^j$. So the matrix will have n rows and at most $d + 1$ columns and in the j-th row it will have monomials $y^{j-1} x^i$, for $i = 0, 1, \dots d$. For a meromorphic function $f = x^i y^j$, the $\operatorname{ord}_\infty f$ is

$$\operatorname{ord}_\infty x^i y^j = ni + dj.$$

In particular,

$$\operatorname{ord}_\infty x^i = n \cdot i \quad \text{and} \quad \operatorname{ord}_\infty y^j = d \cdot j.$$

We order the basis of $L(\star\infty)$ according to the order at ∞. Let $\{\varphi_i\}$ be the monomial basis of $L(\star\infty)$ ordered as

$$0 = \operatorname{ord}_\infty \varphi_1 < \operatorname{ord}_\infty \varphi_2 < \operatorname{ord}_\infty \varphi_3 < \dots .$$

Notice that $\operatorname{ord}_\infty 1 = 0$, $\operatorname{ord}_\infty x = n$, $\operatorname{ord}_\infty y = d$. The first monomials will be

$$1, x, \dots, x^r, y, \dots$$

for $r = \left\lfloor \frac{d}{n} \right\rfloor$. Hence, if we fill the matrix B only with the first $2g + 1$ monomials and assign zeroes to all the other entries then we call it the **corresponding matrix** to the curve $\mathcal{C}$ and denote it by $B_{\mathcal{C}}$ or in case of superelliptic curves $B_{n,d}$. For a given curve $\mathcal{C}$ we want to determine it corresponding matrix $B_{\mathcal{C}}$.

Example

Consider $n = 4$ and $d = 13$. Then we have a curve $\mathcal{C}$ of genus $g = 18$. The possible orders of monomials $x^i y^j$ at ∞ are

$$0, 4, 8, 12, 13, 16, 17, 20, 21, 24, 25, 26, 28, 29, 30, 32, 33, 34, 36, 37, 38, 39, 40, 41, 42,$$
$$43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54;$$
$$55, 57, 58, 59, 61, 62, 63, 65, 66, 67, 70, 71, 74, 75, 78, 79, 83, 87, 91.$$

The first $2g + 1$ monomials are:

$$1, x, x^2, x^3, y, x^4, xy, x^5, x^2y, x^6, x^3y, y^2, x^7, x^4y, xy^2, x^8, x^5y, x^2y^2, x^9, x^6y, x^3y^2,$$
$$y^3, x^{10}, x^7y, x^4y^2, xy^3, x^{11}, x^8y, x^5y^2, x^2y^3, x^{12}, x^9y, x^6y^2, x^3y^3, x^{12}, x^9y, x^6y^2,$$
$$x^2y^3, x^{13}, x^{10}y, x^7y^2.$$

However, if we rearrange the monomials to their monomial ordering we have

$$1, x, x^2, \ldots, x^{13}, y, yx, yx^2, \ldots, yx^{10}, y^2, y^2x, \ldots, y^2x^7, y^3, y^3x, y^3x^2, y^3x^3.$$

The matrix B in this case is

$$B_{4,13} = \begin{bmatrix} 1 & x & x^2 & x^3 & \ldots & x^7 & \ldots & x^{10} & \ldots & x^{11} & \ldots & x^{13} \\ y & xy & x^2y & x^3y & \ldots & x^7y & \ldots & x^{10}y & 0 & 0 & 0 & 0 \\ y^2 & xy^2 & x^2y^2 & x^3y^2 & \ldots & x^7y^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ y^3 & xy^3 & x^2y^3 & x^3y^3 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \end{bmatrix}$$

□

We try to generalize for the case $B_{n,d}$. Assuming deg $x = n$ and deg $y = d$ we explicitly give the first $2g + 1$ monomials.

Theorem (Kopeliovich-Sh)

Let $\mathcal{C}$ be a superelliptic curve with affine equation $y^n = f(x)$, where deg $f = d$ and $(n, d) = 1$. Then $B_{n,d}$ is an $n \times (d+1)$ matrix and the non-zero entries in the j-th row, for $j = 0, \ldots, n-1$, are given by monomials are given by $x^i y^j$ for $0 \leq i \leq \left\lfloor \frac{3g - jd}{n} \right\rfloor$.

Corollary

The degree of the curve $\mathcal{Y}$ is given by

$$deg\, \mathcal{Y} = \max \left\{ \frac{3g - j(d-n)}{n} \;:\; 0 \leq j \leq n-1, 0 \leq i \leq \left\lfloor \frac{3g - jd}{n} \right\rfloor \right\}$$

Corollary

$\mathcal{Y}$ has genus zero if and only if $\mathcal{C}$ is hyperelliptic. In this case y is given as a rational function in x.

As an application to our method, let us now consider the simplest case of superelliptic curves, namely $n = 2$. From above we have that the list the non-gaps for hyperelliptic curves are:

$$0, 2, 4, 6, \dots, 2g, 2g+2, \dots$$

The function field $k(\mathcal{C})$ is generated by

$$\mathcal{B} = \{1, x, x^2, x^3, \dots, x^g, y, yx, yx^2, yx^3, \dots, yx^g\}.$$

We take these monomials according to increasing order at ∞, which is given by

$$\mathrm{ord}_\infty x^i y^j = 2i + (2g+1)j.$$

Then, we can reorder $\mathcal{B}$ ordering according to ord_∞ and have the following:

Lemma

Let $\mathcal{C}$ be a genus $g \geq 2$ hyperelliptic curve and $s := \left\lfloor \frac{g-1}{2} \right\rfloor$. The first $2g+1$ monomials of the basis $\mathcal{B}$, ordered according to their order at ∞ are

$$1, x, x^2, x^3, \dots, x^g, y, x^{g+1}, yx, x^{g+2}, yx^2, x^{g+3}, yx^3, \dots, x^{g+s}, yx^s,$$

if g is odd and

$$1, x, x^2, x^3, \dots, x^g, y, x^{g+1}, yx, x^{g+2}, yx^2, x^{g+3}, yx^3, \dots, x^{g+s}, yx^s, x^{g+s+1}$$

if g is even.

Let $P_i := (x_i, y_i)$, $i = 1, \ldots, 2g$ and consider the matrix A as defined in Eq. (6). As before $\mathcal{Y} : \det A(P_1, \ldots, P_{2g}) = 0$. Notice that the equation of $\mathcal{Y}$ is linear in y. Hence, y can be expressed as a rational function

$$y = \frac{h(x)}{g(x)},$$

where $\deg h = g + s$ when g is odd and $\deg h = g + s + 1$ when g is even. The degree of the denominator is $\deg g = s$.

The addition of divisors in hyperelliptic Jacobians is done via Cantor's algorithm. A geometric interpretation of that addition is given by Leitenberger (Leitenberger, 2005).

The results here match exactly those in (Cantor, 1987) and (Leitenberger, 2005), where the interpolating curve becomes and interpolating rational function.

Examples

Example (Genus 2)

Consider the case of genus 2. Hence, $n = 2$ and $d = 5$. The possible orders at ∞ are

$$0, 2, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15$$

and the corresponding monomials

$$\mathcal{B} = \{1, x, x^2, y, x^3, xy, x^4, x^2y, x^5, x^3y, x^4y, x^5y.\}$$

The matrix $\mathcal{B}_{2,5}$ is

$$\mathcal{B}_{2,5} = \begin{vmatrix} 1 & x & x^2 & x^3 \\ y & 0 & 0 & 0 \end{vmatrix}$$

Taking the first $2g + 1 = 5$ monomials we have the basis

$$\mathcal{B} = \{1, x, x^2, y, x^3\}$$

and the curve $\mathcal{Y}$ is

$$c_0 + c_1x + c_2x^2 + c_3y + c_4x^3 = 0.$$

Hence, as previously known, y is a cubic polynomial in x. □

Example (Genus 3 hyperelliptic)

Let $\mathcal{C}$ be the genus 3 hyperelliptic curve with equation $y^2 = f(x)$, where deg $f = 7$. Then $n = 2$ and $d = 7$. The matrix $B_{2,7}$ is

$$B_{2,7} = \begin{bmatrix} 1 & x & x^2 & x^3 & x^4 \\ y & yx & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

So we have the first seven orders at ∞ as

$$0, 2, 4, 6, 7, 8, 9$$

and the corresponding monomials $\{1, x, x^2, x^3, y, x^4, yx\}$. hence our basis will be

$$\mathcal{B} = \{1, x, x^2, x^3, y, x^4, yx\}$$

In this case, $\mathcal{Y}$ will be a curve with equation of the form

$$c_0 + c_1x + c_2x^2 + c_3x^3 + c_4y + c_5x^4 + c_6yx = 0.$$

Hence,

$$y = -\frac{c_0 + c_1x + c_2x^2 + c_3x^3 + c_5x^4}{c_4 + c_6x}$$

is a rational function $y = \frac{h(x)}{g(x)}$, where deg $h = 4$ and deg $g = 1$.

□

Both the above cases are of special interest in hyperelliptic curve cryptography.

Trigonal curves

Lemma

For trigonal curves with equation $y^3 = f(x)$ such that $\deg f = d$, the first $2g + 1$ monomials of our basis $\mathcal{B}$ are

$$1, x, x^2, \ldots, x^{d-1},\ y, yx, \ldots, yx^s,\ y^2, y^2x, \ldots, y^2x^q,$$

where s and q are as follows:

i) *if $d \equiv 1 \mod 3$ then $q = \frac{d-1}{3}$ and $s = 2\frac{d-1}{3}$.*

ii) *if $d \equiv 2 \mod 3$ then $q = \frac{d-2}{3}$ and $s = \frac{d-5}{6}$*

Notice that in both cases $s + q = d - 1$ and $q = \left\lfloor \frac{s}{2} \right\rfloor$. We define $\mathcal{Y}$ as before. Then $\mathcal{Y}$ is a hyperelliptic curve of genus $\frac{d-1}{2}$ or $\frac{d-3}{2}$.

Next we give the first non-trivial example of non-hyperelliptic curves.

Picard curves

Example

A Picard curve has a degree three superelliptic projection $\pi : \mathcal{C} \to \mathbb{P}^1$. This covering has five branch points, one of which we have specified at infinity. The curve has equation

$$\mathcal{C} : \quad y^3 = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \tag{10}$$

The gap sequence is

$$0, 3, 4, 6, 7, 8, 9, 10, \dots$$

with matrix $B_{3,4}$ being

$$B_{3,4} = \begin{bmatrix} 1 & x & x^2 & x^3 \\ y & yx & 0 & 0 \\ y^2 & 0 & 0 & 0 \end{bmatrix}$$

and the ordered basis $\mathcal{B}$ is

$$1, x, y, x^2, xy, y^2, x^3, \tag{11}$$

For six given generic points $P_i(x_i, y_i) \in \mathcal{C}$, the equation of the curve $\mathcal{Y}$ is $\det A = 0$, *where*

$$A = \begin{bmatrix} 1 & x & x^2 & x^3 & y & xy & y^2 \\ 1 & x_1 & x_1^2 & x_1^3 & y_1 & x_1 y_1 & y_1^2 \\ 1 & x_2 & x_2^2 & x_2^3 & y_2 & x_2 y_2 & y_2^2 \\ 1 & x_3 & x_3^2 & x_3^3 & y_3 & x_3 y_3 & y_3^2 \\ 1 & x_4 & x_4^2 & x_4^3 & y_4 & x_4 y_4 & y_4^2 \\ 1 & x_5 & x_5^2 & x_5^3 & y_5 & x_5 y_5 & y_5^2 \\ 1 & x_6 & x_6^2 & x_6^3 & y_6 & x_6 y_6 & y_6^2 \end{bmatrix}$$

Example

Let $\mathcal{C}$ be the Picard curve defined over $\mathbb{R}$ and given by the equation

$$\mathcal{C} : y^3 = (x+12)(x+11)(x+9)(x+5)(x-3)(x-6),$$

over $\mathbb{R}$ and P_i, for $i = 1, \dots, 6$ points on the curve with x-coordinate -12, -11, -9, -5, 3, 6. Then the ordered basis $\mathcal{B}$ is as in Eq. (11)*.*
Given two divisors

$$D_1 = P_1 + P_2 + P_3 - 3\infty \quad \textit{and} \quad D_2 = P_4 + P_5 + P_6 - 3\infty$$

Then the curve $\mathcal{Y}$ has equation

$$\begin{aligned}\mathcal{Y} : \quad & -1.31136 \cdot 10^{11} - 5.1418910^9 x + 3.69043 \cdot 10^9 x^2 + 3.15371 \cdot 10^8 x^3 \\ & + (5.77794 \cdot 109 + 5.01093 \cdot 10^8 x) y + 3.51232 \cdot 108 y^2 = 0\end{aligned}$$

It is an elliptic curve and it intersects the curve $\mathcal{C}$ in exactly 9 points as in **??***. The blue points in the picture are the new points P_7, P_8, P_9 and*

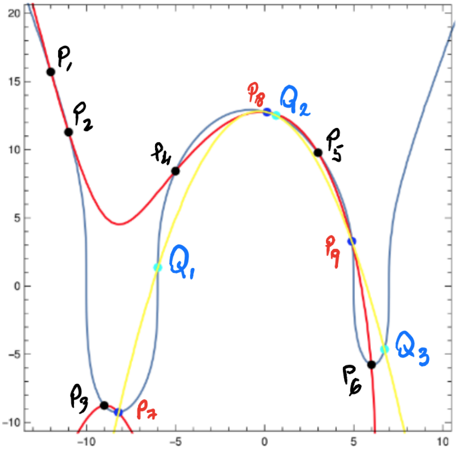
$$-(D_1 + D_2) = P_7 + P_8 + P_9 - 3\infty. \tag{12}$$

Addition on a Picard curve

To find $D_1 + D_2$ we need to invert $D_1 + D_2$ given in Eq. (12). So from Eq. (11) we pick the first 4 monomials, namely $1, x, y, x^2$. Then, the curve $\mathcal{Y}$ for this basis will be

$$\mathcal{Y}: \quad 6658.85 - 110.278x - 183.934x^2 - 520.488y = 0$$

which intersect $\mathcal{C}$ in precisely 6 points. The three new points colored in light blue are denoted by Q_1, Q_2, Q_3. Then $D_1 + D_2 = Q_1 + Q_2 + Q_3 - 3\infty$. □



Further questions

- Torsion points (geometric interpretation)
- Isogenies, (modular surfaces .....)
- Characteristic $p > 0$.

References

Cantor, David G. 1987. *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48**, no. 177, 95–101. MR866101

Frey, Gerhard and Tony Shaska. 2019. *Curves, Jacobians, and cryptography*, Algebraic curves and their applications, pp. 279–344. MR3916746

Fulton, William. 1989. *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. MR1042981

Kopeliovich, Yaacov and Tony Shaska. 2019. *The addition on Jacobian varieties from a geometric viewpoint*.

Leitenberger, Frank. 2005. *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46**, no. 1, 125–130. MR2146447

Thank you for your attention!