Deciding trigonality of algebraic curves

J. Schicho and D. Sevilla

Johann Radon Institute for Computational and Applied Mathematics (RICAM)
Linz, Austria

General framework: radical parametrizations

Rational vs. radical parametrizations

An algebraic curve can be rationally parametrized iff it has genus 0.

But many more curves can be parametrized if we allow radicals.

General framework: radical parametrizations

Rational vs. radical parametrizations

An algebraic curve can be rationally parametrized iff it has genus 0.

But many more curves can be parametrized if we allow radicals.

Examples

All elliptic curves (genus 1) can be expressed as $y^2 = x^3 + ax + b$.
This can be parametrized as $x = t$, $y = \sqrt{t^3 + at + b}$.

Similarly, all hyperelliptic curves (genus ≥ 2) can be written as $y^2 = P(x)$, thus they can be parametrized using one square root.

General framework: radical parametrizations

Rational vs. radical parametrizations

An algebraic curve can be rationally parametrized iff it has genus 0.

But many more curves can be parametrized if we allow radicals.

Examples

All elliptic curves (genus 1) can be expressed as $y^2 = x^3 + ax + b$. This can be parametrized as $x = t$, $y = \sqrt{t^3 + at + b}$.

Similarly, all hyperelliptic curves (genus ≥ 2) can be written as $y^2 = P(x)$, thus they can be parametrized using one square root.

The big problem

Given an algebraic curve, to de$\mathbb{C}$ide whether it admits a radical parametrization, and in the affirmative case to $\mathbb{C}$ompute one.

Trigonality

Definition

The gonality of a curve C is the minimum $n \in \mathbb{N}$ such that there exists an $n : 1$ rational map from C to $\mathbb{P}^1$ (if you prefer, the curve has a g^1_n).

- gonality 3 =: trigonality
- gonality 2 = hyperellipticity

Trigonality

Definition

The gonality of a curve C is the minimum $n \in \mathbb{N}$ such that there exists an $n:1$ rational map from C to $\mathbb{P}^1$ (if you prefer, the curve has a g_n^1).

- gonality 3 =: trigonality
- gonality 2 = hyperellipticity

Trigonality and parametrizability by radicals

In general, inverting a map to $\mathbb{P}^1$ produces a non-rational parametrization.

But inverting a $3:1$ map amounts to solving a degree 3 polynomial in one variable, which can always be done with radicals.

Trigonality

Definition

The gonality of a curve C is the minimum $n \in \mathbb{N}$ such that there exists an $n : 1$ rational map from C to $\mathbb{P}^1$ (if you prefer, the curve has a g^1_n).

- gonality 3 =: trigonality
- gonality 2 = hyperellipticity

Trigonality and parametrizability by radicals

In general, inverting a map to $\mathbb{P}^1$ produces a non-rational parametrization.

But inverting a $3 : 1$ map amounts to solving a degree 3 polynomial in one variable, which can always be done with radicals.

Our result

An algorithm that decides whether a curve with $g \geq 2$ is trigonal and computes a $3 : 1$ map to $\mathbb{P}^1$ in the affirmative case.

Divisors on a trigonal curve

Linear systems: intuitive idea

A g_3^1 is a one-dimensional family of formal sums $P + Q + R$ of points in C such that the difference of any two sums is the zeros and poles of a function on C.

Divisors on a trigonal curve

Linear systems: intuitive idea

A g^1_3 is a one-dimensional family of formal sums $P + Q + R$ of points in C such that the difference of any two sums is the zeros and poles of a function on C.

Passing to the canonical image

The canonical map $\kappa\colon C \to \mathbb{P}^{g-1}$ is an embedding iff C is not hyperelliptic.

Divisors on a trigonal curve

Linear systems: intuitive idea

A g^1_3 is a one-dimensional family of formal sums $P+Q+R$ of points in C such that the difference of any two sums is the zeros and poles of a function on C.

Passing to the canonical image

The canonical map $\kappa\colon C \to \mathbb{P}^{g-1}$ is an embedding iff C is not hyperelliptic.

Using the geometric Riemann-Roch theorem

By the geometric version of Riemann-Roch, the image by κ of each triple of points is a collinear triple in $\mathbb{P}^{g-1}$.

A g^1_3 of C gives rise to a pencil of lines in $\mathbb{P}^{g-1}$ such that each line intersects $\kappa(C)$ in three points.

Classical results on trigonality

Theorem (Enriques 1919, Babbage 1939)

Let C be a canonical curve. Let Q be the intersection of the quadrics containing it. Then $C = Q$ except when C is trigonal or a plane quintic.

(When $C \subsetneq Q$, what is Q?)

Classical results on trigonality

Theorem (Enriques 1919, Babbage 1939)

Let C be a canonical curve. Let Q be the intersection of the quadrics containing it. Then $C = Q$ except when C is trigonal or a plane quintic.

(When $C \subsetneq Q$, what is Q?)

Theorem (Griffiths & Harris, 1978)

Any canonical curve C satisfies exactly one of these:

- $C = Q$;
- C is trigonal, and Q is the rational normal scroll swept out by the trisecants;
- C is a plane quintic, and Q is the Veronese surface in $\mathbb{P}^5$, swept out by the conic curves through five coplanar points of the curve.

Sketch of trigonal algorithm

Algorithm

INPUT: a non-hyperelliptic curve C of genus ≥ 3.
OUTPUT: TRUE and a 3:1 map $C \to \mathbb{P}^1$, or FALSE.

1. Compute the canonical map $\kappa\colon C \to \mathbb{P}^{g-1}$.
2. Compute the intersection Q of all quadrics that contain $\kappa(C)$.
3. Recognize Q.
   1. If $Q = \kappa(C)$ then return FALSE.
   2. If $Q \cong \mathbb{P}^2$ or a rat. normal scroll then compute an isomorphism,
   3. else return FALSE (Veronese).
4. Q is a ruled surface, so compute $\pi\colon Q \to \mathbb{P}^1$.
5. Return TRUE and the map $C \to \cdots \to \mathbb{P}^1$.

Sketch of trigonal algorithm

Algorithm

INPUT: a non-hyperelliptic curve C of genus ≥ 3.
OUTPUT: TRUE and a 3:1 map $C \to \mathbb{P}^1$, or FALSE.

1. Compute the canonical map $\kappa\colon C \to \mathbb{P}^{g-1}$.
2. Compute the intersection Q of all quadrics that contain $\kappa(C)$.
3. Recognize Q.
    1. If $Q = \kappa(C)$ then return FALSE.
    2. If $Q \cong \mathbb{P}^2$ or a rat. normal scroll then compute an isomorphism,
    3. else return FALSE (Veronese).
4. Q is a ruled surface, so compute $\pi\colon Q \to \mathbb{P}^1$.
5. Return TRUE and the map $C \to \cdots \to \mathbb{P}^1$.

How to solve the recognition problem?

The classification of Q and the computation of an isomorphism to the model are done with the Lie algebra method.

The Lie algebra method

Problem

Let M be a "known" variety (a model) and X an arbitrary variety. We want to recognize constructively whether $X \cong M$.

The Lie algebra method

Problem

Let M be a "known" variety (a model) and X an arbitrary variety. We want to recognize constructively whether $X \cong M$.

Idea

1. Precompute or load the Lie algebra associated to M, $L(M)$.
2. Compute $L(X)$.
3. If we can constructively recognize $L(X) \cong L(M)$ or parts of them, maybe we can go back and get an isomorphism $X \longleftrightarrow M$ (via Lie algebra representations).

References

- de Graaf, Harrison, Pílniková, Schicho (JoA 2006)
- Harrison, Schicho (ISSAC 2006)
- de Graaf, Pílniková, Schicho (JSC 2009)

The Lie algebra of a variety

Construction

Given $X \subseteq \mathbb{P}^n$, consider the group

$$\mathrm{Aut}_{\mathcal{L}}(X) := \{\sigma \in \mathrm{Aut}(\mathbb{P}^n) : \sigma(X) = X\} \subseteq \mathrm{PGL}(n+1).$$

We define $L(X)$ to be the Lie algebra associated to the group (that is, the tangent space at the identity).

Examples

- $L(\mathit{curve})$ is trivial in general!
- $L(\mathbb{P}^2) = \mathfrak{sl}_2 = \{\text{Trace zero matrices with } [a, b] = ab - ba\}$

The Lie algebra of a variety

Construction

Given $X \subseteq \mathbb{P}^n$, consider the group

$$\mathrm{Aut}_{\mathcal{L}}(X) := \{\sigma \in \mathrm{Aut}(\mathbb{P}^n) : \sigma(X) = X\} \subseteq \mathrm{PGL}(n+1).$$

We define $L(X)$ to be the Lie algebra associated to the group (that is, the tangent space at the identity).

Examples

- $L(\textit{curve})$ is trivial in general!
- $L(\mathbb{P}^2) = \mathfrak{sl}_2 = \{\text{Trace zero matrices with } [a, b] = ab - ba\}$

Levi subalgebras

The Levi subalgebra L_0 of a Lie algebra L is the semisimple part of L. It can be computed explicitely.

Rational normal scrolls

Definition

A rational normal scroll $S_{m,n}$ is the Zariski closure of the image of $(s,t) \mapsto (1 : s : s^2 : \ldots : s^m : t : st : s^2t : \ldots : s^n t)$. It is defined by equations of degree two involving four terms each.

We will not consider $L(S_{m,n})$ but only its Levi subalgebra, which is $\mathfrak{sl}_2$ for $m \neq n$.

Rational normal scrolls

Definition

A rational normal scroll $S_{m,n}$ is the Zariski closure of the image of $(s,t) \mapsto (1 : s : s^2 : \ldots : s^m : t : st : s^2t : \ldots : s^n t)$. It is defined by equations of degree two involving four terms each.

We will not consider $L(S_{m,n})$ but only its Levi subalgebra, which is $\mathfrak{sl}_2$ for $m \neq n$.

Constructive recognition of $\mathfrak{sl}_2$

- it is the only semisimple Lie algebra of dimension 3 over the complex numbers;
- compute a Chevalley basis $\rightarrow$ isomorphism.

Rational normal scrolls

Definition

A rational normal scroll $S_{m,n}$ is the Zariski closure of the image of $(s,t) \mapsto (1 : s : s^2 : \ldots : s^m : t : st : s^2t : \ldots : s^nt)$. It is defined by equations of degree two involving four terms each.

We will not consider $L(S_{m,n})$ but only its Levi subalgebra, which is $\mathfrak{sl}_2$ for $m \neq n$.

Constructive recognition of $\mathfrak{sl}_2$

- it is the only semisimple Lie algebra of dimension 3 over the complex numbers;
- compute a Chevalley basis → isomorphism.

Conclusion: first test

If $L_0(X)$ is not $\mathfrak{sl}_2$, X is not a scroll. Otherwise, we get an isomorphism $\mathfrak{sl}_2 \to L_0(X)$.

Irreducible representations of $\mathfrak{sl}_2$

Theorem

Every finite-dimensional irreducible representation $\rho : \mathfrak{sl}_2 \to \mathfrak{gl}(W)$ of dimension $k + 1 > 1$ is conjugate to $\mathfrak{sl}_2 \to \mathfrak{gl}(Sym^k(V_2))$ with

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mapsto \begin{pmatrix} k & & & & \\ & k-2 & & & \\ & & \ddots & & \\ & & & -(k-2) & \\ & & & & -k \end{pmatrix}$$

(Note the set of eigenvalues.)

Representations of $L_0(S_{m,n})$

Two representations

$$\begin{tikzcd}
\mathfrak{sl}_2 \arrow[r, hook] \arrow[d, "\cong"] & L(S_{m,n}) \arrow[r, hook] & \mathfrak{sl}_{m+n+2} \arrow[r, hook] & \mathfrak{gl}_{m+n+2} \\
L_0(X) \arrow[r, hook] & L(X) \arrow[r, hook] & \mathfrak{sl}_{m+n+2} \arrow[r, hook] & \mathfrak{gl}_{m+n+2}
\end{tikzcd}$$

The top representation splits into $\mathfrak{gl}(Sym^n(V_2))$ and $\mathfrak{gl}(Sym^m(V_2))$. Thus the bottom one must split in the same way.

Representations of $L_0(S_{m,n})$

Two representations

$$\begin{tikzcd}
\mathfrak{sl}_2 \arrow[r, hook] \arrow[d, "\cong"] & L(S_{m,n}) \arrow[r, hook] & \mathfrak{sl}_{m+n+2} \arrow[r, hook] & \mathfrak{gl}_{m+n+2} \\
L_0(X) \arrow[r, hook] & L(X) \arrow[r, hook] & \mathfrak{sl}_{m+n+2} \arrow[r, hook] & \mathfrak{gl}_{m+n+2}
\end{tikzcd}$$

The top representation splits into $\mathfrak{gl}(Sym^n(V_2))$ and $\mathfrak{gl}(Sym^m(V_2))$. Thus the bottom one must split in the same way.

Second test

If the bottom representation splits in two irreducible components, their dimensions give m, n. The eigenvalues must be the union of two sets as before. An isomorphism between modules is obtained by getting a good basis: eigenvectors.

Pulling back the module map

Theorem

Every automorphism of an irreducible module over a semisimple algebra is a scalar multiplication.

Corollary

The previous pair of conjugate representations induces a map between the vector spaces, unique up to scalar multiplication

$$\sigma\colon K^{m+n+2} \to K^{m+n+2} \quad \Rightarrow \quad \sigma\colon \mathbb{P}^{m+n+1} \to \mathbb{P}^{m+n+1}$$

This is the isomorphism we want.

Pulling back the module map

Theorem

Every automorphism of an irreducible module over a semisimple algebra is a scalar multiplication.

Corollary

The previous pair of conjugate representations induces a map between the vector spaces, unique up to scalar multiplication

$$\sigma \colon K^{m+n+2} \to K^{m+n+2} \quad \Rightarrow \quad \sigma \colon \mathbb{P}^{m+n+1} \to \mathbb{P}^{m+n+1}$$

This is the isomorphism we want.

Last step: projection

If successful, we have a map between X and the rational normal scroll in the form described before. It is trivial to write a map from the scroll to $\mathbb{P}^1$.

Summary

- A classical theorem tells us what is the surface of quadrics containing a trigonal curve: a rational normal scroll.
- We can recognize this surface constructively using Lie algebras.
- The Levi subalgebra of a scroll is easy to recognize.
- If this step is successful, we obtain two representations. If conjugate, they are related by a map that can be turned into a projective isomorphism.
- The scroll in canonical form has an obvious map to $\mathbb{P}^1$. Composition with it provides the final $3:1$ map.