

Determinantal representations of cubic curves

Anita Buckley and Tomaž Košir

Department of Mathematics
Faculty of Mathematics and Physics
University of Ljubljana
Slovenia

Conference on Geometry: Theory and Applications

24-28 June 2013



University of Ljubljana
Faculty of Mathematics and Physics

Outline

- 1 Introduction
 - Background
 - Notation
- 2 Determinantal representations
 - Definition
 - Existence
- 3 Weierstrass form
 - Canonical form
 - Inflection point
 - Algorithm
- 4 Determinantal representation of Weierstrass cubic
 - Explicit Construction
 - Definite representation
 - Semidefinite programming

Background

Elliptic curves have profound influence in mathematics. Since ancient times they turn up in the most astonishing places, joining together algebra and geometry. Recently they have become popular in **number theory** (cryptography of elliptic curves), **optimization** (semidefinite programming SDP) and also in **theoretical physics** (mirror symmetry of elliptic curves).

The abundance of results is due to the following two classical facts for smooth plane cubics:

- It can be brought by a change of coordinates into the Weierstrass canonical form, or equivalently the Hesse canonical form.
- It can be equipped by a group law (induced by the Jacobian group variety).

Background

Elliptic curves have profound influence in mathematics. Since ancient times they turn up in the most astonishing places, joining together algebra and geometry. Recently they have become popular in **number theory** (cryptography of elliptic curves), **optimization** (semidefinite programming SDP) and also in **theoretical physics** (mirror symmetry of elliptic curves).

The abundance of results is due to the following two classical facts for smooth plane cubics:

- It can be brought by a change of coordinates into the Weierstrass canonical form, or equivalently the Hesse canonical form.
- It can be equipped by a group law (induced by the Jacobian group variety).

Notation

- we work over the field \mathbb{C} , sometimes we restrict to \mathbb{R} ,
- $F(x, y, z)$ homogeneous polynomial of degree 3,
- \mathcal{C} a smooth curve defined by $\{F(x, y, z) = 0\} \subset \mathbb{P}^2$.

	projective plane \mathbb{P}^2 :	\iff	affine plane \mathbb{C}^2 :
points:	$(x, y, z) =$ $(x/z, y/z, 1)$		(X, Y)
curves:	$y^2z = (x+z)(x^2 + \varepsilon z^2)$ $y^2z = (x+z)x^2$ $y^2z = (x+z)(x^2 - \varepsilon z^2)$		$Y^2 = (X+1)(X^2 + \varepsilon)$ $Y^2 = (X+1)X^2$ $Y^2 = (X+1)(X^2 - \varepsilon)$

Definition: Determinantal representation

It is very useful to represent F as a determinant of some matrix:
Find a 3×3 matrix with linear terms

$$M(x, y, z) = xA + yB + zC$$

such that

$$\det M(x, y, z) = c F(x, y, z), \text{ for some } c \neq 0.$$

Matrix M is called a **determinantal representation** of C .

Clearly, multiplying a determinantal representation by invertible matrices preserves the underlying curve. Two determinantal representations M and M' **equivalent** if there exist $X, Y \in \text{GL}(3, \mathbb{C})$ such that

$$M' = XMY.$$

We consider determinantal representations up to equivalence.

Definition: Determinantal representation

It is very useful to represent F as a determinant of some matrix:
Find a 3×3 matrix with linear terms

$$M(x, y, z) = xA + yB + zC$$

such that

$$\det M(x, y, z) = c F(x, y, z), \text{ for some } c \neq 0.$$

Matrix M is called a **determinantal representation** of C .
Clearly, multiplying a determinantal representation by invertible matrices preserves the underlying curve. Two determinantal representations M and M' **equivalent** if there exist $X, Y \in \text{GL}(3, \mathbb{C})$ such that

$$M' = XMY.$$

We consider determinantal representations up to equivalence.

Existence of a symmetric determinantal representation

Every cubic curve has a determinantal representation. The following theorem constructs a **symmetric** one:

Theorem (J. Harris, 1979, p. 696)

There exist precisely three points $(a, b) \in \mathbb{C}^2$ such that

$$aF = \text{Hes}(bF + \text{Hes}(F)),$$

where Hes is the Hessian i.e., the determinant of the second partial derivatives matrix. The resulting three symmetric determinantal representations of F are inequivalent.

Using elementary transformations [Vinnikov] we can obtain all determinantal representations of F from a given one.

Existence of a symmetric determinantal representation

Every cubic curve has a determinantal representation. The following theorem constructs a **symmetric** one:

Theorem (J. Harris, 1979, p. 696)

There exist precisely three points $(a, b) \in \mathbb{C}^2$ such that

$$aF = \text{Hes}(bF + \text{Hes}(F)),$$

where Hes is the Hessian i.e., the determinant of the second partial derivatives matrix. The resulting three symmetric determinantal representations of F are inequivalent.

Using elementary transformations [Vinnikov] we can obtain all determinantal representations of F from a given one.

Weierstrass canonical form

Theorem

By a projective change of coordinates, every irreducible curve can be brought into the **Weierstrass form**

$$y^2z = x^3 + pxz^2 + qz^3, \quad p, q \in \mathbb{C}$$

or equivalently $y^2z = x(x + \theta_1z)(x + \theta_2z)$, $\theta_1, \theta_2 \in \mathbb{C}$.

Moreover, every reduced curve is projectively equivalent to one of the

$$\begin{aligned} &x^3, x^2y, xy(x+y), xyz \quad \text{or} \\ &(\alpha x + \beta y + \gamma z)(x^2 - yz) \quad \text{for some } \alpha, \beta, \gamma \in \mathbb{C}. \end{aligned}$$

Weierstrass canonical form

Theorem

By a projective change of coordinates, every irreducible curve can be brought into the **Weierstrass form**

$$y^2z = x^3 + pxz^2 + qz^3, \quad p, q \in \mathbb{C}$$

or equivalently $y^2z = x(x + \theta_1z)(x + \theta_2z)$, $\theta_1, \theta_2 \in \mathbb{C}$.

Moreover, every reduced curve is projectively equivalent to one of the

$$\begin{aligned} &x^3, x^2y, xy(x+y), xyz \quad \text{or} \\ &(\alpha x + \beta y + \gamma z)(x^2 - yz) \quad \text{for some } \alpha, \beta, \gamma \in \mathbb{C}. \end{aligned}$$

Why do we want the Weierstrass canonical form?

Corollary

Any coordinate independent statement that holds for a Weierstrass cubic, holds for any irreducible cubic curve.

We will use this to show:

- Determinantal representations of any cubic curve \mathcal{C} are in one to one correspondence with affine points on \mathcal{C} .

Why do we want the Weierstrass canonical form?

Corollary

Any coordinate independent statement that holds for a Weierstrass cubic, holds for any irreducible cubic curve.

We will use this to show:

- Determinantal representations of any cubic curve \mathcal{C} are in one to one correspondence with affine points on \mathcal{C} .

Inflection point

Every irreducible cubic has **inflection points**:

$$\{F = 0\} \cap \{\text{Hes } F = 0\} \subset \mathbb{P}^2.$$

Proposition

If we find an inflection point on \mathcal{C} , we can put it into the Weierstrass form.

Change the coordinates so that the inflection point is $(0, 1, 0)$ and the inflection tangent is $z = 0$. Considering all possible monomials occurring in F yields the Weierstrass form.

Corollary

When the defining polynomial F is real, a real change of coordinates gives the Weierstrass form with $p, q \in \mathbb{R}$.

Inflection point

Every irreducible cubic has **inflection points**:

$$\{F = 0\} \cap \{\text{Hes } F = 0\} \subset \mathbb{P}^2.$$

Proposition

If we find an inflection point on \mathcal{C} , we can put it into the Weierstrass form.

Change the coordinates so that the inflection point is $(0, 1, 0)$ and the inflection tangent is $z = 0$. Considering all possible monomials occurring in F yields the Weierstrass form.

Corollary

When the defining polynomial F is real, a real change of coordinates gives the Weierstrass form with $p, q \in \mathbb{R}$.

Inflection point

Every irreducible cubic has **inflection points**:

$$\{F = 0\} \cap \{\text{Hes } F = 0\} \subset \mathbb{P}^2.$$

Proposition

If we find an inflection point on \mathcal{C} , we can put it into the Weierstrass form.

Change the coordinates so that the inflection point is $(0, 1, 0)$ and the inflection tangent is $z = 0$. Considering all possible monomials occurring in F yields the Weierstrass form.

Corollary

When the defining polynomial F is real, a real change of coordinates gives the Weierstrass form with $p, q \in \mathbb{R}$.

Algorithm

- The enumerative problem of locating flexes of a plane cubic is solvable, since the corresponding Galois group is solvable [Harris, 1979].
- When \mathcal{C} contains a rational point [Silverman and Tate, 1992] provided an algorithm that puts it into a Weierstrass form.

Main theorem

Theorem

Determinantal representations of $y^2z = x(x + \theta_1z)(x + \theta_2z)$ are

$$M_{l,t}(x, y, z) = x \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} + y \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + z \begin{pmatrix} \frac{3}{4}t^2 + \frac{1}{2}t(\theta_1 + \theta_2) - \frac{1}{4}(\theta_1 - \theta_2)^2 & l & \frac{1}{2}(\theta_1 + \theta_2 + t) \\ -l & -t & 0 \\ \frac{1}{2}(\theta_1 + \theta_2 + t) & 0 & -1 \end{pmatrix}$$

where $l, t \in \mathbb{C}$ and $l^2 = t(t + \theta_1)(t + \theta_2)$.

Real cubic

It is natural to consider the subset of cubics defined by **real** polynomials. Representation $M_{l,t}(x, y, z)$ in the Main theorem is self-adjoint iff t is real and $l = is$ is purely imaginary.

The set of all nonequivalent self-adjoint determinantal representations of \mathcal{C} can thus be parametrised by affine points on $F(t, l)$ whose first coordinate is real and the second coordinate is purely imaginary.

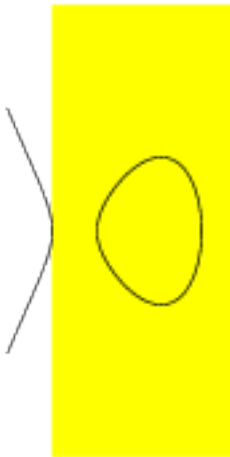
Real cubic

It is natural to consider the subset of cubics defined by **real** polynomials. Representation $M_{l,t}(x, y, z)$ in the Main theorem is self-adjoint iff t is real and $l = is$ is purely imaginary.

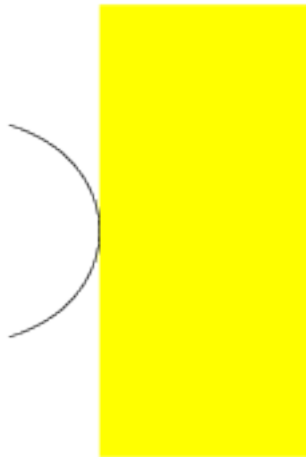
The set of all nonequivalent self-adjoint determinantal representations of \mathcal{C} can thus be parametrised by affine points on $F(t, l)$ whose first coordinate is real and the second coordinate is purely imaginary.

Smooth cubics $-s^2 = t(t + \theta_1)(t + \theta_2)$

$$\theta_1, \theta_2 \in \mathbb{R}$$

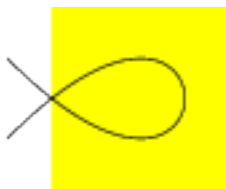
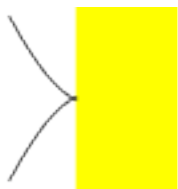


$$\theta_1 = \bar{\theta}_1.$$



Singular cubics

$$-s^2 = t^3, \quad -s^2 = t^2(t - 1), \quad -s^2 = t(t - 1)^2.$$



Definite representation

Definition

A self-adjoint determinantal representation is **definite** if there exists a point $(a, b, c) \in \mathbb{R}^3$ such that $M(a, b, c)$ is positive definite.

Note:

Definiteness is preserved under a real change of coordinates.

Theorem

Let \mathcal{C} be a real cubic

$$y^2z = x(x + \theta_1z)(x + \theta_2z).$$

Determinantal representations $M_{l,t}$ from the Main theorem are definite for $t > 0$.

Semidefinite programming SDP





Definition





The set of points where a given self-adjoint determinantal representation is positive definite,

$\mathcal{S} = \{(x, y, z) \in \mathbb{R}^3 : M(x, y, z) \succeq 0\}$ is called **spectrahedron** and $M(x, y, z) \succeq 0$ is an **LMI (linear matrix inequality)** representation of \mathcal{S} .

Theorem (Vinnikov, 2007)

Rigidly convex sets are exactly spectrahedra bounded by the determinant of some LMI representation. Spectrahedra are precisely the sets on which semidefinite programming can be performed.

-  J. Harris. *Galois groups of enumerative problems*, Duke Math. J., Vol. 46 (1979).
-  D. Plaumann, B. Sturmfels and C. Vinzant. *Computing linear matrix representations of Helton-Vinnikov curves*, Operator Theory: Advances and Applications, Vol. 222 (2012), p. 267.
-  J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer (1992).
-  V. Vinnikov. *Complete description of determinantal representations of smooth irreducible curves*, Linear Algebra and its Applications, Vol. 125 (1989).

-  V. Vinnikov. *Elementary transformations of determinantal representations of algebraic curves*, Linear Algebra and its Applications, Vol. 135 (1990).
-  V. Vinnikov. *LMI Representations of Convex Semialgebraic Sets and Determinantal Representations of Algebraic Hypersurfaces: Past, Present, and Future*, Operator Theory: Advances and Applications, Vol. 222 (2012).
-  V. Vinnikov. *Self-adjoint determinantal representations of real irreducible cubics*, Advances and Applications, Vol. 19, Birkhäuser (1986).
-  H. Wolkowicz, L. Vandenberghe and R. Saigal. *Handbook of Semidefinite Programming - Theory, Algorithms, and Applications*, International Series in Operations Research and Management Science, Kluwer Academic Publ. (2011).