Explicit Kummer surface theory in arbitrary characteristic

Jan Steffen Müller

Jacobs University Bremen

Introduction

Let C denote a hyperelliptic curve of genus g defined over a field k.
Let J denote its Jacobian.

Consider the quotient K of J by $\{\pm 1\}$.
This is a projective variety that can be embedded in $\mathbb{P}^{2^g-1}$, called the Kummer variety of J.

We would like to make this explicit in the case $g = 2$ by finding

- an explicit embedding of K in $\mathbb{P}^3$

- a defining equation for K

- maps that allow us to perform arithmetic on K.

If possible, all of this should be defined over the ground field k.

Classical setup

Suppose C is a smooth projective curve of genus 2 defined over a field k of characteristic $\mathrm{char}(k) \neq 2$ given by

$$C : y^2 = f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + f_6 x^6,$$

with $f_i \in k$ such that $f_5 \neq 0$ or $f_6 \neq 0$.

- Flynn has found an explicit embedding of the Jacobian J of C in $\mathbb{P}^{15}$ and a set of 72 quadratic relations defining J.

- **But**: doing arithmetic in $\mathbb{P}^{15}$ is rather difficult.

- Arithmetic in $\mathbb{P}^3$ is much easier.

- **Idea**: Develop an explicit theory of the Kummer surface K of J and investigate how it could be used to perform arithmetic on J.

Kummer embedding

A point $P \in J$, then P can be represented by a pair of points P_1 and P_2 on C.

Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are affine. Flynn has found the following embedding $\kappa : K \hookrightarrow \mathbb{P}^3$:

$$\begin{aligned}
\kappa_1 &= 1 \\
\kappa_2 &= x_1 + x_2 \\
\kappa_3 &= x_1 x_2 \\
\kappa_4 &= \frac{F_0(x_1, x_2) - 2y_1 y_2}{(x_1 - x_2)^2},
\end{aligned}$$

where

$$\begin{aligned}
F_0(x_1, x_2) = \; & 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1 x_2) + f_3(x_1 + x_2)x_1 x_2 \\
& + 2f_4(x_1 x_2)^2 + f_5(x_1 + x_2)x_1 x_2 + 2f_6(x_1 x_2)^3
\end{aligned}$$

Equation and structure

The functions $\kappa_1, \ldots, \kappa_4$ satisfy a quartic equation $K(\kappa_1, \kappa_2, \kappa_3, \kappa_4) = 0$ defined over k.

How is the group law of J reflected on K?

The Kummer surface doesn't retain the group structure of J, but clearly

- duplication

- translation by a point of order two

both are defined on K.

Duplication & translation by a 2-torsion point

Flynn has found maps $\delta, W_P \colon K \longrightarrow K$ such that the following diagrams commute:

$$\begin{tikzcd} J \arrow[r, "{[2]}"] \arrow[d, "\kappa"] & J \arrow[d, "\kappa"] \\ K \arrow[r, "\delta"] & K \end{tikzcd} \qquad \text{and} \qquad \begin{tikzcd} J \arrow[r, "\tau_P"] \arrow[d, "\kappa"] & J \arrow[d, "\kappa"] \\ K \arrow[r, "W_P"] & K \end{tikzcd}$$

- $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ is a quadruple of quartic polynomials defined over k.

- Here τ_P is translation by $P \in J[2]$.

- W_P is a linear map on $\mathbb{P}^3$ and thus can be given as multiplication by a 4×4-matrix defined over the field of definition of P.

Biquadratic forms

Let $P, Q \in J$.
Let $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ represent $\kappa(P)$ and $\kappa(Q)$, respectively. Then we call them Kummer coordinates for P and Q.

Flynn has constructed a 4×4-matrix $B(x, y)$ of biquadratic forms B_{ij} in x, y and defined over k, such that projectively

$$\begin{aligned} B_{ij}(x,y) &= (\kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q)), \; i \neq j \\ B_{ii}(x,y) &= (\kappa_i(P+Q)\kappa_i(P-Q)) \end{aligned}$$

Flynn and Smart found algorithms for addition and scalar multiplication on the Jacobian using δ and B.

Generalisation

What if char(k) is arbitrary and C/k is given by

$$C : y^2 + h(x)y = f(x), \tag{1}$$

where

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + f_6 x^6 \\ h(x) &= h_0 + h_1 x + h_2 x^2 + h_3 x^3 ? \end{aligned}$$

We would like to extend Flynn's results to this situation.

We will assume that C is given by an equation as in (1).

Other contributions

Duquesne has independently found all of the above when $\mathrm{char}(k) = 2$ and $\deg(h) = 2$. But he uses methods that don't generalize to arbitrary characteristic.

All formulas presented in this talk specialize to Duquesne's results when $\mathrm{char}(k) = 2$ and $\deg(h) = 2$ and to Flynn's results when $\mathrm{char}(k) \neq 2$ and $h = 0$.

A different $\mathbb{P}^3$ embedding of the Kummer surface was found by Gaudry if $\mathrm{char}(k) \neq 2$ and recently by Gaudry and Lubicz for $\mathrm{char}(k) = 2$.

Motivation

In cryptography, one uses Jacobians of genus 2 curves over $\mathbb{F}_{2^q}$ with q large. Here Duquesne, Gaudry and Lubicz have very competitive algorithms for scalar multiplication that use Kummer surfaces.

I wanted to compute canonical heights on genus 2 Jacobians over number fields or function fields by computing canonical local heights for all valuations v of k defined on Kummer coordinates $x = (x_1, x_2, x_3, x_4)$ by

$$\lambda_v(x) = -v(x) - \sum_{n=0}^{\infty} \left(4^{-(n+1)} \varepsilon(\delta^{\circ n}(x))\right)$$

where

$$v(x) = \min\{v(x_1), v(x_2), v(x_3), v(x_4)\} \text{ and } \varepsilon(x) = v(\delta(x)) - 4v(x).$$

For this, allowing more general models of C is computationally attractive.

Kummer Embedding & equation II

The first step is to find an embedding of the Kummer surface K associated to the Jacobian J of $C : y^2 + h(x)y = f(x)$.

Suppose that $P \in J$ is represented by $\{(x_1, y_1), (x_2, y_2)\} \in C$.
An embedding $\kappa : K \hookrightarrow \mathbb{P}^3$: is given by

$$\begin{aligned}
\kappa_1 &= 1 \\
\kappa_2 &= x_1 + x_2 \\
\kappa_3 &= x_1 x_2 \\
\kappa_4 &= \frac{F_0(x_1, x_2) - 2y_1 y_2 - h(x_1)y_2 - h(x_2)y_1}{(x_1 - x_2)^2},
\end{aligned}$$

where $F_0(x_1, x_2)$ is as before.

The defining equation $K(\kappa_1, \kappa_2, \kappa_3, \kappa_4) = 0$ is again a homogeneous quartic equation that is quadratic in κ_4.

Strategy

Our method for finding the duplication map δ, the matrix B of biquadratic forms and the matrix W_P corresponding to translation by a point P of order 2 is as follows:

- First assume char$(k) \neq 2$.

- Let $C' : y^2 = 4f(x) + h(x)^2$. Then C is birationally equivalent to C'.

- Find the Kummer surface K' associated to the Jacobian of C'. Then $K \cong K'$.

- Find an explicit isomorphism $\tau : K \longrightarrow K'$ and use it to map the object at hand from K' to K.

- If possible, modify the result so that it also works when char$(k) = 2$.

The isomorphism and duplication II

Suppose char$(k) \neq 2$. An explicit isomorphism from K to K' is given by

$$\begin{aligned} \tau : K &\longrightarrow K' \\ (\kappa_1, \kappa_2, \kappa_3, \kappa_4) &\mapsto (\kappa_1, \kappa_2, \kappa_3, 4\kappa_4 - 2(h_0h_2\kappa_1 + h_0h_3\kappa_2 + h_1h_2\kappa_3))\,. \end{aligned}$$

We find δ such that

$$\begin{tikzcd} K \arrow[r, "\delta"] \arrow[d, "\tau"] & K \arrow[d, "\tau"] \\ K' \arrow[r, "\delta'"] & K' \end{tikzcd}$$

commutes, where δ' is the duplication map on K'.

We add suitable multiples of the defining equation of K to the entries of δ and divide them by 64 to obtain a map that is defined and non-trivial modulo 2.

Biquadratic forms II

Let x and y be Kummer coordinates on K and $B'(\tau(x), \tau(y))$ the symmetric matrix of biquadratic forms

$$b'_{ij} := B'_{ij}(\tau(x), \tau(y))$$

on K' discussed above.

- Since $\tau(\kappa_i) = \kappa_i$ for $i = 1, 2, 3$, we have $B_{ij}(x, y) = b'_{ij}$ for $i = 1, 2, 3$.

- The last row and column of $B(x, y)$ can be computed as linear combinations of the b'_{ij}.

- We divide the resulting matrix by 16 to make it defined and non-zero modulo 2.

Translation by a 2-torsion point II

Let $P \in J[2]$ and $P' \in J'[2]$ with image $\tau(\kappa(P))$ on K'.

According to our strategy used before, we compute W_P such that

$$\begin{array}{ccc} K & \xrightarrow{W_P} & K \\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau} \\ K' & \xrightarrow{W_{P'}} & K' \end{array}$$

commutes, where $W_{P'}$ corresponds to translation by P' on K'.

However, all attempts to generalize this W_P to characteristic 2 have failed.

Translation by a 2-torsion point III

If $\mathrm{char}(k) = 2$ and $P \in J$ is of order 2, we instead use a method that is very similar to the original one employed by Flynn.
Let $Q \in J$.

- We find the unique cubic M passing through the points on C giving P and Q.

- The x-coordinates of the points on C giving $P + Q$ can be found as the other roots of $M(x)^2 + M(x)h(x) - f(x)$.

- We successively divide this polynomial by other polynomials until it is linear in the x-coordinates of the points giving Q and quadratic in x.

- This gives the first 3 rows of the matrix representing W_P. The fourth row is found using the fact that W_P is an involution on $\mathbb{P}^3$.

Conclusion & outlook

- Given any curve of genus 2, we can explicitly determine the Kummer surface associated to its Jacobian and use several maps on it to perform arithmetic on the Jacobian, which is in particular useful in crytpography. In addition, we can use it to compute (local) heights.

- At the moment it seems infeasible to develop an explicit Kummer variety theory for curves of genus $g \geq 3$ - but it would be very useful.

- Exception: $g = 3$, $\mathrm{char}(k) \neq 2$ and $C : y^2 = f(x)$ such that $\deg(f) = 7$. Here Stubbs has found an embedding into $\mathbb{P}^7$ and a conjectured set of defining relations.